Investigating and Mitigating the Role Of Neutralisation Techniques on Information Security Policies Violation in Healthcare Organisations

Saad Altamimi

Submitted in fulfilment of the requirements for the
Degree of Doctor of Philosophy

School of Computing Science
College of Science and Engineering
University of Glasgow

January 2022

Abstract

Healthcare organisations today rely heavily on Electronic Medical Records systems (EMRs), which have become highly crucial IT assets that require significant security efforts to safeguard patients' information. Individuals who have legitimate access to an organisation's assets to perform their day-to-day duties but intentionally or unintentionally violate information security policies can jeopardise their organisation's information security efforts and cause significant legal and financial losses. In the information security (InfoSec) literature, several studies emphasised the necessity to understand why employees behave in ways that contradict information security requirements but have offered widely different solutions.

In an effort to respond to this situation, this thesis addressed the gap in the information security academic research by providing a deep understanding of the problem of medical practitioners' behavioural justifications to violate information security policies and then determining proper solutions to reduce this undesirable behaviour. Neutralisation theory was used as the theoretical basis for the research. This thesis adopted a mixed-method research approach that comprises four consecutive phases, and each phase represents a research study that was conducted in light of the results from the preceding phase.

The first phase of the thesis started by investigating the relationship between medical practitioners' neutralisation techniques and their intention to violate information security policies that protect a patient's privacy. A quantitative study was conducted to extend the work of Siponen and Vance [1] through a study of the Saudi Arabia healthcare industry. The data was collected via an online questionnaire from 66 Medical Interns (MIs) working in four academic hospitals. The study found that six neutralisation techniques—(1) appeal to higher loyalties, (2) defence of necessity, (3) the metaphor of ledger, (4) denial of responsibility, (5) denial of injury, and (6) condemnation of condemners—significantly contribute to the justifications of the MIs in hypothetically violating information security policies.

The second phase of this research used a series of semi-structured interviews with IT security professionals in one of the largest academic hospitals in Saudi Arabia to explore the environmental factors that motivated the medical practitioners to evoke various neutralisation techniques. The results revealed that social, organisational, and emotional factors all stimulated the behavioural justifications to breach information security policies. During these interviews, it became clear that the IT department needed to ensure that security policies fit the daily tasks

of the medical practitioners by providing alternative solutions to ensure the effectiveness of those policies.

Based on these interviews, the objective of the following two phases was to improve the effectiveness of InfoSec policies against the use of behavioural justification by engaging the end users in the modification of existing policies via a collaborative writing process. Those two phases were conducted in the UK and Saudi Arabia to determine whether the collaborative writing process could produce a more effective security policy that balanced the security requirements with daily business needs, thus leading to a reduction in the use of neutralisation techniques to violate security policies. The overall result confirmed that the involvement of the end users via a collaborative writing process positively improved the effectiveness of the security policy to mitigate the individual behavioural justifications, showing that the process is a promising one to enhance security compliance.

Table of Contents

List of Tables

List Of Figures

Acknowledgements

First, I would thank Allah for giving me the patience and the strength to finish this thesis.

I dedicate this thesis to my parents, brothers, and sisters. To my beloved wife Ashwaq , and my gorgeous children Naif, Joury and Nasser, for their constant patience, constant support, and encouragement throughout my PhD journey.

I would also like to express my gratitude to Imam Muhammad bin Saud Islamic University for providing me with a full scholarship to complete my postgraduate studies.

Additionally, I want to express my deepest appreciation to my first supervisor, Dr.Timothy Storer, for his constant support and advice during this journey. I am grateful to him for his insightful criticisms and suggestions throughout the course of the thesis. Additionally, I'd like to express my gratitude to my second supervisor, Dr. Karen Renaud, for providing several critiques and throughout this research.

I would also like to express my gratitude to the Saudi Arabia Hospital for giving me the opportunity to conduct three studies in their institution. Special thanks also go to my dear friend, Mr. Mohammed Al-Muslim, who provided me with valuable and endless support during the data collection process.

Finally, I would like to thank the PhD students in the School of Computing Sciences at the University of Glasgow for their support and participation in the early phases of experiments. Their constructive comments and criticism were crucial in adapting and strengthening the first drafts of this thesis' studies.

اللهم لك الحمد على اتمام هذه الرسالة العلمية والتي اسال الله ان يجعلها اعانة لي على طاعته وان تكون في خدمة ديني ثم مليكي ووطني

Author’s Declaration

Some of the material presented within this thesis has previously been published in the following papers:

1. Altamimi, Saad, Karen Renaud, and Timothy Storer. "“I do it because they do it”: social-neutralisation in information security practices of Saudi medical interns." *CRiSIS 2019: 14th International Conference on risks and security of internet and systems*. Springer, 2020.

2. *S. Altamimi, T. Storer and A. Alzahrani, "The role of neutralisation techniques in violating hospitals privacy policies in Saudi Arabia," 2018 4th International Conference on Information Management (ICIM), 2018, pp. 133-140, doi: 10.1109/INFOMAN.2018.8392823.*

I declare that this thesis was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification except as specified.

(Saad Altamimi)

Chapter 1 : Introduction

The healthcare sector in Saudi Arabia is one of the largest healthcare industries in the Middle East [2]. The World Health Organisation (WHO) ranked the Saudi healthcare system 26th out of 191 countries, even ahead of the Canadian (30th) and Australian (32nd) health care systems [3]. This sector has received significant investments in human and technical resources from the Saudi authorities, which has led to the expansion and development of healthcare services across the country. Hence, like any other development project, adopting and implementing Healthcare Information Systems (HIS) and associated Information Technology (IT) solutions comes with challenges. Among these challenges, the priority is ensuring the security and privacy of the IT assets that handle, transmit, and process medical records. To ensure that these IT assets are protected, healthcare organisations adopt information security standards that require the organisation to implement various information security controls and best practices.

These security requirements are reflected in Information Security Policies (InfoSec), and compliance with these policies is mandatory for all healthcare personnel. This research focuses on information security policies violation in organisations, specifically in the healthcare industry. The work investigates the extent to which (a) neutralisation theory can explain health practitioners' decisions to violate security policies; and (b) a collaborative policy editing technique can be used to mitigate the rationalisations proposed by practitioners when violating policies. This research has four major studies, and data collection was from respondents in Saudi Arabia and the United Kingdom.

This chapter presents the study's research background and the author's motivation to conduct the research and formulate the thesis questions and statement. It is divided into seven sections and organised as follows: Section 1.1 presents a brief background of the research and the impact of individuals' information security non-compliance on the organisational effort to protect its IT assets, specifically in the healthcare industry. Section 1.2 presents a rationale for adopting neutralisation techniques, a theoretical basis for understanding medical practitioners' tendency to justify non-compliance with the information security policies. Section 1.3 presents the thesis statement. Section 1.4 illustrates the research questions that guide this work. Section 1.5 discusses the research contributions. Section 1.6 introduces a list of key terms.

1.2 Background

Information privacy in the healthcare industry has been defined as "the ability of health care employees to control Electronic Health Records (EMR) during collection, maintaining the

accuracy of EMR during manipulation, ensuring the confidentiality of EMR during transferring and understanding the duration of EMR retention in the organisation" [4]. Securing sensitive patient information against privacy breaches is essential because any leakage of this confidential information could harm both the patient and the organisation. For an employee involved in the disclosure of confidential patient information, either intentionally or unintentionally, the breach may lead to termination, loss of health insurance, charges of identity theft and, at the least, embarrassment. Simultaneously, the healthcare organisation may suffer from loss of reputation and income and incur penalties demanded by regulators and lawsuits [5].

In an effort to preserve EHR integrity, confidentiality, and availability, many countries have developed security laws and require compliance from all health care parties that store, process, and exchange EHR electronically [4][6][7]. Examples include the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the US, the Personal Information Protection and Electronic Documents Act 2000 (PIPEDA Act) in Canada, the General Data Protection Regulation (GDPR) in Europe, the Personal Data Protection Act (PDPA) in Malaysia, and the Ley de Proteccin de Datos law in Spain [7][8]. Saudi Arabia currently lacks specific laws addressing information privacy, apart from some items and articles scattered among several regulations, such as those found in the 1996 Statute of Government (Royal Decree) or the 2007 Communications Law from the Saudi Ministry of Communications and Information Technology (MCIT), which aims to ensure the security of information exchange over public networks. Thus, many organisations in various Saudi industries have adopted different privacy and security regulations and standards from other countries to protect the confidentiality of their information. For example, many hospitals in Saudi Arabia adopted the US Privacy Protection Regulation (HIPAA) to deal with privacy issues[9].

Information security threats can originate from external sources, including intruder and hacker attempts, malware, spyware, or virus attacks, or internal actions such as employees' intentional or unintentional behaviour due to ignorance and curiosity, or password misuse [10]. From the IT perspective, insider threats are individuals who have legitimate access to an organisation's IT assets but do not adhere to information security policies and procedures accidentally or intentionally [11] [12]. Organisations develop Information Security Policies (InfoSec) to guide employees to behave safely while carrying out their tasks using the organisation's information systems [13]. These InfoSec policies explain an employee's expected security roles and responsibilities and the consequences associated with violating them [14].

Despite an organisation's efforts to establish a robust information security department to protect its IT assets by adopting best security practices, which include implementing technological measures and developing related security policies, individuals' non-compliance behaviour may render these efforts unsuccessful [15]. Several security scholars and reports stated that employee behavioural violations of information security measures are considered the weakest part of an organisation's IT defence structure [16][17]. The 2016 report issued by the European Union Cybersecurity Agency (ENISA) ranked the three top security incidents by insiders as follows: privileges abuse (60%), poor handling of data (13%) and use of non-approved hardware (10%). According to the Insider Threat Report, 2019 [18] it stated that carless individuals cause most of the security incidents that lead to accidental data leakages (70%), and (66%) of organisations believed that employee's non-compliance with information security policies was a primary concern for a data breach.

A recent report 2020 by ENISA [19] stated that the security incidents caused by insiders were responsible for (65%) of the damages to organisations' reputation and the financial losses of such security incidents cost the organisation on average around €11,45 million per year. In healthcare, abuse of security privileges and unauthorised access are common types of internal threats in which an employee causes a privacy breach by disclosing patient sensitive information [20]. According to the Verizon 2020 Data Breach Investigation Report (DBIR) [21], there were 32,002 security incidents during that year, 3,950 of which disclosed data. There were approximately 798 security incidents with 521 confirmed data breaches in the healthcare industry in 2020, versus 304 in the 2019 DBIR report; insiders committed 48% of these data breaches, placing the healthcare sector ahead of other industries in the US invulnerability to insider threats [21]. For instance, several celebrities such as pop singers (e.g. Britney Spears), politicians (e.g. Gordon Brown, a former UK prime minister), and movie actors (e.g.Farrah Fawcett) have been victims of unauthorised access to their medical records. This sensitive information has been disclosed to the media by medical practitioners or hospitals' staff without a patient's consent. For instance, in 2007, actress Farrah Fawcett received cancer treatment at the University of California Los Angeles (UCLA) Medical Center. She was embarrassed when her medical condition was revealed publicly in the tabloids before telling family and close friends. The information source was a medical practitioner at UCLA, who sold her information to the media for $4,600. The data breach's consequences damaged the hospital's reputation and forced UCLA to pay a massive settlement to the actress. Also, the medical practitioner's service was terminated and accused of a privacy breach [22].

Information systems literature has extensively investigated the factors that influence employee behaviour towards violation of or compliance with InfoSec policies and has suggested various technical and non-technical solutions to mitigate these problems [23]–[27]. In an effort to improve individual compliance and reduce undesirable behaviours, information security scholars have offered a wide variety of studies incorporating theories from sociology, criminology, psychology, and other disciplines to achieve a deeper understanding of the drivers of non-compliance with information security [28][29]. In this area, several security researchers have argued that employees often utilise moral cognition or neutralisation techniques to diminish the impact and consequences of punishment, guilt, policy and law enforcement, or shame when they intend to commit computer abuse or violate security [30]–[33].

Sykes and Matz [34] introduced the concept of "techniques of neutralisation" in the field of criminology to understand juvenile delinquency. According to Rogers and Buffalo [35], neutralisation is "a method whereby an individual renders behavioural norms inoperative, thereby freeing himself to engage in behaviour which would otherwise be considered deviant." The theory postulates that offenders employ one or more cognitive techniques as defence mechanisms to justify their deviant behaviour prior to or after they commit a crime, thereby convincing themselves that their deviant behaviour is acceptable, regardless of social norms [31]. In their original work, Sykes and Matza proposed five neutralisation (rationalisation) techniques that juvenile criminals may use to justify their deviant behaviour: denial of responsibility, denial of injury, denial of a victim, condemnation of the condemners, and appeal to higher loyalty. Other criminologists extended Sykes and Matza's work adding additional techniques such as the metaphor of the ledger [36], the defence of necessity and claim of entitlement[37], the claim of normalcy [38], and justification by comparison [39].

Previous IS research has demonstrated that employees may also employ neutralisation techniques when explaining violations of security policies [18] [31][32][1]. When an employee violates an organisation's policy, they may defend their non-compliant behaviour by providing justifications. Thus, neutralisation offers a set of cognitive strategies that individuals may use to excuse themselves and explain why they intend to commit a violation of an information security policy. This research, therefore, adopts neutralisation techniques as a theoretical lens for interpreting the non-compliance intentions of medical practitioners toward information security policies and investigates the relevant situational and environmental factors that motivate individual justifications of their violations of information security policy in a healthcare environment. In this research, we explored from a psychological perspective what

justifications might cause an employee not to comply and what motivations can lead them to adopt such justifications for breaking regulations and policies. By doing so, we can discover how to overcome these behavioural justifications by enhancing the InfoSec policies and the related security and privacy awareness programs within healthcare organisations. This socio-technical approach investigates the problem of information security policies violation in the context of neutralisation techniques.

1.3 Motivation

This multimodal research was mainly conducted in academic hospitals in Saudi Arabia using medical interns as a target sample and partly at the University of Glasgow. We chose medical interns because they are authorised individuals with full access privileges to a patient's health information. At the same time, those junior doctors may be considered vulnerable to security breaches due to their limited background in information security and ethical expertise in the field.

This research provides a better psychological understanding of the reasons behind security and privacy violations from such medical practitioners as medical interns and how to mitigate such behaviour. We believe an organisation can strengthen its information security management by paying more attention to the behavioural reasons and justifications users offer for taking actions that violate InfoSec policies. We use neutralisation techniques as a theoretical basis to predict privacy safeguard breaches and to identify the insights such breaches offer to the design of more effective safeguards. In this light, we investigated the situational and environmental factors that led the medical interns to justify their InfoSec violation and identify the impacted policies of such misbehaviour.

As a result of this research, we proposed the collaborative writing of security policies as a communication channel between the policymakers and InfoSec policies audiences to enhance the effectiveness of the information security policies, which can reflect the end user needs and concerns. Thus, we assume that considering the perceptions of end users during policy development via a collaborative writing process can positively impact the medical end user's behaviour, increase their engagement in security practices, and reduce their intention to justify their violations of InfoSec policies. This approach can also indirectly increase the end user's awareness of the risks and consequences of this misconduct, as it allows them to discuss, update, and reflect on their perceptions to mitigate an InfoSec issue related to human behaviour.

Thus, this research can improve current security policies' effectiveness to counter the employee justifications to violate InfoSec policies and compromise patient privacy.

1.4 Thesis Statement

This research examines the role of neutralisation techniques used to violate InfoSec policies and proposes a collaborative writing process to enhance InfoSec policies' effectiveness. Therefore, the thesis statement for this research is as follows:

"Healthcare organisations can strengthen their information security policies to protect against behaviours by medical practitioners that may unintentionally violate patient privacy. We argue that neutralisation techniques provide an explanatory basis for predicting medical practitioners' intent to violate hospital information security policies. We propose that engaging end user perception through a collaborative writing process during the security policy development phase could produce more effective information security policies against medical practitioners justifications for non-compliance."

Addressing this thesis statement will allow healthcare organisations to determine the impact of neutralisation techniques on current information security policies and procedures. Also, addressing the root causes driving these behavioural justifications can provide IT policymakers with a better understanding of privacy breaches problems as well as help them develop solutions to mitigate them. Additionally, incorporating end-user perception during the InfoSec policy development process can mitigate the end-users case of non-compliance.

1.5 Research Questions

The following research questions follow from the above thesis statement:

Research Question 1 (RQ1): What is the association between neutralisation techniques and the intention of medical interns to violate InfoSec policies?

Research Question 2(RQ2): What drives behavioural justification among medical practitioners to violate information security policies in healthcare organisations?

Research Question 3 (RQ3): To what extent does the engagement of the perception of the end-user during information security policy development via a collaborative writing process increase the effectiveness of the InfoSec policies to mitigate the role of neutralisation techniques?

1.6 Purpose and Contribution

This dissertation makes novel contributions to the existing information security literature regarding the understanding and mitigation of the IT risks related to an employee's non-compliance intentions regarding InfoSec policies. It aims to investigate and understand the impact of the justifications of medical interns on violating the InfoSec policies that protect privacy in the healthcare industry. Thus, this thesis makes the following contributions to research that include:

- **Extending the IS literature of neutralisation theory's role in a healthcare setting to predict a medical practitioner's violation of the security policies that protect patient privacy.**

  The quantitative part of this study was conducted in three academic hospitals in Saudi Arabia. It extended the seminal work of Siponen and Vance [1], and responded to Willison and Warkentin's [40] call to evaluate the impact of neutralisation techniques on individual behaviour concerning information security in various cultures and contexts.

  This study provides two novel contributions: (1) the application of neutralisation theory in a healthcare context to predict cognitive justification strategies that may lead to the intention to violate information security policies and privacy safeguards in countries like Saudi Arabia. (2) The provision to IT decision-makers in the field of information technology in healthcare organisations, specifically in Saudi Arabia, with evidence to monitor the impact of neutralisation techniques on employees' non-compliance with the security requirements to improve their efforts to enhance information security policies and privacy awareness programs.

  This study is based on a theoretical model that serves as a starting point for the research to establish data collection on the association between neutralisation theory and its role in anticipating employee justification for non-compliance with InfoSec policies. This study constitutes the first phase of this research and is explained in detail in Chapter Four.

- **Identifying the organisational and individual factors that motivate medical practitioners to justify their violations of the information security policies that may lead to privacy breaches**.

  An exploratory qualitative study of information security policies was conducted in one of the largest hospitals in Saudi Arabia. It contributes to the research body by acquiring and

understanding the various challenges that affect information security management in a healthcare context. An in-depth analysis of a series of semi-structured interviews was conducted with 28 medical interns and eight IT department employees. The results revealed many social, organisational, and operational factors that motivate medical interns to invoke neutralisation techniques to overcome feelings of guilt or shame when violating InfoSec policies that cause a breach to patient privacy. This study is the second phase of this research, and Chapter five explains it in more detail.

- **Designing a framework that integrates the employee's perception during the developing process of the InfoSec policies to mitigate neutralisation techniques via a collaborative writing process.**

An action research study was conducted and intended to demonstrate our proposed approach to developing InfoSec policies that can reduce an individual's propensity to adopt neutralisation techniques. This study contributes to the body of knowledge in three ways. First, it evaluates the effectiveness of engaging end-user perceptions via a collaborative writing process to identify, assess, and analyse an organisation's current information security policies to counter the consequences of violating InfoSec policies via neutralisation techniques.

Second, it provides the IT department with a framework to identify weaknesses in existing security controls and procedures. Therefore, this study assists IT professionals in implementing information security policies and controls that are most appropriate for the healthcare organisation and its complex work environment. Third, the collaborative writing process indirectly helps to increase awareness of information security during a discussion of the consequences of justifying non-compliance with InfoSec policies. These participants were taking on IT department roles to find solutions to an information security problem in an attempt to develop a solution based on their understanding of the business context.

1.7 Key Terms and Definitions

Information Security Policy: a document that contains the appropriate behaviours that the organisation wishes from individuals when using its technological assets and information resources. Also, it outlines a set of security roles, strategies, and responsibilities that the organisation needs to protect these IT resources [13].

Information security policy compliance behaviour: predefined security activities and practices that individuals in the organisation must adopt in order to ensure that security requirements are met.

Privacy breach: a "situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements" [41].

Information security policy violation: individual behaviour that contradicts the predefined behaviours in organisations' information security policy [42].

Neutralisation: "a method whereby an individual renders behavioural norms inoperative, thereby freeing himself to engage in behaviour which would otherwise be considered deviant." [35].

Denial of injury: it is a neutralisation techniques where the offender considers that the outcome of his/her potentially deviant action is harmless. Thus, he/she expresses no concern of the fact that anyone could get harmed severely if he/she engages in that act [34].

Denial of responsibility: the core principle of this Neutralisation technique is that the offender refuses to accept the blame for his/her deviant behaviour and redirect the responsibility of the action in question to an alternative source. In this case, the offender might claim that his/her deviant behaviour had occurred by accident or due to the lack of control [34]

Appeal of Higher loyalty: the offender employed this neutralisation technique in order to escape a dilemma that forces him/her to choose between confrontation of small group interests such as friends, family members, etc. or violating a law [34].

Defence of Necessity: the offender argues based on the idea that nobody should feel shame or guilt if the situation requires an act that can result in breaking the rules[37]

Everybody Else is doing it: It is a neutralisation technique where the perpetrator claims that the action in question is common across the close group or community, so there is no need to feel guilty or ashamed [43].

Effectiveness: a state where a security measure reach a specific degree of success [44].

1.8 Thesis Structure

Figure 1.1, presents an overview of the chapters and their relationships. The rest of this thesis is organised as follows:

Chapter 2: This chapter highlights a gap in the information security research by examining the relevant information systems literature regarding the impact of neutralisation techniques on information security management and privacy protection in the healthcare industry. This chapter reviews the role of neutralisation techniques in criminology and information security

and provides a theoretical basis for improving InfoSec policies to reduce individual justifications for violating such policies.

Chapter 3: This chapter presents the research approaches and methods utilised to construct this thesis and how they helped address the research goals and questions. It describes a mixed-methods approach that includes a description of both the quantitative and qualitative aspects of this study.

Chapter 4: This study was conducted in several academic hospitals in Saudi Arabia and focused on medical interns as the target sample. It introduces the result of an empirical study about the role of neutralisation techniques to predict intentions to violate information security policies and breach patient privacy and used a quantitative method (e-survey) to explore the core association between theory and the intentions of the target group toward security policy violation. This chapter addresses the first research question.

Chapter 5: This chapter addresses research question 2 by investigating the antecedent factors that motivate medical interns to invoke neutralisation techniques to justify non-compliance with InfoSec policies that protect patient privacy. A qualitative study using a series of interviews was conducted with several security experts in the IT department and more than 20 medical interns in one of the largest hospitals in Saudi Arabia. The interviews covered five areas: (1) InfoSec policies development, (2) InfoSec policies awareness/training, (3) InfoSec policies implementation, (4) InfoSec enforcement, and (5) InfoSec incident reporting. The interview results revealed that many organisational and social factors drive interns to justify their InfoSec violations. Therefore, it was decided to focus first on increasing the effectiveness of InfoSec policies to counteract neutralisation techniques by incorporating end user perceptions to update existing policies through a collaborative writing process.

Chapter 6: This chapter addressed research question 3 by conducting a focus group study with several groups of students at the University of Glasgow. The purpose of this experiment was to evaluate if the effectiveness of InfoSec policies could be improved by integrating end users' perceptions to mitigate neutralisation techniques via a collaborative writing process. The study findings showed that such engagement would support the IT department's efforts to produce and implement more effective InfoSec policies and controls, which could play an essential role in countering end user tendency to justify non-compliance behaviour.

Chapter 7: This chapter describes a study in one of the largest hospitals in Saudi Arabia, essentially replicating the study in chapter 6 but inside a healthcare environment. Thus, it

increases generalizability and provides more insight into the intervention evaluation to mitigate neutralisation techniques. This chapter provides answers to research question 3 and reveals that engagement of end user perception can provide a useful basis in IT management efforts to mitigate and reduce InfoSec audiences' tendency to justify their non-compliance behaviour.

Chapter 8: This final chapter provides a summary of the main results and conclusions of the study, as well as providing descriptions of the limitations, challenges, and directions for future work.

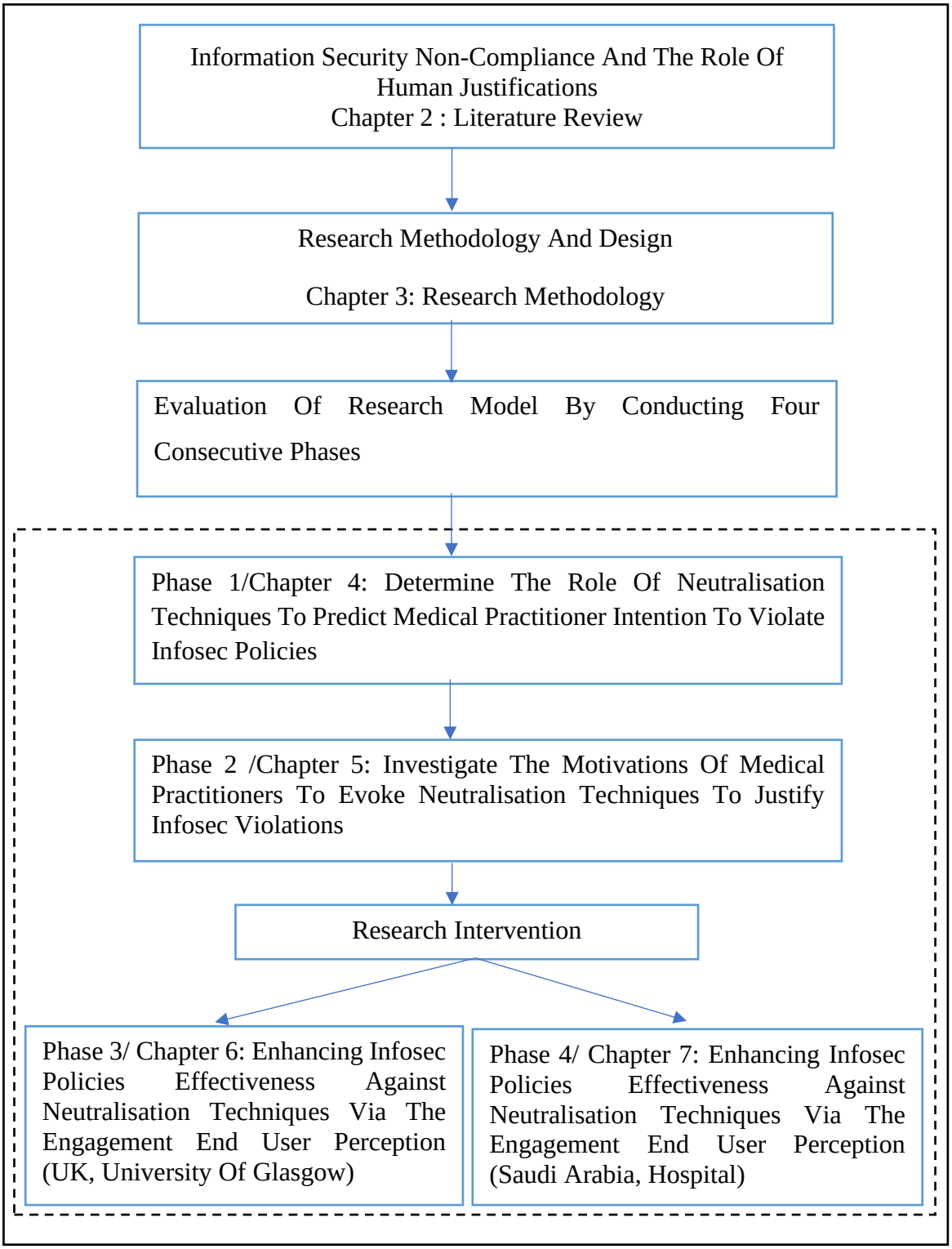


Figure 1.1.1 Thesis Structure

Chapter 2 : Literature Review

This chapter provides a theoretical background for the dissertation by reviewing the relevant literature in information security policies compliance and covers four main areas in information security and privacy. This chapter is essential to understand the personal justifications from the standpoint of criminology and information security non-compliance. Also, it introduces the current counter neutralisation approaches in the information security field and the degree that these approaches are practical to mitigate individual justification to violate information security policies. The chapter introduces general terms related to health security and presents the role of information security policies to protect information and IT assets in organisations. Next, it introduces the overview of the information security policies compliance related to the behavioural security risks, security policies development processes, quality, and effectiveness. Finally, the chapter outlines the influence of neutralisation techniques on individual information security policies violations.

This chapter is divided into four main sections and a summary. Section 2.1 introduces the scoping review method to review the information security literature and explore the theories and related studies applied to investigate information security behavioural violations of the insiders. Section 2.2 the health information systems definitions and roles, explores Electronic Medical Records (EMRs) systems, discusses information security management systems, and presents an overview of security definitions, concepts, and related security standards. Section 2.3.1 discusses privacy in the healthcare context and its associated concerns, risks, and protection initiatives. The section presents an overview of information security policy definitions and the related ISP development approaches, as well as the role of human behaviour in information and insights of security violation as an insider threat. Section 2.4 reviews the literature relating to user behaviour and security risks due to insider threats and includes a description of three important theories in the criminology and psychology fields closely related to individual justifications. Section 2.5 presents the theoretical background of neutralisation techniques. Finally, Section 2.6 offers a summary of this chapter.

2.1 A scoping literature Review

The researcher conducted a scoping review using the Arksey and O'Malley methodology[45]. A scoping review is a preliminary examination of the literature to ascertain the major research ideas, concepts and gaps available in a particular field of study. Colquhoun et al. [46] explained the scoping review or scoping study as:

“a form of knowledge synthesis that addresses an exploratory research question aimed at mapping key concepts, types of evidence, and gaps in research related to a defined area or field by systematically searching, selecting, and synthesizing existing knowledge.” [46]. According to Arksey and O'Malley [45], a scoping review seeks broad and in-depth findings rather than being driven by a fixed research issue and strict criteria of quality and eligibility. It is not restricted by specific search keywords, study selection, or inclusion/exclusion criteria. Furthermore, a scoping review is an iterative process with a series of phases that can be made to ensure that all material is covered thoroughly. Once the researcher's comprehension of the literature has been increased, search terms can be refined, more sensitive searches can be conducted, and procedures can be replicated to assure that all relevant literature is included [45]. Both the traditional (systematic) review and the scoping literature review share similar characteristics to ensure a rigorous and consistent approach during the collection, assessment, and presentation of the research evidence [45][47]. According to Gough et al.[48], the research questions and objectives and the nature of the study are the basis for the research review method selection. The scoping review methodology was determined to be the most appropriate to enhance our understanding of the relationship between individuals' behavioural justifications and their intent to violate information security policies. Also, the current motivations for individuals to excuse non-compliance with workplace information security policies and the countermeasures proposed in the literature to reduce this undesirable behaviour. Thus, the selection of the scoping review over other traditional reviews (Systematic, Critical, rapid and Narrative) can be summarised in the following:

- This research aims to identify and map the critical theories related to the research area. Thus, a scoping review was appropriate in our case as the neutralisation theory in the literature was an integral part of examining different theoretical models across several academic disciplines.
- A scoping review concentrate on breadth based on one or more general research questions. Thus, it provided a common understanding of the research concepts and a broader synthesis of the research issues and gaps.
- A scoping review is more flexible as it does not impose rigid constraints on the researcher's search keywords, study identification, and study selection from the start [45]. Thus, it was an advantageous method in our case as the researcher was unfamiliar with the many psychological, social, and criminal theories and behavioural concepts at the outset of the research.

2.1.1 Search strategy

A critical aspect of conducting a literature search is to develop a search strategy that optimizes the researcher's effort to obtain the studies most relevant to the field of research. Thus, having a clear and consistent research strategy can conserve valuable resources, efforts and time. The search strategy includes carefully selecting the research keywords (terms), bibliographic databases and inclusion and exclusion criteria.

2.1.1.1 Search Keywords

A critical step in conducting a comprehensive review of the literature is developing a list of search terms relevant to the study topic. A good list of research keywords will guarantee that the search is as comprehensive as possible, assisting the researcher in retrieving helpful information from a wide range of electronic databases while reducing the number of irrelevant results. The basic search terms in each database were Information security, Cybersecurity, and Security policy(ies) compliance, Security policy(ies) violation, and were paired with additional terms to limit search findings: neutralisation theory, techniques of neutralisation, behavioural justifications and rationalisation, and insider threat.

2.1.1.2 Inclusion and exclusion criteria

The inclusion and exclusion criteria specify the conditions under which publications were included or excluded from the scoping review. Before the scoping review, these parameters were established to ensure that all articles were handled fairly. The following are the inclusion criteria in this research study to select the publications:

- The initial searches limited results to studies published between 2009 and 2021.
- Deal primarily with individuals behaviour relevant to information security policies compliance or violation.
- Except for seminal studies and books, the researcher narrowed text searches to full-text, peer-reviewed scholarly and journals.

Many publications were excluded from the scoping review was based on the following:

- Written in a non-English language.
- The full article text was unavailable.
- Non- academic articles such as informal reports and white papers.

2.1.1.3 Electronic Databases

The academic materials that produced research literature were collected using various resources, including two critical online databases, the University of Glasgow Library and the Saudi Digital Library. These two libraries offered easy access to a diverse collection of electronic database subscriptions to IEEE, Web of Science, ACM digital library and Scopus. For instance, these massive databases allow the researcher to access and explore many high ranking experimental research journals in the computing and information security field, such as the Journal of Management Information Security (JMIS), European Journal of Information Security (EJIS), and Journal of Information Security (JISSec). In addition, the researcher retrieved many dissertations via online theses databases such as ProQuest and the British Library (EThOS).

2.2 Health Information Systems (HIS)

The healthcare industry is considered one of the most sophisticated businesses that interact with a complex network of entities. Therefore, the use of information and communication technologies (ICT) in the healthcare sector has become imperative to support the activities of these organisations. For example, hospitals often collect vast amounts of data to support their daily medical activities and financial and managerial transactions, which seem to be always increasing. Furthermore, data at hospitals is generated from several sources, including patients, insurance companies, labs, pharmacies, and so forth [49]. Thus, the management of such vast amounts of data requires an effective IT solution that can satisfy many critical requirements such as easily accessible, cost-effective, reliable services and high quality.

Technological advancements to improve healthcare services delivery, quality, and performance have motivated industry stakeholders to implement several health information technologies like Health Information Systems (HIS). The International Organisation for Standardisation ISO 27799: 2016 has defined Health Information Systems (HIS) as “a repository of information regarding the health of a subject of care in computer-processable form, stored and transmitted securely, and accessible by multiple authorised users” [50]. Another HIS definition is based on the fact that such a system “is a computer program, which includes a set of standards-based on healthcare diagnosis, symptoms, cause, healthcare target and measurements” [51]. The adoption of HIS has improved compliance with health care standards and disease control, thus affecting the overall quality delivery of healthcare services. Also, the implementation of clinical decision support tools has improved diagnoses efficiency and has significantly reduced the total rate and time of healthcare utilisation [52][53]. Currently, healthcare organisations are

utilising health information systems as a backbone of their operational services because of the ability to be integrated with hospital clinical care and administrative systems [54].

In light of this utilisation, several health information systems have positively impacted healthcare organisations in such areas as E-Health, Electronic Medical Records (EMR), Mobile health (mHealth), and Telemedicine, cloud computing in healthcare, extensive data analysis, health exchange, and health sensing [55][56].

2.2.1 Electronic Medical Records (EMRs) Systems

Electronic Medical Records (EMR) replaced paper-based charts in hospitals and medical clinics with an electronic version that allows patient information to be integrated, transmitted, stored, and shared in different systems and locations [54]. Establishing a standard definition for these systems is difficult because the same term may have different meanings in different countries or various healthcare sectors. Thus, EMR is considered synonymous with other terms used elsewhere, such as Electronic Health Records (EHR) [55], Computerised Patient Record (CPR), Protected Health Records (PHI), and Personal Health Records (PHR) [54]. Nevertheless, several scholars have provided definitions that attempt to differentiate between EMR, HER, and PHR [57][58]. According to Yang et al. and to the US Department of Health and Human Services [56][59], the main differences between these three terms are as follows:

- **Electronic Medical Record (EMR)**: A healthcare organisation is responsible for generating and controlling the EMR. Each EMR is a legal and digital record that includes all the patient's medical history during inpatient and outpatient visits. Basically, the EMR data are used for diagnoses purposes and are shared locally within one health organisation or institution [56].
- **Electronic Health Record (EHR)**: Several health organisations are responsible for creating, collecting, and maintaining EHR data related to patient healthcare. Thus, the EHR may include more comprehensive information, since many sources contribute to it. Each EHR can be shared across different healthcare members, providers, regions, and so forth. When the EMR data are exchanged with external health organisations or entities, they are considered EHR data, and the EMR will be the primary source of the transferred HER [56].
- **Personal Health Record (PHR)**: Each PHR record contains the same amount of EHR information but the PHR data can be managed and accessed by individuals [56][59].

  The World Health Organization (WHO) [55] describes the Electronic Health Record systems (EHRs) as "real-time, patient-centred records that provide immediate and secure

information to authorised users. EHRs typically contain a patient's medical history, diagnoses and treatment, medications, allergies, immunisations, as well as radiology images and laboratory results." Another WHO report [60] stated that the implementation of the clinical decision tools and laboratory and pharmaceutical systems in a poor African country such as Kenya have reduced practitioner errors and have enhanced both healthcare diagnoses and follow-up services. According to the US Department of Health and Human Services [61], the implementation of EMR has provided healthcare organisations with significant advantages and provide the following benefits:

- **Better quality of care:** The EMR has improved information exchange between doctors, healthcare team members, departments, and off-site health providers. As a result, patient information can be accessed easily if a patient needs emergency care or requires a specific medication. In addition, like any computer system, the system administrators can make a full backup of the EMR, which can decrease the risk and cost of losing data if a disaster occurs [61].
- **Improved care efficiency:** The EMRs receive data from different health information systems so that the patient information can be modified from various sources and locations. Patient data are available to several health practitioners, and they can communicate and exchange data through the EMR. Thus, EMRs can give doctors a simple way to review a patient's medical history or request a specific test or task from others. In addition, such communications can reduce the side effects of repeating some medical procedures such as X-rays and the time and associated costs [61].
- **Improved care convenience:** the patient history can be exchanged and accessed easily, which are the basic principles of the EMR. So, no need for physical space for paper records or forms, which in return can reduce the waiting time for both the patients and doctors to receive or review the medical records [61].

2.3 Information Security Management System (ISMS)

Today, Information and Communication Technologies (ICT) are a critical success factor in any modern society and enhance public services and facilitate interaction and communication among community parties and their authorities [62]. Many new and emerging technologies have improved the lives of people and the service delivery of organisations, including governments, worldwide. The significant shift in the business environment, economic instability, and customers desires and expectations increase the need to develop and adopt IT innovations. Over the last decades, several strategic transformations in enterprises and the

governmental sectors have been based on ICT applications, which brought many benefits. Consequently, the need for Information Security (InfoSec) becomes an essential matter as thousands of organisations worldwide are heavily dependent on information process systems to perform their daily tasks. Thus, it is critical to ensure that the information technology assets are secured and protected against IT threats. InfoSec scholars have defined information security from different perspectives. It includes multidimensional factors that are concentrated on preserving and protecting information assets via the implementation of security technical, operational, and physical controls [63]. Those controls need to be improved, reviewed, and regularly monitored to ensure that an organisation's business and security objectives are achieved [64].

The National Institute of Standards and Technology (NIST) [65] has defined information security as "The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability." Zafar and Clark [66] added more aspects to the NIST InfoSec definition in order to gain a more holistic view. These aspects are: establishing security policies and procedures, understanding and assessing potential security threats and risks, implementing and monitoring security controls, educating and training personnel in security awareness, performing permanent technology assessment, and integrating information security governance. Information security mainly aims to preserve information Confidentiality, Integrity and Availability, which is known as the CIA security triad [67]. Also, ISO 27001 adds authenticity, accountability, and reliability [68]. Thus, any security efforts in an organisation should put these security aspects in effect to ensure security for IT resources.

According to European Network and Information Security Agency (ENISA) [69], information confidentiality means "The protection of communications or stored data against interception and reading by unauthorised persons." Integrity is referred to as "The confirmation that data which has been sent, received, or stored is complete and unchanged." Availability is defined as "The fact that data is accessible and services are operational." In contrast to other personal information, the highly sensitive nature of healthcare information and the growth of dependency on healthcare information systems have increased the need for robust Information Security Management (ISM) in the healthcare sector. The ISM aims to ensure better governance of security controls implementation to counter information security threats and decrease the impact of security incidents.

If a patient's information is compromised, then the health organisation may suffer from a profusion of legal issues, which may result in financial losses and massive damage to the organisation's reputation. Today in many healthcare organisations, the HIS is no longer a standalone system with specific end-users; instead, it includes patients at homes via the internet [70]. This development in network and information exchange technologies has increased the type and capacity of HIS threats and challenges. Such growth in network and information exchange technologies has increased HIS threats and challenges [71].

In response to these security risks, initiatives from several countries and institutions have been launched to improve Information Security Management Systems (ISMS) practices, procedures, and guidelines by developing a broad range of generic and specific security standards. These standards aim to help organisations in many industries utilise their resources and efforts efficiently to gain an adequate security level via the adoption of best security practices [52][54]. According to ISO/IEC 27000, ISMS is "a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organisation's information security to achieve business objectives" [68]. Thus, ISMS's role is to ensure that all resources and procedures available to the organisation are in line with security practices and policies towards creating a secure environment for critical information and IT assets within the organisation. Another definition of ISMS by Eloff and Eloff is "a management system used to establish and maintain a secure information environment" [72]. The successful implementation of ISMS requires the organisation to build such an initiative based on well-known information security standards that direct and govern such efforts toward information security goals. These security standards are developed by several national and international organisations such as the European Standards Organisation (ESO) and the European Network and Information Security Agency in Europe (ENISA), the Federal Information System Controls Audit Manual (FISCAM) and the National Institute of Standard and Technology (NIST) in the US, the British Standards Institute (BSI) in the UK, and China's security standard GB/T22239.

However, these security standards are not strategies in themselves; instead, they assist the organisations in prioritising their security requirements and then provide them with a wide range of possible solutions to counter emerging security issues [73]. Based on an important concept called the PDCA cycle (Plan-Do-Check-Act), most of these standards integrate these four phases within their ISMS frameworks to develop, implement and evaluate ISMS [74]. The "Plan" phase constitutes the ISMS design process, beginning with an assessment of security risks and then the identification of appropriate security solutions and controls. The "Do" phase

aims to implement the security solutions and controls that were identified in the previous phase. The "Check" stage identifies any issues affecting the performance of the ISMS. The "Act" phase seeks to ensure that the ISMS performance is efficient and effective by reviewing and evaluating the overall performance of the security controls.

For instance, the development of the ISMS framework based on ENISA [75] consists of six steps, as shown in Figure 2.1. Step one involves the definition of security policies and requires a clear identification of security policy characteristics, needs, and other relevant information, including regulations, security guidelines, and standards that these policies must obey. Step two defines the scope of the information security management system. It specifies the risk assessment scope and governs the risk assessment and the treatment processes among an organisation's departments. Steps three and four expand the risk assessment and the risk management process.

According to ENISA [75], these two steps can be considered one step, called risk management. It aims to "transform the rules and guidelines of security policy and the targets, and on the other to transform objectives of ISMS into specific plans for the implementation of controls and mechanisms that aim at minimising threats and vulnerabilities." During this step, the organisation seeks to conduct four procedures: (1) classify the IT assets

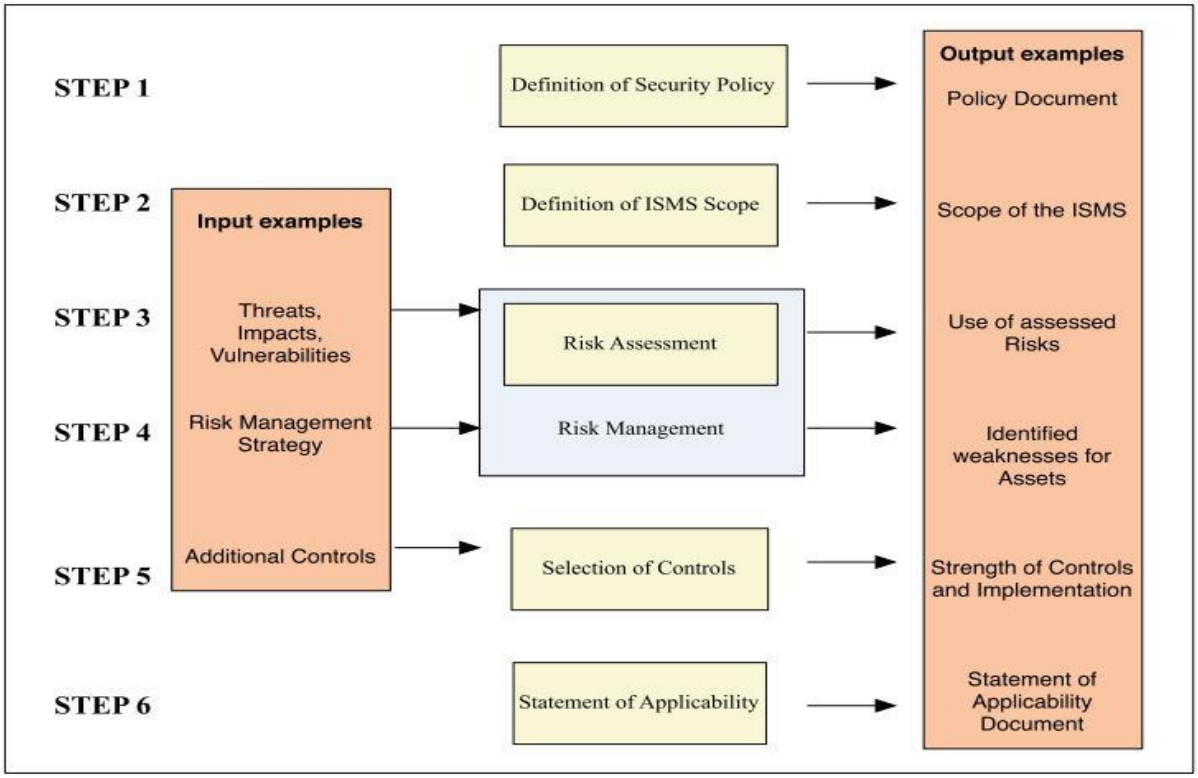


Figure 2.1 ENISA Information Security Management System Framework [71]

based on their sensitivity, (2) identify security risks and vulnerabilities, (3) estimate the impact and the likelihood of security threats on the organisation business process, and (4) conduct overall cost estimation to implement security countermeasures. Finally, steps five and six require iterative actions to select, implement and monitor both technical and non-technical controls. Step five involves the selection of appropriate controls in light of the organisation's security objectives, requirements, and business needs. Finally, step six seeks to assess the effectiveness of selected security controls to counter the security threats and vulnerabilities while at the same time determining the security control's implementation and maintenance plans.

The literature survey conducted by Akowuah et al. [52] reviewed several security standards, including NIST Special Publication 800-53, HITRUST Common Security Framework (CSF), Control Objective for Information and Related Technology (COBIT), ISO/IEC27002:2005, ISO/IEC27001:2005, ISO27799:2008, ISO17090:2008, ISO/TS 25237:2008. Their aim was to facilitate the selection process for a suitable security standard that can guide information security management practices in the healthcare industry. In this survey, many standards were reviewed and analysed to assist IT management in their initial steps toward security program implementation.

Akowuah et al. [52] recommended that ISO 27799:2008 and its associated series ISO 17090:2008 and ISO/TS 25237:2008 were suitable for any size organisations in the healthcare industry as they were tailored to handle various security aspects and technical issues within the healthcare environment. Moreover, the Health Information Trust Alliance (HITRUST) is a specific health security standard that can satisfy the security needs of most large organisations. HITRUST requires a subscription to get access to its health information security materials and training courses. On the other hand, some security standards such as NIST SP 800-53, ISO 27002:2005, and COBIT were more generic standards that provide holistic security approaches and procedures. Thus, they can be used as an alternative reference during the implementation of security programmes in healthcare organisations [52].

2.3.1 Information Security and Privacy In Healthcare

The sensitive nature of patient health information and the widespread usage of EMR/EHR in healthcare organisations have increased the fears related to security, privacy risks, and vulnerabilities. Those security fears can originate from internal sources related to intentional and unintentional behaviour caused by employee ignorance, curiosity, misuse of passwords,

social engineering, and so forth. At the same time, external threats include intruder and hacker attempts, malicious software, spyware, and virus attacks [10].

The aim of the Health Insurance Portability and Accountability Act (HIPPA), for example, is to ensure the confidentiality, availability, and integrity of Protected Health Information (PHI) while being stored, exchanged, and processed in any format (electronic, paper, or oral) between one or several healthcare providers. The PHI includes an individual's mental and physical health history and health providers' information, including bills and any other information that might reveal a patient's identity [76][49]. Moreover, the US Department of Health and Human Services (HHS) produced the Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule) to guide actions during the implementation of (HIPAA). According to HIPPA [49], the Privacy Rule's main objective "is to assure that individual health information is adequately protected while allowing the flow of health information needed to provide and promote high-quality health care and to protect the public's health and well-being." The Privacy Rule requires healthcare organisations to conduct a regular security risk analysis to ensure the CIA security triad, which can help identify the appropriate administrative, physical, and technical safeguards and mitigate existing and future threats.

Scholars and professionals have mainly discussed information security and privacy concerns and threats due to the enormous development of information technologies. The emerging technology trends, such as social networks, e-commerce, e-government, e-health, cloud computing, and so forth, are based on online services, thus sharing several perspectives of security and privacy fears related to their consumers. In the healthcare context, a recent study by Papoutsi et al. [70] examined patients' perceptions of security and privacy due to the widespread adoption of EHR in the UK. The authors used a mixed-method approach involving a survey questionnaire and focus group discussions.

The survey questionnaire was disseminated in general practice surgeries and NHS hospitals in West London. A sample of 2761 participants was included in the final analysis, which included patients and public members. A total of 17 focus group discussions were conducted, 13 with a total of 114 patients having a variety of health conditions. Four of the focus groups involved healthcare members, including NHS managers, health researchers, and professionals. The study found that the ability of the NHS to properly secure EHR was the main concern of 71% of the respondents. Almost 50% thought that integrated EHRs would decrease the security level; in contrast, 43.3% believed that the security risks would not change. Moreover, 78.9%

of respondents reported a negative reaction to the idea of allowing their health information to become part of a national EHR system.

Papoutsi et al.[70] concluded that sharing information on a wide scale via integrated EHR systems has raised public concerns about security and privacy risks. Therefore, more initiatives are required to increase public awareness of the trustworthiness of information security while at the same time establishing more robust techniques for maintaining privacy. Mahfuth et al. [77] conducted a systematic literature review to examine the security and privacy concerns and challenges related to the Electronic Health Record Systems (EMRs) within the healthcare industry. Another objective was to identify and analyse the current security solutions to overcome the confidentiality violation concerns resulting from EMRs' adoption, which includes a range of security frameworks, controls, and policies. The findings showed that there was an increasing rate of EMR adoption in both developed and developing countries worldwide. Therefore, seeking and maintaining an optimal level of EMR privacy against unauthorised access was a serious security challenge for healthcare team members, patients, IT experts, and stakeholders.

Mahfuth et al. [77] argued that the developing countries had more significant privacy risks regarding EMRs than the developed ones. These privacy and security risks are due to poor IT experience and infrastructure, insufficient security awareness levels, inadequate financial resources, and the absence of clear security laws and regulations. Moreover, the authors noted that the existing security solutions and policies were insufficient to ensure comprehensive protection of the EMRs health data privacy, which may affect the healthcare Quality of Service [35].

Rahim et al. [54] conducted a systematic literature review followed by a qualitative study. The aim was to identify and understand healthcare employees' perspectives on Information Privacy Concerns (IPC) and its influential factors when using the EMR. Afterwards, nine interviews were conducted to validate literature review findings with three groups from different backgrounds that included HIS users, IT experts, and legal professionals. Based on the literature review and the quantitative study, the authors have identified three factors that significantly influence IPC: privacy awareness, privacy policy, and privacy risk.

Bensefia and Zarrad [30] proposed a novel EMRs privacy-layered architecture model to overcome privacy concerns. It aimed to establish a balance between maintaining EMR privacy while at the same time ensuring EMR availability for authorised health providers. The model

encompassed three main layers, which were administrative decisions, the hardware infrastructure, and technological issues. The administrative decisions layer included security rules, regulations, and standards to satisfy all healthcare parties. The hardware infrastructure included all the physical types of equipment that were involved in handling EMR. The last layer included technological issues, which were responsible for distinguishing sensitive EMR data from common EMR information and then placing that sensitive data in a private database to restrict access. Thus, this private database and its sensitive EMR data would be accessed and shared via a proxy server to grant IP addresses to authorised clients.

Park et al. [78] proposed a research model to examine the relationship between Health Information Security Awareness (HISA), individual characteristics, and the intention of nursing students to naïvely disclose patients' health information. In the model, HISA constitutes three awareness learning constructs: General Information Security Awareness (GSA), Health Information Security Regulation Awareness (HRA), and Punishment Severity Awareness (PSA). Furthermore, the individual factors, including personal norms and self-control, are placed between the HISA and the nursing intention to disclose patient information. The model was empirically tested through a survey questionnaire of 123 nursing students within an urban university in South Korea.

The study by Park et al. [78] revealed that the GSA, HRA, and PSA were essential awareness learning elements to improve overall HISA and compliance with HIPAA. Moreover, the GSA, HRA, and PSA positively affect individual personal norms and self-control, consequently inhibiting nursing students from disclosing patients' information. Also, the study emphasised the importance of upgrading information security awareness of nursing students by updating the education curriculum to include more specific topics in security policies and practices in a medical context.

2.3.2 Information Security Policies

Ayyagari and Figueroa [79] stated that organisations in the public and private sectors have rapidly adopted different information and communication systems, and therefore the security of these technological systems is an essential concern. These technological systems support employees to perform their daily work in more efficient ways. Many public and private organisations rely on their IT assets to manage and process a wide range of valuable data, which increases the importance of information security to protect these assets from any security threats [79]. Thus, organisations invest heavily to safeguard critical information by developing

and implementing innovative technological tools and controls like firewalls, Antivirus, access controls, intrusion detections, and so forth [80]. However, employees are an integral part of an organisation's sociotechnical environment. Their interaction with the organisation's IT assets and information is an essential part of processing and delivering products and services. As a result, employees may intentionally or unintentionally put their organisations at significant risk, and sometimes the consequences of their behaviour exceed the impact of external threats [81]. Hence, organisations need to develop and implement information security policies as a primary approach to mitigate these internal threats [28].

ISO27001:2020 stated that the development and implementation of information security policies is one of the critical success factors in information security management. Organisations need to ensure that their information security objectives are consistent with their information security policies [82]. An essential aim of creating security policies is to inform the end users about their rights and responsibilities during their use of IT resources [24]. According to Höne and Eloff [83], an effective security policy will direct the targeted audience during their daily use of IT resources on how to perform actions securely by clarifying their acceptable behaviours and responsibilities. In addition, information security policies improve the organisation security governance as these policies define and manage boundaries between individuals and the organisation's IT resources [83].

The National Institute of Standards and Technology (NIST) [84] defines security policy as "The aggregate of directives, regulations, rules, and practices that prescribes how an organisation manages, protects, and distributes information." Likewise, ISO 27001 points out that the function and objective of information security policy aims to "provide management direction and support for information security following business requirements and relevant laws and regulations." Both definitions emphasise that developing and implementing information policies is an essential part of the security effort in organisations. However, Paananen et al. [85] pointed out that the information security literature has various definitions and functions of information security policy based on its rules, values, objectives, or characteristics. For instance, Klaic [86] defines a security policy as "a document in the narrow sense [that] represents a statement or declaration of the most important management persons (CEO, Executive Board, Minister...), about beliefs, goals, and reasons, and also general ways to accomplish desirable achievements in the field of information security." Also, other security scholars consider the security policy as a "rulebook" that mandated all IT users follow [87].

In addition, many security researchers stress that the security policy document needs to clearly distinguish between the subject and the object of the information security policy and describe the security roles and responsibilities for all users. Thus, the policy subject is referred to a security policy target audience such as employees, while the security policy object refers to the IT assets that require protection [22][88][86]. The security policy function can support individuals (subjects) to make better security decisions and actions when dealing with IT assets (objects) [85]. Paananen et al. [85], in their intensive literature review, summarised these different perceptions of the information security policy definitions in the security field under two main categories, information security characteristics and information security functions, as seen in Table 2.1.

Table 2.1 Information security policy characteristics and functions adapted from Paananen et al. [39]

	ISP characteristics	ISP functions
Steering the organisation	Statement of security goals/strategy	Supports business goals
	Guidance/instruction	Control
	Statement of rules	The basis for performance measuring
The actor and the asset	Defines subjects	State's responsibilities and authority
	Defines objects	Provides an overview of information assets
Preparing for incidents	Comprehensive plan	The basis for security culture
	Addresses risks	Prevents loss/misuse of information
	Recovery plan	Ensures continuity
	Communication tool	Evidence of IS program

Variation in InfoSec policy definitions and functions caused a variation in the development process approach of information security policy. Several security scholars [89] [90][91][92] proposed various InfoSec policy approaches that share a formulation model based on the British international standard, ISO/IEC17799:2000 [93], which consists of inputs from security standards and advice from experts, policy development through the analysis of existing assets, and controls in consultation with stakeholders and outputs comprising the policy itself and associated activities for dissemination, awareness-raising, and education.

In addition, Baskerville and Siponen [90] suggested a meta-policy approach for InfoSec policy development that includes four steps: (1) policy requirements, (2) design, (3) implementation, and (4) testing. The first step requires identifying policy users, available technological assets, and a classification of roles and responsibilities when accessing those assets. The second is the design process, which aims to identify the InfoSec policy architecture, boundary, and scope, as well as how the policy will be developed and implemented. This includes creating a policy and sub-policy hierarchy, which requires the policymakers to identify the high level (abstract) and low level (detailed) policies, along with the users and assets at each level. The third step is implementation, which aims to determine the best ways to implement the policy, taking into account the culture and environment. The last step is testing, which includes evaluating the interaction between the security policy and its subjects to determine if the implementation of the policy satisfies the organisation's security requirements and objectives. This phase seeks to evaluate the security policy design and investigate any issues or security threats that emerge as a result of policy implementation.

Ress et al. [91] proposed the Policy Framework for Interpreting Risk in E-Business Security (PFIRES), which integrates the system development life cycle (SDLC) concept and the new product life cycle. Their framework consists of four phases to develop a security policy—Access, Plan, Deliver, and Operate—as shown in Figure 2.2.

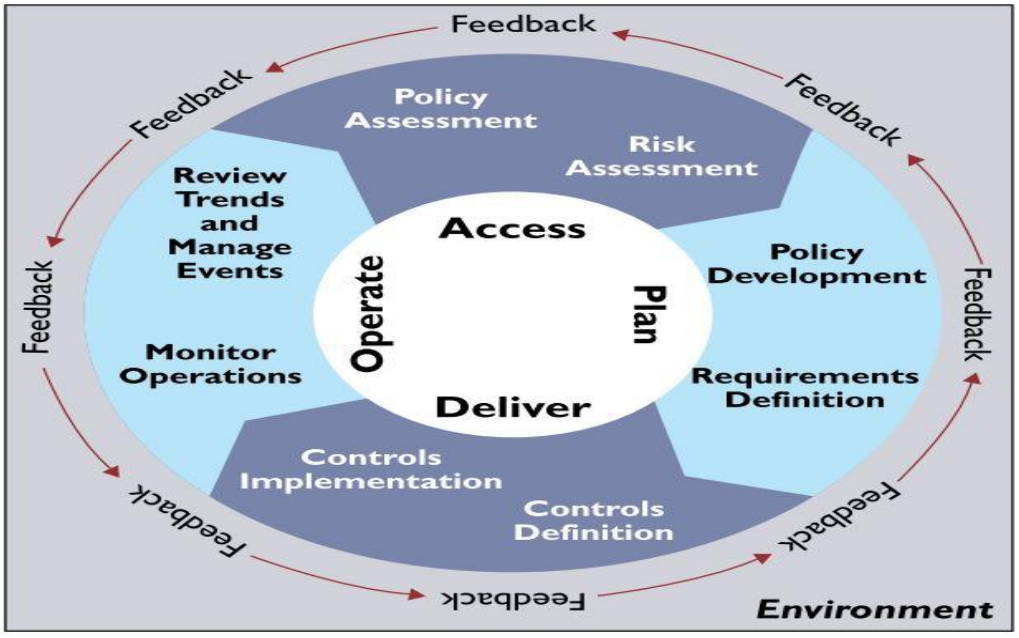


Figure 2.2 PFIRES Life Cycle Model For Information Security Development By Ress et al. [87]

The assessment phase includes policy and risk assessments. The policy assessment process requires reviewing the existing legislation, security policies, and best recommendations list.

Risk assessment encompasses (1) security assessment to identify security threats and vulnerabilities; (2) assess business risks which aim to determine the most vulnerable IT assets that can be compromised and their value in the business; (3) produce a final security recommendation report that includes the result of both the policy and risk assessments.

The second phase is planning, and it involves policy development, which reflects the strategic decision to create or update a security strategy. In both cases, the key steps are "identifying areas for security policy, drafting security policy, reviewing security policy and publishing security policy" [91]. The third phase, delivery, includes defining and implementing controls, in which security controls are selected, evaluated, tested, and implemented. The final stage is operating, which aims to communicate the security policy to all of its potential audiences, monitor the impact of security controls on day-to-day business activities, investigate security incidents and the root cause of security threats, and enforce compliance with the security policy.

Similarly, Flowerday and Tuyikeze [92] suggested an Information Security Policy Development Life Cycle (ISPDLC) as an iterative framework for security policy development with five phases (codes). The ISPDLC was derived from the information security literature, security standards, and security professionals. The initial phase is performing risk assessment as the main input method to the development process, which targets the identification of the security threats and vulnerabilities, IT assets, and related regulations. The following phases are policy construction, policy implementation, policy compliance, and, lastly, policy monitoring.

Policy construction is the process of writing a security policy with the stakeholders; the precondition of this process requires an agreement between the policymakers and the stakeholders to decide the level of the security policy, either abstract (high level) or detailed (low level). During the policy implementation phase, the stakeholders' roles and responsibilities should be clearly defined, and the subject of the security policy should be educated and trained. The compliance phase focuses on analysing the interaction between the security policy and its audience in terms of their knowledge and attitude of its requirements and perceived benefits and social pressure. The last phase is monitoring to audit compliance level and review any emergent issues. Based on a qualitative study with certified information security professionals, Knapp et al.[94] proposed a repeatable organisational-level process model for the development of information security policy that contains eleven stages. Likewise, the model by Rees et al. [91] and Flowerday and Tuyikeze [92] have an iterative portion in between and within the main and the substages. The first stage requires a risk assessment as an

initial activity to identify any existing or potential security risks that need immediate attention; the risk assessment report is the primary input into the framework. This is followed by what Knapp et al. [48] called the policy management processes. It contains four stages: (1) policy development, (2) policy review, (3) policy approval, and (4) policy retirement (if the policy is no longer needed). In the policy management processes, the policymakers can use an iterative process between these four stages until they reach a consensus and accept the policy, as shown in Figure 2.3; they then can proceed to the next stage of information security awareness and training.

Once the subjects of the security policy have been trained, the policy is ready for implementation. The monitoring and policy enforcement are the last two stages. According to Knapp et al. [94], both stages require ongoing effort from management to ensure successful implementation of the security policies; therefore, management needs to equip the IT department with the necessary audit and automated tools to facilitate the monitoring process so it can contribute to the enforcement effort. Knapp et al. [94] state that "policy enforcement is an ongoing activity affording the opportunity for management to put the 'teeth' into formal policies. If, for example, an employee is caught knowingly violating a policy, managerial-directed corrective action can occur" [94].

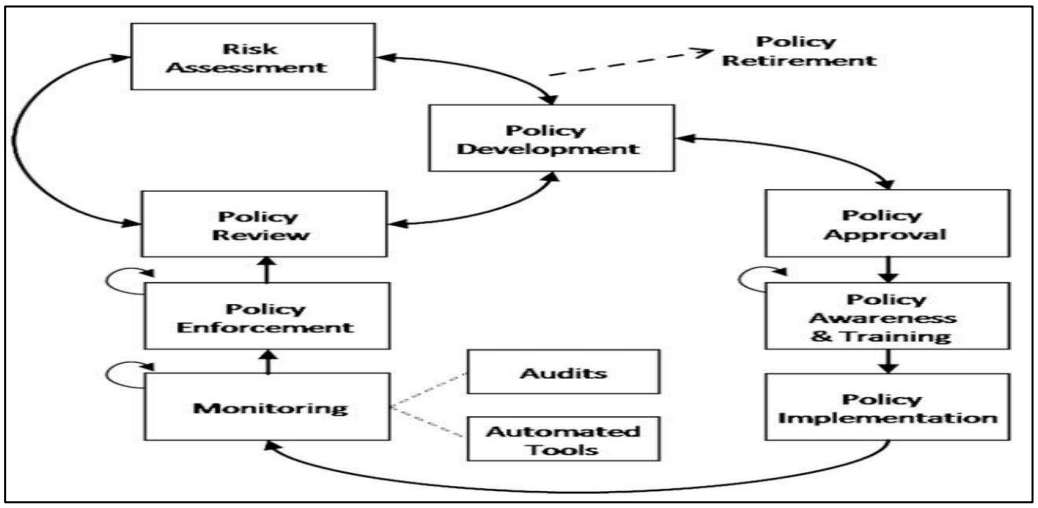


Figure 2.3 Organisational-Level Process Model For Developing Information Security Policy By Knapp et al.[90]

2.3.3 Information Security Policies Effectiveness and Quality

According to the Oxford Living Dictionary, effectiveness is defined as "The degree to which something is successful in producing the desired result; success" [25]. Several studies in the IS compliance context have introduced a wide range of both proactive and reactive factors that

can minimise or maximise the efficacy of ISP implementation. These factors may include end user awareness and training, end user compliance level, the influence of ISP standards and regulations, organisational culture, the level of top management commitment and enforcement, alignment between organisational goals and the ISP objectives, and ISP workarounds [26][27] [6]. In addition, several information security scholars proposed criteria that can support the efforts of policymakers to produce a more effective security policy, as summarised as follows [95]:

- **Consistent with the organisational culture:** The security policy must be aligned with the culture of the organisation. The policymaker must know that the notion of one-size-fits-all is not applicable in a security context as each organisation has unique security requirements and objectives.
- **A policy must be efficient and dynamic**: The rapid emergence of security threats requires policymakers to review and update the security policy on a regular basis. It is recommended that the security policies be reviewed every six months.
- **A policy must use simple and easy language**: Policymakers need to ensure that the policy is not a highly technical document that includes complex technical details and jargon. Instead, the policy language needs to be simple, free of complex IT terms and written in a clear style so that the policy end user can understand it without any confusion.
- **Clarify the policy purpose and scope:** The policy must have a clear answer to why a policy was created. Policymakers must state the purpose of the security policy, its scope and aim, thus enhancing end-user understanding of the needs and benefits of the policy.
- **Clarify end-user role and responsibilities**: Policymakers should indicate the role and responsibilities of the end-users of the policy when using the organisation's IT assets also, their obligation to comply with the policy and the consequences of policy violation.

Information quality is an essential factor in policy effectiveness. Quality is a multidimensional concept and has several definitions based on the context. In general, quality as a concept has been defined as conformance to essential requirements. Beverly et al. [96] referred to information quality as the fitness of use, which covers both usability and usefulness. In the information security context, Bulgurcu et al. [13] conceptualise quality of the ISP as "the requirements or expectations of employees from the ISP document." Having unclear requirements of the InfoSec policy document can impact the reader's understanding of the security requirements and decrease their intention to adhere to them. Thus, Höne and Eloff [83] postulated that an effective security policy should be "an understandable, meaningful, practical

and inviting document that addresses the users directly and convinces them of the need to handle information resources securely." They believed that a poorly written security policy could be a problem itself and a source of security incidents if the employees do not fully understand its contents or cannot fulfil its requirements [83]. Therefore, policymakers should take great care when writing security policies to ensure that they are easy to understand for the targeted audience.

According to Pahnila et al. [9], the quality of information security policies impacts employee satisfaction, which can then positively influence their actual compliance with the ISPs. This result is consistent with Care [5], who found that the quality of information security policies significantly impacted both the employee's compliance and their sense of the fairness of InfoSec policies. Similarly, Pahnila et al. [28] conducted a model to investigate how ISP knowledge levels between two groups—one with low ISP knowledge and the other with high ISP knowledge—impacted compliance among the employees. The result revealed that the quality of the InfoSec policy document significantly impacted the employees with high knowledge of the ISP and that the quality of the ISP documents was reflected in the design, relevance, and currency of the policy.

The term quality covers many factors, and several researchers have suggested different attributes of information quality. Huh et al. [97] indicated accuracy, consistency, completeness, and currency as important dimensions for information quality. Nelson et al. [98] adopted three of these dimensions while substituting the formation format for consistency. Furthermore, Miller and Doyle [99] stated the information quality of a report covered completeness of information, the accuracy of the information, the relevance of the report, and the timeliness of the report. In addition, Doll et al. [100] postulated that information quality comprises five elements: (1) attributes of content, (2) timeliness, (3) ease of use, (4) accuracy, and (5) format. Quality dimensions for information security policies have been proposed by Bulgurcu et al. [23], which comprise three central quality characteristics: (1) clarity, (2) adaptability, and (3) consistency. Clearly, information quality has a substantial impact on employee satisfaction and the perception of fairness of the ISPs [23],[27].

2.3.4 The Human Factor in Information Security Policies

Many scholars have examined individuals' neglect to comply with information security requirements and practices in the information security literature and have come to the not surprising conclusion that that improving InfoSec policies compliance is challenging and

requires significant efforts [101][102]. Implementing more advanced and expensive security technical controls is not always a successful approach in ensuring IT assets' security if the end-users, for instance, avoid the necessity of password confidentiality and share it with others. According to Adams and Sasse [103], useful development of IT security mechanisms should consider the user-centred design and technical design. Being solely dependent on technological solutions would not return the expected security protection. Sometimes, reliance on technological solutions to enforce security compliance can backfire and encourage devastating behaviour [104][105].

Recently, a wide range of information security studies has investigated the role of individual users in information security compliance, focusing mainly on those factors that influence end-user behaviour to comply with or violate InfoSec policies. Frequently, individuals cause security threats when they unintentionally act in risk-taking ways such as careless information handling, accessing unsecured links or webpages, or thoughtless data disclosure [1][106]. These unintended behaviours can open gaps in the security architecture of organisations and allow malicious parties internally or externally to damage the IT infrastructure. In this light, we will focus on the following subsection's security threats resulting from employee behaviour within an organisational environment.

2.3.5 Insider Threats and Information Security Policies

Security threat actors can be internal or external [107]. External threats are those entities who want to penetrate the organisations IT assets, such as hackers, malware attacks, and those intruders with no right to access the organisation's systems or network [10]. Frequently, external attacks aim to make financial gains, commit sabotage, or steal information [107][108]. Internal threats are often as severe as external threats, and organisations have long recognised that internal human agents can trigger security threats, which has motivated them to improve their information security governance. An insider is a human agent like an employee who has valid reasons and privileges to access and interact with the organisation's IT assets [109]. Thus, there is a call-in information security governance literature for more studies of insider motivations and to consider employee non-compliance with the information security policies as a significant source of security problems [110][111].

According to Proofpoint [108], insider threats may be intentional or unintentional. Intentional threats refer to those members of the organisation. These members act maliciously and deliberately to violate or harm the IT infrastructure, as when, for example, an employee steals

information to sell it [10]. In contrast, unintentional threats involve those individuals who violate security requirements through human error, carelessness, ignorance, privilege misuse, computer and password abuse, and so forth [10]. According to Barlow et al. [112], even accidental modification of the data can make the data incorrect, which can be considered a security violation of information integrity.

Seh et al. [20] define healthcare data breaches as "illegitimate access or disclosure of the protected health information that compromises the privacy and security of it," and reported the following four root sources of data disclosure in healthcare:

1. **Hacking:** this includes all types of malicious cyberattacks that aim to overcome the organisation's security controls to gain unauthorised access to IT resources such as network, systems, and data. It includes hackers penetration attempts via ransomware and malicious software [20].
2. **Unauthorised internal access:** this includes all types of incidents that lead to data leakage by an internal actor in the organisation. For instance, the security incident causes data breaches due to employee abuse of privileges, unauthorised disclosure, and so forth. [20].
3. **Theft or loss of devices:** these include all data leakage incidents due to the theft or loss of devices (USB memory devices, laptops, hard drives, and so forth) that contain unencrypted sensitive information such as medical records [20].
4. **Improper disposal of unnecessary data:** this includes all accidents that cause data breaches of old but still sensitive medical records by, for example, throwing away old hospital computers without properly destroying internal hard drives or placing medical files and documents in unlocked storage rooms or open areas.

Insiders can be the source of devastating internal security incidents and "can be much more costly than an attack from external incidents, and are more likely to succeed due to internal knowledge of the corporation" [113]. Data disclosure is a critical type of security threat that can cause massive financial and reputation losses for healthcare organisations and harm individuals' privacy. The 2019 Ponemon Institute report on the costs of data breaches [114] indicated that for nine consecutive years, "healthcare organisations had the highest costs associated with data breaches at $6.45 million—over 60 per cent more than the global average of all industries." In 2019, the average cost per medical record breached in the United States was $ 429. This was the highest cost per breach among the other sixteen industries in the report and was well above the overall average of $150 per breach. Unintended violations due to human behaviours were the root cause of nearly 49% of data breaches in healthcare, with an average

loss of $ 3.5 million. These costly breaches resulted from individual fault, negligence, use of infected devices, access to an untrusted link, and loss or stolen devices [114].

According to the 2019 Verizon Data Breach Investigation Report (DBIR), insiders were the source of 30% of the total 23,399 cybersecurity incidents reported, while 72% of these internal incidents were caused by miscellaneous errors and privileges misuse. The same DBIR report stated that there were 304 data breach incidents in the U.S. healthcare industry that year and that internal actors were the cause of 59% of these breaches. Compared to the 16 industries covered by the report, healthcare had the highest percentage of confirmed data disclosures linked to internal actors [115].

The recent 2020 Verizon DBIR report revealed a total of 521 confirmed data breach incidents in healthcare organisations in contrast to the 304 reported in 2019; insider actors committed 48% of these data breaches. Therefore, the DBIR 2019 and 2020 reports indicated that insider actors remain the leading cause of data breach incidents in the healthcare industry, making it the industry with the highest percentage associated with internal threats for two consecutive years.

Further, Seh et al. [20] conducted a literature review analysing healthcare data breaches sources, types, and costs between 2005 and 2019. They found that health information systems were the primary targets for external attacks by hackers and malicious software compared with other industries. They reported that between 2010 and 2019, there were 3051 HIPPA data violation incidents that disclosed sensitive data for more than 255.18 million people in the US. According to these researchers, a total of 2,860 confirmations of HIPPA data disclosure incidents were reported between 2010 and 2019, and internal actors were the central source of 67% of incidents. In particular, nearly thirty per cent of these data breach incidents were related to unauthorised disclosure of sensitive data by employees or practitioners, while data leakage due to theft or loss of devices represented just over 37 % of these incidents.

2.3.6 Insights on Information Security Policies Violations

Several organisations recently defined information security policies as an essential defence mechanism to counter the insider security threat resulting from employees non-compliance behaviour with security requirements [116]. Thus, a comprehensive analysis of the InfoSec policies violations can enhance our understanding of security policy violations and provide better solutions.

Many scholars have conducted extensive and comprehensive analysis and review studies of the information security literature to more fully understand security breaches and their influence on security efforts [117][118][119]. Njenga [117] conducted a systematic literature review (SLR) of 175 rigorous studies collected from several academic and journal databases such as ScienceDirect, ACM, IEEE, Google scholars, and ProQuest. The SLR aimed to identify "the theories that have been used in information systems security violations literature, categorisation of security violations as presented in literature; and the contexts that these violations occur" [117]. This effort can help scholars understand why IS researchers classify information security violations by internal actors differently. Njenga's [117] SLR revealed the failure of the studies to provide constant meanings of the information security violation as behaviour. Thus, having various senses of security violations can complicate behavioural categorisation related to insider threats and the relative understanding of those behaviours.

Nonetheless, proper categorisation for InfoSec violations is necessary to increase the effectiveness and applicability of security controls during the enforcement process in organisations [120]. In addition, meaningful categorisation would support the security effort to implement more counteractive actions toward improving behavioural compliance with InfoSec policies [117]. Loch et al. [121] highlighted the importance of getting proper classification of information security violations. A classification can improve the effort to identify the security threats and enhance the organisation's capability to develop suitable mitigation solutions. For instance, Willison and Warkentin [122] indicated an extensive concentration in the IS literature on the insiders' deliberate and malicious violations, consequences, and related deterrence mechanisms in the computer abuse context and asserted the importance to establish a more holistic understanding of the employees' security deliberate actions that should precede any effort to design and implement the deterrence controls [122]. However, the difficulty of establishing "a more holistic understanding" of the categories of InfoSec violations is dramatically revealed by Njenga's systematic literature review discussed above [117] as shown in Table 2.2 below.

Table 2.2 Njenga [117] ***Categories of Information Security Violations***

Source	**Proposed Categories of Information Security Violations**
Aurigemma and Mattson [123]	**1. Malicious** **2. Non-malicious: :** any action that leads to security violation but without intention to damage the organisation IT assets [124]
Barlow, Warkentin, Ormond and Dennis [125]	**1. Malicious** **2. Non-malicious** **3. Deviant behavior**
Dang [126]	**1. Non-volitional noncompliance** **2. Volitional but not malicious noncompliance** **3. Intentional malicious abuse.**
Guo and Yuan [124]	**1. Knowingly break rules:** (employees violate the existing security policies that they are known). **2. Voluntary: (**the employee violates the policy without any pressure from their social context). **3. Intentional** **4. Non-malicious**
Kraemer and Carayon [127]	**1. Violations of malicious intent** **2. Violations of a non-malicious nature**
Warkentin and Willison [128]	**1. Passive, non-volitional** (laziness, sloppiness, poor training, etc.) **2. Volitional, non-malicious** **3. Intentional, malicious.**
Siponen and Vance [129]	**1. Non-deliberate violations** **2. Deliberate violations**

Other scholars not reviewed by Njenga [117] have attempted to describe categories of InfoSec violations by borrowing concepts from other disciplines to expand internal security threats classifications. Cheng et al. [130] conducted a study for understanding the violation of information security policies in organisations. They used the social bond and social pressure concepts along with deterrence theory to explore whether the relationship between the employees and their managers can explain the employee intention to violate information security policies. The study findings reveal that social bonds and social pressure can positively influence compliance intention with information security policies. Kraemer et al. [127] developed a security framework to examine the human factors that lead to computer and information security abuse. In particular, they conducted 16 interviews with IT experts to create human error taxonomies that contribute to computer and information security violations. They found that network administrators were strict and classified most human errors by employees as intentional more than unintentional. In contrast, the same administrators categorised most IT department employees errors as unintentional more than intentional.

Finally, from criminology, Maasberg [131] proposed an insider threats taxonomy to explain IT espionage attacks by an internal party in the organisation. They identified four insider threats

categories and distinguished insiders by their motivations and methods. These threats were espionage, intellectual property (IP) theft, fraud, and information technology (IT) sabotage. Thus, they argued that having such security threats classification can support the efforts to determine the technical indicators of espionage and implement effective and robust technical detection and preventive measures.

For the purposes of this study, it is best to assume that all external threats to information security should be considered malicious and intentional, while insider threats are either non-deliberate (i.e., accidental) or deliberate [129]. Those that are deliberate may be either malicious or non-malicious in nature [127]. Further categorisation would seem non-productive since the motivations behind malicious violations will vary significantly from individual to individual and not lend themselves to convenient and perhaps overly nuanced categories.

In summary, section 2.2 contributes to this thesis by providing a holistic overview of healthcare information systems (HIS) evolution in the current days. Utilising these technologies (EMR, PHI, and PHI) enhances healthcare services' availability, reliability, integrity and serviceability to patients and assists organisations with more cost and time efficiency in managing and sharing patients' information with internal and external parties. However, the widespread adoption of the HIS comes with serious information security complications. These technological systems are valuable targets for intruders seeking financial gain, identity theft, and insurance fraud. Any data breach can cause devastating and non-financial losses for individuals and organisations. Thus, Section 2.3 explains security challenges and risks and details why organisations, specifically in healthcare, struggle to find the right balance between the critical nature of patient care and the security measures required to protect personal data.

In particular, Section 2.3 expands our understanding of the current efforts of organisations and governments to conduct and implement a wide range of regulations, security frameworks, and best practices to secure and protect IT assets and the privacy of individuals from internal and external threats. In addition, it helps the researcher identify the internal threats (insiders) as a critical topic for a research project based on numerous reports and security studies in the information security literature that cites insider threat behaviour as a primary security source for data breach incidents. Also, a review of the information systems literature shows that the number of security breach incidents and associated costs is increased explicitly by the non-malicious behaviour of employees regardless of the presence of different technical and non-technical security controls. Thus, it identifies the necessity of improving cybersecurity in healthcare organisations and the urgent need to reduce undesirable employees behaviour, such

as adopting various behavioural justifications to violate information security policies. The next sections establish the theoretical background for individuals behavioural rationalisation and address related criminological and psychological fields. Then, we detail the role of neutralisation theory in the context of information security non-compliance.

2.4 Behavioural Research in Information Security

An information security policy defines the appropriate use of organisational information and its assets, including providing a set of guidelines, procedures, and technical controls for users to follow [42]. An employee's non-compliance with security policies is a severe information security problem. To address this phenomenon, information security researchers have conducted several empirical studies based on well-known behavioural theories [132]. Thus, the integration of behavioural theories generates extended theoretical models that support the efforts of IS scholars to understand different issues associated with human behaviour in a security context. These theories include, among others, social control theory and general deterrence theory [91][92], self-determination theory [135], protection motivation theory [116][136], and social bond theory [137]. The following sections discuss three essential theories from the criminology and psychology fields that are strongly related to the neutralisation techniques in an information security context: the Theory of Planned Behaviour (TPB), General Deterrence Theory (GDT), and Social Learning Theory (SLT).

2.4.1 Theory of Planned Behaviour (TPB)

Ajzen [138] proposed the Theory of Planned Behaviour (TPB), which has become one of the most widely adopted theories used to examine human social behaviour, itself an extension of the Theory of Reasoned Action (TRA) [139]. The essence of the TRA and TBP depends on the intrinsic relationship between individual intent and behaviour, which considers behavioural intention as the most important factor in determining actual behaviour [140]. TRA, according to Ajzen [141], hypothesised that the intent behind individual behaviour is influenced by two factors: *attitudes* and *subjective norms.* Attitude is "determined by the individual's beliefs about outcomes or attributes of performing the behaviour (behavioural beliefs), weighted by evaluations of those outcomes or attributes" [140]. Subjective norms refer to the perceived social pressure from friends, family members, or colleagues on an individual whether to move forward and perform the behaviour or not. The TRA constructs are illustrated in the orange dotted area in Figure 2.4. Based on the TRA concept, Ajzen [138] proposed the TPB, which also suggested that the intention behind the behaviour is a significant predictor that precedes

actual individual behaviour. Stronger intent increases the likelihood that an intention will convert into actual behaviour [140]. Ajzen extended the primary constructs of TRA—attitude and subjective norms—to include *perceived behavioural control*, the only difference between the TRA and TPB. Ajzen [138] defined perceived behavioural control as " people's perception of the ease or difficulty of performing the behaviour of interest." Figure 2.4 illustrates the primary constructs and subconstructs of TRA and TBP, as well as external constructs that might impact the behavioural intention. Both TRA and TBA have been widely adopted to predict and investigate various undesirable health-related behaviours and intentions such as excessive drinking, smoking addiction, lack of exercise, and so forth [140].

In an information security context, there is evidence of a close relationship between behavioural intention and both information security compliance and violation [62][101][42].

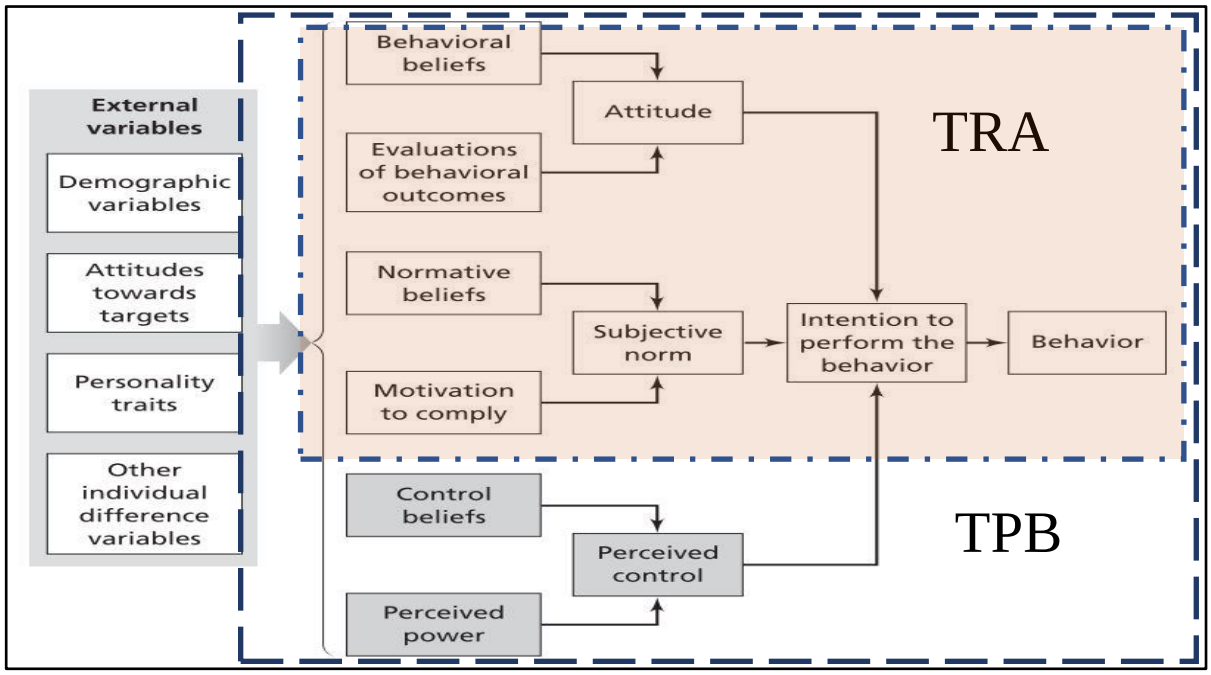


Figure 2.4 Theory Reasoned Action and Theory Of Planned Behaviour Adapted From Montano And Danuta [94]

Cram et al. [28] conducted a comprehensive review of 114 articles in the information security compliance literature and found that normative beliefs and attitudes were critical variables in several theoretical models investigating various information security compliance issues. Several scholars found a link between attitude and information security compliance, including studies by Bulgurcu et al. [23], Foth [143], Hu et al. [144], and Ifinedo [145]. In contrast, other researchers employed the TPB construct to establish the relationship between intention and information security violations, including studies by Siponen and Vance [1], Chen et al. [146], Guo [124], and Cheng et al. [130].

2.4.2 General Deterrence Theory (GDT)

General deterrence theory (GDT) comes from the criminology field and is based on a rational decision between cost-benefits to commit an act that violates laws and regulations [147]. The GDT claims that individuals rationally evaluate the consequences of breaking laws or rules to decide whether to proceed. The GDT has been widely adopted in the information security literature to motivate employees to comply with information security policies [148]. When an individual's assessment of the cost associated with a practice that violates a security control or policy is greater than the expected benefits resulting from the violation, that cost will discourage the individual from committing the breach and staying committed to the security requirements [149][150]. Sanctions are defined as "tangible or intangible penalties such as demotions, loss of reputation, reprimands, monetary or nonmonetary penalties, and unfavourable personal mention in oral or written assessment reports incurred by the employee for non-compliance with the requirements of the ISP" [23].

The GDT asserts that formal sanctions such as disciplinary actions as incarceration, salary reduction, loss of privileges; informal sanctions such as negative feedback from colleagues or management; and shame can be effective methods to deter undesirable behaviour [23]. Shame is defined as "a feeling of guilt as a result of others knowing of one's socially undesirable actions" [151]. Barlow et al. [125] stated that "as an employee feels more certain of formal consequences from the organisation or social consequences from others, or perceives that those consequences will be more severe or swift, he or she will perceive those actions as too risky and will be less likely to violate the IT security policy." In general, punishments or sanctions may increase the deterrence effect in two ways: by increasing the certainty of the sanctions and by increasing the severity of sanctions. Certainty of sanctions refers to the belief that deviant or undesirable behaviour will be detected by the authorities, thus increasing the risk of discovery [149]. The severity of the sanctions is based on the offender's belief that the potential cost associated with the punishment is too severe to be risked [133].

The application of the GDT has mixed results in the information security literature. For instance, several studies found evidence that the severity and certainty of formal and informal punishments have a deterrence effect and can dissuade an individual's intention from computer misuse and information security violation [133]. Herath and Rao [152] found that both formal and informal punishments significantly influence employees' InfoSec compliance intentions. Hovav and D'Arcy [133] examined the deterrent effect of formal and informal sanctions on the

misuse of IS between two national cultures, South Korea and the United States. The result revealed that individual perception of the perceived severity of formal sanctions for each security control differed between cultures. Still, only the severity of formal sanctions was positively associated with reducing information security misuse in Korean and American participants. Similarly, Cheng et al. [130] investigated the effect of the severity and certainty of sanctions on information security violation intention and found that only a perceived severity of formal sanctions had a significant influence on reducing individuals violation intention. Further, Chen et al. [153] proposed that an effective enforcement system should combine the severity and certainty of sanctions with rewards for compliance to mitigate internal risks related to employee non-compliance with information security policies.

Sometimes employees violate information security policies regardless of the presence of deterrence methods. For example, under the stress of a particular situation, some individuals make a willful infringement based on their moral judgment; hence, they ignore the simple intuition of following regulations. Such decisions occur because these individuals provide reasons to justify or neutralise their violations [49]. Consistently, Silic et al. [76] found that formal sanctions, informal sanctions, and shame had a little deterrent effect on individual IT intentions. Likewise, Siponen and Vance [49] found that individual justifications outweighed the impact of formal and informal sanctions.

2.4.3 Social Learning Theory (SLT)

The SLT is a general theory in the criminology field introduced by Bandura and McClelland in 1977 [154]. SLT is a theory of behavioural imitation [155]. According to Bandura and McClelland [154], human learning is an ongoing cognitive process and an essential step for the acquisition of knowledge or new behaviour, beginning with direct observation, interaction, and imitation of other behaviours in a social context. Bandura and McClelland [154] stated that a new behaviour learning process starts when an individual directly observes or experiences a behaviour from an admired person or social model and then imitates the model's behaviour at a later stage. In the SLT, the observer does not automatically shift from the observation stage to the social model behaviour replication stage. The individual's learning process also includes what is known as vicarious reinforcement, which is a learning process that involves observing the sequence of events to achieve the behaviour in light of the probable punishments or rewards for repeating the behaviour of the model. In addition, before replicating the model's behaviour, the observer goes through what is known as mediational processes, which are a series of

cognitive processes to determine the desired response, regardless of whether or not the person imitates the model's behaviour [156]. According to McLeod [156], the description of these cognitive processes of observation include the following:

- **Attention:** The degree to which the observer notices and focuses on the model's behaviour. A high degree of attention toward the model behaviour makes it noteworthy and can influence others to imitate the behaviour [156].
- **Retention:** the extent to which a model behaviour is not forgotten but instead remembered in detail by the observer. When an observer remembers all events and features that led to a behaviour, the person is more likely to reproduce it later [156].
- **Reproduction:** This indicates the physical and mental capabilities of a person to imitate behaviour. For example, an observer will not attempt to repeat a particular behaviour if their physical ability is limited and would not serve them to achieve their purpose [156].
- **Motivation:** This is the degree to which the observer will evaluate rewards and punishment that follow the behaviour. Model behaviour is more likely to be reproduced by the observer if the perceived rewards offset the perceived costs. On the other hand, the observer will not repeat the behaviour if vicarious reinforcement is not seen as essential [156].

According to Holt et al. [157], SLT is one of the most popular learning theories to explain cybercrime, including software and movie piracy. In the behavioural security context, the application of the SLT provides a theoretical framework to improve security and is reflected in the confidence or self-efficacy of individuals in their computer and security skills as influenced by situational factors like security awareness programs [158]. In the information security context, self-efficacy is defined as "the confidence in one's ability to undertake a recommended preventative behaviour" [159]. Self-efficacy is an essential factor in Bandura's 1986 extension of SLT, which he called Social Cognitive Theory (SCT) to account for the amount of mental control individuals have over their behaviour, a level of control not reflected in Social Learning Theory. Furthermore, Social Cognitive Theory reflects the perception of an individual's self-judgement about their ability to perform a specific course of action or behaviour [160]. The SCT asserts that individuals are more likely to begin challenging behaviours when their confidence in their abilities are high, which is reflected in "a user's self-confidence in his/her skills or ability in practising computer security" [161]. Finally, Rhee et al. [162] describe self-efficacy as "a belief in one's capability to protect information and information systems from unauthorised disclosure, modification, loss, destruction, and lack of availability."

Several security studies that have adopted SLT and, by extension, SCT, have reported that improving employees security self-efficacy to comply with the information security and privacy policies required the organisations to enhance the employee formal and informal social learning environment settings to be more supportive. For instance, Warkentin et al. [158] conducted an empirical study to evaluate the influence of external social cues such as situational support, verbal persuasion and vicarious experience on an employee's self-efficacy to perform compliant actions. The results indicated that a supportive social environment could improve the employees' security perceived self-efficacy to perform compliance security actions. In particular, employees perceived self-efficacy could be enhanced informally via three social learning factors: (1) provide employees with situational support, which includes the right tools, opportunity, and time to perform their jobs and protect IT assets; (2) provide the employee with appropriate and continuous feedback and instructions from superordinates and managers to enhance their security confidence to stay in compliance; and (3) provide them with indirect experience by allowing them to learn from other expert colleagues.

As a consequence of the use of SLT and SCT in InfoSec studies, self-efficacy in information security emerge in the literature and has been widely used as an antecedent of employees' compliance with information security policies. Rhee et al. [162] conducted an empirical study based on the SLT and a survey of 415 graduate students. This study aimed to investigate the relationship among the antecedents of self-efficacy in the information security domain. The study revealed that self-efficacy is a significant factor to predict individual security practices that secure information and information systems. Individuals with high self-efficacy tend to adopt a proactive approach and formulate solutions for the security problems more than individuals with low self-efficacy. Other studies also found that self-efficacy is an essential factor that can effectively impact and promote compliance intentions with organisational information security policies and practices [23][25]. Further studies revealed that individuals' self-efficacy increase their tendencies to perform security practices such as antivirus software and scanning emails attachments before downloading them [163]. In the healthcare industry, Brady [164] stated the importance of employees computer self-efficacy toward HIPPA security compliance, defining self-efficacy as "individual judgment of one's capability to safeguard and protect patient information privacy" [165].

2.5 Neutralisation Theory

This section will describe the origin of neutralisation theory and its applications in criminology, digital, and information security. Also, it will discuss the results of several studies that

specifically relate to the tendency of individuals to justify violations of information security policies. The final section will provide approaches to combating neutralisation techniques in the context of information security.

2.5.1 Neutralisation Techniques in Criminology

In 1955, E. H. Sutherland [166] introduced a theory of differential association, asserting that two factors influenced an individual to become delinquent: (1) discovering suitable methods to conduct the crime and (2) attitudes in favour of violating the law. Sutherland discussed rationalisations as a part of the attitudes that motivated breaking the law. Building upon this concept, in 1957, the concept of Techniques of Neutralisation was introduced by Sykes and Matza [34] in the criminology field to explain the deviant behaviour of juveniles. Deviant behaviour is any action that conflicts with social norms as expressed either explicitly through policies, rules, regulations, laws or implicitly through shared group values [167]. Rogers and Buffalo [35] then defined neutralisation techniques as "a method whereby an individual renders behavioural norms inoperative, thereby freeing himself to engage in behaviour which would otherwise be considered deviant." These neutralisation techniques help the offender balance and negate the impact of shame or guilt and make it possible for an offender to commit non-compliant behaviour without self-blaming.

When an individual engages in an act that violates common and known social norms of a group or community, they tend to adopt neutralisation techniques to decrease or avoid negative feelings such as guilt or shame and undesirable consequences such as punishment by justifying the violation of the rule in question [168][169]. Sykes and Matza [34] argued that techniques of neutralisation are "critical in lessening the effectiveness of social controls and that they lie behind a large share of delinquent behaviour." However, the sequence of neutralisation techniques became controversial in the field of criminology as it was difficult to define which came first—the neutralisation or the crime—a classic "chicken or egg" dilemma [170]. Sykes and Matza [34] believed that juveniles prepared themselves by learning these neutralisation techniques before committing delinquency or violating social control. In particular, they suggested that these justifications precede the delinquent act and thus make the behaviour possible [34][170]. In contrast, other scholars asserted that these techniques were "ex post facto rationalisations" after the fact of the act to rationalise undesirable action or behaviour. Individuals used these techniques as a protection mechanism to preserve their self-image or safeguard themselves from the blame of others [171][172][37].

In their original work, Sykes and Matza [58] proposed five neutralisation or rationalisation techniques that juvenile criminals may use to explain their deviant behaviour as follows.

- **The denial of responsibility:** The major principle of this technique is that the offender refuses to accept blame for the deviant behaviour and redirects responsibility for the action in question to an alternative source. Here, the offender may claim that the deviant behaviour occurred due to an accident or lack of control. An individual might say, “I didn’t mean to do it” or “It was an accident” [34].
- **The Denial of Injury**: The offender argues that the result of the deviant action would be harmless, and thus no one would get hurt by the behaviour. An individual might say, “I was only ‘borrowing’ the money and had every intention of paying it back” or “No harm is done” [34].
- **The denial of a victim:** The offender claims that the injury that would result from the wrong action is a kind of rightful punishment or retaliation since the victim deserved the consequences of the action [34]. For instance, someone might say, “He started it” or “She had it coming to her.”
- **The condemnation of the condemner:** In this technique, the offender tends to develop “a rejection of the rejectors” and shifts the focus of attention from his own deviant acts to the motives and behaviour of those who disapprove of his violations. Like saying, “You have no right to stand in judgment of me” or “The entire system is corrupt” [34].
- **The appeal to higher loyalty**: Offenders use this neutralisation technique to escape a dilemma that forces them to choose between conforming with small group interests such as friends or family members or violating a law. Like saying, “I would never snitch on my friends” or “I did it for my family” [34].

  Later, criminology scientists like Klockars [36] introduced the Metaphor of the Ledger:

- **The metaphor of the ledger**: The offender argues that their previous good acts and compliance recompense occasional wrongdoing behaviour [51]. An individual might say, “Yes, I acted unlawfully, but I have done a lot of charitable work in my community over the years”, or “I’m a good person; this isn’t a reflection of my character.”

  Next, Minor [37] introduced Defence of Necessity as an extension to Sykes and Matza’s [58] theory:

- **Defence of necessity:** Here, the offender argues that nobody should feel shame or guilt if the situation requires an act that can result in breaking the rules [38]. An individual might say, “I had no other choice” or “I needed the money to provide for my family” [37].

Further applications of Sykes and Matza’s original work have identified additional neutralisation techniques that support the effort to explain different types of crimes and deviant behaviours; these include the “Claim of Normalcy,” the “Claim of Relative Acceptability,” the “Claim of Entitlement,” [38] “Justification by Postponement,” “Justification by Comparison,” [172], the “Claim of Individuality,” and the “Denial of Negative Intent” [173]. (See Appendix 2. for more details of neutralisation techniques and examples.)

Neutralisation theory became the basis for various studies in the criminology and sociology fields to investigate juvenile delinquency, providing the theoretical framework to study a wide range of criminal and deviant behaviours such as hate crimes [174], car theft [175], white-collar deviance [176], political corruption [177], dogfighting [178], and terrorism [179]. Finally, several information security scholars found neutralisation theory suitable for predicting and explaining various undesirable behaviours in the information security and cybercrime realm. The following section explains several implications of the neutralisation theory to explore its influence on individuals to justify theirto apply undesirable behaviour in the digital and information security context.

2.5.2 Neutralisation Theory in the IT and IS Context

Neutralisation theory has provided a theoretical explanation to investigate deviant behaviour such as computer abuse [14], cyber-loafing [15], digital piracy [16], IT shadow security [151], software piracy [180], digital and music piracy [181][182], and hacking [183]. Willison and Warkentin [17] suggested that neutralisation theory could be used to explore employees’ undesirable behaviour within organisations, arguing that the employee might evoke neutralisation techniques to offset feelings of guilt or shame when they intend to break organisational rules.

Many scholars have explored the impact of neutralisation theory on such cyber crimes as digital piracy, software piracy, and music piracy with differing results. Morris and Higgins [181] examined digital piracy as an illegal behaviour using several theories from the criminology field. Using retrospective (self-reported) and prospective (willingness to engage) models, authors explored the role of neutralisation techniques from well-known criminology theories such as Self-Control (SC), social learning (SL), and micro anomie (strain). Using a sample of

585 undergraduate students from two universities, they found that techniques of neutralisation had a positive and direct effect on students' willingness to participate in illegal downloading of music CDs over video piracy. From the retrospective model point of view, the role of neutralisation had a modest effect on music and video piracy over software piracy. Therefore, it can be considered as a theoretical predictor of a student's potential digital piracy.

Likewise, Siponen et al. [180] conducted a study to identify which neutralisation techniques could contribute more to individuals' software piracy intentions in the presence of deterrence mechanisms. The study tested the direct influence of seven neutralisation techniques on individuals' intention to commit software piracy: (1) condemn the condemner, (2) denial of injury, (3) metaphor of the ledger, (4) appeal to higher loyalties, (5) defence of necessity, (6) denial of responsibility, and (7) denial of the victim. Also, the authors tested the effectiveness of formal deterrence, shame, and moral beliefs against the adoption of neutralisation techniques. Moral belief refers to the degree that individuals evaluate software piracy as morally right or wrong. The empirical results of a questionnaire administered to 183 graduate students from a European business school revealed that two neutralisation techniques—appeal to higher loyalties and condemn the condemners—had the most direct impact and significantly predicted software piracy intention. Also, shame and moral beliefs had a strong negative effect on an individual's intention to pirate software. Consequently, the study suggested that software organisations need to design their anti-piracy awareness and education campaigns or other behavioural interventions to mitigate the appeal to higher loyalties and condemn the condemners. Also, the study encouraged organisations not to rely on formal sanctions but instead should consider incorporating informal sanctions such as shame and moral beliefs in their deterrence effort.

These findings were consistent with Ingram's [182] quantitative study, which empirically investigated the impact of neutralisation techniques on online music piracy in a sample of 2,032 undergraduate students in several US universities. The study found that denial of responsibility, denial of injury, denial of victim, and appeal to higher loyalties were significant in predicting a student's potential willingness to copy online music. In contrast, Hinduja [184] collected data via a questionnaire of 433 undergraduate students at a large university in the United States. The central premise was that those "university students who engage in online software piracy utilise at least one or more techniques of neutralisation." The results showed that there was generally a weak relationship between online software piracy and the role of neutralisation techniques to form such intentions.

However, in their seminal work, Siponen and Vance [53] conducted the first empirical study that employed neutralisation theory in the information security context and highlighted the essential role of the theory as a predictor of an individual's non-compliance intentions toward information security policies. Siponen and Vance [1] argued that neutralisation techniques could explain the intention to violate information security policies. The study proposed a theoretical model to assess the impact of formal and informal sanctions and shame on employee violation intentions and the effects of techniques of neutralisation to rationalise such behaviour. The model conceptualized neutralisation as a multidimensional second-order construct consisting of six sub-constructs: (1) defence of necessity, (2) appeal to higher loyalties, (3) condemn the condemners, (4) the metaphor of the ledger, (5) denial of injury, and (6) denial of responsibility.

Siponen and Vance [1] collected data from a sample of 1449 employees in administrative positions in three organisations located in Finland. The findings revealed that organisational sanctions alone were insufficient to decrease or prevent information policies violation intentions since the employees tended to justify violations using neutralisation techniques to minimise the perceived harm of formal and informal sanctions. Based on these findings, the authors asserted the importance of neutralisation to explain and predict InfoSec policies non-compliance. Also, they suggested that organisations need to consider the significant role of neutralisation techniques in their efforts to develop, implement, and promote information security policies and practices. Similarly, an empirical study in Malaysia by Teh et al. [31] found that neutralisation theory offers a significant predictor of an individual's intention to violate information security policies. In contrast, Silic et al. [151] found that only a single neutralisation component, the metaphor of the ledger, directly and significantly affected employees' intention toward violating shadow IT policies.

The study by Teh et al. [31] mentioned above aimed to investigate the organisational factors that motivate employees to adopt neutralisation techniques and violate information security policies. Their theoretical model used the concepts of role conflict and role ambiguity from the security literature and the concepts of job satisfaction and organisational commitment drawn from social exchange theory. A total sample of 246 employees working in nine Malaysian banks participated in this quantitative study. The results showed that role conflict significantly influenced neutralisation techniques in the InfoSec policies violations context. Teh et al. [31]

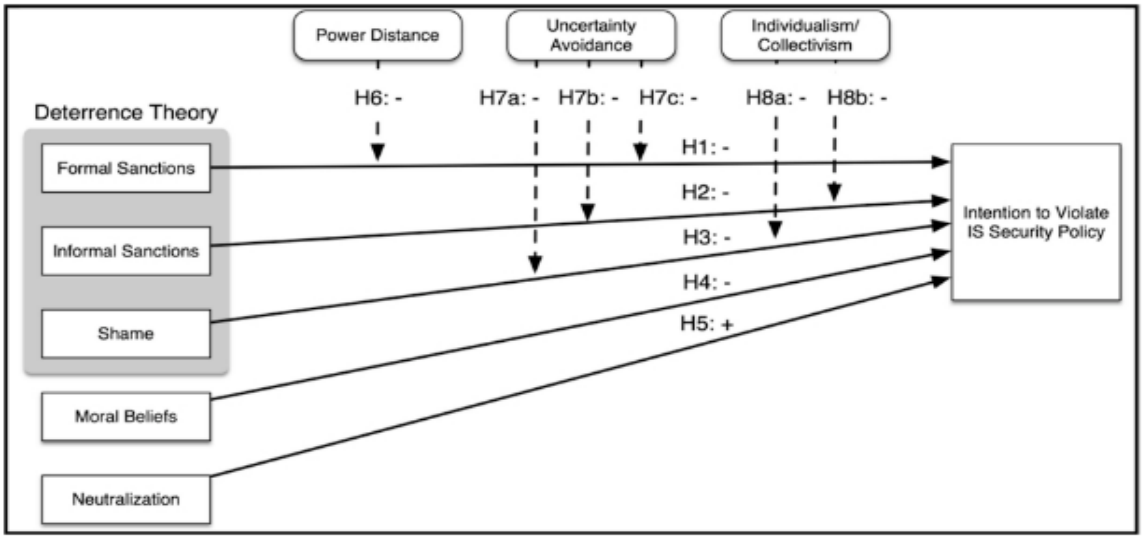


Figure 2.5 Vance et al. [180] Research Model

explained the relationship between role conflict and neutralisation techniques by asserting that "when employees are faced with competing demands in the workplace that expend their time and presumably deplete their cognitive resources (in the form of role conflict), they appear more prone towards rationalisations of information security violations." They also provided evidence that organisational commitment was negatively and indirectly associated with the employee tendency to neutralise non-compliance.

In contrast, job satisfaction and role ambiguity had an insignificant impact on neutralisation techniques toward employee propensity to justify information security policy violation; the authors link this finding to the influence of Malaysians' high power distance national culture. Therefore, Teh et al. [31] emphasised a potential relationship between national culture and the tendency of individuals to evoke neutralisation techniques. Consequently, they suggested that future research could study the influence of Hofstede's theory of cultural dimensions [68]—and specifically power distance—on individuals' justifications in the context of information security compliance. To address the influence of cultural differences on individuals' tendency to adopt neutralisation techniques and violate information security policies, a recent study by Vance et al. [185] examined such a relationship via a theoretical model to test the influence of the deterrence theory, neutralisation techniques, shame, and moral belief on an individual's intention to violate information security policies. The authors incorporated three of Hofstede's cultural dimensions, power distance, uncertainty avoidance, and individualism/collectivism—as moderators of the relationships, as shown in Figure 2.5.

According to Hofstede [186], power distance refers to "the extent to which the less powerful members of organisations and institutions accept and expect that power is distributed unequally." Uncertainty avoidance is "the degree to which members of a society feel

uncomfortable with uncertainty and ambiguity." The difference between individualism and collectivism depends on the individual's perception of themselves and how they distinguish between their interests, values, thoughts, emotions, and behaviour from their larger group. The individualist has more independence regarding their thoughts and beliefs and feels less related to the typical behaviour of the larger group, while collectivists, in contrast, "view themselves as dependent on a larger group and place a high priority on the needs and welfare of the whole above their individual needs and desires" [185]. This quantitative study collected data from a global company and received a total sample of 618 respondents from 48 nationalities. The findings showed that the impact of neutralisation techniques, moral beliefs, and shame was significant on individual intention to violate InfoSec policies. Thus, it implied that the effect of those three factors on individuals' intent remained significant across different cultures and that the model's cultural dimensions (power distance, uncertainty avoidance, and individualism/collectivism) did not moderate the relationship. In contrast, formal and informal sanctions were insignificant. The exception was that individuals from a collectivistic society such as those found in Asia were more affected by informal sanctions. In contrast, formal sanction was insignificant to mitigate individuals tendency to violate InfoSec policies across all nationalities.

Another empirical study by Silic et al. [151] was aimed to gain a better understanding of shadow IT usage through the lens of neutralisation theory. According to the authors, shadow IT involves the use of IT tools, software, services, or systems in a workplace without formal permission from the IT department. The study examined the role of neutralisation techniques, shame, and deterrence mechanisms (formal and informal sanctions) on both intention and actual behaviour. According to the study, shame mediated the relationship between neutralisation techniques and formal and informal sanctions toward an individual's intent to use shadow IT and thus violate organisation policy. They tested the indirect effect of six neutralisation techniques on intention to use shadow IT via shame as a theoretical mediator. Further, they measured the direct effect of these neutralisation techniques on the actual use of shadow IT and finally tested the direct and indirect influence of formal and informal sanctions on individual intention to use unauthorised software.

The respondents of the questionnaire used in the study were 440 managers in all levels from various departments such as marketing, finance, and administration in four European organisations. The findings revealed that only the metaphor of the ledger had a direct positive and significant influence on the intention of the managers to use shadow IT. Also, formal and

informal sanctions were insignificant to discourage employee intention to use unauthorised software. Silic et al. [151] pointed out that "neutralisation techniques and deterrence techniques are both related to the levels of shame that employees perceive when violating a security policy such as using Shadow IT." The practical implications of the study by Silic et al. [151] would help organisations reduce the security threats of shadow IT usage by designing and implementing more effective security awareness and educational sessions that consider discouraging employees from justifying their use of unauthorised software through the metaphor of the ledger.

A further empirical study by Kim et al. [187] proposed an integrative behavioural model based upon three factors drawn from the theory of planned behaviour (attitude, normative belief, and self-efficacy) and response efficacy derived from protraction motivation theory. In addition, they incorporated three aspects of rational choice theory (benefit of compliance, cost of compliance, and cost of non-compliance). Neutralisation theory was conceptualised in the model as a multidimensional second-order construct as advised by Siponen and Vance [1]. The goal was to understand the behavioural factors that affected the employees' attitudes and their actions toward compliance with information security policies. The authors disseminated a survey to 32 companies in South Korea and collected data from a sample of 194 respondents. The results showed that response-efficacy and normative belief positively impacted employees' intention to comply with their organisations' security policies. In the study context, response-efficacy referred to the degree to which an individual's confidence in the effectiveness of the information security policies can adequately protect the organisation's IT assets from security threats. Also, normative belief definition is "the degree of perceptive social pressure of neighbours such as the supervisor, colleague, and manager when they comply with the policy" [187]. In contrast, neutralisation techniques significantly weaken an employee's intent towards compliance with information security policies. Thus, Kim et al. [69] concluded that organisations need to take the impact of individuals' neutralisation into account when designing their security awareness and education programs.

In summary, this section revealed the following: (1) Neutralisation techniques are significant predictors of an individual's intention to violate information security policies. (2) The existence of neutralisation techniques overcomes the effect of formal and informal deterrence, and thus any future application of deterrence mechanisms in organisations must take into account the impact of neutralisation techniques on the behaviour of individuals. (3) Shame and moral beliefs are strong predictors and can negatively impact intention to commit deviant behaviour

such as violating InfoSec policies. However, the impact of these two factors can differ between national cultures. (4) Most information security scholars emphasised the importance of designing security awareness and education programs to counter individuals' neutralisation intention to violate InfoSec policies, thus improving behavioural compliance. The following section discusses the efforts of information security scholars to develop security awareness programs to mitigate the influence of neutralisation techniques in the IS context.

2.5.3 Counter Neutralisation Approaches in Information Security

In recent years there has been growing interest to counter the influence of neutralisation techniques on individuals' non-compliant behaviour with information security policies. Research in information security behaviour has addressed individual justifications to circumvent the security policies requirements as critical information and to consider such behaviour as a serious insider security threat [62][110][154][185]. However, none of these studies endeavoured to change the intent of individuals to act securely nor to find ways to change behaviour from violation to compliance through the lens of neutralisation theory. According to Siponen et al. [188], the majority of studies only reported on the importance of investigating the context relevant to insecure behaviour and not on finding possible behavioural or technical approaches to change such insecure behaviour.

The studies mentioned earlier [62][110][154][185] encouraged organisations to design behavioural interventions to mitigate the effect of neutralisation techniques rather than rely on the traditional enforcement approach of implementing formal and informal sanctions. These scholarly studies did recommend mitigation interventions to minimise the influence of neutralisation techniques on information security non-compliance behaviour by advising organisations to carefully tailor their information security policies and education programs to consider the role of neutralisation techniques. Siponen et al. [1] stated that "policy awareness campaigns and educational sessions on neutralisation need to be examined to identify effective means of inhibiting the use of neutralisation techniques and thus improve IS security policy compliance."

Information security awareness programs aim to enhance positive and secure individual behaviours [150]. "Information security awareness" is defined as "a state where users in an organization are aware of [and] ideally committed [to] their security mission." Thus, increased individual security awareness should lead to better use of IT assets [189]. But the rapid innovation of technologies, cyber threats, and vulnerabilities have made the security awareness

process continuous and challenging [190]. Employees repeatedly fail to act according to InfoSec policies requirements, thus, reinforcing the perception of experts that non-compliance behaviour with InfoSec policies is a critical risk and a primary source of security incidents [132]. Therefore, it is necessary to improve employees' compliance in organisations by educating employees and increasing their knowledge of security policies, secure practices, and emerging security threats. Organisations can use structured and unstructured Security Education, Training, and Awareness (SETA) programs to obtain their security awareness goals [191]. Structured awareness is an intervention that continuously educates individuals about the most recent security information via the Intranet, posters, text messages, face-to-face classes, and e-learning methods. In comparison, unstructured awareness interventions warn individuals about security threats and vulnerabilities by conveying the necessary contents of security controls, practices, and policies [191].

Only a few information security scholars have conducted studies seeking to mitigate the effect of neutralisation techniques as a predictor of information security non-compliance intentions. According to Siponen et al. [192], neutralisation theory was primarily used as a theoretical basis for exploring behavioural intent but without any attempt at altering that behaviour. Consequently, they emphasised the importance of finding effective ways to improve individual compliance with information security policies and proposed a security awareness program that discourages individuals from adopting neutralisation techniques as a practical approach [192]. In the information security literature, a handful of information security scholars have conducted empirical studies to mitigate the effect of neutralisation techniques on behavioural non-compliance with information security policies by developing either information security awareness materials or security awareness education and training programs. For instance, Barlow et al. [125][112] conducted SETA program that aimed to deliver security awareness messages to inhibit individuals from using neutralisation techniques to violate password policy. Also, Siponen et al. [192] conducted a field experiment and developed a security educational training program to counter neutralisation and thus improve compliance with password policy.

In 2013, Barlow et al. [125] designed an IT security awareness and communication program that focused on how deterrence and neutralisation messages could alter an individual's InfoSec violation intentions. The study aimed to reduce password policy violations by concentrating on a communication security program that framed particular messages to expand the deterrence effect and counter neutralisation techniques. The program designed by Barlow et al. [125] used a sample of 257 US employees to explore the relationship of three commonly used

neutralisation techniques—(1) denial of injury, (2) defence of necessity, and (3) the metaphor of the ledger—to password policy breaches. The study revealed that the intention of employees to justify password violation was more significant when the respondents' received questions related to the defence of necessity scenario, suggesting that violation of password security policies would be acceptable if those involved felt it served a good cause. In contrast, the metaphor of the ledger and denial of injury had only a marginal association with an intent to justify non-compliance with password policies. The study found no statistical difference between using security awareness communication messages focused on mitigating neutralisation techniques and sanctions, implying that a security awareness communication approach that aimed to dissuade employees from adopting neutralisation techniques was a practical approach to alleviate password sharing.

In 2018, Barlow et al. [112] extended their earlier work and conducted a SETA program based on the persuasive communication concept for security training. They developed a theoretical model to test the impact of persuasive communication on rationalising password policy violation by examining the influence of three SETA communication approaches (1) normative, (2) information, and (3) anti-neutralisation. The authors argued that employing these communication approaches in the SETA program could improve individual compliance with the password policy. In the context of this study, informational communication design referred to providing individuals with useful information that explained why compliance with the password policy is essential, which allowed participants in their study to evaluate password policy compliance costs and benefits. Also, normative communication design aimed to convey why other colleagues complied with the password policy and showed compliance with the password policy was a typical norm among other colleagues. Anti-neutralisation communication design described why rationalisation of password sharing via a denial of injury or defence of necessity was unacceptable. Data were collected through the Factorial Survey Method (FSM), and the sample consisted of 200 respondents recruited via Qualtrics, an online service firm.

The study found that an organisation can reinforce password policy compliance when designing a security awareness program that effectively communicates anti-neutralisation informational messages to employees. Thus, the findings revealed that anti-neutralisation communication—essentially a short statement that counters denial of injury or defence of necessity—had a significant influence on decreasing the intention of respondents to share their passwords. The authors reported that "Reinforcing communication that states that

neutralisation is unacceptable effectively combats rationalizations that lead to deviant behaviour, whether rationalizations are explicitly triggered by the communication or spontaneously invoked by the users."

Also, solid informational communication can lower an individual's intention to violate the password policy; thus, providing informational statements that explain the cost and benefits of compliance directly can improve an individual's ability to make a more rational decision aligned with password policy requirements. Finally, according to Barlow et al. [112], normative statements were less effective for reducing the intent of individuals to share the passwords. They stated that it was difficult to persuade individuals in some situations not to share a password if they found it possible to justify sharing in a particular cause. In such cases, the existence of neutralisation techniques overcame the effect of normative communication to reinforce compliance.

While the studies by Barlow et al.[112] [125]offered one-way communication approaches that utilised persuasive messages to counter neutralisation techniques; a recent quasi-experimental study by Siponen et al. [192] investigated whether security awareness and education programs can reduce behavioural justifications and improve password policy compliance. The proposed educational training intervention was based on a two-way (face-to-face) communication design that adopted the cognitive dissonance theory concept to counter the tendency to justify password policy violation. The authors argued that "not just any educational training intervention or message framing would change the minds of those using neutralisations." Thus, they asserted the need to find strategies or tactics to change behavioural justifications that could transform InfoSec violation behaviour to compliance.

Following the assumptions of Sykes and Matza [34] that placing a juvenile in certain circumstances could produce a feeling of guilt or a negative self-image and thus dissuade deviant behaviour, Siponen et al. [192] speculated that by placing the participant in a situation that leads to feelings of guilt, shame, or negative self-image through cognitive dissonance might discourage the tendency to neutralise non-compliance with the password policy. According to Festinger [83], the fundamental concept of cognitive dissonance theory was that people feel discomfort when there is a contradiction between their true actions (their behaviour) and their cognitions such as beliefs, ideas, and values. To overcome discomfort caused by dissonance, people tend to modify either one or more mental cognitions or their behaviour to restore a state of comfort and harmony.

The study by Siponen et al. [192] was conducted in a multinational company in the United Arab Emirates (UAE) and involved 98 participants, 66 of whom were randomly assigned to the experimental group, while the rest constituted the control group. Both groups received similar security educational training materials and sessions that emphasised the importance of company password policy requirements and explained the principles of robust passwords. The experimental group then received lectures that aimed to "address learners' use of neutralisation techniques explicitly by creating dissonance between individuals' prevailing ideas on password security and proper use of strong passwords." In addition to presenting counter-arguments to mitigate commonly used neutralisation techniques. The training used mnemonics to counter each of the neutralisation techniques by showing how it was possible to create a solid and easy password. Thus, creating dissonance between employees' concerns that complying with the password policy required a complex and challenging password. At the same time, a simple process using mnemonics made it an easy method to develop passwords that were easy to remember but difficult for hackers to predict.

The key finding of this study was that the educational training based on the application of cognitive theory could counter neutralisation techniques and effectively improve the employee compliance intention to use a secure and robust password. This implied that organisations need to strengthen their SETA program by explaining why neutralisation techniques contradict the requirements of security policies. Therefore, it was essential to include several counterarguments for neutralisation techniques that individuals might adopt to violate the security policies.

2.6 Summary of The Literature Review

This chapter aims to provide a comprehensive overview of the role of information security policies in protecting information and IT assets in organisations. In particular, this literature review clarified why an individual's behavioural noncompliance is a serious internal threat facing organisations—specifically in the healthcare industry—and outlined the high cost of information security violations to both organisations and individuals. However, many researchers found inconsistent and contradictory results regarding the efficacy of formal and informal sanctions to enforce information security compliance. They stated that deterrence mechanisms are not always the best countermeasure to mitigate information security policy violations, although the application of severe penalties has been partially successful in changing individual behavioural intentions toward compliance, particularly in the presence of neutralisation techniques.

As the field of criminology has shown, individuals sometimes tend to neutralise their unwanted behaviour to overcome feelings of guilt or shame. In the information security literature, many security scholars have investigated information security policy violations under the lens of neutralisation techniques and found it an excellent indicator of insider threats. However, most of these studies have looked at different types of cybercrime—digital piracy, music piracy, shadow security, and information security policy violation—and collected data from university students or employees working in managerial positions. Nevertheless, in the healthcare industry, no current studies explore the role of neutralisation theory in predicting medical practitioners' intention to violate information security policies and the impact of their justifications on patient privacy. This gap will be addressed in chapter four, which presents a quantitative study that collected data from medical interns in several academic hospitals in Saudi Arabia. Finally, the existing literature has made only a limited attempt to understand in-depth the drivers behind individual propensity to evoke neutralisation techniques and violate information security policies. Chapter five addresses this problem via a set of interviews with medical interns and IT department employees in one of the biggest hospitals in Saudi Arabia.

This chapter shows that only a few attempts in the IS literature have been made to mitigate the effect of neutralisation techniques. The majority of the current interventions to discourage individuals from adopting neutralisation techniques and violate information security policies were based on the development of SETA programs. These security awareness programmes address the individual justifications by anti-neutralisation awareness communication [80][69] or via security training that employed cognitive concepts to counter individual intention for non-compliance. Thus, there was little attention to improving information security policies by finding a methodological way to balance the work needs of employees and the security policy requirements rather than the interventions that aim to change individual behaviour. We address this gap in chapters six and seven by utilising the concept of a collaborative wiring process of security policies to increase individual engagement and create user-centred policies that, in return, can enhance the employee intention to comply with the security policies.

Chapter 3 : Research Design and Methodology

Research methods are systematic plans used to conduct research[193]. This thesis will use a variety of research methodologies, including qualitative and quantitative methods. The quantitative approach will attempt to categorise and count characteristics and will enable the researcher to develop a statistical model to test the hypothesis and explain the observed data[1]. Additionally, this thesis will use qualitative methods to conduct a thorough observation of both circumstances and events. Thus, this chapter will review the researcher's different research methods. The chapter will be divided into several sections. Section 3.1 will introduce an overview of the research methodology. The next section, which is 3.2, will present an introduction to a mixed-methods research approach. A rationale for the research design will be introduced in Section 3.3. Selected research methods and techniques will be covered in sections 3.3.1 to 3.3.5. Sub-sections 3.3.1 to 3.3.5 will illustrate selected research methods, which are questionnaires and interviews, action research, focus groups and content analysis, respectively. Section 3.3.3.1 will address thematic analysis. Focus groups will be introduced in section 3.3.4. Content analysis will be highlighted in 3.3.6, and the collaborative writing process explained in section 3.3.6.2. Lastly, Section 3.5 presents a summary of the chapter.

3.1 Overview of The Research Methodology

This research is divided into four phases (as shown in Table 3.1), with the overriding objective to investigate the role of neutralisation techniques on individual behavioural non-compliance. Below is a brief description of each phase regarding it related research question, purpose, data collection method and data analysis:

Table 3.1 Integration of Research Questions, purposes, and Mixed Methods Research Design and Analysis

Research question and purpose (Chapter 4/Phase1)	**Research Design (Methods and Analysis)**
Research Question1 (RQ1): What is the association between neutralisation techniques and the intention of medical interns to violate InfoSec policies? **Purpose:** Determine the role of Neutralisation techniques to predict medical practitioner intention to violate InfoSec policies.	**A quantitative study**: tests and validates a theoretical model based on neutralisation techniques to test whether the is a positive effect on the medical interns' intention to violate the information security policies. **Data collection method**: A closed-ended questionnaire. **Study Sample:** 66 completed questionnaires from medical interns within four universities in Saudi Arabia. **Analysis**: In the test of theoretical model and hypotheses, we applied Structural Equation Modelling (SEM) using the partial least square (PLS) technique.
Research question and purpose (Chapter 5/Phase2)	**Research Design (Methods and Analysis)**
Research Question2 (RQ2): What drives behavioural justification among medical practitioners to violate information security policies in healthcare organisations*?* **Purpose:** Investigate the motivations of medical practitioners to evoke neutralisation techniques to justify InfoSec violations.	**A qualitative study:** It was conducted in one of the biggest hospitals in Saudi Arabia to determine the contextual factors that influence the MI to adopt neutralisation techniques and violate the information security policies. **Data collection:** a series of semi-structured interviews. **Study sample:** twenty medical interns and eight employees from the I.T. department (total N=28 participants). **Analysis:** we adopted Braun and Clarke's [194] thematic analysis to generate themes and codes from the textual interview transcripts.
Research question and purpose (Chapter 6/Phase 3)	**Research Design (Methods and Analysis)**
Research Question 3 (RQ3): To what extent does the engagement of the perception of end user during information security policy development via a collaborative writing process increase the effectiveness of the InfoSec policies to mitigate the role of neutralisation techniques **Purpose:** Enhance InfoSec policies effectiveness against neutralisation techniques via the engagement end-user perception. The UK.	**A qualitative study:** This study aimed to explore the proposed intervention by redesigning information security policies (password policy) to reduce individuals' inclination to justify information security policies. **Data collection method:** we used a mixed-method approach to collect data in this phase that included a quantitative part (pre- and post-assessment questionnaire) and a qualitative part (a focus group to conduct a collaborative writing process of a security policy). **Study Sample:** 24 graduate students were divided into six groups at the University of Glasgow, the U.K. **Data Analysis:** ***Statistical****:* We used Medians variation and a non-parametric statistical hypothesis test via the Wilcoxon signed-rank test to analyse the pre and post assessment questionnaire for the quantitative part in this phase.

	Qualitative: We used the content analysis using Krippendorff [195] six-step procedure to analyse the qualitative part (the document resulted from the collaborative writing process) in this phase.
Research question and purpose (Chapter 7/Phase 4)	**Research Design (Methods and Analysis)**
Research Question 3 (RQ3): To what extent does the engagement of the perception of end user during information security policy development via a collaborative writing process increase the effectiveness of the InfoSec policies to mitigate the role of neutralisation techniques	**Qualitative study:** This study aimed to explore the proposed intervention by redesigning information security policies (password policy) to reduce individuals' inclination to justify information security policies. **Data collection method:** we used a mixed-method approach to collect data in this phase that included a quantitative part (pre- and post-assessment questionnaire) and a qualitative part (a focus group to conduct collaborative writing process of a security policy). **Study Sample:** 42 medical interns formed ten groups at one of the biggest hospitals in Saudi Arabia. **Data Analysis:** ***Statistical****:* We used Median's variation and a non-parametric statistical hypothesis test via the Wilcoxon signed-rank test to analyse the pre and post-assessment questionnaire for the quantitative part in this phase. ***Qualitative****:* We used Content analysis using Krippendorff [195] six steps procedure to analyse the qualitative part (the document resulted from the collaborative writing process) in this phase.
Purpose: Enhance InfoSec policies effectiveness against neutralisation techniques via the engagement end-user perception. Saudi Arabia.	

3.2 Introduction To Mix Methods Research Approaches

Several discipline fields of sociology, psychology, education advocate the case for the merging of quantitative and qualitative research methodologies. A distinguishing aspect of mixed methods research is its methodological diversity, which usually leads to research with broader views than monomethod approaches. The primary goal and core premise of mixed methods research is that combining quantitative and qualitative approaches yields more knowledge of study challenges and complicated phenomena than each methodology alone. Johnson and Onwuegbuzie [196] defined the mixed methods research approach as "the type of research in which a researcher or team of researchers combines elements of qualitative and quantitative research approaches (e.g., use of qualitative and quantitative viewpoints, data collection, analysis, inference techniques) for the broad purposes of breadth and depth of understanding and corroboration" [196]. Thus, to understand the mixed method, we need to comprehend the two main pillars, the quantitative and qualitative research approaches.

- **Quantitative Research:**

According to Zyphur[197], quantitative research is an approach that systematically investigates a phenomenon during which quantifiable data is gathered and statistical analysis is conducted [197]. After the data is collected, mathematical and computational techniques are used to analyse that data. Generally, quantifiable research is linked with the positivistic model and entails collecting and converting raw data into a mathematical arrangement for statistical calculations needed to draw explanations and conclusions[197]. Quantitative research uses deductive reasoning that moves from the general to the specific, and it is also known as the "top-down" approach. As illustrated by Howe [198], the conclusions drawn from a quantitative study are dependent on one or more statements or findings. In quantitative methods, the researchers have either one or more hypotheses, and these hypotheses are questions that will be addressed [197]. They include predictions about relationships between variables. To find the answers, the researcher utilises different instruments such as statistical tests.

In quantitative research, information is gathered from the existing sample using various techniques such as sampling [193]. Online surveys, polls and questionnaires are also utilised in retrieving the data. The results are then numerically depicted and used to analyse a particular phenomenon. A structured method is applied to gather data from a particular group representative of the views of the population at large. Primary and secondary quantitative research methods are some of the various techniques that are used to carry out quantitative research.

Primary quantitative research can be used in a wide variety of areas, and one of the essential aspects of primary research is that the researcher aims to conduct a new study to address a particular issue. Thus, a primary quantitative research design is flexible, which means that the researcher can use a variety of techniques the researcher needs to collect and analyse data directly instead of utilising previous research results. However, in secondary quantitative research, the researcher utilises existing data from previous primary research or other reliable sources such as government records, organisations reports, etc. Secondary research assists in validating data gathered through primary quantitative research and in improving or disproving previously collected data. The following sections will demonstrate four primary quantitative research methods: Survey research, Correlational research, Causal-comparative research, and Experimental research.

Survey research, the nature of the study dictates the type of primary quantitative research that will be conducted [1]. The most fundamental technique utilised in quantitative analysis in

survey research. Additionally, online polls, questionnaires and surveys are used to obtain data from respondents [3]. In general, survey research enables a researcher to ask relevant survey questions and collect data directly from respondents, which can then be analysed numerically. The prerequisite of survey research is that the study sample should be comprised of randomly selected members.

Correlational research. This type of quantitative research is conducted to determine the relationship that exists between two entities[199]. It is a method of conducting research that is used to generate value for naturally occurring relationships. Of course, to meet the threshold, a minimum of two groups is required to perform this kind of research. Normally, scholars use a correlation research strategy to assess two or more variables using statistical analysis. Jokela [199] asserts that a researcher manipulates an independent variable to generate the desired outcome. For that reason, it is not always possible to make conclusions based on correlational research.

In Causal-comparative research, Vance [200] defines this approach as a research method used to establish the cause-effect relationship among different variables, and it is mainly used to perform a comparison. Vance [200] suggests that, in this type of research, one of the variables is always dependent while the other one is independent. According to Vance[200], the causal-comparative technique is not dependent on the statistical analysis of two variables. Instead, it examines how variables change when factors in the research change. It is a research method that is conducted irrespective of the relationship between variables[201].

Experimental research. This type of research relies on one or more theories to deduce a conclusion [202]. In experimental research, an investigation is conducted to accept or reject a theory or assumption. According to Libby et al.[203], an essential aspect of experimental studies is that its ability to integrate multidisciplinary theories to test a phenomenon. Thus, it can help the researcher to disentangle the impact of variables confounded in natural settings and ascertain the conditions and processes under which specific phenomena occurs. Also, it provides the researcher with the capacity to create a unique research environment in which a causal theory of events can be tested with the greatest possible internal validity[203].

- **Qualitative Research**

Qualitative study is presumed to be a research approach associated with the interpretivism paradigm[204]. It endeavours to discover the more profound meaning and significance of human behaviour and investigate influential factors that influence behaviour, such as

contradictory beliefs and emotions. Researchers intend to gain a rich and complex understanding of people's experiences. Subsequently, the qualitative approach involves acquiring information through human communication and interaction. It explains what and why people have a certain perspective or opinion concerning a particular phenomenon. Unlike the quantitative method, it focuses on non-numerical data. Qualitative researchers have adopted various techniques of retrieving qualitative data. The researchers tend to use an inductive technique, "a bottom-up" approach," to develop a theory based on the collected data. Still, most research uses deductive reasoning. Qualitative researchers do not argue based on pre-determined hypotheses[204]. Instead, they identify a problem and use an overarching theory to create a space for their investigations.

The data in a qualitative study is retrieved in textual form through interactions with the participants[205]. Data collection is accomplished in several stages, and the researcher may drop or add questions mid-way through the study. Qualitative research is conducted on a smaller number of subjects than is characteristic of quantitative research, and it is mainly a function of methods used, which are labour-intensive. The small sample size involved in a qualitative study has a great degree of flexibility[206], and a small sample size doesn't make the research "less scientific." Commonly used methods include observations, interviews, focus groups, and informal surveys. According to Asenahabi[207], the qualitative research designs can be classified into six types; (1) case study research, (2) narrative research, (3) phenomenological research, (4) grounded theory research, (5) ethnography research, and (6) action research.

Several data collection methods are used for qualitative research. The first and popular method used to collect data in a qualitative study is conducted through interviews [208]. This method involves a one-on-one conversation between the researcher and the subject, and each respondent is interviewed individually and privately to give them a platform to express themselves safely and, often, in great detail. While using this conversational method, any individual answer may generate a new question, which allows further investigation of the research question. A significant advantage of this method is getting to know what people believe and their emotions feel[206]. By presenting the right questions, the researcher will get valuable information. If a need arises for getting more information, the interviewer should present follow up questions to the respondents, thus, generating meaningful information and expanding the understanding of the study topic. Although these conversations can be conducted

remotely, face-to-face interviews are more suitable because the interviewer can read the respondent's emotions and body language in relation to the answers given.

Observation is a method that allows the researchers to use all five senses to gather information and is the basis of every data collection method, calling for behavioural rather than numerical characteristics[209]. For the observation method to be effective, the researchers need to have carried out their observations over some extended period. Sekayi and Kennedy[208] stated that an essential advantage of observation is that the researcher collects the information at the time it occurs and in its natural environment. Interviews also have their disadvantages in that they may collect only minimal information from some participants, and the information may not be accurate since the researcher does not generally have access to past occurrences [208].

According to Ricci [210], another method of qualitative research uses focus groups. The researcher sets out to reach a small set of individuals for a face-to-face group interview, generally in person, although online focus groups can be used. This method is commonly used to seek the opinions or emotions of individuals such as customers on a particular product or phenomenon (more details in section 3.3.5.)

Gathering qualitative data helps its audience to comprehend the reasoning behind particular findings and assumptions. The data must be analysed to come to a specific conclusion, and text analysis is one of the most often used ways of data assessment. It entails the documentation of ongoing events[210]. Additionally, images are frequently utilised, and conclusions are derived from them. Other formats include handwritten notes, audio-visual recordings, and films. Qualitative research is typically employed when a need for knowledge about a specific problem emerges and gives importance to people's feelings above numerical values[205].

3.3 Justification of Research Design

Research design includes both research methods and procedures selected by the researcher[211]. The research design enables the scholar to utilise the methods of research that are relevant to the study. It is an overall strategy that is integrated logically into the study and guarantees that the problem investigated in the research will be successfully addressed. It provides a basis for the researcher to collect, measure and analyse the data. Fundamentally, a research design is divided into three major categories, (1) data collection, (2) measurement, and (3) analysis. Ideally, the research problem determines the research design appropriate to that particular research problem. Usually, an impactful research design eliminates bias and reinforces trust in the accurateness of the data collected by the researcher [207]. A design that

has the most negligible margin of error yields the desired outcome. A proper research design allows the researcher to present an accurate and unbiased picture [211].

This thesis adopted a mixed research design, which uses a combination of both qualitative and quantitative approaches in a research project or study [212]. Thus, this approach builds on the idea that both qualitative and quantitative research designs have their limitations, and incorporating them into a single study can improve the study's overall goal of expanding the breadth and depth of understanding and verification[196]. Asenahabi [207] stated that "….a researcher collects and analyses both qualitative and quantitative data in either sequential and/or simultaneous and the exhaustive manner in which the researcher integrates the two forms of data will depend upon the nature of the inquiry and the philosophical outlook of the researcher."

Following the taxonomy of Creswell's et al.[212], this thesis adopts a sequential explanatory mixed methods design, which consists of three consecutive stages: (1) the quantitative stage followed by (2) the qualitative stage, and 3) A mix method stage, each of which includes data collection, analysis and reporting. This research design begins with a quantitative stage to provide a theoretical basis that produces numerical results. These results are used as inputs to inform and plan the qualitative stage. Then the researcher initiates the qualitative stage by gathering and analysing data qualitatively. The result of the second stage is qualitative (text) data to clarify, explain or support the quantitative numerical data produced in the initial stage[213], and to use these as the basis to develop and implement the proposed intervention in stage three. The last stage includes two consecutive studies introduced in Chapters 6 and 7 (Phases 3 and 4). These last two phases adopted a mixed method to collect data. Each consisted of a quantitative part (pre and post-assessment surveys) and a qualitative part (focus group). The aim of phases three and four in this thesis was to evaluate the proposed intervention to enhance the information security policies and reduce the individuals' tendency to justify the information security policies via a collaborative writing process.

The justification for adopting this approach in this thesis is that the quantitative stage findings provided a better understanding of the research problem (the role of neutralisation techniques in violating security policies and patient privacy in hospitals). Thus, the quantitative study would test a research model and its hypothesis that assess the relationship between neutralisation theory and behavioural violation of information security policies to confirm or reject such a role via a questionnaire distributed to medical interns, the study's sample. The following qualitative stage and its subsequent data collection and analysis processes elaborated and improved the numerical

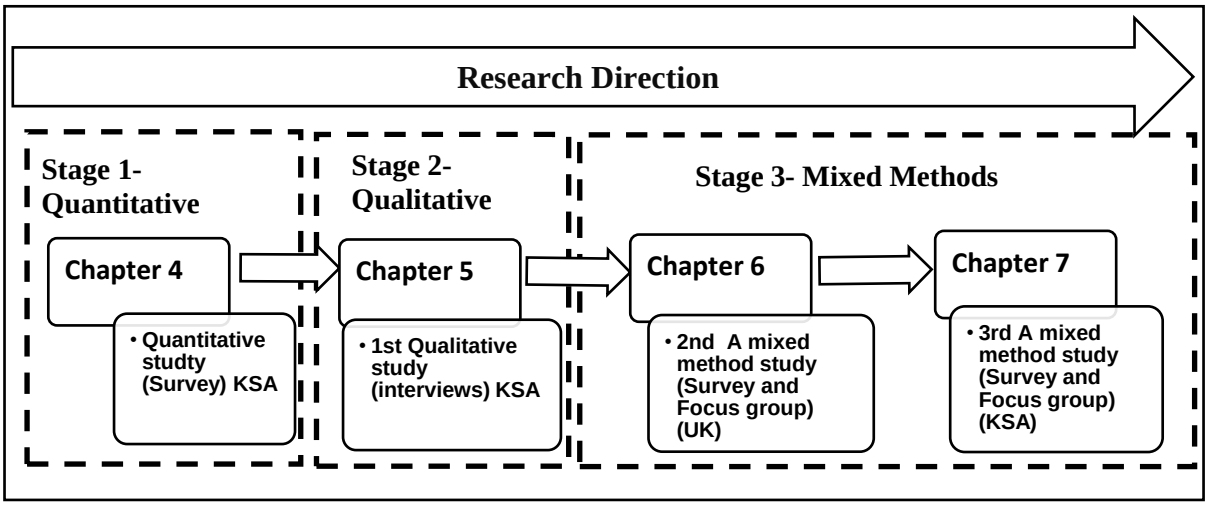


Figure 3.1 Mixed Methods Sequential Explanatory Research Design of The Dissertation

outcome by investigating in-depth participants' views [213]. In particular, the interviews assessed the research understanding of the environmental factors that influence the medical interns to violate information security policies and justify such behaviour. Additionally, the results of the questionnaires and interviews will be used to develop two related action research studies that will test and implement an intervention to decrease individuals' likelihood of using neutralisation techniques for information security non-compliance in two different countries, the United Kingdom and Saudi Arabia.

In summary, this thesis includes three inter-connected stages structured with two central quantitative and qualitative studies (Phase four and five). In addition, stage three comprising two mixed methods studies (Chapters 6 and 7). Figure 3.1 illustrates the multi-studies sequential explanatory mixed methods design of the thesis and its corresponding chapters.

An essential purpose of mixed methods research design in this thesis is to validate the role of an existing theory (Neutralisation techniques) in the information security field and investigate the relevant environmental factors that motivate the medical practitioners to evoke these justification techniques. Thus, the selection of the mixed methods research approach allowed the researcher to provide comprehensive, contextualised insights and draw new conclusions about the potential impact of the neutralisation techniques as a behavioural issue in security context within hospitals. Also, it allows the researcher to identify and design an intervention that aims to reduce individual tendencies to adopt these techniques for non-compliance with the information security policies. In general, three essential imperatives justify the selection of a mixed-method research design for this thesis:

- This approach can link research questions and objectives for each study together under a

single theoretical umbrella, facilitating the explanation of the phenomena (InfoSec policies justification for non-compliance) and serving the thesis purpose.

- This approach can ensure that each data collection method for these four empirical studies is consistent with the theoretical purpose and the direction of the investigation.
- This approach can help the researcher achieve the study's goals by verifying the results using various data generating methods. As a result, it enhances the researcher's capacity to investigate the influence of neutralisation theory on information security compliance (behavioural phenomenon) by allowing the consideration of multiple perspectives to plan and develop a relevant intervention.

According to Oates[214], data generation is defined as the process of producing empirical data or evidence. The data and evidence can be quantitative or qualitative. Thus, four different data generating methods were employed throughout this thesis, as introduced in Table 3.2. However, Creswell's et al.[212], they stated that the sequential explanatory mixed methods design has two significant challenges: (1) the variation of the sample sizes between the two stages and (2) the difficulties in identifying which part of the quantitative result needs more exploration.

Table 3.2 Data Generation Methods

Chapter/ phase	**Data Generation Method**	**Definition**
Chapter 4	Questionnaires	"A predefined set of questions assembled in a pre-determined order. Respondents are asked to answer the questions, often via multiple-choice options, thus providing the researcher with data that can be analysed and interpreted." [214]
Chapter 5	Interviews	"A particular kind of conversation between people where, at least at the beginning of the interview if not all the way through, the researcher controls both the agenda and the proceedings and will ask most of the questions". [214]
Chapters 6 and 7 (Mix Methods)	Focus Group	" A qualitative approach to behavioural science research consists of group interviews that involve a small number of appropriate persons discussing the topics raised by a moderator who guides the interview process." [215]
	Content Analysis	"A research technique for making replicable and valid inferences from text to their context of use." [195]
	Questionnaire (pre and post-assessment survey)	"A predefined set of questions assembled in a pre-determined order. Respondents are asked to answer the questions, often via multiple-choice options, thus providing the researcher with data that can be analysed and interpreted." [214].

3.3.1 Selected Research Methods and Techniques

This thesis aims to use a mixed-method approach in its design, incorporating qualitative and quantitative research features. Mixed research has been found to use and produce a variety of philosophical perspectives[216], although scholars with different philosophical beliefs may encounter difficulties because they may be at odds with each other philosophically [216]. This research approach was chosen to raise the overall reliability, increase the insights gained from the research data, assist in triangulating the research data, and strengthen the research findings and relevant interpretations. The research problem and the type of data required are among the fundamental factors that guide the effort to choose the appropriate research methodology. According to Creswell et al. [212], a mixed-method approach is more than just collecting and analysing qualitative and quantitative data; it combines the two methodologies to improve the study's overall strength. Several data collection methods and sources were employed to generate data for this thesis, as illustrated in Table 3.2. The following section provides more details of the data gathering methods that have been used to conduct the thesis.

3.3.2 Questionnaires (Chapter 4 / Phase1):

- **Research Paradigm**

Chapter four / phase one adopted a positivism research philosophy to predict and test a theoretical research model. Positivists conduct research using quantitative methodologies to explain or predict social phenomena. Their findings are based on the statistical analysis that leads to empirical validation of theories or hypotheses testing [217]. DaVeiga [218] stated that "The objective of positivist research is to obtain research results that are reliable, consistent, unbiased and replicable through other research studies in order to represent reality". From the current research perspective, the first phase aimed to examine, collect, and analyse a hypothetical relationship using a theoretical model via a quantitative method. Thus, a questionnaire was developed to collect data from medical interns (MI) in several academic hospitals in Saudi Arabia to investigate the relationship between medical practitioners' neutralisation techniques and non-compliance intentions. The theoretical study model was conducted to answer the following research question:

RQ1: What is the association between neutralisation techniques and the intention of medical interns to violate InfoSec policies?

- **Data collection method**

In phase one, the researcher developed a questionnaire to explore the impact of neutralisation techniques in predicting the violation of information security policies that protect patient privacy and how these techniques affect medical interns' intentions of non-compliance. Thus, a theoretical model was created to gather data on the relationship between neutralisation theory and its role in predicting employee justifications for non-compliance with InfoSec policies, as Park et al. [4] proposed. The questionnaire was composed of a series of closed-ended structured questions that corresponded to the research's primary interests and objectives. This technique can assure that each participant reads the same set of questions and has the same response options. Thus, it could aid and verify the consistency and clarity with which the queries are phrased[219]. Scholars often develop surveys and deliver them to many people in a short time and at a realistic and reasonable cost. For these reasons, the researcher chose a questionnaire because it can be administered easily, distributed quickly and gathered a lot of raw data from the targeted research sample [220].

- **Research Sample and analysis**

We utilised a planned and non-probability sampling technique. Purposeful sampling occurs when the researcher selects a sample on purpose, for example, because it is conveniently accessible or available[217]. The targeted research sample for this quantitative study was the medical interns in Saudi Arabia. Medical colleges in Saudi Arabia have developed the Medical Internship (MI) program for students who have completed all required medical school courses. Over four weeks, the researcher collected data from medical interns at four universities in Saudi Arabia. These universities were selected for their medical colleges and formal medical training programs for medical interns. Also, all four universities had information security policies and controls in their academic hospitals. Before the questionnaires were administered, the researcher asked eight medical practitioners in Saudi Arabia and three academic members to evaluate and validate the survey questions and scenarios. Then, a pilot study was conducted with a group of 15 graduate students in the School of Computing Science at Glasgow University. The survey was developed using an online platform (SurveyMonkey.com), which offers a fast and cost-effective solution with a rich set of features that enable more rapid data analysis and visualisation. Thus, the researcher sent an email invitation that included a study description and details to the medical interns using the email lists of universities. This invitation approach resulted in 66 completed questionnaires analysed statistically via Structural Equation Modelling (SEM) software using the partial least square (PLS) technique.

3.3.3 Interviews (Chapter 5 / Phase 2):

- **Research Paradigm**

According to Creswell [221], the interpretivism paradigm might be considered a fundamental approach for qualitative research because of its ability to explore participants' subjective realities. Howcroft and Trauth [222] stated that "Interpretive research provides in-depth insights into social, cultural and historical contexts within which particular events and actions are described and interpreted as grounded in the authentic experiences of the people studied" [222]. This paradigm was appropriate for the current research, which aimed to expand the first phase by examining the effect of contextual variables on medical practitioners' motives to abstain from compliance with a hospital's information security policy. As described in Chapter 2, the information security literature revealed that individuals occasionally use cognitive rationalisations to avoid emotions of shame or guilt when they commit or contemplate violating InfoSec policies and controls. Thus, Chapter 5 (phase two) will examine the factors (antecedents) contributing to healthcare practitioners' behavioural justifications for violating InfoSec policies protecting patient privacy. We specifically seek to address the following research question:

RQ2: ***What drives behavioural justification among medical practitioners to violate information security policies in healthcare organisations?***

- **Data collection method**

To address the second research question (RQ2) and explore the environmental causes, the researcher conducted a series of semi-structured interviews with two groups of participants in one of the largest hospitals in Saudi Arabia. Eight of those interviewed were from the Information Technology (IT) department, while twenty participants were medical interns, for a total of twenty-eight interviews. Interviewing is a qualitative method under the interpretivism paradigm that entails asking questions such as open-ended ones to collect elicit data from the participants[223]. The researcher intends to understand the participants' opinions and experiences in a structured way through the interviews, using verbal questions. This thesis used semi-structured interviews that included inquiries regarding violations of Infosec policies in an academic hospital. Semi-structured interviews will be employed to maintain consistency during sessions. Depending on the target audience, a combination of open-ended questions was utilized to help the researcher understand the environmental factors that motivated the behaviour of medical practitioners to violate information security policies that protect patient privacy.

Semi-structured interviews provided leeway to the researcher to probe the participants thoroughly. These semi-guided conversations provided flexibility for the researcher compared to structured interviews because the questions are not bound to a specific item. However, the researcher kept the interview structure in mind while being creative in acquiring data [223]. Also, this type of interview allows for follow-up questions based on the responses, enabling researchers to understand the respondent's circumstances and experience better. In addition, all interviews were face-to-face, involving asking questions directly to the respondents to ensure higher response rates. The advantage of this approach is that the researcher could note down the participant's body language for later analysis [224].

All semi-structured interview questions were checked for validity and reliability by an independent academic researcher, an IT expert, and a hospital physician. This feedback was mainly intended to simplify some open-ended questions and paraphrase to increase clarity. Further, the researcher conducted a pilot study to assess the interview questions with three medical interns to confirm that the questions were comprehensible and straightforward. Finally, we repeated the data collection and analysis process until we reached the point of saturation [225], where no more new themes emerged from the interviews and the findings repeated across the participants.

- **Research sample and analysis**

This study employed a non-probability snowball sampling strategy, which is ideal when the target sample is hard to reach. A non-probability method suggested that selecting the target population is dependent on the researcher's judgment; thus, not everyone has an equal chance of being picked. A snowball sampling strategy is based on the initial participants' social network to identify and communicate the researcher with the rest of the target sample members, the medical interns [226]. Thus, these initial participants assisted the researcher by increasing the study participation rate while inviting and recruiting additional study participants. In this case, each initial medical intern participant referred the study invitation email to their peers and encouraged them to contribute to the study.

The interview protocol consists of three main parts: (1) the introduction, (2) the general questions, and (3) the questions on information security. The first part of the interview started when the researcher explained the study goal and purpose and then asked the participant to sign the consent form. Once the participant agreed to participate, the interview started by collecting data about demographics, job descriptions, and information security background. The last part,

which was the core of the interview, consisted of five sets of semi-structured interview questions to explore in-depth the information security environment in the hospital in five major areas: (1) InfoSec policies development, (2) implementation, (3) enforcement, (4) awareness and training, and (5) incident reporting. These interview areas improved the study's understanding of the level of information security compliance and awareness within the hospital, which includes:

1. Verifying the employees' perception of the relationship between sensitive data that they were managed daily and the impact of information security policies and controls on their daily work.

2. Assessing the employee's awareness of the security efforts implemented by the hospital administration for information security. It included employee awareness of current security policies and associated controls that the hospital used to protect medical records and mitigate security risks.

3. Identifying the contexts, situations, and circumstances prompted medical practitioners to violate information security policies. It included identifying the violating information security policies, associated procedures, and related justifications.

A total of 26 participants agreed to audio-record their answers during the interview, while two preferred the interviewer take notes. All interview discussions were in English and conducted face-to-face in a hospital and carried out by the author between September 2018 and November 2019. Finally, in this study, the researcher used Braun and Clarke's [194] thematic analysis method described to analyse the interviews, as will be described in the following subsection.

- **Thematic Analysis**

Thematic analysis is regularly adopted in qualitative research and was developed in 2006 by Braun and Clarke [194] to help novice researchers conduct a thematic analysis in a step-by-step style. Braun and Clarke's [194] thematic approach towards qualitative data analysis is widely used in the field of social sciences. Their approach seeks to answer questions about experiences, views and perceptions. The results are a group of themes that explain people's opinions and observations of a particular topic. They recommend that a thematic analysis should start with research questions or themes. In their approach, Braun and Clarke [194] argue that themes are conceptualised based on the data, and themes tend to express the participants' meaning and representation in the researcher's eyes.

According to Braun and Clarke [194], two basic approaches to thematic analysis (T.A.) may be used to find themes or patterns in data: these are deductive and inductive approaches. The deductive or theory-driven approach is a top-down approach where the researcher analyses data using an explicit structure or predefined theoretical framework. Thus, the coding and analysis process is conducted based on the researcher's theoretical interest in the area. In contrast, the inductive approach is bottom-up and involves "a process of coding the data without trying to fit it into a pre-existing coding frame, or the researcher's analytic preconceptions". [194]. This technique is data-driven and may rely on little or no predefined theory, structure, or framework. When there is little to no knowledge regarding the research phenomena, this approach is most suitable. However, the inductive approach is more time-consuming and cumbersome than the deductive approach.

The two approaches define themes quite differently. The inductive approach involves the researcher analysing and coding data in an open or unconstrained manner, followed by a comprehensive optimisation of patterns to provide a relevant collection of themes for the data in question. This approach has some similarities to grounded theory. However, with the deductive approach, the researcher's orientation is to analyse the given transcript based on well-defined concepts, ideas, or theories closely mapped to a specific research question. This study utilised the six steps framework as presented in Figure 3.2. to execute the thematic analysis.

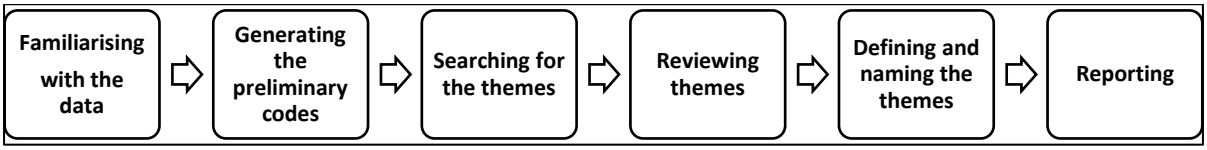


Figure 3.2 Phases of Thematic Analysis

Braun and Clarke [194] prescribe a six-step framework as the following:

1. **The first step is to become familiar with the data:** The researcher will be fully engaged in the data by performing a transcription of the interactions and then listening to the recordings after re-reading the transcripts. During the first phase, any initial ideas will be noted down.
2. **The next step is generating the preliminary codes**: Once the researcher is familiar with the data, introductory codes will be identified.
3. **The third step is searching for the themes:** The researcher's thought process would indicate the relationships between the codes and themes. This step might include combining

codes to conduct central themes to represent data better.

4. **The next step is reviewing themes:** The researcher will question whether to combine or discard the primary themes, confirming that the data within the theme cohere together in a meaningful manner.

5. **The fifth step is defining and naming the themes:** During this step, the researcher will refine and define the themes to determine their relationship to the data and research questions. The analysis will be performed to enhance the identified themes further. The essence of each theme will be captured in an effective manner.

6. **The final step is producing a report**: The researcher will interpret the text and report the outcome using vivid and compelling examples, which should relate to specific themes and related codes. The report must be convincingly formulated with regard to the validity of the thematic analysis [194]. Themes should be supported by textual evidence that addresses the research question.

3.3.4 Action Research (Chapter 6 / Phase 3) and (Chapter 7 / Phase 4)

- **Research paradigm**

As will be discussed in Chapters 6 and 7, these two chapters comprised phases three and four in this thesis. An interpretive paradigm was followed in both phases, which was concerned with understanding individuals' experiences with information security controls.William[227] explained the importance of this paradigm in information security research and stated that "interpretivism is concerned with the results 'making sense' and being understandable within a given context. Therefore, the investigation into information systems intrinsically includes the way humans interact and function with others and technology". Thus, it is appropriate for the current research to expand our knowledge of the psychological, managerial and social experiences when individuals interact with information security policies in the workplace. In particular, we applied an action research approach that included an intervention to improve information security policies effectiveness.

Action research aims to develop and test an intervention that might, in the case of this study, mitigate the role of neutralisation techniques in violating information security regulations. The term "action research" refers to a mix of theoretical and practical research combined with action [215]. Davison et al.[228] add that the action research " involves solving organisational problems through intervention while at the same time contributing to knowledge". Thus, a significant outcome of action research is generating new knowledge based on real-world

solutions to a specific problem. Action research may be able to address, for example, the relevance of information system research [229]. For instance, action research is essential when experimental settings can easily modify observed behaviour due to the Hawthorne effect, in which participants behave differently and convey perhaps different intentions when conscious of being observed. As a result, action research has evolved as a critical method of investigation in the social sciences.

Numerous distinct forms of action research have been proposed in the literature. Action research may be broadly classified into two types: (1) participatory action research and (2) canonical intervention. Because participatory action research is conducted in the researchers' natural environment of the subjects, researchers simultaneously assume the roles of participant and researcher throughout the procedure. Outsiders perceive researchers who follow the traditional research approach as interfering. This thesis was influenced by the style of canonical action research as discussed in Chapters 6 and 7, which is based on five fundamental concepts defined by Davison et al.[228]:

1. **Researcher–Client Agreement (RCA**): The researchers and the client must reach an agreement that assures a shared knowledge of the study objectives, the project's approved behaviours, and the anticipated rewards and dangers. Holding such an agreement in place can help establish the trust necessary for the research project to proceed.
2. **The Cyclical Process Model (CPM):** An iterative process that proceeds sequentially through five stages: (1) diagnosis of the organisation's condition and problem, (2) action planning, (3) intervention (action taking), (4) evaluating the intervention, and (5) reflection on lessons learned.
3. **The Principle of Theory:** The importance of a theoretical framework that supports the investigation of the phenomena of interest.
4. **The Principle of Change through Action:** This reflects the intervention's ability to make a suitable change that solves the organisation's problem. Davison et al.[228] stated that "A lack of change in the unsatisfactory conditions suggests that there was no meaningful problem [or] that the intervention failed to address the existing problem".
5. **Learning through Reflection:** This indicates the impact of action research on the organisation and research; Thus, action research results can enhance the organisation's practice and the knowledge of the research community.

Action research is the optimal way for validating the research method and reducing information security policies violation. The purpose of this thesis is to examine the validity and potential improvement of interventions used to reduce information security policies violations. As a result, action research is an acceptable method for performing this study [230]. The fundamental objective of action research is to effect change while actually doing the research [228]. Thus, the Cyclical Process Model (CPM) was an appropriate approach to adopt for this research and includes five steps, as is illustrated in Figure 3.3.

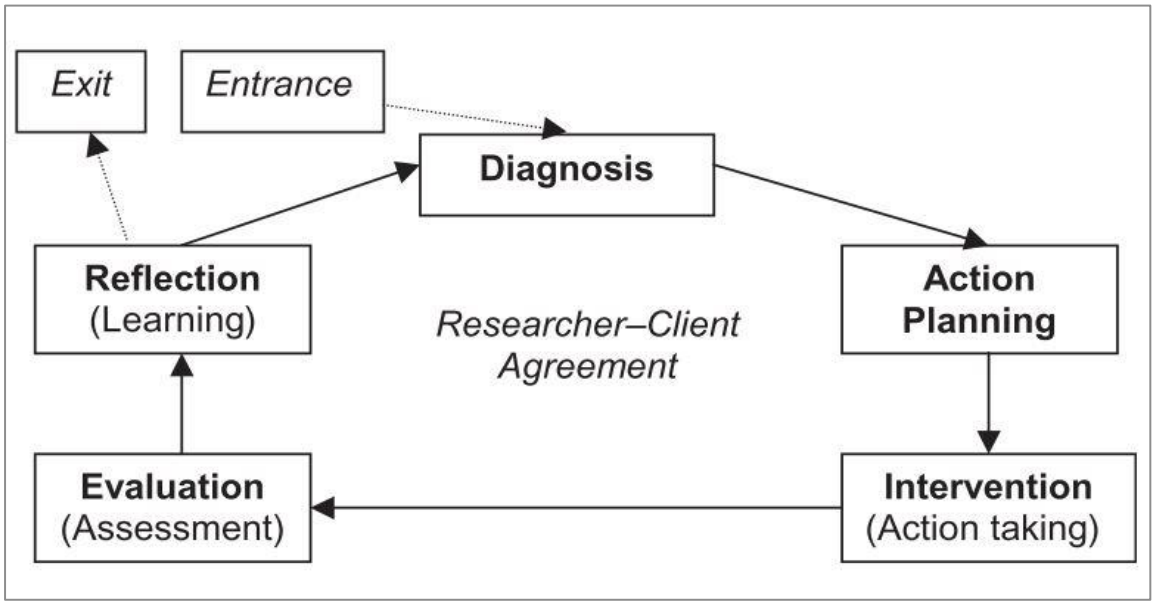


Figure 3.3 Canonical Action Research Process Model Adapted From Davison et al.[228]

- **Step 1- Diagnosis:** The researcher focuses on organisational issues, causes, objectives, and desired changes. The analysis of the organisation's situation is an important step to inform the action plan phase. In this thesis, the result of both quantitative and qualitative studies in Chapters 4 and 5 provided background information for diagnosing the challenges that hospitals encountered due to individual justifications for violating information security policies.

- **Step 2 - Action plan:** This is a collaborative process between the researcher and the organisation to improve problem diagnoses; for instance, the organisation's share of the responsibility for data gathering and other logistic support is defined. This phase enables the researcher to determine and plan the appropriate intervention. In this thesis, the researcher had previous working experience in the healthcare industry, which helped to communicate with higher management and the IT department in one of the biggest hospitals in Saudi Arabia. During this study, the researcher held several Skype calls and

personal meetings to discuss the research opportunities and the possibility of reducing violations of security policies by the medical interns. Thus, the organisations provided supported in conducting three studies (Chapter 4, 5, and 7).

- **Step 3 – Intervention:** This involves implementing actions that aim to resolve the organisation's issue. This action has been prepared and designed based on the previous phase. In this thesis, as illustrated in Figure 3.1**,** the researcher quantitatively tested a theoretical model investigating the relationship between medical practitioners' justifications and information security non-compliance, as described in Chapter 4. The result helped the researcher confirm the relationship. A further qualitative investigation reported in Chapter 5 aimed to explore the environmental factors that motivated the individuals to justify the information security policies violations using a series of semi-structured interviews. The results of these two studies helped the researcher to identify the most common security breach behaviours, affected policies, and related justifications adopted by medical practitioners to violate the information security policies. Thus, the proposed intervention was to involve end-users in developing information security policies, which could align better security requirements with the work needs of medical practitioners and enhance the overall security policies effectiveness against individual justifications, as presented in Chapters 6 and 7.

- **Step 4 – Evaluation:** This stage assessed the consequences of the intervention. The evaluation process includes determining the impact of the intervention on the problem. Any change in behaviour is examined to ensure that it is a consequence of the research. In this thesis, the impact of end-user participation in the password policy development process via the collaborative writing process was evaluated using pre-post assessments, as described in Chapters 6 and 7. Thus, examination revealed that this approach was promising to enhance the overall effectiveness of password policy by targeting neutralisation techniques that lead to password sharing.

- **Step 5 – Reflection:** This includes examining the outcomes of the quantitative and qualitative analyses and identifying valuable knowledge to improve information security policies and information security compliance in dealing with comparable future study situations. The last chapter summarises the proposed future work connected to this thesis.

In short, Chapters 6 and 7 (Phases III and IV) will present the proposed intervention to mitigate the role of neutralisation techniques in information security non-compliance by engaging the

end-user via a collaborative writing process to improve information security policies. We specifically seek to address the following research question:

RQ3: ***To what extent does the engagement of the perception of end user during information security policy development via a collaborative writing process increase the effectiveness of the InfoSec policies to mitigate the role of neutralisation techniques?***

3.3.4.1 Focus Groups

A focus group involves a group of selected participants. These individuals contribute to an open discussion and help the researcher answer research questions [223]. This information is more prosperous than the interview because the researcher simultaneously gets different opinions from people [210]. The researcher selected a limited number of participants for this study who mirrored the larger target population. The focus group looked at topics of interest to capture the populations' reactions. The focus group in this study had a moderator to ensure the legitimacy of the results, answer individual questions, and encourage participants to engage[210]. However, it comes with several setbacks; for instance, some group members overpower others as those with substantial influence often tend to control the thinking and perspective of other members. This makes the information biased as it comes from a one-sided view of members. Another issue is that the group may not be open to an interviewer by a particular organisation [206]. They may feel nervous in the presence of a moderator and so hesitate from expressing their opinions openly. Additionally, there is an issue with generalising a group's opinions to the general population, as the beliefs or emotions of one group may not reflect the views of other groups in the population [231].

- **Research Sample and analysis**

The steps of conducting focus group research will begin by recruiting the right participants [232]. Thus, the researcher selected a small number of participants in the third and fourth phases, reflecting the target population. Two studies were conducted in the United Kingdom and Saudi Arabia and included two research samples to participate in several focus group discussions. Phase III study was established in the United Kingdom and recruited twenty-four postgraduate students divided into six groups at the University of Glasgow. In addition, phase four was conducted in one of the largest hospitals in Sudi Arabia and the researcher recruited 42 medical interns formed ten groups. Participants contributed in several focus group discussions to update information security policy through a collaborative writing process in each of phase III and IV studies. In particular, the focus group looked at topics of interest (four

neutralisation techniques scenarios DoI , DON, AoHL and EEIDI) and captured the populations' reactions.

The focus group in this study had a moderator who would ensure the legitimacy of the results, answer individual questions, encourage participants to engage [233]. The moderator will also seek to eliminate or reduce bias in the discussion. Then a moderator will be selected who understand the research questions and motivates the members through supportive words. The researcher should clearly write down the discussion guideline.

The researcher provided discussion guidelines and a written plan to the focus group members. A written explanation to clarify the objectives of this thesis was illustrated upfront. After the focus group had been set up, the researcher presented questions and the topics of interest to the focus group [223]. The questions aligned with the research objectives and also complemented each other. The researcher focused on the crucial issues in the study, and open-ended questions were used to increase the effectiveness of the discussion. The focus group was held in person, but participants who could not make time for a face-to-face interaction delivered their opinions through an online platform. Focus groups are advantageous for eliciting diverse perspectives such as health concerns, treatments, and research.

The Wilcoxon signed-rank test is nonparametric that was used to assess the significance of median differences of the MI's perception about the effectiveness of password policy to mitigate the neutralisation techniques before and after the collaborative writing activity. This test is an alternative to the paired samples t-test to calculate whether the median differences differ from zero in the population. Therefore, the Wilcoxon signed-rank test was adopted to measure the variation of the end users' perception regarding the password policy's effectiveness from the same individuals before and after the collaborative writing session.

In this thesis, a collaborative writing activity was employed, which included an in-person discussion with four or five participants comprising one group. This discussion aimed to explore and reflect the participants' perspectives to counter their adoption of neutralisation techniques to violate password policy. Thus, it can improve the policy effectiveness against password sharing as undesirable behaviour in the security context.

3.3.4.2 Collaborative Writing Process

Collaborative writing (CW) is a critical group process whose prominence has increased over the years and has been widely used in numerous industries, the government, and healthcare

[234]. Lowry et al.[235] state that collaborative writing is becoming used gradually because of its potential benefits. Thus, collaborative writing can be described as:
“ an iterative and social process that involves a team focused on a common objective that negotiates, coordinates, and communicates during the creation of a common document. The potential scope of CW goes beyond the more basic act of joint composition to include the likelihood of pre-and post-task activities, team formation, and planning. Furthermore, based on the desired writing task, CW includes the possibility of many different writing strategies, activities, document control approaches, team roles, and work modes.” [235]

The CW includes several key iterative activities that occur in dynamic ways during the actual production of a group document, such as brainstorming, outlining, drafting, reviewing, editing, and revising [235]. These activities can provide benefits that include learning, socialisation, and the injection of new ideas [234]. The benefits of collaborative writing are most apparent if the business need involves collaborative work [235]. In collaborative writing, all the team members in the group contribute to the decision-making process during document production. Through collaborative writing, complex challenges that seek to bolster the effectiveness of the InfoSec policies to mitigate the role of neutralisation techniques can be proposed as solutions. The collaborative groups also draw strength from the members. Even if one member has strong critical thinking skills, the other may excel in organising or writing [235]. Working as a group will allow members to learn from each other; according to Lowry et al. [235], Enabling employees to work collaboratively helps them prepare for the benefits and pitfalls they encounter in completing their tasks.

Through collaborative writing, a diversity of opinion can be articulated, which has the benefit of increasing possible options in addressing the InfoSec policies needed to mitigate the role of neutralisation techniques. More minds at work mean that there are a variety of perspectives. Division of duties will allow each member to be held accountable for their actions. To master the skills of collaborative writing, a researcher should follow four steps: (1) acquire the needed skills, which include active listening, self-reflection, trustworthiness, and reliability [235]. (2) determine writing strategies and roles; (3) organise work assignments based on individual expertise; and (4) establish a clear timeline and highlight deadlines. Regular communication should be done to enhance collaboration within a group [234].

In the third and fourth phases, all the collaborative writing sessions were face-to-face and were held inside the organisations' premises. The purpose of the collaborative writing process was to determine whether the involvement of end-users during security policy development could

enhance the effectiveness of policies against individuals intending to adopt neutralisation techniques. In the beginning, each groups member will complete a preassessment survey to evaluate the organisation current password policy effectiveness to counter a set of neutralisation techniques claims. The collaborative writing process is a group activity to modify a givin security policy. Thus, each group reads several scenarios designed to represent a neutralisation technique that an end-user might use to violate an organization's password policy. Next, each group's task is to collaboratively modify the password policy to reflect their perception to counter these behavioural justification scenarios that may lead to a password policy violation. The collaborative writing process was based on a focus group effort and discussion to alter the password policy to reduce the tendency for employees to justify non-compliance. Once each group has completed a collaborative writing session, the researcher will perform a content analysis based on Situational Crime Prevention Theory (SCPT) as a basis to generate a list of themes and codes from the text of the updated password policy.

3.3.4.3 Content Analysis

The first phase of content analysis is to identify the intentions and focus on communication trends [236]. Describing attitudinal and behavioural responses is the second step, and the researcher should determine the emotional state of the groups. Also, the thesis revealed patterns in communication content, per-test and improved surveys prior to launching. Moreover, focus group interviews and open-ended questions were analysed to supplement the quantitative data.

The researcher performed content analysis to determine the presence of certain words, themes and concepts in the qualitative data. The content analysis allowed the researcher to measure and analyse the meanings and relationships that exist in specific themes [237]. The researcher also used content analysis to evaluate languages used in an interview to locate bias or partiality [210]. To fully analyse the text using content analysis, the researcher coded all the text and broke it down into manageable pieces. Once the texts were coded, the codes were further categorised into codes or themes to summarise the data further. Thus, the Situational Crime Prevention Theory (SCPT) was adopted in phases three and four as theoretical bases to create a list of themes and codes of countermeasures that the participants added in the updated version of the password policy.

In criminology, Cornish and Clarke [238] introduced five main crime prevention strategies that aimed to reduce the opportunity of a specific crime to occur by altering the immediate environment. The five strategies are as the following:

1. **Increase the offenders' effort to commit a crime:** this strategy includes a set of five techniques that aim to increase the effort that the offender needs to commit a crime. It includes target harden, control access to facilities, screen exits, deflects offenders and control tools/ weapons [238].
2. **Increase the offenders' perceived risk of being caught:** this strategy aims to increase "the risk apprehension"[239]. It includes extending guardianship, assisting natural surveillance, reducing anonymity, utilising place managers, and strengthening formal surveillance [238].
3. **Reduce offenders' rewards of the crime:** this strategy aims to distract the offenders expected gains of a crime. It includes conceal targets, remove targets, identify a property, and disrupt markets, and deny benefits [238].
4. **Reduce the provocation that stimulates the offender to commit a crime:** this strategy aims to enhance the situational sittings or conditions that can trigger the individual to commit a crime. It includes reducing frustrations and stress, avoiding disputes, reducing emotional arousal, neutralising peer pressure and discouraging imitation [238].
5. **Remove offenders' excuse to commit the crime**: this strategy aims to neutralise the justifications that the offender used to commit a crime. It includes set rules, post instructions, alert conscience, assisting compliance, and controlling drugs and alcohol [238].

According to Krippendorff [195], content analysis is "a research technique for making replicable and valid inferences from text to their context of use, with the purpose of providing knowledge, new insights, a representation of facts and a practical guide to action." Du Preez [240] asserted that content analysis must follow a well-structured procedure to gain more reliable and valid results. In Chapters 6 and 7 of this thesis, Krippendorff [195] procedure for the content analysis were adopted to examine the updated password policy developed by several groups during the collaborative writing process. Krippendorff [195] procedure includes six phases, as follows:

1- **Unitizing:** This is a systematic process to identify and distinguish specific text segments (sample text units) that are relevant to the purpose of the content analysis. A united text can be a complete sentence, portion of it or a word [241].

2- **Sampling:** this phase refers to drawing a controllable set of test segments from a population when it is unrealistic to perform a content analysis over the entire set of transcripts[195].

3- **Coding**: This phase refers to the process of classifying texts identified from the sampling phase into analysable text units [195]. This process can be conducted by either emerging coding or prior coding. Emerging coding aims to create new themes and codes to build a new theory based on the ground theory concepts [242]. Prior coding refers to the usage of predefined codes and themes from well-established theories [242].

4- **Reducing:** This phase aims to reduce duplication of data by counting the frequency of codes to decide whether there is a need to reduce these codes to enhance the interpretation process, and the statistical efficiency [195].

5- **Inferring:** Krippendorff [195] described this process as searching for " the contextual phenomena from texts ……..It bridges the gap between descriptive accounts of texts and what they mean, refer to, entail, provoke, or cause.".

6- **Narrating**: This involves the process of reporting the content analysis results in an understandable and meaningful manner. This phase discusses the inferences and reports the results that answer and address the research questions [240].

3.4 Summary

This chapter discusses the research paradigms, methods, and study designs used in this thesis. It also reviewed the procedures, participants, data collecting instruments, analysis methodologies, and their benefits and drawbacks. The sequential explanatory mixed methods design was employed in the thesis to test the theoretical model and examine the environment, which plays an essential role in the decision to adopt the action research method for intervention development. The data was generated and analysed primarily using a mixed approach of qualitative and quantitative methodologies, with each approach having its own set of benefits and drawbacks. The researcher can achieve the best results by combining qualitative and quantitative research methodologies. This strategy compensates for the flaws of each method.

Chapter 4 : Determine The Role Of Neutralisation Techniques To Predict Medical Practitioner Intention To Violate Infosec Policies.

This chapter introduces the first phase of this research, as presented in Figure 4.1 below. It investigates whether neutralisation techniques significantly predict medical practitioners' behavioural intent to violate Information Security (InfoSec) policies and patient privacy.

Phase 1	Phase 2	Phase 3	Phase 4
Determine the role of Neutralisation techniques to predict medical practitioner intention to violate InfoSec policies. A quantitative study using a questionnaire in Saudi Arabia.	Investigate the motivations of medical practitioners to evoke neutralisation techniques to justify InfoSec violations. A qualitative study using semi-structured interviews in a Saudi Arabian hospital.	Enhancing InfoSec policies effectiveness against neutralisation techniques via the engagement end user perception. An action research study using focus groups and pre and post questionnaires in the UK, University of Glasgow.	Enhancing InfoSec policies effectiveness against neutralisation techniques via the engagement end user perception. An action research study using focus groups and pre and post questionnaires in a Saudi Arabian Hospital.

Figure 4.1 Phase One of The Research Study

4.1 Purpose of The Study

Based on previous IS literature results [1][31][187], individuals tend to justify behaviour that diverges from security policy requirements [187]. When an employee breaks an organisation's policy, they may defend their non-compliance behaviour by providing specific justifications. Thus, neutralisation theory proposes a set of justifications that may be deployed by users to rationalise a violation of security policy. Neutralisation theory can be used to study and model why a user may intend to commit a violation of security policy. In this study, we have investigated the role of neutralisation techniques to predict the problem of privacy breach in violating InfoSec policies and how these techniques affect medical interns' intention for non-compliance behaviour. Therefore, following Park et al. [78], we employ neutralisation theory as a theoretical framework to answer the following research question:

RQ1: What is the association between neutralisation techniques and the intention of medical interns to violate InfoSec policies?

To address the research question, we proposed a study model as illustrates in Figure 4.2. In this study, we adopted the Siponen and Vance [1] and Teh et al.[31] approach and analysed neutralisation as a formative- multidimensional (single second-order) construct, consisting of the six neutralisation techniques as reflective first-order subconstructs, which are the condemnation the condemner, the denial of injury, the denial of responsibility, the appeal of higher loyalty, a metaphor of ledger and defence of necessity. Several reasons contribute to choose conceptualising neutralisation as a second-order construct. According to Siponen and Vance [1], neutralisation theory consists of several techniques, and each of them represents a distinct dimension of the theory and describes a different angle of the overall neutralisation as a complex construct[243]. Consistent with Petter et al.[244], they stated that "*a complex construct that is the main topic of study may deserve to be modelled as a multidimensional construct to permit a more thorough measurement and analysis* ". This approach is valuable when we need to gain a deeper understanding of a specific theoretical construct [245] , and " Whereas two or three measurement items might suffice to define a construct of peripheral interest, a multidimensional construct allows researchers to develop items that describe a construct in terms of multiple subconstructs, bringing the nature of the construct into sharper relief "[1].
Also, this approach is applicable in this study as each of the first-order constructs is considered as a distinctive dimension with a set of corresponding measurement items (e.g., yellow squares in Figure 4.2). A reflective relationship was modelled between the first order constructs and their measurements because these measurement items (indicators) are manifestations of the constructs, conceptually interchangeable as each measurement item is highly correlated with other items in the same construct and represent a common characteristic or a sample of the construct [245]. In addition, the formative first-order constructs (six neutralisation techniques in blue squares) load their results obtained from the questionnaire (indicators) in the second-order construct (Neutralisation).
Therefore, we have hypothesised the following to test the proposed study model (Figure 4.2):

Hypothesis one (H1): ***Neutralisation directly and positively affects the intention of Medical Interns (MI) to violate the hospital's information security policies intended to protect patient privacy.***

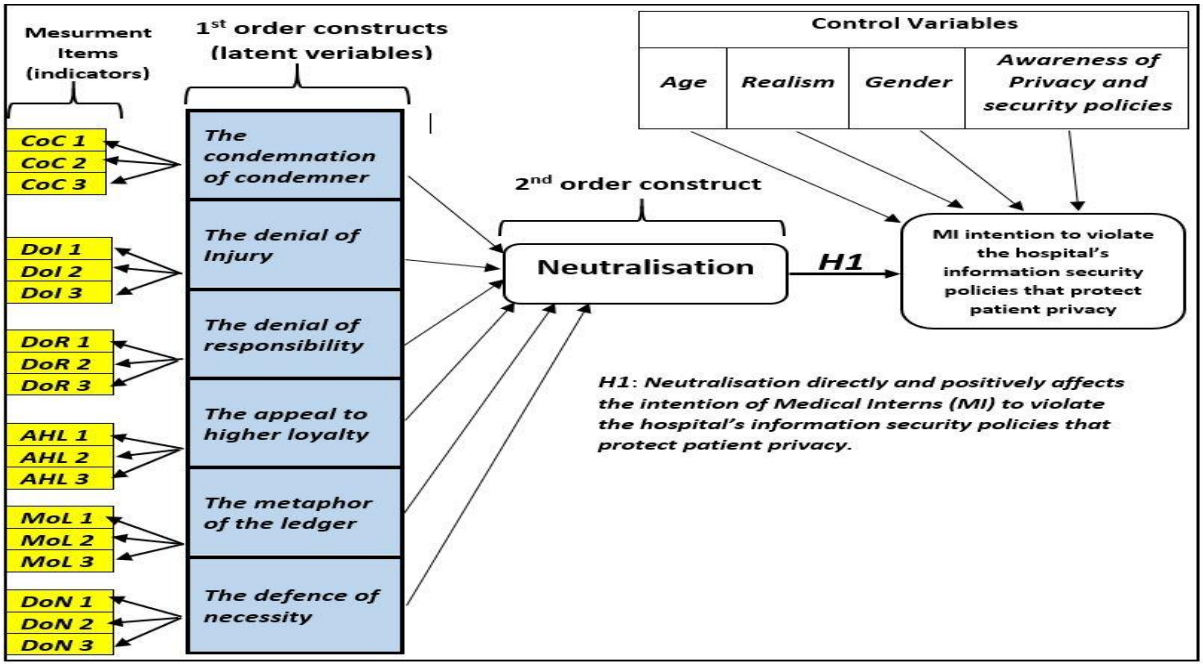


Figure 4.2 The Proposed Study Model Represents Neutralisation as A Second-Order Construct.

4.2 Ethical Approval

The Ethics Committee of the College of Science and Engineering at the University of Glasgow agreed to conduct this study in several hospitals in Saudi Arabia under approval number 300160167. (See Appendix A.4 for the ethical study approval.)

4.3 The Research Methodology

This study adopted a quantitative approach to investigate the role of neutralisation techniques to predict the tendency of medical interns to violate existing InfoSec policies to provide maximum protection of patient medical information. Thus, we developed a quantitative online questionnaire divided into five sections. All respondents were asked to select one choice from a drop-down list and tick a mandatory box in some cases. These sections are as follows:

- **Participant information sheet**: this section provides brief details about the study. It includes necessary information about the study authors, purposes, risks, and benefits and includes a confidentiality agreement. This section helps the participant decide whether or not to participate in the study. (See Appendix A.5 for the participant sheet)
- **Consent form:** Questions 1–4. This section requires the respondent to accept all terms and conditions listed in the participant information sheets. Once the respondent has checked (accepted) all the boxes, a new page will start the survey.
- **General questions:** Questions 5–7. This section aims to collect certain necessary information from the participant, specifically to confirm that the respondent has the right to

access the hospital Electronic Medical Records system (EMRs) or Electronic Health Records (EHRs) at their medical institution. These questions will also determine the respondent's level of awareness of information privacy and related security policies at their institutions. If the participant does not have access to the EMRs or EHRs, the questionnaire ends, and the participant receives a thank you letter.

- **Demographic information, computer experience, and Internet usage:** Questions 8–12. This section gathers the respondent's age, gender, and daily use of EMRs or EHRs and the Internet.
- **Neutralisation theory and its relationship to employee behavioural intention to violate InfoSec policies and patient privacy:** Questions 13–34. This section was divided into two subsections to cover neutralisation theory. The first subsection started with two security scenarios (section 4.3.1) to capture employee behavioural intention to evoke cognitive justifications for InfoSec policies non-compliance (questions 13 and 14). Both security scenarios were measured using a 10-point Likert scale. The second subsection (questions 15–34) includes self-reported responses that correspond to each of the neutralisation techniques in the study research model.

Once the respondent clicks the invitation link, they are taken to the survey instrument configured on surveymonkey.com, and a welcome page appears alongside the participants' sheet. If the respondent agrees with the study details, they then proceed to check the accept box to all terms and conditions in the consent form. Once that step has been completed, the survey starts, and the respondent answers each section's questions as presented in Figure 4.3. Participation is voluntary, and the respondent can leave the survey at any time and complete it later.

Figure 4.3 Questionnaire Sequential Sections

4.4 The Research Instruments

4.4.1 Scenario Design

This section describes the scenario-based survey method employed for investigating the effect of neutralisation on interns' hypothetical behaviour. According to O'Fallon and Butterfield [246], Scenario methodology is widely recognised to explore unethical issues. In addition, several IS scholars have been adopted it in the information security field to investigate various behavioural issues such as individuals' InfoSec violation [125][247], software piracy[248], and

computer abuse [148]. According to Trevino [249], a scenario is a vignette that "presents subjects with written descriptions of realistic situations and then requests responses on several rating scales that measure the dependent variables of interest."

In their seminal work, Siponen and Vance [1] postulated that a scenario method is an appropriate approach to indirectly assess deviant or abusive behaviour intentions in an information security context. They stated two advantages of using a scenario-based method to measure the individuals' intent to commit unethical or undesirable behaviour such as InfoSec policies violation. First, it helps the researcher to reduce the responses error associated with social desirability bias, which refers to the respondents' tendency to answer survey questions in a favourable manner consistent with expected social norms [250]. Thus, a scenario-based method can encourage the respondents to provide more honest answers as individuals in general are not willing to admit their engagement in anti-social unethical behaviour [148] [120] . In this approach, the scenario relies on a fictional actor performing undesirable behaviour. Hence, the respondents feel more comfortable reporting their behavioural intentions when asked to read the scenario and answer related questions. In particular, the scenario aims to obtain indirectly how would respondents behave if they imagined themselves (hypothetically) in a similar situation as the scenario character[247] [148].

The second advantage, according to Siponen and Vance [1], is that using a scenario-based can provide " a way to enhance the realism of decision-making situations by providing contextual detail while simultaneously ensuring that these details are uniform across respondents". Therefore, it offers a practical way to indirectly obtain the respondents' behavioural intention instead of measuring actual undesirable behaviour by observing the respondents or asking them direct questions [112].

In the same direction, we developed four scenarios covering several security areas where a medical intern might violate InfoSec policies and disclose patient information intentionally or unintentionally. These scenarios include the handling of information, the use of social media, the process for reporting incidents, and the use of official email. Piquero and Hickman's[251] reported that the scenario should be framed to fit a specific context and reflect details that are familiar to the respondents' environment. Likewise, the researcher contacted seven medical practitioners in two hospitals in Saudi Arabia to review and validate all four of these scenarios. Thus, based on their feedback, only two of the four scenarios (information handling and the use of social media) were selected and presented to the participants. After reading the scenarios, the respondents were asked: Do they believe the scenarios are realistic? Do they believe their behaviour would follow the character's behaviour in the scenario that violated patient privacy

and information security policies? What justification would they present for violating patient privacy in the face of current information security policies? (See Appendix A.1 for the scenarios list)

4.4.2 Questionnaire Development and Validity

This study used a survey to test the research model and hypothesis to obtain empirical evidence to answer the research question (RQ1). Thus, all constructs and variables were derived from several validated instruments and were adjusted to fit this context. We followed the approach of Siponen and Vance [1] and Teh et al. [31] to measure the dependent variable, MI intention to violate hospital information security policies using a single item that came directly after each scenario. The MI intention construct formed a combination of two variables: the likelihood variables coming from the two different scenarios. Based on a seven-point Likert scale ranging from "very unlikely" (1) to "very likely" (7), the MI intention was measured by the following question: "How likely would you do what [one of the scenario characters] did in the described scenario?"

After that, a single item requested the respondent to evaluate the realism of the given security scenario on a seven-point Likert scale ranging from "very unrealistic" (1) to "very realistic" (7) by answering the following question: "How realistic was the given scenario?"

Based on the work of Siponen and Vance [1] and Thurman [252], we tailored three measurement items for each of the neutralisation techniques to match our study objectives. Thus, the survey included 18 adapted items indicating six neutralisation techniques: (1) the defence of necessity, (2) denial of injury, (3) the metaphor of ledger, (4) condemnation of condemners, (5) denial of responsibility, and (6) appeal to higher loyalties. The medical interns were requested to reveal their agreement level based on a seven-point Likert scale ranging from "Strongly Disagree" (1) to "Strongly Agree" (7). (See Appendix A.2. for independent variables measurement items)

The Study tools and scenarios were reviewed and modified by eight medical consultants and interns in Saudi Arabia and three faculty members at the University of Glasgow. It took three rounds for all the reviewers to agree that the survey items and scenarios were understandable and relevant. Then, a pilot study was then conducted, where the author asked a group of 15 PhD students in the School of Computing Science at Glasgow University to estimate the time the survey would take and validate the questions before distributing them to the target sample (medical interns) in health care institutions in the Kingdom of Saudi Arabia.

4.4.3 Data Collection Procedures

We collected our data from medical interns at academic hospitals in the Kingdom of Saudi Arabia over four weeks. Four universities had been selected based on the fact that each has a medical college and a formal medical training program for medical interns. Academic hospitals are also required to have information security policies and procedures in place to protect the privacy of patient information. These universities are located in the central and western regions of the country.

The author has had previous experience in the Saudi healthcare sector as an application analyst for three years, which enabled contact with MI program directors in each of the target universities to explain the study's purpose. Subsequently, permission and assistance were granted to publish the survey via their official channels. We sent an online invitation to medical interns via their official university email, and each invitation included an online link to the questionnaire using the SurveyMonkey website. We collected responses from 94 medical interns, but 28 were excluded due to partial or incomplete responses to the survey items. Therefore, our sample contained 66 participants.

4.5 Data Analysis and Results

This section presents the survey results from the medical interns in the four academic hospitals in Saudi Arabia. It includes the descriptive statistics for all participants of the study, explanation of model formation and analysis, which includes the result of the measurement model and the structural model assessments. The last section includes the result of structural path coefficients for all relationships in the model to test the theoretical hypothesis.

4.5.1 Descriptive Statistics For All Participants

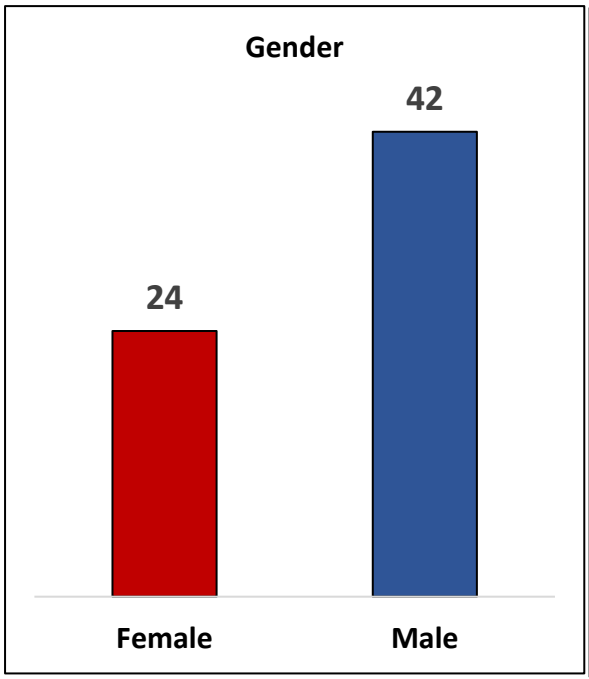


Figure 4.4 MI Gender

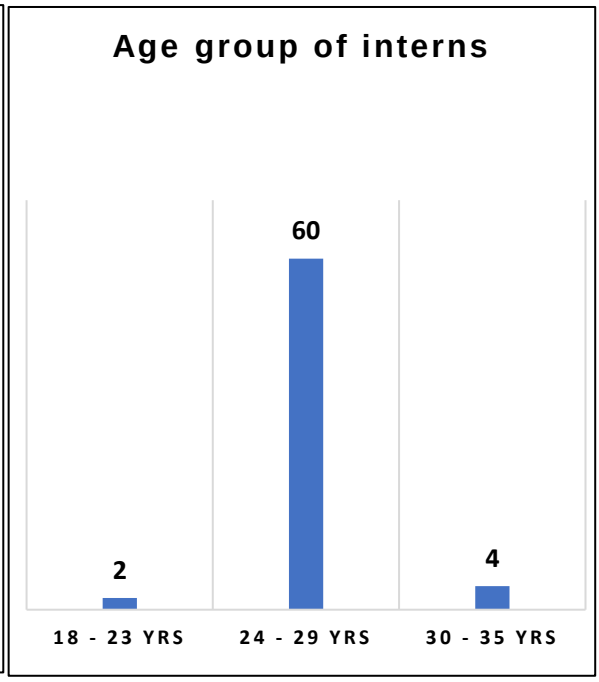


Figure 4.5 MI Age group

Figure 4.4 shows that the gender of the majority (N = 66) was male (64%), and the rest of the study MI respondents were female (36%) as shown in Figure 4.4 and 90% of the respondents were between 24 and 29 years old, as shown in Figure 4.5. Fifty of the MI respondents (76%) spent at least 2 hours or less daily accessing the internet in the hospital as shown in Figure 4.7. According to Figure 4.6, all MI respondents had access to Electronic Medical Record systems (EMRs), and approximately 77% of them spent at least 1 to 4 hours per day using these systems to review or modify patient medical records. Thirty-four of the MIs (51%) reported that they had been informed of the information security measures and policies set by the hospital administration to protect the privacy and confidentiality of patient information, while the rest of those junior doctors reported that they were not informed at all. Figure 4.8 shows that forty

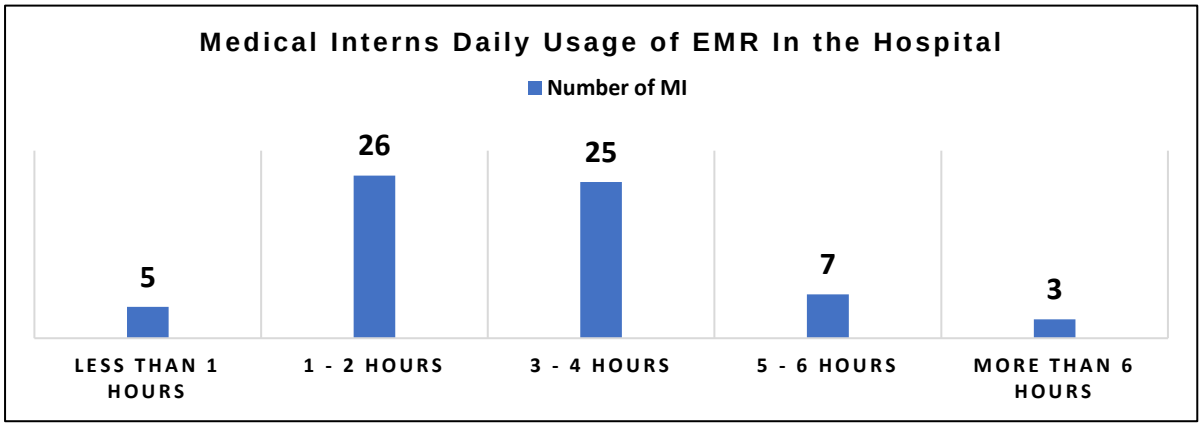


Figure 4.6 MI Daily EMR Usage In The Hospital

(60%) out of the 66 interns were partially or completely unaware of the security measures set out by the hospital's information security policies. At the same time, 32 MI's reported that they were partially or completely aware of the existence of those information security policies. (see appendices A.3 for descriptive statistics in tabulation format).

4.5.2 Model Formation and Analysis

We applied Structural Equation Modelling (SEM) using the partial least square (PLS) technique and SmartPLS (Version 2.0) to test the theoretical research model and the relationship among its latent constructs [253]. We chose this SEM method rather than regression because of the SEM's ability to deal with multidimensional second-order constructs (Neutralisation) as presented in Figure 4.2. Also, PLS is useful when a larger sample is unavailable [1][254]. In addition, the PLS-SEM is a powerful tool in predictive and exploratory studies because its algorithm ability to test and analyse both the measurement model (the relationship between the

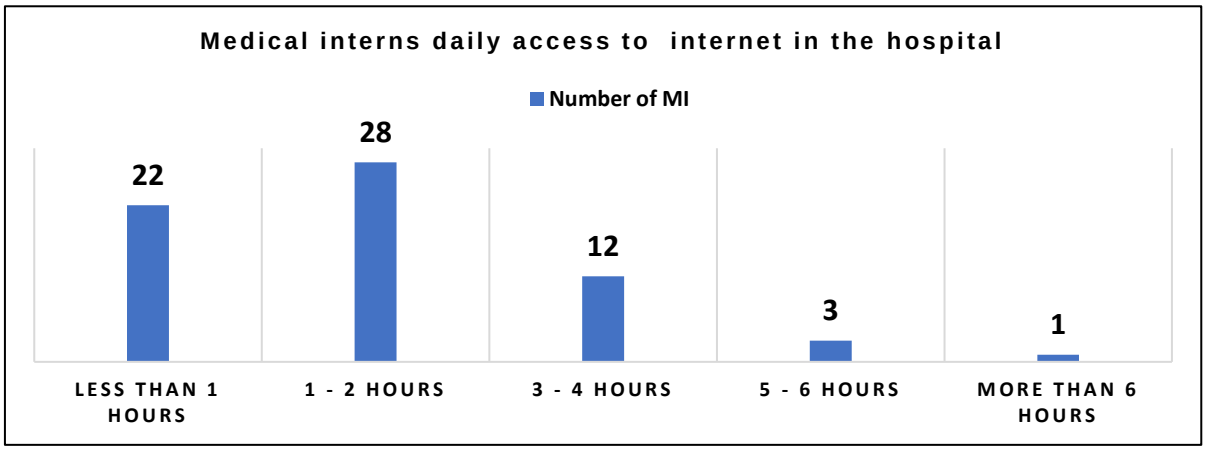


Figure 4.7 MI Internet Daily Usage

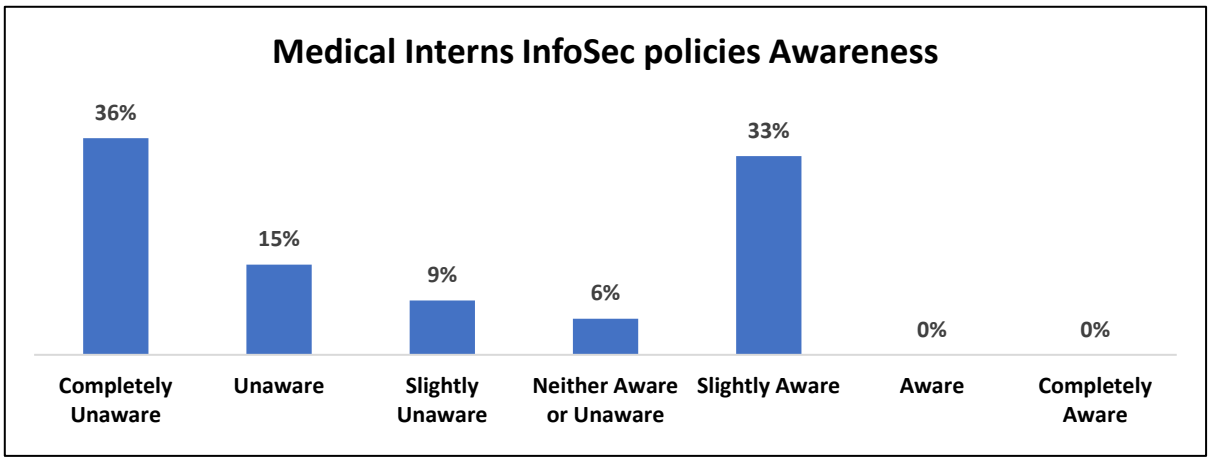


Figure 4.8 MI General Information Security Awareness

constructs and their indicators) and structural model (the relationship among the constructs) [1][253][254] simultaneously. Also, as illustrated in Figure 4.2, we are using six sub-constructs to measure neutralisation, and these reflective sub-constructs are measured with three indicator variables for each. Then we have a path from Neutralisation to MI intention to violate information security policies and patient privacy.

We applied PLS-SEM approach for model evaluation. In the following sections we used PLS-SEM to evaluate: (1) the measurement model, which is referred as outer model in the PLS-SEM) and (2) the path (structural) model, which is known as Inner model in the PLS-SEM.

4.5.2.4 Assessment of The Measurement Model

Assessment of the measurement model, also known as Outer model in the PLS-SEM, aims to ensure that the models' indicators and constructs are statistically reliable and valid. Thus, to establish model reliability, we needed to check Internal Consistency Reliability, and Indicator Reliability of the measurement items. In addition, both Convergent Validity (CV) and Discriminant Validity (DV) are essential tests to check model validity for evaluating the indicators of the measurement model. Figure 4.9 shows the required statistical tests to analyse the measurement model for validity and reliability.

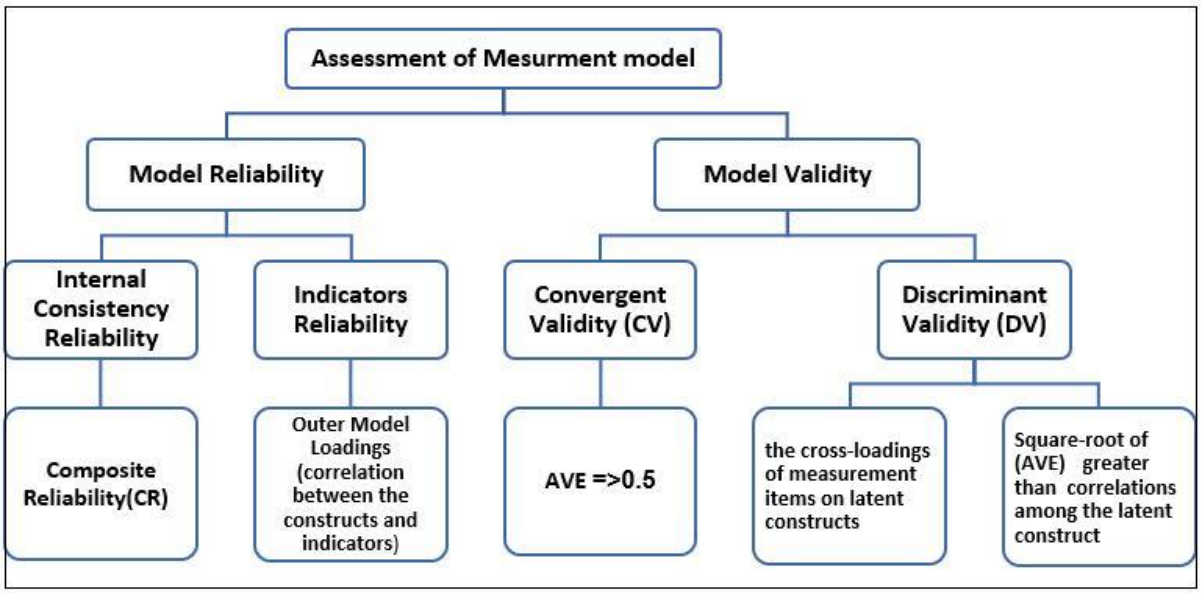


Figure 4.9 Assessment of Measurement Model Reliability And Validity Required Tests.

- **Model Reliability**

According to Taber [255], internal consistency reliability is a synonym term for reliability, and both terms can be used interchangeably. Internal consistency reliability of the collected data via the questionnaires' questions meaning that "all of the items (indicators) are measuring the same

phenomenon and if the value for one of the measures changes, then all of the other values should move in the same direction [p.634]"[244]. According to Hair et al. [254] and Bagozzi and Yi [256], the Composite Reliability (CR) is an essential measure of the internal consistency reliability for the indicators set, and the PLS-SEM use it as an alternative to the traditional Cronbach alpha's. The justification behind this is that the PLS-SEM prioritise indicators based on their individual variation of the outer loading, which means that the indicators' loadings on their respective construct are not equal. Therefore, it is applicable in our case as the indicators (survey questions) were redundant and have been rephrased to reflect the same theoretical construct [254]. It is recommended that the CR score should be equal to a cut off of 0.7 or greater (0.6 or higher for exploratory studies)[256]. Table 4.1 shows that the CR score for each of the constructs in the model was at least 0.8 and above, demonstrating that each item in the model was appropriate to represent all related constructs, hence satisfying the criteria for establishing internal consistency reliability for the measurement model.

Another benchmark for model reliability is to check Indicator Reliability, which refers to the extent that a construct can explain the variation in its individual indicators as they share a common characteristic of their associated construct [254]. Sarstedt et al.[257] suggested that indicators outer loadings should be greater or equal to 0.5. Indicators outer loadings, as shown in Figure 4.10, are represented as a set of arrows pointed from each of neutralisations' six reflective sub-constructs to their associate indicators. They demonstrate the correlation between the constructs (latent variable) and their indicators (items). The value of each indicator loading (arrow) defines a distinct contribution on its associate theoretical construct [254]. In our model, all the indicators' outer loadings are acceptable (all are greater than threshold 0.70), and thus, they are statistically significant for all the reflective six sub-constructs, as shown in Table 4.1.

An additional test of indicator reliability put forward by Hulland [258] is that the square root of each of the indicators outer loading should be 0.708 or higher (0.6 or higher for exploratory). The principle behind this specific value is that each construct should hold 50% (0.5) or higher to exceed the potential measurement errors of the variation in each of its indicators. Thus, the square root of (0.708) is equal to 0.5, which implies that any indicator has outer loading on its construct less than the threshold (0.708) and does not meet the minimum acceptable level of outer loadings to be considered as a reliable indicator [254]. For instance, all outer loadings for the reflective construct denial of injury are higher than the threshold (0.708). Here, the indicator outer loading (DoI1) is (0.966). Thus, it has the highest indicator reliability with the value of 0.934, which is the square root of its outer loading $(0.966)^2$. Also, the outer loading of the

indicator (DoI2) is (0.948). Therefore, it has the smallest indicator reliability among denial of injury indicators with a value of 0.899 $(0.948)^2$. All the three indicators outer loadings for denial of injury holed the minimum acceptable level of indicator reliability. Based on result, all indicators of the reflective first order constructs hold acceptable level of outer loadings and meet the criteria for indicator reliability. Thus, our results satisfy *internal consistency* and *indicator reliability*, which indicates that the measurement model is statistically reliable.

- **Model Validity**

To establish model validity, two tests were performed to measure Convergent Validity (CV) and Discriminant Validity (DV). According to Gefen and Straub [259], convergent validity is exhibited when all the measurement items load significantly with a higher t-statistic on its associate theoretical construct more than other constructs in the model. We used Fornell and Larcker's criteria [260] for checking Convergent Validity, which asserts that the Average Variance Extracted (AVE) score should be equal to or exceed 0.5. The AVE is "the degree to which a latent construct explains the variance of its indicators" [254]. Thus, if the AVE value for a construct is less than (0.5), it indicates that the construct explains less than 50% of its measurement items variance. Therefore, the measurement items' remaining error exceeds the variance explained by the given construct [254]. Our results show that all AVEs for first-order constructs' values are higher than 0.5 and hence satisfy this criterion.

Discriminant Validity (DV) is the extent to which a given construct distinctly represents a specific phenomenon as its associated measures uniquely differentiate it from other constructs in the model [244]. Gefen and Straub [259] stated that "each measurement item correlates weakly with all other constructs except for the one to which it is theoretically associated". Thus, two statistical tests were conducted to address the DV, as shown in Figure 4.9. The first one is Fornell and Larcker's criterion [260] that suggests that each constructs' square root of AVE should be larger than the correlations among all the constructs in the model. The right half of Table 4.1 is shown the square root of AVE for each construct, where the values in the diagonal boldface are presented. It reveals that AVE's square root value for each construct in the diagonal boldface is higher than all other cross-correlations numbers on the same row or same column. For example, AVE's square root value for Condemnation of Condemners' construct is found to be (0.931). This value is higher than the correlation value on its left side (0.797) and all other values in the same column. As a result, it satisfies the first criterion analysis for establishing DV.

The second test for assessing the DV is by analysing the indicators outer loadings. This test suggests that each indicator loading on its theoretical construct should be much higher than its cross-loading on other constructs [261][254]. For instance, as shown in Table 4.2, the indicators outer loadings (AHL1=0.932, AHL2 = 0.966, and AHL3=0.945) respectively on their associated construct appeal of higher loyalty are more significant than their cross-loading on other constructs on the same row and column. Thus, those indicators AHL1, AHL2 and AHL3 satisfy the DV criteria for model validity as these indicators outer loadings are higher in their theoretical construct appeal of higher loyalty. According to Tables 4.1 and 4.2, our analysis validates CV and DV criteria, and hence the measurement model holds all the validity requirements. According to Hair et al.[254], the measurement model reliability and validity confirmation are prerequisites for proceeding and conducting a structural model evaluation. As a result, Tables 4.1 and 4.2 show that we have enough evidence that the measurement model holds all the reliability and validity criteria, allowing us to proceed and conduct the structural model assessment.

Table 4.1 Results of Measurements Model – Convergent Validity

							Correlation of constructs scores with the Square Root of AVE (The values in the diagonal boldface are the square root of AVE)					
Construct	**Items (Indicators)**	**outer Loadings**	**Indicators Reliability (i.e., square of outer loadings)**	**T - Statistic**	**AVE**	**CR**	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**
Appeal of Higher Loyalty (1)	**AHL1**	0.932	0.869	37.01	0.897	0.963	**0.947**					
	AHL2	0.966	0.934	104.58								
	AHL3	0.945	0.894	57.33								
Condemn of Condemners (2)	**Coc1**	0.897	0.777	31.9	0.866	0.951	0.797	**0.931**				
	Coc2	0.957	0.913	95.18								
	Coc3	0.938	0.878	59.96								
Denial of Injury (3)	**DoI1**	0.968	0.934	11.25	0.915	0.97	0.783	0.72	**0.957**			
	DoI2	0.948	0.899	84.97								
	DoI3	0.955	0.913	16.34								
Defence of Necessity (4)	**DoN1**	0.81	0.657	142.88	0.744	0.897	0.81	0.742	0.784	**0.862**		
	DoN2	0.925	0.856	49.3								
	DoN3	0.849	0.721	58.31								
Denial of Responsibility (5)	**DoR1**	0.92	0.847	47.46	0.796	0.921	0.642	0.599	0.593	0.656	**0.892**	
	DoR2	0.884	0.785	26.23								
	DoR3	0.873	0.757	24.25								
Metaphor of Ledger (6)	**MoL1**	0.927	0.86	49.61	0.912	0.969	0.734	0.721	0.689	0.728	0.583	**0.955**
	MoL2	0.967	0.936	86.93								
	MoL3	0.971	0.943	129.85								

Note: Composite Reliability (CR), and Average Valance Extracted (AVE)

Table 4.2 Discriminant Validity and Cross Loadings

Indicators\Constructs	Appeal Of higher Loyalties	Condemnation of the Condemners	Denial of Injury	Defence of necessity	Denial of Responsibility	Metaphor of the Ledger
AHL1	**0.932**	0.751	0.699	0.664	0.555	0.604
AHL2	**0.966**	0.82	0.787	0.759	0.623	0.754
AHL3	**0.945**	0.697	0.812	0.798	0.644	0.721
Coc1	0.641	**0.897**	0.621	0.613	0.587	0.6
Coc2	0.776	**0.957**	0.713	0.707	0.561	0.684
Coc3	0.803	**0.938**	0.734	0.688	0.53	0.726
Doi1	0.78	0.705	**0.968**	0.757	0.611	0.656
Doi2	0.766	0.674	**0.948**	0.773	0.662	0.75
Doi3	0.78	0.753	**0.955**	0.721	0.612	0.685
Don1	0.615	0.568	0.571	**0.81**	0.291	0.508
Don2	0.76	0.773	0.796	**0.925**	0.587	0.651
Don3	0.642	0.5	0.64	**0.849**	0.627	0.615
Dor1	0.611	0.562	0.59	0.541	**0.92**	0.567
Dor2	0.578	0.475	0.576	0.521	**0.884**	0.461
Dor3	0.528	0.564	0.592	0.527	**0.873**	0.53
Mol1	0.69	0.704	0.693	0.7	0.526	**0.927**
Mol2	0.7	0.677	0.683	0.609	0.533	**0.967**
Mol3	0.714	0.687	0.712	0.665	0.611	**0.971**

Note: Appeal of higher Loyalties (AHL), Condemnation of the Condemners (CoC), Denial of Injury (DoI), Defence of necessity (DoN), Denial of Responsibility (DoR) and Metaphor of the Ledger (MoL)

4.1.1.1 Structural Model Evaluation (Inner model)

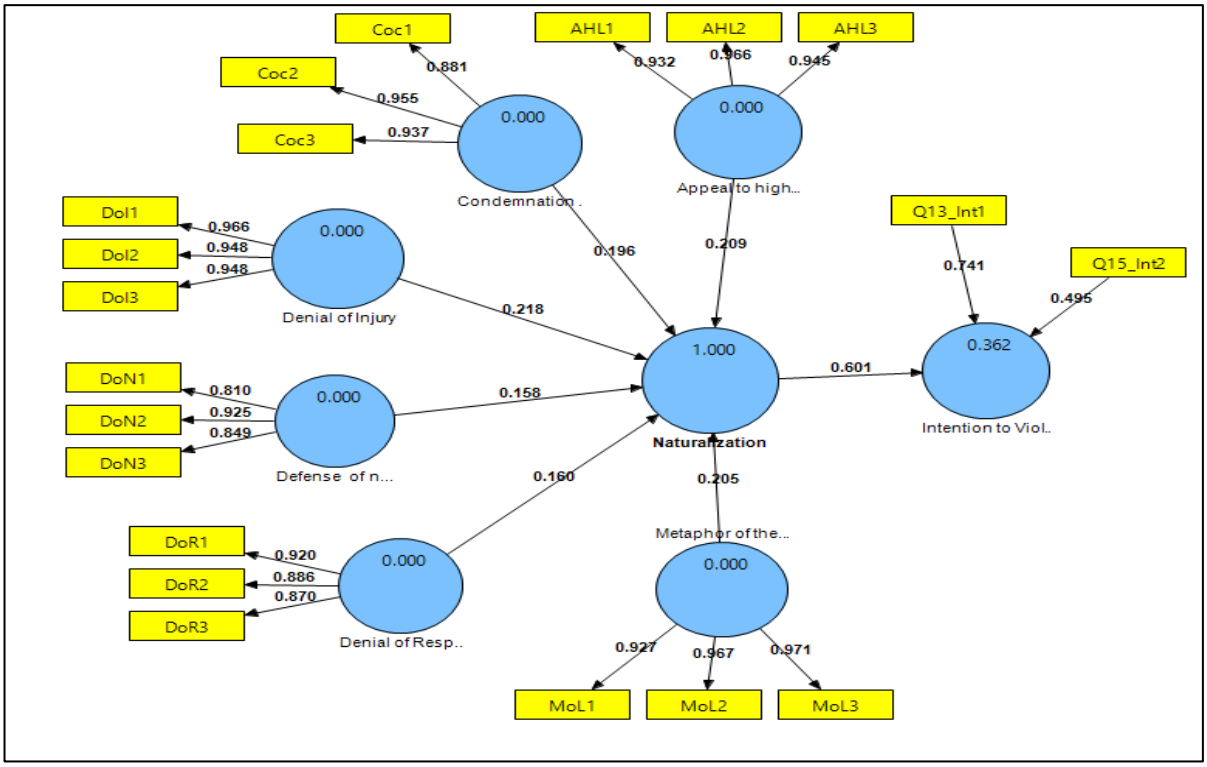


Figure 4.10 Assessment of The Structural Model Using Smart PLS

The assessment of the structural model comprises of two important tests to evaluate the inner model: 1) the capability of the inner model to serve the prediction goals, and 2) the relationship

between the inner model constructs (path coefficients) [254]. The inner model represents the relationships between the independent (exogenous) and dependent (endogenous) constructs in the model, as shown in Figure 4.10. It is represented by the arrow's path pointed outward between the exogenous constructs and the endogenous constructs. Figure 4.10 demonstrates that all the first-order constructs are exogenous constructs as each of them has an arrow path directing outward to another construct without any arrow pointing to them. In contrast, the endogenous variable is a construct that receives at least one path arrow from the exogenous construct loading into it, such as the construct in the model. We checked the explanation amount of target endogenous variable variance (MI intention to violate hospital information security policies) in the structural model by evaluating the coefficient of determination, known as R-Square (R^2). The evaluation of the coefficients of determination (R^2) is useful for any study model with prediction purposes, which is applicable in our model as the aim is to predict the influence/relationship of the neutralisation and its associate constructs on the MI intention to violate the hospital InfoSec policies. Statistically, the value of the R^2 should be higher than the suggested threshold 0.2 [254], and Chin [262] indicated that if the R^2 above 0.67 is considered high. In contrast, values ranging from 0.33 to 0.67 are moderate, whereas values between 0.19 to 0.33 are weak, and any R square values less than 0.19 are unacceptable. As illustrated in Figure 4.10, our analysis indicated that the value of the $R^2 = 0.374$, which is acceptable and is considered moderate. According to Figure 4.10, the R^2 value means that second-order construct Neutralisations explains 37.5 % variance of MI's intention to violate hospitals' information security policies and patient privacy.

4.5.3 Results Of the Hypotheses and Theoretical Model Testing

The row data collected for the study are based on an ordinal scale. Thus none of the parametric tests, such as the linear regression, are applicable to evaluate significance (t-value) to test the hypotheses significance path. In contrast, the PLS-SEM algorithm can deal with data that are not normally distributed to perform non-parametric tests by means of a bootstrapping procedure to compute the hypothesised structural relationship's significance. Thus, the PLS-SEM can calculate standard bootstrap errors (t-statistics) as an alternative to estimate the t-values for the significance evaluation of the structural model [263].

Bootstrapping procedure is "a resampling technique that draws a large number of subsamples from the original data (with replacement) and estimates models for each subsample. It is used to determine standard errors of coefficient estimates to assess the coefficient's statistical significance without relying on distributional assumptions."[254]. In our case, we applied bootstrapping procedure with a large number of sub-samples (800 samples) taken with

replacement from the original sample to determine the bootstrap standard errors T-statistics. A path coefficient is significant if T-statistics are larger than the critical value 1.96 at 5% level of significance for a two-tailed test [254]. Consequently, T-statistics were calculated for each path coefficient. As Table 4.3 shows, the results demonstrate that all the structural path coefficients are significant. Finally, the hypothesised path relationship between neutralisation and intention to violate information security policies is statistically significant, as shown in Table 4.3.

Table 4.3 Path Coefficient Using Bootstrapping

Relationship	**Path Coefficient T-Statistics**
Appeal to Higher Loyalties → Neutralisation	24.209989
Condemnation of the Condemners → Neutralisation	19.682286
Defence of necessity → Neutralisation	17.412531
Denial of Injury → Neutralisation	20.17556
Denial of Responsibility → Neutralisation	16.604468
Metaphor of the Ledger → Neutralisation	19.482651
Neutralisation → Neutralisation	8.462579

We have further analysed the sub-constructs effect on both neutralisation and intention to violate information security policies constructs. The results, as shown in Table 4.4, indicate that the denial of injury technique has the highest contribution towards making the neutralisation construct (19.08%), followed by appeal to higher loyalties (18.23%), metaphor of the ledger (17.94%), condemnation of the condemners (17.18%), and denial of responsibility. Relatively, the defence of necessity technique has the least contribution for making these constructs by 13.85%.

In addition to the neutralisation theory, we tested the control variables of age, gender, and level of MI privacy and security policies awareness towards the "MI intention to violate information security policies" construct. We included these variables in our model to test whether these variables exert a significant effect on the final dependent construct. After the analysis, as shown in Figure 4.11, we found that age and gender have no significant impact on intention, while the level of privacy and security awareness has a weak negative impact. Separately, we analysed the realism of the scenarios and found them significantly correlated with the intention ($r = 0.28$, $P < 0.005$). Figure 4.11 illustrates the model testing result for all constructs in the study.

Table 4.4 The Effect of Neutralisation Sub-Constructs On Both Neutralisation And Intention To Violate Constructs

Construct	Relationships	Total Effect	Normalised %	Overall Rank
MI Intention to violate Hospital information security policies and patient privacy	Appeal to higher Loyalties → Intention to Violate	0.129449	18.23%	2
	Condemnation of the Condemners → Intention to Violate	0.122021	17.18%	4
	Defence of Necessity → Intention to Violate	0.097461	13.72%	6
	Denial of Injury → Intention to Violate	0.13548	19.08%	1
	Denial of Responsibility → Intention to Violate	0.098378	13.85%	5
	Metaphor of the Ledger → Intention to Violate	0.12739	17.94%	3
Neutralisation	Appeal to higher Loyalties →Neutralisation	0.208726	18.23%	2
	Condemnation of the Condemners → Neutralisation	0.196593	17.17%	4
	Defence of necessity → Neutralisation	0.157242	13.74%	6
	Denial of Injury → Neutralisation	0.218429	19.08%	1
	Denial of Responsibility → Neutralisation	0.158349	13.83%	5
	Metaphor of the Ledger → Neutralisation	0.205431	17.95%	3

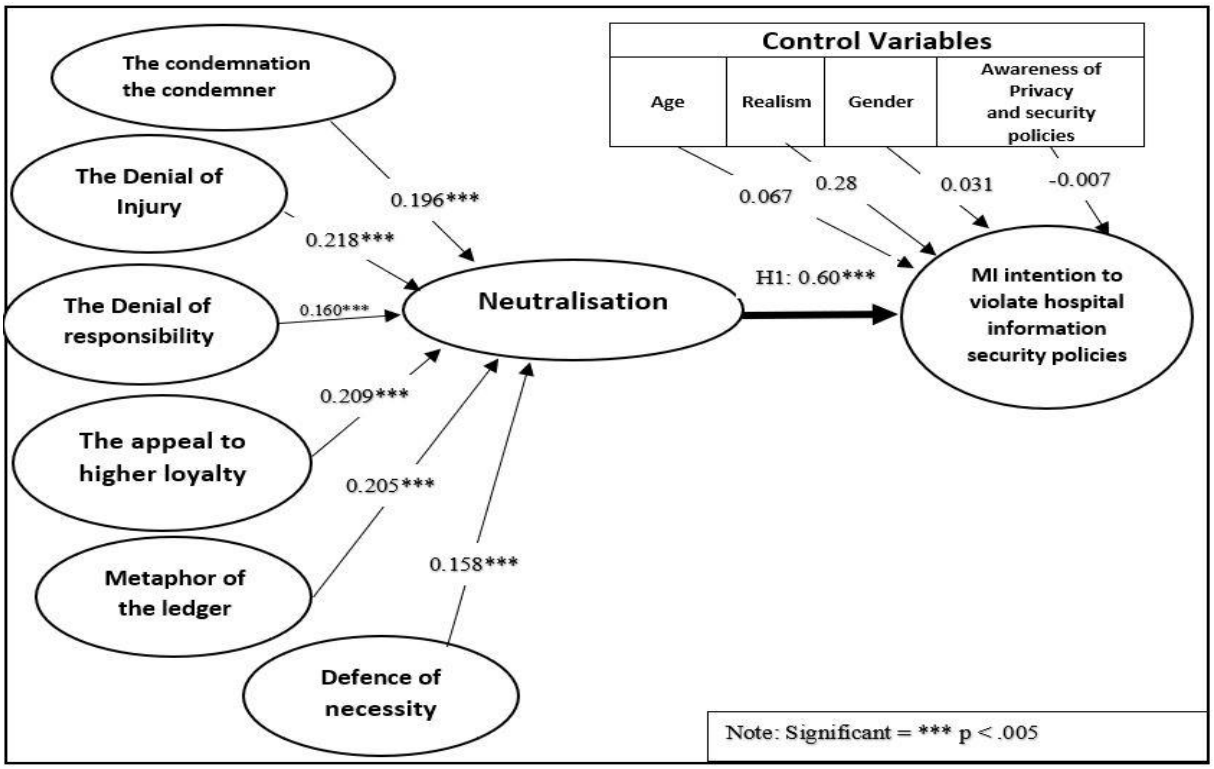


Figure 4.11Study Model Depicting the PLS Results

4.6 Discussion and limitations

Our research is consistent with the extant neutralisation studies in the field of criminology that examined hate crimes [264] , deer poaching [265], and corporate crimes [176]. Our results show that neutralisation can explain behaviour that deviates from expected norms and can be used as a predictor (or explanatory variable) of the intention of medical interns to violate hospital security policies that secure patient privacy in the health care industry. We defined intention as "an indicator of a motivational state that exists just before the commission of an act. We think of it as a measured reflection of a predisposition to commit [an act]" [266] rather than a direct proxy to the actual behaviour. In this study, we investigated Sykes and Matza's [34] techniques: (1) denial of injury, (2) condemnation of condemners, (3) denial of responsibility, and (4) appeal to higher loyalties, in addition to (5) the defence of necessity [37] and (6) metaphor of the ledger [35].

Some neutralisation studies have suggested that certain techniques have a more powerful influence on individual behaviour than others in specific contexts [151][125]. Our results reveal new insight into how medical staff employs justifications to engage in undesirable behaviour (violation) that might abuse information security policies and breach patient privacy. Consistent with the findings of Kim et al. [187] and Siponen et al. [267], the results reveal that all of the six techniques contribute significantly to the non-compliance intention of medical interns and therefore add risks to the hospital security and privacy efforts to protect patient sensitive information. This study also extends the IS literature beyond North America and Europe [31] and investigates the influence of the neutralisation techniques on privacy protection efforts within the healthcare environment in the Middle East countries, specifically Saudi Arabia.

Another important factor is that 90% of the respondents are between 23 and 29 years old and have less than a year's work experience. These factors could explain why MIs justify their non-compliant behaviour without considering the consequences by denying injury and appealing to higher loyalties. Also, poor awareness of privacy and information security policies among these junior doctors (more than 50% in our study) adds a more significant burden on hospital administration to protect IT infrastructure and resources from insiders. Thus, these employees may unintentionally commit an action that could lead to a malicious information technology breach or leakage of sensitive patient information [78]. The adoption of deterrence mechanisms such as informal or formal sanctions may not be sufficient to protect the privacy of patient information from abuse when neutralisation techniques are present [1] [151].

We suggest future research should investigate the usefulness of privacy awareness strategies and educational programs (seminars, face-to-face interactions, web-based courses, and so forth) in prohibiting employees from justifying their behaviour to violate information security policies. By doing so, the health care organisations can add an extra layer of protection based on the psychological perspective alongside their technical controls. Thus, they can reduce internal actors from abusing their IT privileges to breach patient privacy.

The findings in this chapter reveal that it is essential for medical schools in Saudi Arabia to continuously update their current curriculum to increase their student awareness of several emerging topics in health care information security. They can improve their students' understanding of IT security threats, controls and solutions, the importance of patient privacy and confidentiality, and the benefits and consequences of compliance or non-compliance with information security policies, laws, and IT best practices.

This study was conducted with three main limitations that should be recognised. First, the study sample was specific and relatively small (66 medical trainees) and was collected from only four academic hospitals in Saudi Arabia, so caution must be exercised when generalising the results of this study. Thus, future research may consider a qualitative approach and a larger sample. Second, all survey respondents were Saudi citizens, and thus the influence of national cultural differences must be taken into account when generalising our results. Finally, this study is based on the self-reported approach that demonstrated MI's intent to violate information security policies that protect patient information privacy across assumed scenarios. Thus, the realism degree of the scenario significantly influenced the intention rather than the actual behaviour.

4.7 Summary

Health care employee adherences to privacy and related information security policies can safeguard their organisations from many financial and non-financial losses. In this context, we studied the behavioural intention of medical interns to breach the hospital privacy policies through the leans of the theory of Neutralisation in Saudi Arabia. Our result in this study revealed that neutralisation techniques are a critical factor influencing the intentions of medical interns to violate information security policies. The study also highlights the granular level contribution for controlling the neutralisation construct, the defence of necessity, denial of injury, metaphor of ledger, condemnation of condemners, denial of responsibility, and appeal to higher loyalties, which contribute to the justifications used by the interns. Thereby, policymakers and security experts in the health care industry need to reconsider security policies

to ensure that they mitigate the impact of neutralisation techniques. Furthermore, our contribution sheds light on the importance of healthcare organisations developing security and privacy awareness programs that consider neutralisation techniques to protect their information security infrastructure and patient privacy.

The following chapter will extend this study by investigating the environmental factors that motivate medical practitioners to evoke neutralisation techniques and violate information security policies.

Chapter 5 : Investigating The Environmental Factors That Influence Individuals Behavioural Justifications in Hospitals.

Phase 1	Phase 2	Phase 3	Phase 4
Determine the role of Neutralisation techniques to predict medical practitioner intention to violate InfoSec policies. A quantitative study using a questionnaire in Saudi Arabia.	Investigate the motivations of medical practitioners to evoke neutralisation techniques to justify InfoSec violations. A qualitative study using semi-structured interviews in a Saudi Arabian hospital.	Enhancing InfoSec policies effectiveness against neutralisation techniques via the engagement end-user perception. An action research study using focus groups and pre and post questionnaires in the UK, University of Glasgow.	Enhancing InfoSec policies effectiveness against neutralisation techniques via the engagement end-user perception. An action research study using focus groups and pre and post questionnaires in a Saudi Arabian Hospital.

Figure 5.1 Phase Two of The Research Study

The previous chapter found that the defence of necessity, denial of injury, the metaphor of the ledger, condemnation of condemners, denial of responsibility and appeal to higher loyalties identified by Neutralisation theory have a significant impact on the study participants (medical interns) behavioural intention to violate hospital information security policies and breach patient privacy. This chapter introduces the second phase of the research study, as presented in Figure 5.1.

This stage argues that human behaviour plays a vital role in the success of the organisation's efforts to protect IT assets. In spite of a growing awareness that implementing technological measures alone cannot guarantee information security protection without considering human behaviour, the question remains as to why healthcare industry employees violate the InfoSec policies of their organisations and breach patient privacy. This stage of the research uses semi-structured interviews to explore the level of compliance of medical trainees with the hospital's InfoSec policies and explore their motives and related justifications for violating these policies. The thesis concentrates on the same healthcare organisation during phases 2 and 4 to learn more about their InfoSec noncompliance behaviour and the proposed intervention's effectiveness.

This chapter contains the following sections: Section 5.1 provides a brief introduction to information policies and employee behaviour regarding those policies. Section 5.2 explains the purpose of conducting this qualitative study in a healthcare context. Section 5.3 presents the study's methodology, data collection, sampling method, and data analysis process. Sections 5.4 and 5.5 present data analysis and the results of the study, while Section 5.6 discusses the implications of those results. Finally, Section 5.7 presents the chapter summary.

5.1 Introduction

Technical security controls have been widely recommended as a traditional strategy in the information systems literature to mitigate information security threats and vulnerabilities and counter network and data breaches [1][2]. However, as previously explained in Chapter 2, several IS scholars acknowledge that technical controls alone cannot guarantee the integrity, availability, and confidentiality of the organisation's information without encouraging employees to achieve the organisation's information security objectives [122][1][268]. Consequently, many laws and regulations require organisations, particularly in the healthcare field, to manage their data and IT assets by mainly adopting security standards and best practices to confront security threats and vulnerabilities.

An essential approach for organisations to comply with security standards such as NIST and ISO 27001 and ensure a consistent security level is to develop and disseminate information policies [28]. These security policies present instructions and guidance as to the desired employee behaviours and actions to ensure the protection of an organisations IT resources. According to Wall et al. [3] and Safa et al. [6], an employee's failure to comply with information security policies, whether inadvertently or intentionally, is a critical risk factor in security incidents that lead to data leaks and privacy breaches.

Many information security scholars call for more studies to explore the motivations behind individuals' intentions to violate or comply with ISPs [269][137][261]. Thus, instead of focusing on the effects or the consequences of an individual's ISP violations or compliance with organisational ISPs, there is a need to take a step back to understand the environmental factors that contribute to their security behaviour.

5.2 Purpose of The Study

Implementing information security policies can enhance an organisation's compliance with its IT regulations and standards. However, assessing the interaction between these policies and their audience reveals low effectiveness because security incidents keep happening, particularly

in healthcare organisations [21]. The information security experts in organisations need to increase their understanding of the activities of their employees in their work environment and the impact of security policies on employees' daily tasks. Usually, employee noncompliance with information security policies is attributed to a lack of InfoSec awareness. Hence, many organisations attempt to increase their employees' awareness via security training campaigns or security awareness programs [270]. However, few organisations have made a reasonable effort to assess the degree to which security policies fit the actual work duties of their employees [271]. Poor alignment between the security requirements and the work tasks can lead the employee to violate the policy and justify such behaviour.

This study extends previously published work related to information security compliance and neutralisation theory [11][12][13], which found that individuals sometimes adopt cognitive justifications to overcome feelings of shame or guilt when they commit or consider committing InfoSec policy violation. This study extends previous work by investigating the influence of environmental factors on medical practitioners' motivations to free themselves from a hospital's InfoSec policy compliance obligations. Thus, this chapter will investigate the drivers (antecedents) of healthcare practitioners' behavioural justifications to violate the security policies that safeguard patient privacy. In particular, we try to answer the following research question:

RQ2: ***What drives behavioural justification among medical practitioners to violate information security policies in healthcare organisations?***

5.3 Study Methodology

The study conducted a series of semi-structured interviews to collect data and applied a thematic analysis approach [194] to obtain answers to the research question. The research environment was one of the largest academic hospitals in Saudi Arabia. It has more than 1400 beds in various specialities and several medical facilities and research centres around the country. Every year, the hospital admits more than 30,000 patients and provides health care services to more than 250,000 registered patients. In the hospital, medical interns (MIs) have access to the hospital's IT systems. MI's privileges include accessing the hospital health care systems (HIS), which allows them to enter, view, and edit patients' medical records. Over the last few years, the hospital has been faced with several security incidents from internal sources. This noncompliance with the hospital's InfoSec policies was the primary cause of internal security incidents, such as unauthorised access to the hospital's HIS, the use of infected USB devices, and the exchange of photos that include medical records via social media applications.

We sought to investigate whether interns used neutralisation techniques to justify their InfoSec violations and the reasoning behind their justifications. Therefore, the Engineering Ethics Committee of the College of Science and Engineering at the University of Glasgow agreed to conduct this study in one of the hospitals in Saudi Arabia under the approval number (300190026). (Appendices B.1 Consent form and B.2 Participant sheets).

5.3.1 Data Collection

The interview protocol had three main parts. During the first part, the author explained the study's purpose and asked the interviewee to sign the consent form for participation. The second part consisted of general questions to collect demographics, job descriptions, and information security backgrounds. The last part of the interview had five sets of semi-structured interview questions adopted from the IS literature [272] to explore in-depth the information security environment in the hospital in five major areas: (1) InfoSec policy development, (2) implementation, (3) enforcement, (4) awareness and training, and (5) incident reporting (Appendix B.3 for the list of interview questions). Specifically, we investigated the impact of the existing security policies on health practitioners' daily practices and activities. Also, we explored the drivers of neutralisation technique adoption.

The semi-structured interviews were conducted in English with the medical interns and the IT department managers and employees. The initial questions were revised after the first interview to include more probing questions, which were used to explore the reactions of interns to InfoSec policies. The questions were open-ended to encourage participants to freely reveal their ideas, opinions, and experience with information security requirements and procedures. In total, we interviewed twenty-eight participants, including twenty MIs and eight IT staff members. Each interview lasted between 45 and 60 minutes. The schedule of the interviews was based on the participants' convenient time and location. All the interviews were conducted within the hospital clinics, offices, or meeting rooms. All the interviewees' names, work titles, and related identifiable information were anonymised. Figure 5.3 presents the interview data procedures.

At the beginning of each interview, the author asked for permission to audio-record the interview. A total of 26 participants agreed to audio-record their answers during the interview, while two participants preferred the interviewer take notes. All interviews were conducted face-to-face in the hospital and were carried out by the author between September 2018 and November 2019.

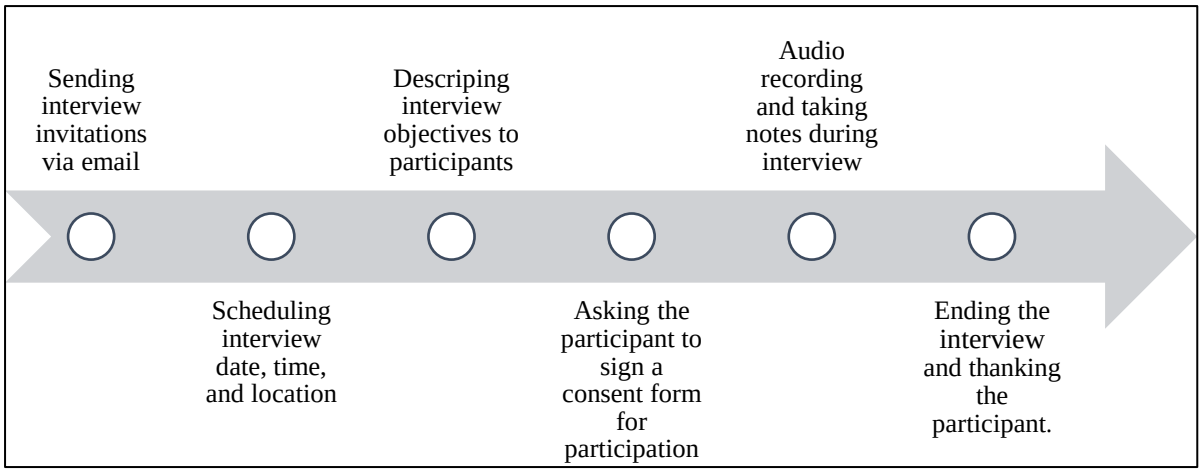


Figure 5.2 Interview Data Collection Procedures

5.3.2 Sampling Method

We used the snowball sampling method to reach medical interns working full-time in the hospital. This process is known as "chain-referral sampling"; it continues until the researcher determines that the study sample is sufficient [226]. Our interviews aimed to gain a closer look at the interaction between medical interns as a group and information security policies and procedures during their daily activities to evaluate their overall security practices and awareness. We focused on investigating the environmental factors that influence medical interns to violate information security policies and controls that safeguard patient privacy, leading them to justify such behaviour via neutralisation techniques. We repeated the data collection and analysis process until we reached the point of saturation [225], where no more themes emerged from the interviews and the findings repeated across the participants.

5.3.3 Participants

- **IT participants:** We were interested in interviewing IT managers and staff who interact directly with health practitioners in meetings or discussions. These IT professionals were primarily responsible for developing, implementing, and enforcing information security policies and controls to protect the hospital's IT infrastructure and patient privacy. The hospital's IT department's Associate Executive Director kindly assisted us by appointing a coordinator to help us communicate, select, and invite participation by distributing interview invitations to the targeted employees via the hospital's official emails. We interviewed six IT managers and two IT personnel with at least seven years of experience in the information security field and who hold a bachelor's degree in computer science or similar qualifications. These IT experts deal with IT security requirements daily, and we

needed their help to understand their current information security practices and solutions to improve overall hospital security, specifically security non-compliance due to human behaviour. We aimed to obtain the following:

- To understand their perceptions of current InfoSec policy violations in the hospital and the IT department's efforts to mitigate the conflict between IT security needs and the healthcare practitioners' work performances.
- To assess the IT department's awareness of the medical interns' justifications (neutralisation techniques) leading to InfoSec violations and the existence of any mitigation solutions for such behaviour.

- **Medical Interns (MI):** The medical school in the hospital assigned a coordinator who introduced the study objectives, details, ethical considerations (participant sheet and consent form), and contact information to all the medical interns via the hospital official email. We recruited twenty medical interns (9 females and 11 males) in the hospital via a snowball sampling method [273], which allowed us to reach this group of participants most efficiently. It is based on the initial participants' social network to identify and communicate with the rest of the target sample members [231]. Thus, each of the initial participants forwarded the interview invitations to their other colleagues. Due to the close relationship between MI during academic study and work, this sampling approach was practical for reaching and attracting the MI more than official emails from the university. However, medical interns perform many clinical duties and share several working characteristics with consultants and other senior practitioners. The only difference relates to the EMR privileges because the IT department limits the MI privileges in the EMR system to access and view patients' medical records without conducting any medical order. For example, a medical intern cannot request a lab test or issue a prescription to a patient. At the same time, a consultant can make any potential medical orders required for medical services. Thus, the researcher does not expect significant differences in the result of the study if the interviews include only senior practitioners.

5.4 Data Analysis

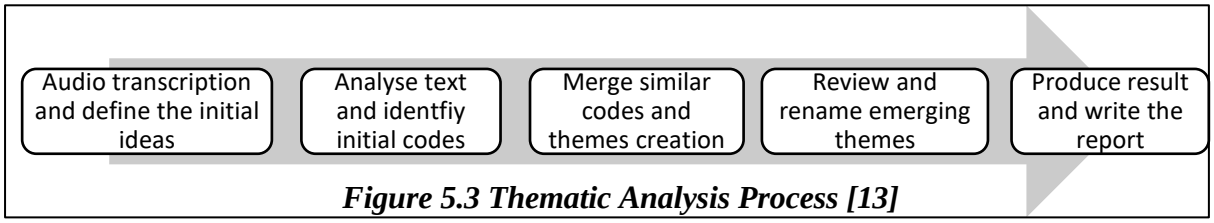


Figure 5.3 Thematic Analysis Process [13]

The audio files and transcripts of the interviews were analysed as advised by Braun and Clarke [194] (Figure 5.3). Thematic analysis (TA) is a "method for identifying, analysing and reporting patterns (themes) within data. It minimally organises and describes your data set in (rich) detail"[194]. It encourages a better understanding of the context and ensures consistent organising of the dataset. The TA is a flexible approach that searches for common patterns within a qualitative data set and systematically underlines repeated themes (patterns), each of which are assigned codes. Each code is a short piece or segment of the row data in the textual interview transcript that identifies an aspect of the phenomena of interest [274]. Thus, we identified all the relative passages in the responses that revealed security policy violations and the corresponding neutralisation techniques used to justify such violations, as well as the possible reasons that led the interns to invoke such techniques. The data relating to neutralisation techniques and InfoSec policies' violations were analysed thematically using a deductive approach to code any relevant information in the text excerpt. Afterwards, all the codes that reflected a similar concept were grouped to create meaningful themes. QSR NVivo Version 12 was used to conduct the thematic analysis and facilitate the management of the audio files, documents, and textual transcripts.

5.5 Interviews Results

Using a thematic analysis, we identified several social, emotional, and organisational factors that motivated the medical interns to justify their violations of hospital InfoSec policies. The new codes and themes from the interview are presented in Figure 5.4.

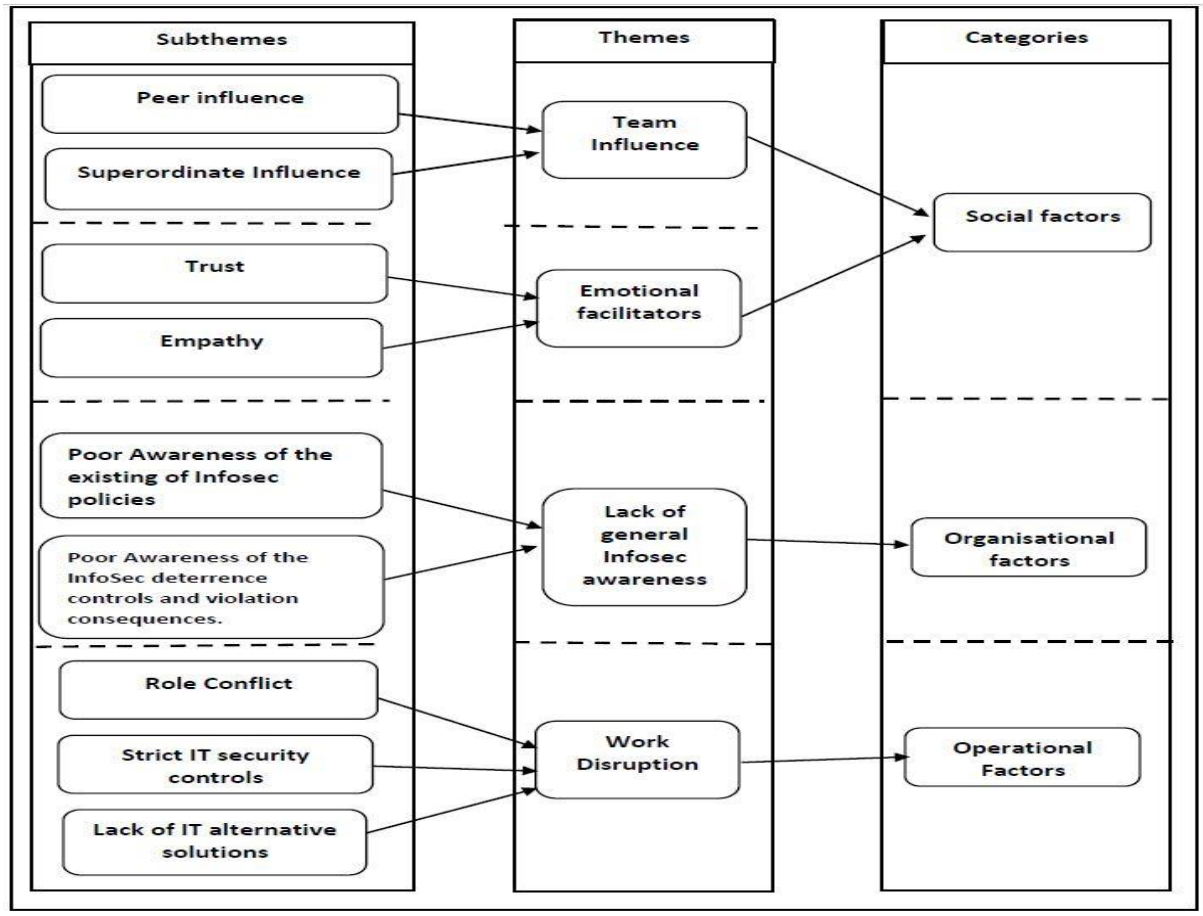


Figure 5.4 Interview Themes and Sub-Themes

5.5.1 Social Factors and Neutralisation Techniques

We found that the social factors influencing the MIs to use neutralisation techniques fell into two main themes, each consisting of four subthemes: the two main themes were: (1) Team Influence (peer and superordinate influence) and Emotional Facilitators (trust and empathy). Table 5.1 provides a general summary of the interrelationship of the social factors, security threats, and neutralisation techniques. The horizontal orange row indicates four major security

threats that we identified and that interns confirmed using at least one of them during their daily tasks. The vertical beige and orange columns show the identified interview themes and subthemes, highlighting a tendency to evoke justifications for these security threats.

For example, violating the security standard of "sharing patient screen images of HIS via social media applications" was justified by believing the expected harm of such behaviour was minimal because they shared those images only with their team members, whom they viewed as trusted parties, which would not harm patient safety or information privacy. Hence, they reduced the security risk of a data breach by sharing these screenshots via social media. Also, under the influence of the team, Table 5.1 shows that some MIs share their HIS account with other peers because some of them started their internships without an active HIS account. In such a case, interns reported that they temporarily shared the HIS account with a colleague until that person obtained an account and provided various justifications, such as the sharing was some kind of support (appeal of higher loyalty), a necessary action to maintain work performance (Defence of necessity), a common norm among the team (everybody else is doing

Table 5.1 Mapping Social Factors to InfoSec policies threats via Neutralisation techniques.

Mapping social factors to InfoSec threat Via Neutralisation Techniques			**Information security Threats**			
			Share images of the HIS patient screen via Social media Apps	**Share HIS account/ password**	**Leave PC unlocked**	**Bring External Internet router**
Social Factors	**Team Influence**	**Peer Influence**	•Denial of Injury	• Appeal to Higher Loyalties •Défense of Necessity •Everybody else is doing it •Denial of Injury	•Everybody else is doing it	•Everybody else is doing it
		Superordinate Influence	•Denial of Injury •Défense of Convenience	• Denial of Responsibility •Défense of necessity •Everybody else is doing it •Denial of Injury	•Défense of Convenience	
	Emotional facilitators	**Trust**	•Denial of Injury •Défense of Necessity	•Denial of Injury •Défense of Necessity • Appeal to Higher Loyalty		
		Empathy		• Appeal to Higher Loyalties •Défense of Necessity		

it), or a harmless act (denial of injury). Empathy, for example, was identified as an emotional facilitator and emerged as a driver of MI's behavioural justifications (appeal to higher loyalty

and Defence of necessity) when an intern shares an account with peers. The following subsections explain the relationship between security threats, social factors, and neutralisation techniques in more detail.

5.5.1.5 Peer Influence

Sutherland et al.[275] stated that an "individual learns not only the techniques of committing the crime, no matter how complex or simple, but he/she learns specific motives, drives, rationalisations and attitude" [p. 75]. Medical interns are a subgroup of health care members working to improve their practical healthcare skills. Those interns share many individual characteristics such as age, medical experience, and educational background, making their relationships close and their approaches to solving work issues similar. They are practising their medical duties in healthcare teams during their rotation in clinics. Consequently, they get most of the training benefits from interacting with peers and practitioners such as medical residents, consultants, or nurses. At this stage in their careers, these medical interns are working hard to prove their medical competencies to get a residency position after the internship year ends. This passion motivates them to focus on medical training practices and duties more than on InfoSec policies. Several MIs indicated that accomplishing their medical responsibilities were the top of their priorities and more important than complying with the security policies.

MI-4: "*We take things based on the priorities, and we don't consider the information security a priority for us, and unfortunately, it might be considered the least of the priorities between our colleagues."*

Other interns stated the importance of their medical duties compared with the hospital's concerns to comply with the security policies:

MI-13: "*To be honest, we don't focus on this topic; we focus more on patient treatment management. For us, as medical interns, we focus more on the medical skills and how to make a diagnosis or read its result, and so on. But the information security topics are not a priority for us."*

Many interns indicated that the healthcare team norms impact their behaviour by imitating the noncompliance actions of their colleagues. Thus, they inherit and commit the same security policies violations and tend to evoke the same justifications.

MI-11: "*To be honest, I have not read a security policy document, but I have heard that from my colleagues about what I can do or not, all of my knowledge are pieces of advice that are coming from people in the practices."*

MI-16 *"You see what people around you are doing, and you will do the same. Even though the person supposed to know the wrong or right by himself."*

The majority of the interns indicated that they heavily rely on each other to overcome their daily practice issues, primarily related to such security controls as limited Internet access.

MI-20: "*When I face a situation, I read about it or inquire from someone who knows, such as my colleagues. For instance, I need to print files in the hospital, so I ask my colleagues how to do that. Therefore, each one of them gave me his experience to solve my issue with controls here because we have limited Internet access, and we cannot open Gmail, Hotmail, etc. So, I get benefits from their feedback and experiences."*

MI-24: "M*y colleagues teach me how to do certain things such as email attachments, but no one from the IT."*

Therefore, the social impact of their peers forms their perceptions as they imitate each other's actions and use the same justifications for their non-compliant behaviour with the hospital information security policies. We identified four neutralisation techniques that the interns tend to adopt to justify their non-compliance behaviour: Defence of Necessity, Appeal of a Higher Loyalty. Everybody else is doing it, and Denial of Injury.

5.5.1.5.1 Defence of Necessity

Many of the interns (N=16) indicated that they tend to adopt this technique to justify their behaviour when sharing their passwords or healthcare system accounts with peers. The common belief among those participants who used this technique was that complying with the information security policies was not an urgent matter for them. Thus, their attention focused on their primary mission to provide treatment to the patients and deal with the clinic workload. Some of the medical interns argued that they shared the password with a colleague when it was necessary. In their opinion, being a part of a medical team required them to collaborate with their peers, sometimes forcing them to perform some acts regardless of compliance with the information security policies and procedures. They stated that if a medical intern in the team found it difficult to access their account, this might impact the team performance. In this situation, the argument was the necessity to improve the work performance, which was justifiable from their perspective to share HIS password or account. As respondents reported:

MI-16: "*.... in the end, you have to see the big picture, there is a patient interest might disrupt or delay because one of the medical team members does not have access."*
MI-9: "*If someone refuses to give you the password of his account, this will delay the work because I would wait until he comes and opens his account to complete the order. It would delay work performance."*

5.5.1.5.2 Appeal to Higher Loyalty

Participants who used this technique tend to "legitimise deviant behaviour when a non-conventional social bond creates more immediate and pressing demands than one consistent with conventional society" [10]. This technique was the second most common neutralisation technique reported by the medical interns (N=15). The primary InfoSec policy violation that evoked "Appeal to Higher Loyalties" was sharing the password or the HIS account between those medical interns who had just started their internship and had not yet received access to the hospital health care system.

The medical interns who indicated support for this technique felt that they were taking the right action. They were providing a kind of professional help to other peers to accomplish the duties of the team without disruption. In particular, several respondents argued that they were sharing the password or the HIS account, neutralising their behaviour by referring to the greater good. For instance, some of the medical interns justified their sharing password behaviour as support and help, especially during the internship period where any disruption of the work performance might impact the MI training and evaluation.

MI-17: " *I think it is a kind of that we need to get the work done. It is professional support."*

MI-13: "*To be honest, here we have this kind of behaviour that we like to help people sometimes more than what is supposed to be. So, this is considered a sort of help in our culture*."

5.5.1.5.3 Everybody Else Is Doing It

This technique refers to the impression that the damaging behaviour is typical of the group, so there was no need to feel guilty or ashamed. Six interns (N=6) justified their behaviour by saying, "every one of my peers is doing it," especially when they left their PCs without logging out, shared a password or account with others, or used an external Internet router to bypass Internet access restrictions. The participants argued that their behaviour was normal because other team members were commonly doing the same thing.

MI-9: "*I mean, the behaviours of others because the majority are doing this thing; we will do the same, even if it is wrong."*

They argued their behaviour was acceptable and referred to the fact that many of their colleagues commonly shared passwords, left their PCs unlocked, or utilised their own Internet routers:

MI-14: "*I see the majority share their passwords, for example, and leave their account open without logging out. Sometimes, I leave my account open to let my colleague work on the same medical note*."

MI-7: "*I have to use my mobile Internet router, which I bring with me. Actually, a lot of my colleagues do the same, not only me."*

The interns stated that no one got caught or punished for performing such actions, which implied that the IT department really did not consider these acts to be information security breaches. They referred to the existence or absence of InfoSec violation sanctions to evaluate which of the typical behaviours in their peer groups was considered a violation of the hospital's InfoSec policies. The MIs evoked this technique based on their observation of the social context that influenced their decision-making processes to decide which behaviour was acceptable:

MI-22: "*Also, as I have mentioned, everybody is doing it, from the physicians to the nurses and residents. Everyone leaves their account open, and there is no specific punishment."*

5.5.1.5.4 Denial of Injury

Those individuals who use this technique claim that the outcomes of their deviant behaviour are harmless and show no concern about the expected consequences of non-compliant behaviour [34]. More than half of the medical interns (N=13) referred to this neutralisation technique when they revealed some of their daily practices. The MIs who adopted this technique refused to acknowledge the fact that sending photos from patients' medical records via a social media application or sharing the password or the HIS account with a colleague could cause any harm or breach to the patient privacy or the hospital information security policies.

Three main arguments behind these noncompliance actions were offered. The first argument was that the medical interns' HIS accounts had limited privileges, as they could only access the patient records to write patients' diagnoses without any authority to issue any medical orders, such as prescribing medicines or ordering lab tests. The MI judgment prioritised the physical harm that could impact the patients' health due to incorrect medical orders. Thus, they ignored the information security risks that could originate from sharing passwords or the HIS accounts. They reported that:

MI-10: "*Technically speaking, my account is limited as a medical intern, and we only can write notes. So, she is going to write notes like me, and she cannot do something major. There is no security breach in my perspective because we both know what the limit is*."

MI-7: "*We are not allowed as medical interns to make medical orders, so I'm not worried that the person with who I share my account will do something that can harm me in future or the patient."*

The second argument offered a type of risk comparison as a way to decrease the injury that could occur from sharing their HIS account password. Denial of injury via reducing the impact and magnitude of the risk was compared to other team members in a higher position of authority and wider HIS privileges, such as consultants. They thought that sharing passwords would have only a small negative impact on the hospital's security. This thought affected the interns reporting of any observed violations of InfoSec policies. An MI explained:

MI-15: "*.....what I'm saying is I know there is something that is important, but what interns think themselves is that they are only interns. So, whatever threats that come from us, no one is going to consider it. Threats coming from medical interns are less impact than threats coming from CIOs or the heads of department*."

The last argument was that taking a picture and sharing it via social media applications was habitual behaviour among their peers. They believed that the recipient of a medical record or photo was a trusted person who would use them for medical purposes and keep it confidential. Some medical interns confirmed that they had sent or received an image of a patient's records—such as lab results or x-ray—where the patient's information was clear. In comparison, others revealed that they had taken some precautions to protect patient confidentiality by hiding the patient's personal information. This action was explained by different medical interns as follows:

MI-5: "*Today, one of my colleagues took a picture of a screen, and all the information was there except the patient MRN. However, there were some cases where the MRN and the patient name have appeared."*

MI-11: "*I have seen a lot of my colleagues directly take a picture of the X-ray without considering covering the patient information located at the corner. They usually say we share it with our colleagues, so they don't hide such information*."

MI-16*: "Yes, I have sent some pictures for discussion with my medical team but without the name or MRN of the patient."*

5.5.1.6 Superordinate Influence

During their monthly rotation between clinics at the hospital, the medical intern's central role was learning from their superordinate's medical expertise, such as the consultants or the residents, working closely with them to provide healthcare services. The interaction between the medical interns and their medical supervisors was considered an essential part of the learning

process during the internship. In addition, the consultant had the power to offer a residency position to any interns who successfully met the practical training criteria. Thus, the superordinate's decision was a significant part of the evaluation process to get a residency position later in the hospital.

Most of the interns reported that their superordinate influenced their behaviour both directly and indirectly in several situations related to the information security policies. Therefore, this impacted their tendencies to evoke several neutralisation techniques as a part of the decision-making process to deal with their superordinates' requests, even if these orders could lead to an InfoSec violation. In addition, the medical interns offered evidence of several neutralisation techniques to justify their InfoSec policy violations, showing how the influence of their superordinate had motivated them directly and indirectly to justify their abuse of the password and the HIS access policies. Four main neutralisation techniques were identified that were attributed to the superordinate's influence: Denial of Responsibility, Denial of Injury, Defence of Necessity, and the Appeal to Higher Loyalties.

5.5.1.6.1 Denial Of Responsibility

Many interns cited their superordinates' or seniors' authority as an essential factor that helped them to accomplish their aims, do their duties, and gain better practical experience in the medical field. This close relationship might extend to informing InfoSec related perceptions, as an MI indicated:

MI-12: "*I observe what my seniors are doing regarding information security, and I do whatever they do*."

The MIs revealed that accountability towards the hospital's InfoSec policies was influenced by the orders issued by their superordinates, such as consultants or residents. Therefore, they shifted the responsibility of any potential harm of the violations to their superordinate.

MI-6: "*It is coming from the attending consultant, so usually people obey the person in authority even if it is the wrong action, they will follow it*."

Furthermore, they explained that their work environment was complex and required full collaboration from the entire medical team to deliver health care services to patients. So, being a trainee in a medical team made it difficult for any MI to refuse carrying out an order from a consultant, even if the request could lead to an InfoSec policy violation or privacy breach. For instance, an MI explained his fears of the consequences of a refusal on his application for a residency position when a consultant asked him to share his account with another intern:

MI-4: "*for seeking approval or recommendation from the supervisors. They might see you as part of the team, which increases your chance of acceptance as a resident. I will lose if I refuse to do it. If I say no because I want to follow the security rules, they might abuse you and isolate you from the team.*"

Besides, a few MIs felt that their superordinates used their authority to violate the InfoSec policies by delegating more responsibilities to the MIs than expected by hospital management. For instance, some of the consultants shared their HIS accounts with MIs to allow them to perform extra work duties, such as issuing medical orders. Thus, the interns were forced to exceed their designated privileges to use the healthcare information system, which is considered a violation of the hospital's HIS access control policy.

MI-7: "*Some physicians abuse the medical interns by letting them do more duties, so if medical interns said that his/her account privileges are limited in order to conduct the requested order, the physician simply responded by saying, that's ok, take my account or password and conduct the order."*

5.5.1.6.2 Denial of Injury

Several MIs reported using this neutralisation technique to justify their superordinates' impact on the hospital's InfoSec policy noncompliance. For example, some of the MIs explained their use of the consultant's HIS account if the medical orders included only routine and straightforward procedures. In this case, the expected consequences of any wrong order on patient health were minor, regardless of the fact that the behaviour itself was a violation of an InfoSec policy:

MI-5: *"It depends on the case. If the MI will use the consultant's account for minor orders or routine medical procedures like ordering Paracetamol, X-rays, or blood tests, the harm of these procedures, such as increasing the dose or asking for the X-ray, is trivial."*

Two of the IT managers acknowledged the occurrence of this kind of violation and described the consultants' perceptions as harmless when sharing their HIS account credentials with others:

ITE1: "*They say nobody will be harmed if I share my password, and I will simply change the password if there is a risk."*

ITD1: "*Also, the fact is that the consultant and the resident don't see sharing their password as an issue for the email and [the health care system], and they think it is ok.*"

Other interns invoked this position to justify their behaviour of sending a photo of the HIS screen to their superordinate's. They referred to this as a practical way of getting things done, enhancing convenience, and not wasting a superordinate time. They sometimes received a

physician's request to send a photo of a patient's record, and sometimes they sent the picture to the physician's mobile seeking treatment advice. In fact, the MIs blamed the IT department's technical restrictions, such as the lack of remote access, as being responsible for this type of security violation. Instead of verbally reading the patient's information over the phone or asking the consultant to come to the clinic to read the patient's diagnoses or lab results, they took photos of the patients' screen records and sent them to the consultants' mobiles. They argued that they sent the photo to the consultants' phone directly, as requested, and since only two people had the images, the chances that these sensitive pictures would be leaked would be reduced.

MI-17: "*I understand there is a risk, but what is the probability of it happening? Your example has a very minimal chance of occurring."*

M-11: *"Most of the people in the medical field are looking for practicality rather than professionalism. They prefer practicality, so instead of asking the physician to come to the hospital, they take a picture and send him the findings and the lab results to let him give his diagnoses or treatment plan. So, they think it is more practical, and it is better to get the job done."*

Several MIs stated that their superordinate's had sent photos containing patient records to their mobiles via social media applications, where the identifiable patient information was clearly shown. Sometimes a superordinate took the pictures of the medical record screen for unique cases and shared them with the entire team as part of the learning and educational process.

MI-9: "*It is the wrong behaviour, but they do it a lot. The seniors might also take a picture of the patient information that includes the name and the MRN and share it with other colleagues or medical interns; they don't care about hiding this information that much. They do that for many reasons, such as teaching or discussion. That frequently occurs, even it is a wrong action."*

5.5.1.6.3 Defence of Necessity

Several medical interns reported no other choice for them to perform their work efficiently with their superordinate's without sharing a password or the HIS account. Some of the medical interns reported situations where their superordinate's shared their HIS account with them temporarily. For instance, they indicated that some of them had started their internship program without an active account for the HIS, which conflicted with their training objectives to gain practical experience, and a significant part of it contained writing documentation for patients' cases. Thus, the consultant or the resident would share their HIS account or password until the IT department activated the intern's HIS account.

MI-09: *"The problem is that many medical interns don't receive their healthcare system account from the IT department before they start the program... If the resident realised that the Medical Intern don't have an account, in this case, the resident usually shares his/her health care system account with the medical intern and log out when he/she finished writing the notes."*

Another group of medical interns reported that a large number of the patients in some clinics created a significant burden on the physicians, which forced them to seek all the team's possible help to provide healthcare services and reduce treatment time. If physicians spent most of their time handling routine duties such as writing medical notes rather than examining the patients, treatment time would be increased, therefore reducing the overall clinic performance to provide health care services to all patients in an acceptable time.

M-18: "*If the doctor strictly complies with security policies and does not share his account, I think that may impact his work performance. Thus, we solve the security issue here, but other problems will appear and can impact the medical services for the patients, such as delay of treatment, and so on. In the end, when the doctor stops dealing with the patient in order to do some simple tasks that can impact the doctor's performance in the clinic."*

An IT security employee confirmed the justification when she was asked why she shared the password of her HIS account with other medical team members:

ITE1*: "The doctors' justification for such behaviour, which I have heard that from them, here I will quote the doctors speech 'I'm here in the clinic for patient treatment, and I have many patients to look after their health, so I don't have time to access the system each time to make medical orders or procedures such as lab orders or pharmacy orders and so on. Thus, this is a part of the nurse duties as she is an assistant to the doctors; therefore, I give her my password to conduct such orders while I'm doing my primary work to meet and examine the patients' end of quote."*

Also, several interns justified the impact of their superordinate's behaviours on them, which could increase their tendency in violating the password policy. They indicated the importance of sharing passwords, especially when the consultant was too busy dealing with patients all day or dealing with many urgent cases that might increase the risk of making mistakes in HIS orders. Their argument was that the consultant benefits from sharing their HIS account credentials in this situation, and this justified the InfoSec policy non-compliance behaviour.

MI-12: "*Sometimes when a person is tired, he is more likely to make mistakes because he maybe does the medical orders quickly to finish the work. So, I think it is justifiable in this situation if the doctor gives other colleagues, a trusted person, his account to overcome the tiredness risk."*

5.5.2 Emotional Facilitators and Neutralisation Techniques:

We identified the two emotional facilitators of trust and empathy that influence the social context and the MI tendency to evoke behavioural justifications when violating information security policies. These emotional factors function more as facilitators of the social factors' pressure described in the previous section. Figure 5.4 illustrates these themes and subthemes. Also, Table 5.1 provides the relationship between emotional facilitators and security threats and the associated neutralisation techniques.

5.5.2.1 Trust

Healthcare practitioners work collaboratively to provide essential services to patients. Providing such service requires a high level of interaction between team members. Thus, trust was identified by all the medical interns as an essential social factor that facilitated the interaction and contributed positively to work performance in a complex environment like a hospital. According to Peikari et al. [276], in a healthcare context, if trust is lost between the medical practitioners for any reason, it might impact work productivity and the perceived importance of information security. We found that sharing the HIS accounts, passwords, and mobile photos of the patient records were common violations among both the medical interns and their superordinate's.

These InfoSec policy violations were influenced by the social impact of trust, which motivated them to justify their undesirable behaviour. Thus, the medical interns rely on trust as a way to reduce violation consequences (denial of injury), to provide or receive colleagues support (appeal of higher loyalty), and to overcome work obstacles (defence of necessity). The majority of the medical interns reported that being a part of the same team was an essential part of gaining their trust and sharing their HIS account with another colleague. Thus, they revealed the same

answer when we asked them the following question: "If your colleague is working with you for the first time, would you share with him/her your account?

MI-17: *" Honestly, if this medical intern is within my team, and we are dealing with the same patients, I will consider giving him my account because he has some issue in his account. But if this colleague is working in a different clinic, I will not consider giving him my account.....it is based on the trust."*

Also, other medical interns said that the trust level impacted their decision to share or not share their account with others:

MI-17: *"Yes, the trust level can change my decision. But this trust is not easy to get."*

Some of the medical interns (N=14) denied that their violations of the organisation's security policies caused injury and stated that their colleagues were trustworthy as a justification for this. Thus, they would not misuse their account in a way that could cause any harm to the account owner or the patient health or privacy:

MI-24: *"They also think that it is not that a big deal with someone I trust; they might think like this way."*

MI-10: *"Here, we are talking about a different thing. I will not give my password to a colleague or friend, only someone I can trust. This is an essential part; I must trust she will treat my account as her own account."*

Other interns justified sharing passwords by the necessity of doing such behaviour due to the time and workload pressure.

MI-14: *"In the perfect situation NO. Under the pressure of the situation, you don't sometimes know how to deal with it. The resident might think this medical intern is in my team and a colleague as well as I know her personally, and I trust her, so it is ok to share the password."*

One of the IT managers expressed a consultant's perception of doing such behaviour:

ITD2: *"Some of them [the consultants]think that by sharing their account with other colleagues, they can accelerate the work performance. Also, the level of trust between the peers motivates them to share their passwords."*

5.5.2.2 Empathy

Empathy is a difficult concept that researchers have found challenging to measure and define [16]. This study adopts the definition of Sutherland et al. [15] that empathy refers to " the degree to which individual notices and is concerned about the needs or concerns of others." In health care such as nursing, empathy is an essential skill required to improve patient care and the

nursing students' professional development [25]. The Association of American Medical Colleges listed the development of empathy as one of a medical student's educational objectives. Researchers in health care found that the use of empathic behaviour in inpatient care by a healthcare practitioner can improve patient treatment compliance and satisfaction and reduce patient anxiety, stress, and depression [16][43].

Empathy is presented in this study as the caring behaviour medical interns show toward other team members. Several MI students showed empathic behaviour by caring about their peers and superordinates, which motivated their intention to justify their InfoSec policy violation of sharing their HIS account or passwords. For instance, they showed empathy toward their MI peers when they could not perform their duties because the IT department had not activated their HIS accounts at the beginning of the internship. They argued that a part of the MI training was examining the patients and writing the related medical notes, and if a new intern could not access the HIS/EMR, they would be considered not working by the superordinates and other team members. This, in turn, might impact the intern's final evaluation, which could cost them to lose the chance to get a residency position in the future.

To overcome these concerns, the interns temporally shared their active accounts with their colleagues until their accounts were activated and justified sharing the HIS accounts or passwords as a kind of support—an appeal of a higher loyalty.

MI-13: *"We as MI, the patients are divided between us, so each one of us is responsible for specific patients. So, if I don't give him an account, this is bad for him because he is not working from the clinic perspective; regardless of this is his mistake or another person mistake, he is only watching us without working. So, the first thing I did that for him as a colleague, secondly to keep work continuous."*

Caring for others and providing help or support is essential in a teamwork environment. Thus, several interns stated that following certain InfoSec policies would contradict the basic concept of caring. Thus there was no need to justify the action because it was not wrong, even if the act in question was a security policy violation from the IT perspective. In this situation, the MI adopted a form of "defence of necessity" to justify sharing a password with a colleague, as in the following:

MI-14: *"I don't consider sharing my account with a co-worker who doesn't have an account; as a security breach, personally, I share my password. This is because at the beginning of the internship takes a long time to get an account".*

MI-20: *"To help him, he is stuck and cannot work. So, I try to help him to work and to do that, I have been compelled to give him access to the system via my account, by sharing my account after I open it for him or by giving him the password."*

Furthermore, the empathic feeling prevented the MI from reporting the InfoSec policy violation to the IT department. This is because the caring of other peers reduced their willingness to report the MI violation action as it could cause harmful consequences to their colleagues. Therefore, many interns stated that they preferred to talk to the person who violated the InfoSec policy rather than reporting the incident to any other party.

MI-14: *"I don't know the reporting sequence and what happens after my reporting as well as the result of reporting. For me, I will start by advising him if this is the first time."*

MI-11: *" I will discuss this issue with him personally because if he is a close friend, I will tell him to log out from other accounts, I will say don't share your password, I will discuss that with him personally...I will not consider reporting him."*

Also, a few interns reported that their empathic emotions were motivated by the age difference between them and their consultants. They described some situations where many of the older consultants were struggling when using the HIS, so they spent more time performing simple tasks such as writing a patient treatment plan or diagnosis. A medical intern stated that:

MI-16: *"Usually, the consultants, for instance, are old people, and they might not understand the technology like us. So, a lot of the consultants ask their juniors, such as the residents and the MIs to write patients' diagnoses and make the system's medical orders. This is because the system is complex for them to use, or the consultant is too slow to write in the system. So, they ask the juniors fellow to do these tasks."*

Several MIs also mentioned that some senior consultants viewed rapid technology changes as a challenge, especially in relation to information security. Therefore, MIs felt in certain situations that it would be appropriate to assist the superordinate consultant in overcoming a struggle with technology, even if their activities, such as using the physician's account, could violate InfoSec's policies.

MI-20: *"So, in general, our generation is more adaptive to the technology and has a good experience and awareness how to deal with the information security risks compared to the people who are 15 years older than us. Don't forget that there is personal deference between individuals."*

An IT manager stated that the generational difference when dealing with the information security requirements could play an essential role in the InfoSec policies violations and provided

the password policy as an example to illustrate the difficulties that the consultant experienced with the password requirements.

ITD-3: *"The new generation that born and raised in a time where technology and computer are surrounding them, they will be more adaptive to them and any related changes. But, people from the old school or generations who never or rarely use the computer for specific clinical purposes on daily or weekly basis. Thus, informing him to remember or create several passwords for several services (hospital email, bank, MEd systems and so on) will be too much and a complicated process."*

5.5.3 Organisational Factors and Neutralisation Techniques

The study reveals that the lack of awareness of InfoSec policies influenced the MIs to evoke neutralisation techniques. Two main sub-themes emerged: (1) poor awareness of the existing information security policies; and (2) poor awareness of the consequences of InfoSec violation and corresponding deterrence mechanisms. According to interview recordings, we found that a lack of general awareness of information security influences a tendency to justify violations using condemnation of condemners and denial of responsibility. These two justifications prevail among MIs to justify non-compliance behaviour in four areas: (1) sharing the HIS account/password; (2) sharing images of the HIS screen via social media; (3) leaving their computers unlocked; and (4) bringing in an external internet router. The following sections explain these behavioural motivations that influence the decision to justify security non-compliance.

5.5.3.1 Lack of General Information Security Awareness

In information security literature, organisations strive to protect their information technology assets by developing and implementing strict information security policies and technical controls to enforce InfoSec policy compliance. Despite the large investment made by organisations to implement these solutions, they still experience costly security incidents, and many of them were related to employee misbehaviour. At times employees may decide not to comply with the security policies and act in a way that contradicts the prescribed behaviour in the security policies. From the information security perspective, this is an internal security threat that can cause severe damage. In this situation, some of the security recommendations to address this problem are increasing formal and informal deterrence mechanisms such as punishments [277].

Other security scholars [278][279] attributed this risky behaviour to the employees' inadequate knowledge of the information security policies, which impact their attitude toward compliance.

As a consequence, they advised the security experts to develop and implement effective information security awareness programmes and campaigns, which aimed to motivate the employees to adhere to the prescribed security behaviour and procedures. Also, such an effort could inform the employees about noncompliance consequences on both the organisation's IT infrastructure and individuals.

Several studies illustrated the importance for organisations to develop a comprehensive information security culture within the organisations [280][281][282], where information security education, training, and awareness programs can play a significant role in improving the effectiveness of the technical security mechanisms and an organisation's security efforts [146]. Solms [283] states that improving employee security knowledge and awareness is crucial to developing a proper information security subculture within the organisation's larger culture, where all employees consider the information security goals and concerns during their daily activities [281]. According to Veiga and Eloff [280], information security culture refers to

"*The attitudes, assumptions, beliefs, values and knowledge that employees use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour evident in the artefacts and creations that become part of the way things are done in the organisation to protect its information assets*."

Thus, creating an information security culture in the organisation can shift the employees from being "the weakest link" [284] to be an essential part of the protection of the organisation IT assets. Also, a strong information security culture can reduce the impact of the "Not-knowing, Not-doing" mindset, which refers to the employee's noncompliance with the organisation information security policies and requirements due to their insufficient security knowledge. As a result, they do not perform the right security behaviour and violate security rules [285].

In the context of this study, several medical interns revealed that they were working within a poor information security culture in the hospital. They were unaware of the hospital's information security policies and revealed a lack of knowledge about the security roles and the necessary precautions to protect the hospital IT infrastructure and patient privacy. Thus, this study found that lack of MI awareness of information security policies and practices as a theme that motivates the employee to adopt some of the neutralisation strategies, particularly condemnation of condemners and denial of responsibility to violate the security policies. In particular, the interns showed a lack of general security awareness about (1) the existence of the security policies; (2) the hospital's current deterrence mechanisms and the consequences of their violations of hospital IT assets and patient privacy. Thus, these findings confirm the importance of developing an effective security culture in the hospital.

5.5.3.1.1 Poor Awareness of The Existing Information Security Policies

Proper training is the first step to motivating the employee to comply with security policies. It is illogical to request information security compliance from individuals who are "Not-Knowing" the information security policies and procedures and presume behaviour rather than "Not-Doing" [285]. In this direction, most of the interns reported that they had not received any meaningful security training related to hospital security policies. Many of them rely on their own judgment to improve their information security awareness instead. Many answered the interview question "Have you been given any sort of training related to information security in the hospital?" in the same way:

MI-11: *"Since I started this program three months ago, NO, I have not received any training in security."*

MI-1: *"No, we are really learning by experiments, and everyone who knows something he will tell the others, that's what is happening to be honest."*

MI-20: *"NO, not in medical school or the hospital."*

MI-16: *"Personally, I do not know anything about information security."*

A member of the information security team confirmed that they did not provide any information security training and education sessions to the hospital employees, and specifically to the medical interns. Also, he acknowledged that the MI security awareness was a weak part of the information security efforts in the hospital; he stated that:

ITE1: *"We don't conduct any security training session, only an awareness program...In future, we plan to develop training sessions in Information Security for all medical employees, specifically the medical interns. The medical interns might be the most dangerous people on the hospital IT infrastructure because of their lack of knowledge of the work environment."*

Moreover, a manager in the IT department mentioned that during the hospital's annual orientation for newcomers, the IT department only provided the interns with instructions on how to use HIS functions and applications in the hospital; a small portion of the guidance was linked to InfoSec policies in hospital on simple topics like how to create a secure password.

ITD2: *"Yes, they take the applications training, and the information security is a small part of it. But, we don't have any training in security policies."*

Therefore, the intern's severe lack of awareness about the information security policies motivated them to justify their violation via "condemnation of the condemners" if their InfoSec violations were criticised. This technique refers to individuals attempts to justify their undesirable behaviour by pointing to the people who condemn them to shift the blame and attention away from their own deviant acts [34]. Here, the interns blame the IT department for

not providing them with a proper security awareness program and training. Thus, they implicitly claimed that their lack of awareness of security policies could lead them to violate InfoSec policies inadvertently, so instead, they rely on common sense to assess situations without much consideration for hospital security practices or the consequences of their actions. For example, many interns showed a limited understanding that sharing a password with others would violate the organisation's security policy and relied on their own judgment rather than their awareness of any hospital password policy requirements.

MI-11: *"It is common knowledge, as I know if there is security hacking this will be the harm on the organisation, such as the leakage of patient information will affect patient's privacy; thus I think it is a bad thing from common sense. I don't know that there is a security policy tell me do not do this, or you will be exposed to this risk."*

MI-15: *"Some of the policies that you have mentioned I did it as common sense, such as the log-out. But, I have not read a document about them."*

Many interns also condemned the IT department's efforts and claimed that some of the current technology controls had restricted their daily duties. They argued that it is unfair to comply with security policies and controls without adequate explanation of the expected benefits from compliance and the costs of a breach for both the organisation and the individual. Consequently, they assumed that it was unreasonable to require medical practitioners to comply with security policies that were not clearly publicised. For example, most of the interns criticised certain hospital security policies such as banning USB use, blocking email attachments, limited Internet access, and the absence of remote access to the HIS system. Implementing these strict security policies and controls without proper explanation leads the interns to bypass or circumvent them. Therefore, they condemned the IT department for their poor compliance and linked this to the IT department's insufficient effort to explain the reasons behind these security initiatives and solutions. They explained that as the following:

MI-14: *"I have some questions regarding why I can't open the "hospital HIS" in my house, also, why there is a restriction on the internet access in the hospital, in general, I know this is related to the information security, but I'm not convinced. So, I think we deserve to know the justifications behind those security controls."*

MI-18: *"Sometimes we found the rule that it does not make sense for us. In a way that why would I follow this policy or rule."*

5.5.3.1.2 Poor Awareness of Infosec Policy Violation Consequences and Deterrence Mechanisms

In the IS literature, General Deterrence Theory (GDT) from the criminology field [286] was widely adopted to study the influence of formal and informal sanctions on the rational decision-making of individuals related to computer abuse and InfoSec policy compliance [287][133][288]. In our context, the GDT posits that individuals' decisions toward InfoSec policy compliance are influenced by the perceived certainty of detection and the severity of formal and informal punishments [1]. In particular, individuals evaluate the costs and benefits when they intend to commit undesirable behaviour such as InfoSec violations. Thus, the GDT postulates that individuals' intention toward InfoSec policies noncompliance would be diminished if the risk of being caught is high (certainty of detection) and the consequences of the InfoSec policies violation to the violator is also high (severity of sanctions) [1][289].

Several interns, as previously mentioned, have not received any security training related to the information security policies. Thus, they reported insufficient knowledge of the security enforcement methods that were in place to ensure InfoSec policy compliance. This situation weakened the interns' information security attention as they believed that the hospital had not applied any formal sanctions. They link this conclusion to their observation that no one of their co-workers had been caught and punished because of a security violation. In particular, the perception was that the hospital had not enforced any sanctions related to the InfoSec policies violation because the IT department had only a limited capacity to detect individuals who routinely breach security policies.

The researcher asked the interns several questions to assess their awareness level of the hospital ISP enforcement efforts, which involved questions about their awareness of the hospital security detection mechanisms, ISP risks and violation consequences, and their knowledge of any formal and informal punishments related to ISP violations. The majority of the interns provided similar answers that pointed to inadequate effectiveness of the hospital enforcement methods, as in response to questions like the following: "Would people get reprimanded for not complying with security policies, for example, if somebody was in the habit of not putting the lock on the screen when they left their desk?"

MI-15: *"NO, I have not heard any story that someone getting punished from that. Never. I don't even think that there is any punishment for people who are violating security policies."*

MI-24: *"By taking pictures, they are violating patient privacy and probably the hospital's policy, then what? I don't know what could happen after that and what are the consequences that can impact the physician specifically."*

MI-10: *"I never hear there are punishments for not complying with the security policies. I hear that there are some stories about the punishment that was related to the consequences on patient health. But, I never hear that someone has been caught and punished because of the IT."*

Poor awareness of the ISP security led the interns to rely on their social context (peers and superordinates) to build their knowledge about the accepted behaviours and actions, especially in complex topics like information security. The MIs showed little understanding of the hospital security requirements and stated that they were uncertain about adhering to the InfoSec policies. Therefore, this perception led the interns to blame the IT department for not communicating the hospital's ISP appropriately, which motivated the MI to evoke cognitive rationalisation by denying their responsibilities toward any consequences of the ISP violation. Thus, the interns reported this implicit perception as a criticism of the IT department's IS awareness effort:

MI-7: *"Also, as I have mentioned, everybody is doing it, from the physicians to the nurses and residents. Everyone leaves their account open, and there is no specific punishment."*

MI-20*: "If someone has poor awareness of the risks, they can violate without knowing that. Poor awareness is not their mistake; it is the IT department mistake; they are not given information."*

Moreover, one of the IT managers stated that the interns, like other health care practitioners in the hospital, had little awareness of the threats and associated costs of ISP noncompliance; thus, they underestimated InfoSec policies violation consequences on the personal and organisational levels:

ITH: *"The end-user main problem is they don't know the consequences of the IT risks that resulted from their misbehaviour. For example, how sharing your password can be abused to access your email and send a fake email to your management that includes bad words or an official resignation. Another example is the consequences of abuse of the [hospital HIS] account to violate some patients' privacy. Those end-users who are doing these violations do not realise the level of damage that could happen for them and for the hospital of such misbehaviour."*

5.6 Discussion

This study identifies several organisational and social factors that motivate an employee to deviate from the security requirements prescribed in InfoSec policies and the several justifications used to free themselves from guilt or shame. We outline the drivers of the MI's justifications for noncompliance under two categories: (1) neutralisation and lack of general information security awareness; and (2) neutralisation and work disruption. This section

discusses how all of the above demonstrates its impact on the medical practitioner's daily activities and related security perceptions. Also, this explains how those motivate medical practitioners to justify their InfoSec violation.

5.6.1 Neutralisation and The Lack of General Infosec Awareness

Hospital IT departments confirmed that they had developed their version of information security policies based on a combination of ISO 27001 and NIST. The hospital's IT experts also claimed that all information security policies can be accessed over the hospital's web portal and that every employee can access that portal through the hospital's local network. However, the results reveal that most of the interns who participated in this study had only limited awareness of information security policies and the importance of compliance. The interns reported that they received general training only at the beginning of the internship, which was concentrated on using the HIS system's services, and the only security part of the training was focused on creating a secure password. Consequently, these MIs felt less competent to participate positively in the hospital's efforts to protect IT assets and information privacy. The results also indicated that most interns appeared to be surprised at the existence of security policies and did not understand the benefits and the need for implementing those policies in practice to mitigate the security risks. Thus, they underestimated the consequences of their behaviour and tended to justify their actions by condemning the IT department for not providing adequate security training. So they claimed they were not responsible for any violation because they did not know the rules. Likewise, Zurko and Simon [290] stated that, in the course of their daily tasks, individuals make many decisions and practices that challenge security policies and procedures because they are simply not aware of the consequences of their practices on an organisation's security infrastructure.

The findings indicated that a lack of proper security training and education program leads individuals with less experience to obtain knowledge from their close social group. Thus, they learn from their observation several norms and behaviours. Many interns asserted that they notice what other people are doing and repeat their actions. For instance, they believed that sharing a picture from the HIS medical records via social media was a regular occurrence because their fellow senior physicians were doing it. In this context, the leaders and subordinates were unaware of the desired security behaviour and relevant security objectives, values, and risks.

The findings indicate that hospital management needs to improve MI's general security awareness, which is defined as an "employee's overall knowledge and understanding of potential issues related to information security and their ramification" [13]. Information technology management also needs to understand the impact of the social context (colleagues and superordinates) and how to utilise social factors and emotional facilitators to advocate for general awareness of information security. This approach can be accomplished by ensuring that medical team leaders have an adequate security awareness level and play a supportive role in the organisation's information security efforts to protect healthcare IT assets and their information privacy. The IT department can also enhance its security awareness program by emphasising the importance of security policy compliance to countering cybersecurity threats. Also, it needs to explain how the failure to comply with information security policies is unacceptable behaviour and cannot be justified under any circumstances.

5.6.2 Neutralisation and The Work Disruption

The result of this study reveals that poor awareness and communication of the InfoSec policies within the medical teams' subculture put the MI in a complicated position when these policies disrupt business and reduce productivity. Under the pressure of time, clinic workload, team norms, and leaders' requests, these factors increase the medical practitioner's cognitive burden to deal with security requirements [101] that are not well known in the first place. Thus, this situation causes what is called role-related strain or role conflict [291], which refers to the employee perception that they are "not able to satisfy incompatible demands and expectations of different parties such as managers and customers" [31]. The findings indicate that medical practitioners confront role conflict, which increases their tendency to rationalise their noncompliance behaviour with InfoSec policies.

For example, many interns described a situation when a physician shares their account or password with a medical intern to perform routine duties such as prescribing medication or ordering laboratory tests to enhance work performance. Here, the medical intern's and the physician's priority is to provide and maintain healthcare services. Thus, in the presence of strong emotions such as trust and empathy, they view sharing the password as acceptable behaviour from their perception to satisfy both the workload's demands and teams norms and justify their InfoSec policy violation with different neutralisation techniques like a defence of necessity and contamination of condemners.

According to David [292], developing formal security policies without careful consideration of real practices is useless. Many organisations have implemented a set of excessive security policies and controls following the abstract ideas of "one size fits all " [293] or " just in case" [294], which could lead to the disruption of the employees' primary tasks and add more complexity to meet the productivity needs, thus increasing the InfoSec policy users tendency to justify their violation or find their custom solutions to bypass existing security mechanisms. In our case, the hospital's IT department, for example, prevents any remote access to the hospital's EMR system, even via the VPN. Thus, if the doctor is outside of the hospital and receives a medical request for a patient's diagnosis, as reported by several interviewees, they will end up sharing their password with a colleague or asking a colleague to take a screenshot of the patient's medical records and send it via social media.

The medical practitioners, in such difficult situations, would be faced with three choices: (1) accepting the disruption of the healthcare service, (2) neglecting the compliance with the policies security requirements, (3) or creating an ad-hoc security solution to balance between the security requirements and work goals [272]. Thus, the need to make such decisions results in a negative perception of the hospital's security efforts, which would reduce the expected value of compliance with the existing InfoSec policies. This leads to the emergence of behavioural justifications when they violate or intend to violate any of the InfoSec policies and link this behaviour to the need to maintain work productivity. According to several interns, the practitioner generally chooses to serve the patient as a priority over security concerns.

To address this friction between the work tasks and security demands, the IT department needs to ensure that security policies fit the daily healthcare tasks and provide alternative solutions to manage such situations. More importantly, the hospital IT department needs to make InfoSec policies reasonable, practical, and easy to follow [295]. One way to achieve this goal comes from the marketing field, which suggests that a "customer focus" approach could improve the quality of the product, and thus, increase customer satisfaction [296][297]. According to ISO 9001:2015 for Quality Management Principles, customer focus refers to the interaction between the customer and the organisation during the development process of the product, which advises the organisation to view the customer as a key player who can help to create a more valuable and attractive product. This approach requires the organisation to carefully determine the customer's current and future needs, expectations, and risks to ensure that the product will satisfy the customer.

Similarly, the hospital IT department needs to view InfoSec policies from the user's point of view and see the security policy as a product for its targeted customers. In such a situation, the organisation needs to ensure that the security policies achieve a certain quality level, and one way to obtain such quality is to improve the alignment between security requirements and work needs. Thus, the integration of the perceptions of the users during InfoSec policy development could increase the policy usability and provide an opportunity to create more valuable InfoSec policies, which could, in return, reduce the medical practitioner's tendency to justify their non-compliance behaviour. Also, this approach could provide the IT department with ideas and solutions that fit the better healthcare context and replace the organisation perception of the security policies from organisation-centric to end user-centric [298]. Chapter 6 and 7 present in detail our approach by integrating the perception of the end-users via a collaborative writing process to produce what we hope would result in more usable InfoSec policies, which can improve the hospital security efforts to mitigate behavioural justification via neutralisation techniques and enhance compliance with the security policies.

5.7 Chapter Summary

This chapter contributed to this thesis by providing a detailed description of the second phase of the research study. Based on a qualitative approach, this phase involved a series of interviews with IT department staff and medical practitioners in one of the largest hospitals in Saudi Arabia. The aim is to explore the behaviour and attitudes of medical practitioners toward current information security policies and the environmental constraints that increase the tendency to justify InfoSec violations. This chapter provided an in-depth analysis of the current state of the hospital information security policies and indicated the MI perception and experience of the information security policies during their daily tasks.

The result of this study confirms the findings in the information security literature that human behaviour can play a critical role in an organisation's information security efforts, and employee noncompliance can be a prominent cause of data breach incidents. The findings indicated an imbalance between the IT department's efforts to develop and implement InfoSec policies and controls and the security awareness program to advertise these security initiatives in a way that medical practitioners can appreciate its existence and understand the cost of noncompliance. Also, the IT department needs to show a level of enforcement of the InfoSec policies, and this cannot be done without proper monitoring mechanisms to detect InfoSec violations and then implement corresponding sanctions.

The finding reveals that employees' adherence to InfoSec policies cannot be taken for granted. Medical practitioners sometimes drift into noncompliance and adopt neutralisation techniques to justify their noncompliance with InfoSec policy requirements. On the other hand, sometimes the organisational and social norms explicitly encourage noncompliance: people follow what others are doing rather than what the security policy tells them to do. The study illustrates many motivations that encourage interns to invoke behavioural justifications when not complying with information security policies: neutralisation techniques that helped them feel better about not complying. Thus, understanding these motivations and related justifications can help the IT department to better understand why practitioners violate security policy, thus creating security policies and controls in a way that help the practitioner comfortably adopt the required security behaviours and reduce a tendency to justify or workaround hospital security controls.

In the following chapters, we present an improvement strategy for the security policies that can reduce the likelihood that an end-user will use neutralisation techniques rather than comply with the organisation's security policies. We have suggested that including end-user perceptions during the development process of security policies through a collaborative writing process can help the IT department develop security policies that fit the business context and reduce end-user justifications for non-compliance behaviour.

Chapter 6 : Enhancing Infosec Policy Effectiveness Against Neutralisation Techniques Via The Engagement Of End Users In Policy Development (The UK, University Of Glasgow).

Phase 1	Phase 2	Phase 3	Phase 4
Determine the role of neutralisation techniques to predict medical practitioner intention to violate InfoSec policies. A quantitative study using a questionnaire in Saudi Arabia.	Investigate the motivations of medical practitioners to evoke neutralisation techniques to justify InfoSec violations. A qualitative study using semi-structured interviews in a Saudi Arabian hospital.	Enhancing InfoSec policies effectiveness against neutralisation techniques via the engagement end-user perception. An action research study using focus groups and pre and post questionnaires in the UK, University of Glasgow.	Enhancing InfoSec policies effectiveness against neutralisation techniques via the engagement end-user perception. An action research study using focus groups and pre and post questionnaires in a Saudi Arabian Hospital.

Figure 6.1 Phase Three of The Research Study

The previous chapter identified the behavioural motivations that influence medical interns' intention to justify password/account sharing in the workplace. We have determined that social factors (peer and superordinate influence), emotional facilitators (trust and empathy) and organisational factors (poor awareness of the current InfoSec policies and poor awareness of the InfoSec policies' violation consequences and deterrence mechanisms) have a significant impact on the medical interns' tendency to justify non-compliance action with the password policy. The theory of planned behaviour (TBP) [138] also explains how and why people engage in non-compliance. This theory focuses on three aspects, namely attitude towards the behaviours, subjective norms and behavioural controls (see section 2.3.1 for more details of TBP). Medical interns often gain a positive attitude towards sharing their passwords, and they are often in control of engaging in this behaviour, thereby increasing their chances of non-compliance. Jackson et al.[299] explained that people are likely to accept and comply with a policy if they believe that it has a moral purpose of benefiting both the institution and the employees. Therefore, including end-users in this study was also a strategy to help them see that the password policy is created to benefit both the organisations and the employees. As shown in Figure 6.1, this chapter presents the third phase of the research study and the steps of the

proposed intervention to discover whether the engagement of end users' perception by integrating neutralisation techniques mitigations via a collaborative writing process can improve the overall effectiveness of the security policy.

This chapter contains the following sections. Section 6.1 explains the study's aim and objectives, and section 6.2 provides details about the study methodology. Section 6.3 describes data and outcome analysis and provides comprehensive information about the study analysis procedure and the qualitative analysis of neutralisation techniques and mitigation strategies to improve the current University of Glasgow password policy. Lastly, section 6.4 will summarise the outcome of the chapter and the contribution of findings to the general body of literature.

6.1 Purpose of The Study

This study explores whether the engagement of end-users in IS policy development through a collaborative writing process can help mitigate the use of neutralisation techniques to justify Infosec policies non-compliance. The previous chapter identified several environmental factors that influence end users' propensity to invoke several neutralisation techniques (sections 5.4 and 5.5). The results showed that the lack of general awareness of information security and the negative impact of security policies on work performance increases the behavioural justifications for end users' non-compliance. Jackson et al.[299] explained that people are likely to accept and comply with a policy if they believe that it has a moral purpose of benefiting both the institution and the employees. Therefore, including end-users in this study was also a strategy to help them see that the password policy is created to benefit both the institution and the employees.

In information security literature, few scholars have attempted to confront the role of neutralisation techniques on non-compliant individuals' behaviour through interventions that focus on changing individuals' unsecured behavioural intent through information security awareness and training programmes (see Section 2.7.3 for more details). For instance, Barlow et al. [125] reported that a security awareness program that focused on crafting persuasive messages that took into account the impact of neutralisation techniques was an effective way to discourage individuals' intent to justify non-compliance behaviour. Likewise, another study by Barlow et al. [112] also found that incorporating anti-neutralisation communication messages into security education, training and awareness (SETA) programs can reduce individuals' intent to violate information security policies.

Moreover, a recent field intervention study by Siponen et al. [188] reported that an educational information security training based on cognitive dissonance theory to counter neutralisation techniques could be a practical approach to reinforce individuals' behaviour to comply with password policy requirements by creating and using secure passwords. However, while the results of the educational and awareness training interventions [125][112][188] show a decrease in the behaviour of individuals to adopt neutralisation techniques; It is challenging to assume that the use of an information security awareness program can change individuals' intention to adopt neutralisation techniques in the long term or that it will change the rationale of the individuals' who might justify it. Also, the organisation argues that its current security policies are already optimal, and no benefit in terms of overall security behaviour could be achieved by manipulating them.

Thus, we argue that focusing on changing the undesirable behaviour intention that leads to the adoption of neutralisation techniques without understanding the connection between the InfoSec policies requirements and its relevant influence on individuals' justifications remains a gap in the IS literature. Chapter five found a poor alignment of the security policy requirements and the work needs causing operational disruption in complex environments such as healthcare. Thus, it motivates individuals' behavioural intent under the pressure of social and organisational factors to evoke several neutralisation tactics and violate the InfoSec policies (password policy). The reason for choosing the password policy for the collaborative writing process in Chapters six and seven (Phases three and four) was based on our findings in Chapter 5. The result of semi-structured interviews with both IT staff and medical interns showed that password policy was the most violating security policy in the hospital. The results revealed that medical practitioners regularly shared their EMR account passwords during their daily tasks, and they adopted several neutralisation techniques to justify such undesirable behaviour.

In this chapter, our intervention is based on enhancing the alignment between the security policy requirements and the business needs through a collaborative writing process reflecting end users perception of usability-security trade-off [272], to confront the neutralisation techniques. Thus, we aim to take an initial step by developing user-centric InfoSec policies that fit the work needs *and* serve IT department security objectives. This can go on to reduce the influence of environmental and situational factors that increase the individuals' tendency to rationalise their violation in the password policy context. This study also develops pre-and post-assessments surveys to examine whether there was a significant variation in the end users' perception of the InfoSec policy effectiveness to counter a set of neutralisation techniques after they

collaboratively modified the policy based on their understanding of their work and social contexts.

6.2 Study Methodology

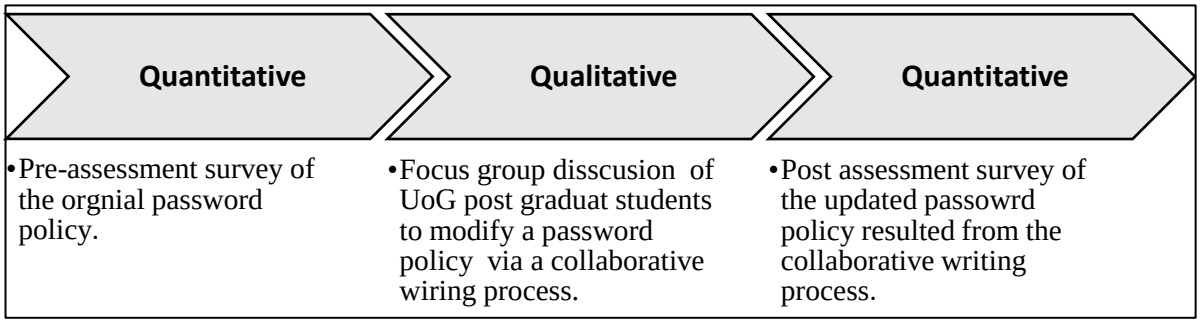


Figure 6.2 Study Methodology and Data collection for Phase three

The study aimed to evaluate Infosec policies effectiveness to counter neutralisation techniques before and after the engagement of the end-users to modify the ISP via a collaborative writing process. According to Lowry et al. [235], a collaborative writing process is "an iterative and social process that involves a team focused on a common objective that negotiates, and communicates during the creation of a common document". As illustrated in Figure 6.2, the study includes a mixed-method approach that includes two interconnected quantitative parts (pre and post-assessment surveys) and a qualitative part (a group of students engaged in a focus group discussion to modify the password policy via a collaborative writing activity).

The collaborative writing process is a group activity, where each group reads several scenarios, and each scenario represents a neutralisation technique that the end-user may use to violate the password policy. Then, each group's task was to modify the password policy collaboratively to reflect their perception to counter these behavioural justifications for non-compliance with the password policy. The collaborative writing process was based on a focus group effort and discussion to change the password policy to reduce the employees' tendency to justify non-compliance.

- **Data Collection Method**

Each group was asked to read four security scenarios representing four neutralisation techniques. All scenarios were designed to reflect several behavioural justifications that had been identified in interviews with the Medical Interns (Sections 5.4.1 and 5.4.2). Also, all scenarios were designed to reflect the impact of the social factor (peer influence) between the co-workers. Thus, each security scenario's outcome can lead to sharing the password, which is a violation of the policy. All participants in each group were asked to modify the password

policy using a collaborative writing activity to reduce individuals' propensity for password violations outlined in the hypothetical scenarios.

A pre and post surveys instrument was developed to measure the impact of the collaborative writing process. The pre and post surveys are identical and include a total of 21 questions. Each survey is designed to be completed individually to determine each participant's perception of the existing security policy (password policy in our case) before the participants' engagement in a collaborative writing process with a group. All the questions were derived from IS literature (Appendix C.1 for a complete list of questions) with a slight modification to fit the current study context. Both the pre-and post-assessment surveys were identical and contained five main parts. However, only the pre-assessment survey required each participant to complete demographic information. Both the pre-and post-assessments asked the participants to answer questions related to neutralisation techniques, self-efficacy, work impediment and provided their evaluation of the overall effectiveness for the given password policy against five neutralisation claims. The demographic part in the pre-assessment survey aimed to gain some information about the participants, such as level of education, gender, and their ability to access the University IT assets. The Neutralisation technique's part included ten questions that represented five justification strategies: Denial of Responsibility (DoR), Denial of Injury (DoI), Defence of Necessity (DoN), Everybody else is doing it (EEIDI) and Appeal of Higher loyalty (AOHL). Questions in this part aimed to measure the end user's perception regarding the effectiveness of the password policy to counter several claims that the end-users might adopt to justify their behavioural violation of password policy.

The third part included questions to evaluate the end user's self-efficacy and capability to perform all the necessary security actions and requirements illustrated in the password policy. The fourth part covered the work impediment, which concentrated on the end user's evaluation of the complexity level that the password policy could add to their daily work activities. The last part included a single question that came directly after the neutralisation technique's part, which aimed to determine the overall effectiveness of the password policy to counter all the justification claims that had been presented in the survey to violate the password policy. The post-assessment survey aimed to measure the variation of end users' perceptions by evaluating a new version of the password policy that a different group would have updated through a collaborative writing process. Questions in the post-assessment are identical to the pre-assessment. All questions in the post-assessment were randomly presented. Also, all the participants completed the post-assessment at least one week after the pre-assessment. This was

to reduce questions order bias and minimise the participants' chance to remember pre-assessment questions.

- **Study validity and reliability**

The researcher got validation approval from asked three independent researchers who agreed that the questions in both the pre- and post-assessments surveys and security scenarios in the collaborative writing process could serve the purpose of the study. Later, the researcher conducted a test study that included a sample of 8 participants divided into two groups (group A and B). The aim of the test study was to determine whether the pre and post-assessments questions and the related scenarios were readable and understandable. Also, it helped to evaluate and enhance the feasibility of the study procedures (in person Vs online collaborative writing using Google Docs). The primary results from the test study improved this research study by refining its measurements and enhancing our expectations about the prospective difficulties in the study procedure and design. For example, the test study made the researcher aware of the challenges in managing online sessions for a collaborative writing activity. Some participants may experience technical and non-technical difficulties when using Google Docs. Also, some participants revealed less motivation during online group discussions, reflecting less interest in contributing to the password policy modification process.

Figure 6.3 Data Collection Procedure

An ethical approval application was approved to conduct this study under the number 300190026 (Appendices D.4 for Ethical Approval and D.5 for Participant consent form).

- **Study Sample and analysis**

The researcher contacted the University of Glasgow Graduate School of Science and Engineering to send an email invitation to study on the email list of all graduate students. The email invitation contained several documents, such as the study description and the consent form for participation. Moreover, the invitation provided a link to a scheduling website where everyone interested in participating in the study could choose the time slots that fit their schedule. In addition to the pre-and post-assessment online surveys, the study included a focus group discussion, in which each group worked collaboratively face-to-face to amend the security

policy (University of Glasgow Password Policy). The study recruited a total of 24 participants (postgraduate students) divided into six groups (A, B, C, D, E, and F). Each participant was assigned randomly into a group once a suitable number of individuals agreed on a specific time slot (at least four participants in each group). The group discussion for the collaborative writing process lasted up to 90 minutes.

Figure 6.2, Figure 6.3 and Figure 6.4 show the sequential data collection and procedures of the study. The first phase was to obtain each participants' evaluation of the effectiveness of a given security policy (password policy) against a set of claims based on the neutralisation theory via an online-based pre-assessment survey. The pre-assessment was disseminated to each group member one day ahead of the group meeting for the collaborative writing process. Each participant was asked to complete the consent and the demographic information parts. Then, each individual was required to create a nickname to link his/her evaluation in the pre-and post-assessment surveys for comparison purposes before and after the collaborative writing of the password policy.

At the beginning of the collaborative writing phase, the experimenter distributed the study instructions to all participants. Afterwards, each group was inquired to nominate one member to lead the discussion and take the writer role to edit the given policy based on the changes the group would have agreed on. This phase started when the experimenter projected the study instructions on a screen so the group could read and discuss four different security scenarios corresponding to four neutralisation techniques. Once they reached a consensus on how to mitigate each scenario, they reflected their decisions by directly editing the given password policy. The experimenter stayed in the room for observation and note-taking without any intervening in the group discussion. If the group thought that no more modifications to the policy were needed, the group leader notified the experimenter that they were done. At the end of this phase, the experimenter thanked all the group participants and told them to expect an email after at least one week, which would include a website link to a post-assessment survey. When the post-assessment is completed by all members in each group members, this is considered the last phase of the study for each group. During all phases, no identifiable personal information was gathered. Participants were only asked to provide an email to receive both pre-and post-assessments links and the study instructions and documents. We use a data analysis procedure that includes three main steps:

1. **Pre-assessment:** We used a pre-assessment survey to determine the end-user evaluation of the password policy's effectiveness to counter several justification claims corresponding to

the neutralisation techniques. Each claim was designed based on a single neutralisation technique that the end-user might use to justify password violation. This step is essential to capture the end-user perception of the existing password policy before the modification via collaborative writing.

2. **During the collaborative writing process:** We observed participants' discussions to counter each of the justification scenarios presented during collaborative writing of a security policy. The aim was to understand the participants' behavioural intention to accept or reject each justification. Therefore, we can indirectly evaluate their understanding of the importance of security compliance during their daily activities. Moreover, we were keen to understand how each group provide a solution to mitigate the consequences of each neutralisation technique under the lens of SCPT theory, which can be reflected as a text by modifying a given security policy (password policy).
3. **Post Assessment:** Like the pre-assessment, the post-assessment survey was used to measure the shift of each group's perception about the password policy after the modification via the collaborative writing process. During this stage, the participants evaluate the updated version of the password policy resulting from another group collaborative writing activity. The purpose of exchanging versions of the updated password policy between groups was based on the idea that each group spent time and effort discussing and modifying the original password policy. Thus, we hypothesized that each participant's awareness of password policy requirements was improved to assess whether modifications made by another group to counteract neutralisation techniques were effective. The mean difference between pre and post evaluations can reveal whether the effectiveness of a modified password policy to mitigate neutralisation techniques has improved.

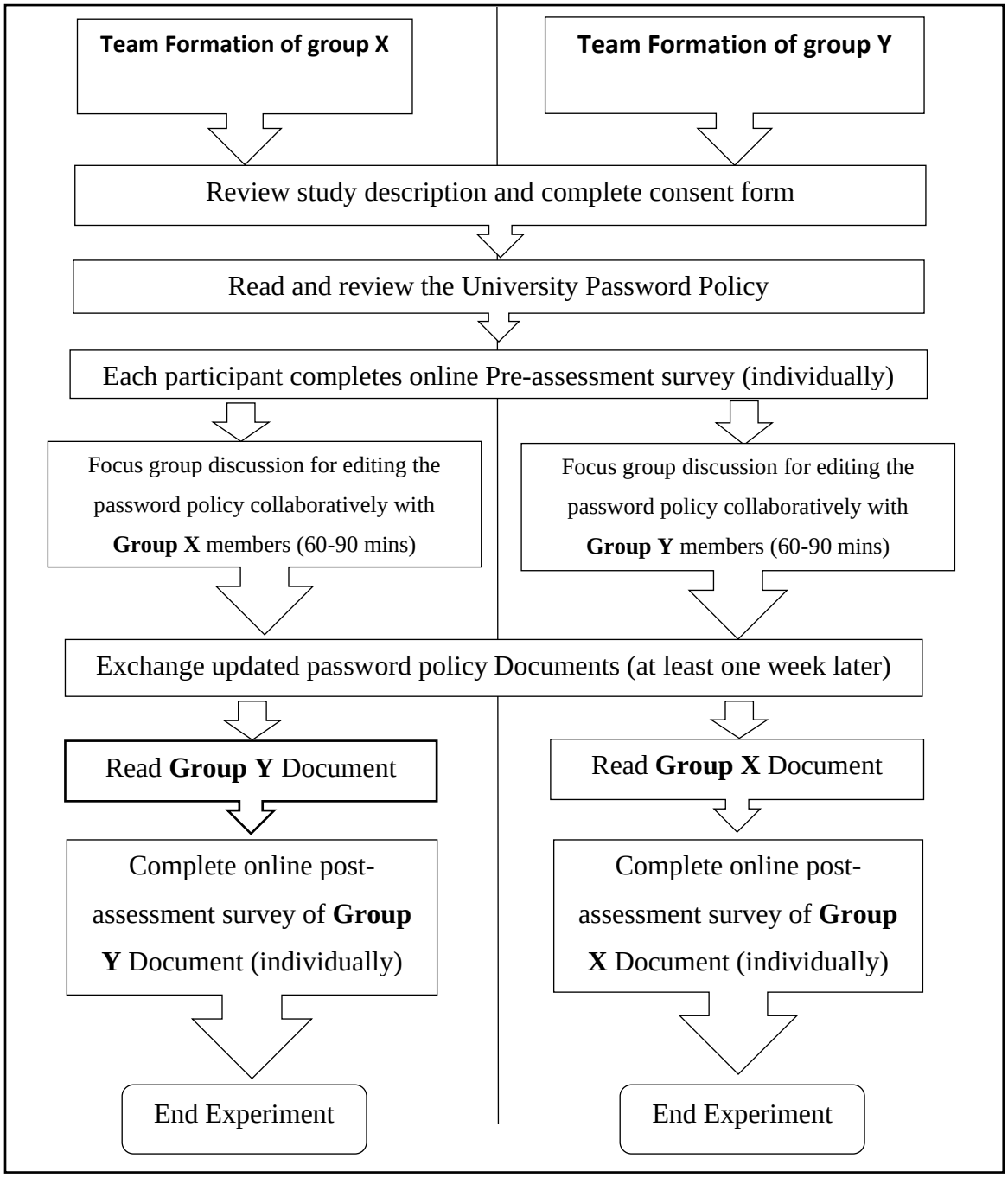


Figure 6.4 The Collaborative Writing Procedure

6.3 Analysis and Results

For the purpose of this study, we designed four security scenarios that represent four neutralisation techniques (DoI, DoN, AHL and EEIDI) that the end-users revealed they adopted to violate the password policy. According to Siponen and Vance [6], these scenarios utilised the impact of social context on the employees' behaviour. In this thesis, Chapter five identified several motivations that influenced the individuals' behaviour to justify password policy violation. Therefore, in this chapter, we chose the social factor (peer pressure) and the social facilitator (trust) as important motivations to adopt the neutralisation techniques (DoI, DoN, AHL and EEIDI). Thus, during the collaborative writing activity, each group was asked to respond to these scenarios by updating the existing password policy to reduce or mitigate the end users' tendency to utilise the neutralisation techniques and violate the policy.

In addition, we employed the opportunity reduction concept from Situational Crime Prevention Theory (SCPT), which asserts that a crime is committed when a criminal finds an opportunity to do so [300]. Freilich et al.[301] define the SCPT as " an intervention in the environmental setting where a specific crime occurs with the aim of eliminating all opportunity to commit that crime. This is the ultimate and pristine approach of traditional Situational Crime Prevention." Thus, the SCPT strategies were used for thematical categorisation (coded) of the end-user approaches to mitigate each of the justification that a person might use to violate the password policy. In particular, each of the modification to the policy content was coded and relate to each of the SCPT strategies. Table 6.1 provides the thirty techniques of SCPT that we adopted to code each of the statement for each group added or changed in the password policy. In criminology, Cornish and Clarke [238] introduced five main crime prevention strategies that aimed to reduce the opportunity of a specific crime to occur by altering the immediate environment. The five strategies are as the following:

6. **Increase the offenders' effort to commit a crime:** this strategy includes a set of five techniques that aim to increase the effort that the offender needs to commit a crime. It includes target harden, control access to facilities, screen exits, deflects offenders and control tools/ weapons [238].
7. **Increase the offenders' perceived risk of being caught:** this strategy aims to increase "the risk apprehension"[239]. It includes extending guardianship, assisting natural surveillance, reducing anonymity, utilising place managers, and strengthening formal surveillance [238].

8. **Reduce offenders' rewards of the crime:** this strategy aims to distract the offenders expected gains of a crime. It includes concealing targets, removing targets, identifying a property, and disrupt markets, and denying benefits [238].
9. **Reduce the provocation that stimulates the offender to commit a crime:** this strategy aims to enhance the situational settings or conditions that can trigger the individual to commit a crime. It includes reducing frustrations and stress, avoiding disputes, reducing emotional arousal, neutralising peer pressure and discouraging imitation [238].
10. **Remove offenders' excuse to commit the crime**: this strategy aims to neutralise the justifications that the offender used to commit a crime. It includes set rules, post instructions, alert conscience, assisting compliance, and controlling drugs and alcohol [238].

Later, Freilich and Newman [301] extended Clarke and Cornish's [238] twenty-five SCPT techniques by adding a sixth column of opportunity-crime reducing techniques and calling it "provide an opportunity to the offender". This strategy aims to " remove the crime opportunity by providing an alternative, non-criminal one" and contains five sub-strategies [301]. These are: facilitating obedience to the law, the forgiveness of previous crimes, offering of alternatives that are more attractive to the criminal and less harmful, subsidise resources that the criminal desires access to, and legalisation and regulation of the previous criminal behaviour [301] Data were analysed using descriptive statistics Microsoft Excel and a qualitative content analysis approach to identify and analyse all password policy documents modified via CW. According to Krippendorff [195], content analysis is "a research technique for making replicable and valid inferences from text to their context of use, with the purpose of providing knowledge, new insights, a representation of facts and a practical guide to action". Du Preez[240] asserted that content analysis must follow a well-structured procedure to gain more reliable and valid results. Thus, we adopt Krippendorff [195] procedure that includes six phases as the following:

1. **Unitizing:** a systematic process to identify and distinguish specific text segments (a sample text unites) that are relevant to the purpose of the content analysis. A text unit can be a complete sentence, portion of it or a word [241]. In our case, we identified all sentences added or modified in the password policy by groups during the CW process, and these sentences represent a collective contribution to alleviating the tendency of individuals to justify password sharing.
2. **Sampling:** this phase refers to drawing a controllable set of test segments from a population when it is unrealistic to perform a content analysis over the entire set of transcripts [195]. In

our case, the sample was six password policies documents that had been modified by six groups via the CW process. All added or modified statements by the various groups in the password policy were manageable. Thus, we used the entire statements for the analysis without excluding any text segments. In each modified password documents via the CW, the added or modified statements were highlighted and extracted to a Microsoft Excel sheet for coding.

3. **Coding**: This phase refers to the process of classifying texts identified from the sampling phase into analysable text units[195]. This process can be conducted by either emerging coding or prior coding. Emerging coding aims to create new themes and codes to build a new theory based on the ground theory concepts [242]. Prior coding refers to the usage of predefined codes and themes from well-established theories [242]. In our case, we used the prior coding approach, and all the extracted text segments were coded based on the SCPT themes and codes illustrated in Table 6.1.

4. **Reducing:** this phase aims to reduce duplication of data by counting the frequency of codes to decide whether there is a need to reduce these codes to enhance the interpretation process and the statistical efficiency [195]. In our case, we coded the entire text segments because the added or the modified statements were manageable (the added or modified statements to the original password policy document by the groups via the CW). Thus, the duplication of codes was aggregated under one theme, which was later used for statistics to count the frequency of each of them.

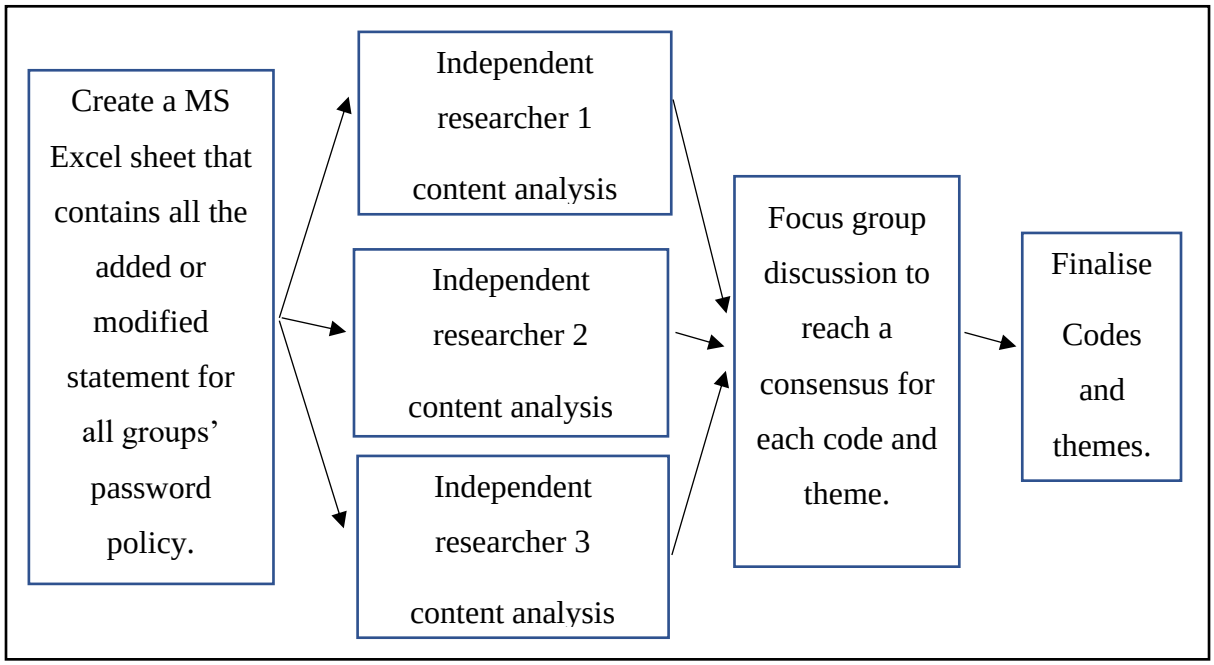
5. **Inferring:** Krippendorff [195] described this process as searching for " the contextual phenomena from texts ……..It bridges the gap between descriptive accounts of texts and what they mean, refer to, entail, provoke, or cause.". In our case, each text segment was assigned to one or two SCPT codes under specific themes to gain a better understanding of the relationship between the individuals' neutralisation techniques (contextual phenomena) and the suggested SCPT approaches to mitigate password sharing.

6. **Narrating**: the process of reporting the content analysis results in an understandable and meaningful manner. This phase discusses the inferences and reports the results that answer and address the research question(s)[240].

We utilised the thirty SCPT strategies shown in Table 6.1(green row is the themes and light blue columns are the codes) to conduct a content analysis of the updated password policy after the collaborative writing process. In this study, all statements in the modified password policy

were deductively analysed to develop a list of themes and codes in Table 6.1. Then, the researcher created an excel sheet that contained all the modified statements for each group and asked three independent researchers to conduct content analysis based on the thirty SCPT strategies illustrated in Table 6.1 to increase the rigour and reduce the bias in the qualitative studies [302]. Once all three researchers had coded each of the added or modified statements, the study author conducted a focus group discussion that included all the independent researchers to reach a consensus on each added statement's code for each added statement in the updated password policy and its corresponding theme. This process continued until each added or modified statement was assigned to one or two themes. 6.5 illustrates the content analysis and the focus group process for this study.

The following subsections provide more details about the quantitative surveys (per and post-assessments) results along with qualitative content analysis of modified password policy via the collaborative writing process. Each subsection addresses one of the neutralisation techniques in the study scope, which are Denial of Injury (DoI), Defence of Necessity (DoN), Appeal of Higher Loyalty (AOHL) and Everybody else is doing it (EEIDI).



6.5 Independent Researchers Content Analysis and Focus Group Processes

Table 6.1 Thirty techniques of The Situational Crime Prevention Theory (SCPT)

Clarke and Cornish [238] twenty five SCPT techniques						Freilich and Newman [301] SCPT extension
Themes	**1. Increase the Effort**	**2. Increase the Risks**	**3. Reduce the Rewards**	**4.Reduce Provocations**	**5. Remove Excuses**	**6.Provide opportunity**
Codes	**1.Target harden** *Anti-robbery screens*	**6.Extend guardianship.** *Take routine precautions: go out in group at night*	**11. Conceal targets.** *Off-street parking* *Minimise ID of offices*	**16. Reduce frustrations and stress.** *Efficient queues and polite service*	**21. Set rules.** *harassment cods* *information security policies*	**26.Facilitate.** *Easy to fill income tax return forms*
	2.Control access to facilities *Electronic card access*	**7.Assist natural surveillance** *Improved street lighting* *Support whistleblowers*	**12. Remove targets** *Removable car radio* *Clear desk policy*	**17. Avoid disputes** *Reduce crowding in pubs*	**22. Post instructions** *"No Parking"* *"Private Property"*	**27.Fogive** *Amnesty for illegal immigrants*
	3.Screen exits *Ticket needed for exit*	**8.Reduce anonymity.** *Taxi driver IDs* *School uniforms*	**13. Identify property.** *Property marking*	**18. Reduce emotional arousal.** *Controls on violent pornography*	**23. Alert conscience.** *Rod side display board* *"Shoplifting is stealing"*	**28.offer alternative.** *Provide an official racing park to reduce "drag" car or street racing*
	4.Deflect offenders. *Street closures*	**9.Utilise place managers.** *Two clerks for convenience stores*	**14. Disrupt markets.** *Monitor pawn shops*	**19. Neutralise peer pressure.** *"Idiots drink and drive"* *"It's OK to say No"*	**24. Assist compliance.** *Easy library checkout* *Litter bins*	**29.Subsidise.** *Paying illegal loggers not to log*
	5.Control tools/weapons *Disabling stolen cell phones*	**10.Strengthen formal surveillance.** *Burglar alarms, guards*	**15.Deny benefits.** *Ink merchandise tags Graffiti clean*	**20. Discourage imitation.** *Disperse troublemakers at schools*	**25. Control drugs and alcohol.** *intervention Alcohol-free*	**30. Legalise.** *Legalise Marijuana for medical purposes*

Table 6.2 The Overall Pre-Assessment and Post-Assessment Frequency (%) Of Neutralisation Techniques

	Preassessment	*Denial Injury*	*Defence of Necessity*	*Everybody Else Doing it*	*Appeal of higher Loyalty*	*Policy Effectiveness*
7 points Likert Scale		*Frequency (%)*	*Frequency (%)*	*Frequency (%)*	*Frequency (%)*	*Frequency (%)*
1	*Strongly Ineffective*	1 (4%)	1 (4%)	3 (13%)	3 (13%)	0 (0%)
2	*Ineffective*	3 (13%)	3 (13%)	5 (21%)	4 (17%)	7 (29%)
3	*Somewhat Ineffective*	5 (21%)	4 (17%)	4 (17%)	2 (8%)	4 (17%)
4	*Not effective or ineffective*	1 (4%)	2 (8%)	1 (4%)	2 (8%)	1 (4%)
5	*Somewhat effective*	3 (13%)	6 (25%)	2 (8%)	4 (17%)	3 (13%)
6	*Effective*	5 (21%)	5 (21%)	7 (29%)	7 (29%)	7 (29%)
7	*Strongly effective*	6 (25%)	3 (13%)	2 (8%)	2 (8%)	2 (8%)
	Total # of Participants	24 (100%)	24 (100%)	24 (100%)	24 (100%)	24 (100%)
	Post-assessment	*Denial Injury*	*Defence of Necessity*	*Everybody Else Doing it*	*Appeal of higher Loyalty*	*Policy Effectiveness*
7 points Likert Scale		*Frequency (%)*	*Frequency (%)*	*Frequency (%)*	*Frequency (%)*	*Frequency (%)*
1	*Strongly Ineffective*	2 (8%)	0 (0%)	1 (4%)	1 (4%)	1 (4%)
2	*Ineffective*	2 (8%)	4 (17%)	1 (4%)	2 (8%)	2 (8%)
3	*Somewhat Ineffective*	2 (8%)	1 (4%)	3 (13%)	2 (8%)	2 (8%)
4	*Neither effective nor ineffective*	0 (0%)	3 (13%)	2 (8%)	1 (4%)	1 (4%)
5	*Somewhat effective*	3 (13%)	4 (17%)	4 (17%)	3 (13%)	5 (21%)
6	*Effective*	6 (25%)	7 (29%)	5 (21%)	8 (33%)	11 (46%)
7	*Strongly effective*	9 (38%)	5 (21%)	8 (33%)	7 (29%)	2 (8%)
	Total # of Participants	24 (100%)	24 (100%)	24 (100%)	24 (100%)	24 (100%)

The following subsections describe the content analysis results and the focus group of independent researchers, as mentioned in the above section. Descriptive statistics across pre and post-assessments captured the change in participants' perception of password policy before and after the collaborative writing process. Also, we conducted a qualitative content analysis of all updated password documents based on SCPT to identify suggested solutions that participants added to the password policy to reduce the opportunity of justification for a password policy violation. Four neutralisation techniques were analysed DoI, DoN, AoHL, and EEIDI.

6.3.1 Denial of Injury (DoI)

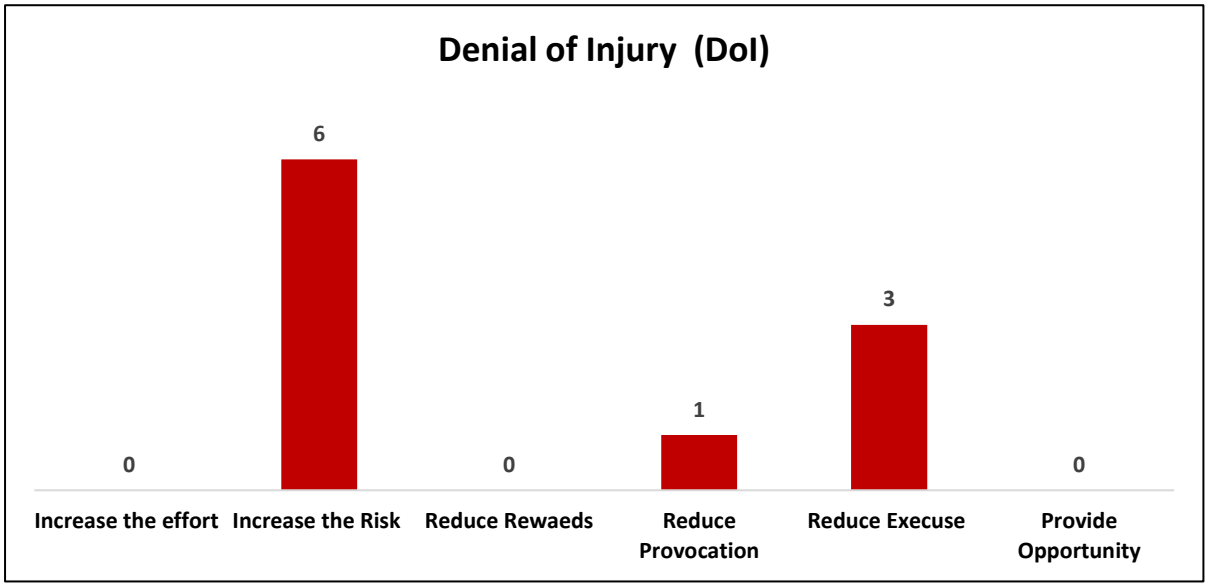


Figure 6.7 Mapping Frequency of codes between Denial Of Injury And The Situational Crime Prevention Theory

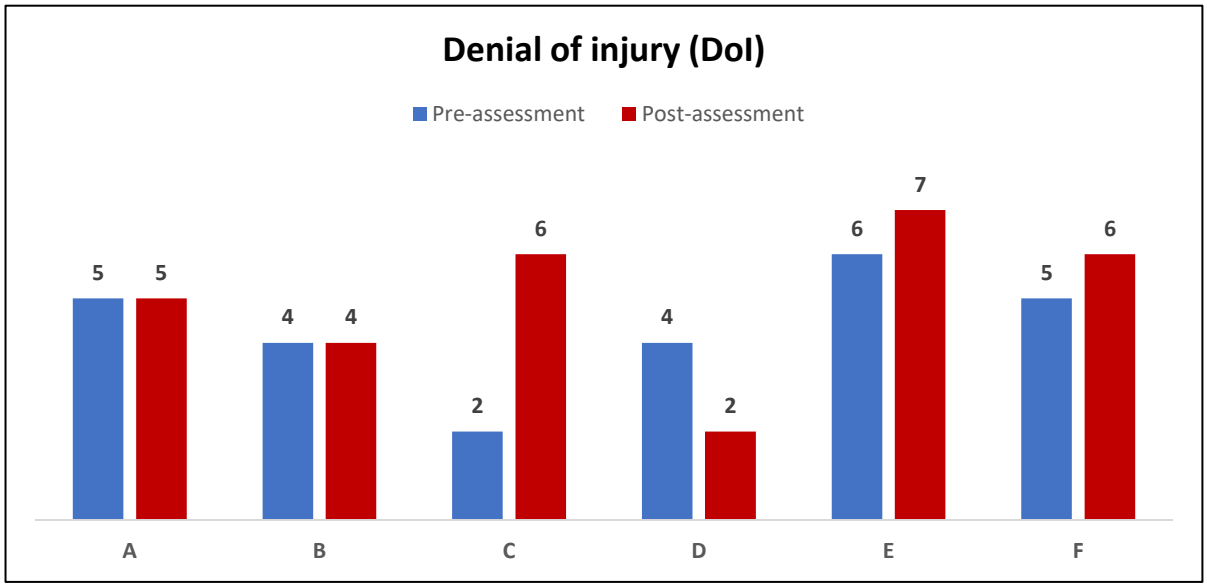


Figure 6.6 Median Comparison Between All Groups For Denial Of Injury (DoI)

- **Pre assessment evaluation:**

As shown in Table 6.2, the respondent's evaluation of the university password policy with regard to the denial of injury seems to have two main sides. The perception of the majority of the respondents (N=14, 58%) reported that the given policy is strongly effective(N=6), effective (N=5) or somewhat effective (N=3) to prevent the DoI security claims to share the password. In addition, only one (4%) participant considered the policy-neutral, while the rest of them (N=9, 38%) indicated that the password policy in its current situation is ineffective or strongly

ineffective to mitigate the employees' tendency to adopt the DoI claims and share the password (Mdn=5, Stdev= 1.99, and IQR3-IQR1= 3.25).

- **During the collaborative writing**:

The participants' perception of the DoI was analysed through their arguments to accept or reject that such justifications would occur, along with their understanding of the consequences of sharing a password. Also, their decision-making process to update the current password policy to better represent the expected harm of sharing passwords for all parties and the proposed modifications to the policy to overcome the end users' tendency to adopt such a justification. The following scenario was projected on the screen:

"Sarah is an employee in ABC university, and she has access to the ABC University systems. To ensure that University systems information is preserved securely, the university has a firm password policy that all employees must keep their passwords confidential. One day, Sarah was approached by another employee named Tony, who asked Sarah to share her password with him in order to edit and review student records as Tony's had difficulties to log-in the system. Sarah knew that Tony was a trustworthy colleague. ***So, she felt that nobody would get harm if she shared her password with Tony. Therefore, Sarah gives Tony her password to let him edit the student records****."*

We employed a qualitative analysis of the groups' discussion and text analysis of the updated password policy after the collaborative wiring activity. It was noted that each group read the DoI scenario and considered the possibility of such a scenario occurring (A, B, C, F). These groups spent some time providing examples of potential risks and consequences of sharing the passwords. Afterwards, they discussed some of the potential solutions to mitigate the related risks when an employee adopted such a justification. Other groups (D and E) took a more methodological procedure by taking a step back to view the big picture of the situation that caused the employee to justify via DoI. For instance, a member of the group D stated that:

> ***Member from D:*** *"it feels to me like the easiest way to counter it is to target the cause like the fact that Tony password expired was the reason for using this justification."*

Also, it was noted that in all groups, after reading the DoI scenario, the participants read the policy again and discussed if there was any mentioning of any existing IT controls or deterrence actions to discourage the employees from violating the password policy as many security risks might occur because of the employees' misjudgement of the harm and the related consequences of the security policy violation [1]. Thus, we examined the usefulness of the situational crime

prevention theory as a theoretical lens to understand the end user perception to improve the existing password policy effectiveness and analyse their approaches to reduce end-user justification that sharing a password is harmless behaviour. In this direction, all groups agreed that the given policy lacked any mention of the existing IT security controls in place to detect and prevent such violations and the associated cost to the individual. Also, the importance of reporting such violations to the organisation management. A total of 10 out of the 54 modifications were added to mitigate DoI from the end-user perception.

As shown in Figure 6.5, all groups reached a consensus that three strategies of SCPT can discourage the end-user willingness to deny the harmful consequences of sharing their password. Increased perceived risk was the first and most recommended strategy against DoI. The strategy aims to influence the individual decision-making process by clarifying the cost of non-compliance on both organisational and personal levels. The second strategy was to remove the end-user excuses by altering their conscience about the potential risk of sharing the password. This could be done by posting clear instructions to follow in the policy and assisting compliance during the daily work. The last strategy was reducing the end-user provocation by minimising the emotional triggers such as stress and frustration, which can motivate the end-users to rationalise his/her behaviour of committing password policy violations [2, 3].

The modifications relating to increasing perceived risk were concentrated around the idea that any effective prevention strategy requires better management and illustration of security controls in the environment (workplace), which includes a declaration of the IT department capabilities to monitor and detect any violation [1, 2] as well as clarifying potential risks and consequences associated of the password policy violation. All the groups except (C) agreed that there was a need to improve the end-user perception of the harmful consequences of sharing the password to all parties involved in such behaviour, which can, in turn, mitigate their tendency to justify the violation and deny the related consequences. Group (A), for instance, provided a new section called “password recovery” and added a brief statement that gave no exception for accessing the system using a colleagues’ accounts or passwords and considered it a violation of the policy. Thus, group (A) added:

Group A:“*Attempts to access university systems by means other than password resets will result in disciplinary matters for all parties involved, including the sharing of passwords between colleagues.”*

In addition, Group B and F members agreed that it was essential to explicitly remind end-users of their password policy obligations to ensure compliance with legislation such as the General Data Protection Regulation (GDPR). GDRP requires keeping passwords confidential and not sharing them with anyone, even a trusted colleague. This therefore, targets the root of justification itself (DoI) by reporting the security risks of password sharing and the harmful consequences associated with this behaviour at both the individual and organisational levels. For instance, a member of group B during the discussion of the DoI scenario stated that:

> ***Member from B:*** *"The policy doesn't really tell you or say anything what could happen if you share your password and what are the potential harms that could be caused. That was not clear."*

Also, group F discussed whether it was worth mentioning the consequences if someone violated the policy, and the group agreed with a member's point of view that it is important to show that the policy violation will come with a price:

> ***Member from F:*** *"The given policy did not say anything about the consequences for you if violates the policy because in real-world people will break the policy anyway. So, the policy needs to show the associated cost."*

Group B added a new section that focuses on the end users' responsibility to protect their password and potential cost if sensitive data leaks due to sharing the password or account with others. Based on their discussion, group B assumed that addressing this part in the policy would leave no room for the end-users to claim that they were unaware of the risks and consequences of not complying with the policy. Consequently, they added a new section using the question pattern to grab the attention of the policy reader by targeting the violation "password sharing" to discourage the end-user from reducing the cost of non-compliance. They added the following:

Group B*:" What might happen if I share my password?*

- *Remember - Any activity taken on your account is linked back to you.*
- *Sensitive data may be exposed - this may cause serious legal consequences for your organisation - GDPR fines, etc.*
- *You may be disciplined at work - cautioned or fired.*

In the same direction, group D and E members argued that denial of injury could be discouraged by clearly putting the guilt and blame on the person who allows others to use his/her account password.

Group D*:* *"Giving anyone your password or direct access to your account can directly threaten or compromise University systems or data. If this is discovered, then you may receive disciplinary action."*

Group E: *"Just a reminder, violating this policy may result in penalties. For more information, please refer to the university code of conduct."*

In addition, group (F) took a similar approach to dissuade the end-user tendency to adopt DoI by indicating the undesirable damages to the personal reputation and integrity that one is likely to face should they violate the policy. They asserted that the damage resulting from sharing their password credentials with other colleagues, which can, in turn, cause a data breach to the organisation information. The group added the following points to the policy:

Group F*:* *"It takes just ONE instance of sharing your password to have a massive data breach.*

- *You are in contempt of the GDPR.*
- *Your professional integrity and reputation are at risk by sharing your credentials."*

In the participants' point of view, removing excuses was the second recommended strategy from SCPT while writing collaboratively to improve the existing password policy to reduce end-user justification via DoI. In our context, participants responded to a DoI scenario by indicating the need to alert the employees' conscience about their accountability for protecting system credentials. According to Clarke [7], some of the SPCT strategies can "serve simply to stimulate feelings of conscience at the point of contemplating the commission of a specific type of offence". In information security, changing the conscience of employees can be addressed by setting and posting clear security rules and instructions and improving employee security awareness of cyber security threats/consequences [18]. Thus, clarifying the type of acceptable or unacceptable behaviours in a security policy can increase employees' awareness during their daily interactions with other co-workers. It can improve their sense of responsibility to follow policy guidelines that ultimately aim to reduce potential harm to both the employee and the organisation. A member in group B stated that:

> ***Member from B:*** *"Writing a policy without considering the social context by providing clear instructions on how to deal with others in a safe manner is misleading. Without it, the employee may be pushed indirectly to justify a policy violation."*

Also, a member in group D restated the importance of alerting the consciences of the employees' responsibility in the policy:

> ***Member from D:*** *"There is a need to clarify the employee's responsibility to keep the password confidential and to remind the employee that your colleague may not be aware of password security like you."*

Therefore, the group reflected this argument by adding the following statement to mitigate the DoI claim:

Group D: *"Misuse of your account from a stolen or shared password is your responsibility. Remember that your co-workers may not be aware of security measures or are as careful as you."*

- **Post assessment evaluation:**

As shown in Table 6.2, there was an improvement of the participant's perception of the ability of the modified policy via a collaborative writing process to discourage the end-users from adopting the DoI to violate the policy. The post-assessment showed that the majority of the participants (N= 18, 75%) believed that the modified policy was strongly effective (N=9), effective (N=6) and somehow effective (N=3) to discourage the end-users tendency to underestimate the harmful consequences of sharing password between colleagues. However, the rest of the participants (N=6, 24%) reported that the modified policy was still ineffective and unable to dissuade the end-user from justifying the password policy violation via DoI. As shown in Figure 6.6, the median of the end users' perception across all groups, except D, has been slightly improved regarding the ability of the updated policy to mitigate the end user's adoption of the DoI. Therefore, the change of median value in the participants' perception revealed more agreement that the updated policy that considered the DoI scenario could reduce the end users' tendency to justify the consequences of sharing policy between colleagues as harmless (Mdn=6, Stdev=2.07 and IQR3-IQR1= 2.5).

6.3.2 Defence of Necessity (DoN)

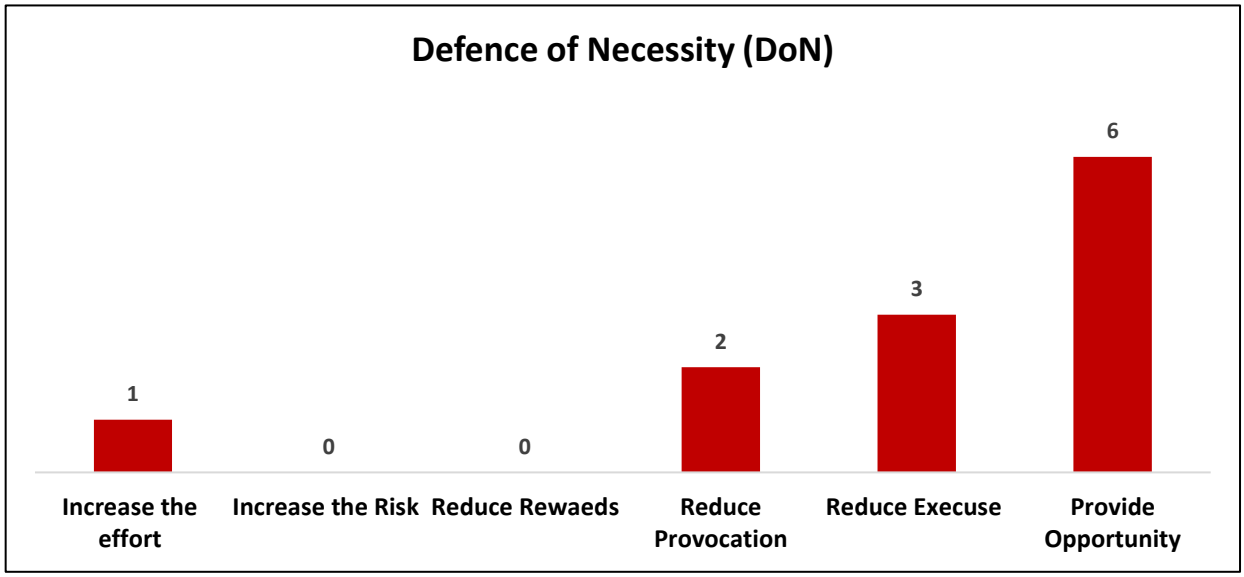


Figure 6.8 Mapping Frequency of codes between Defence of Necessity (DoN) and the Situational Crime Prevention Theory

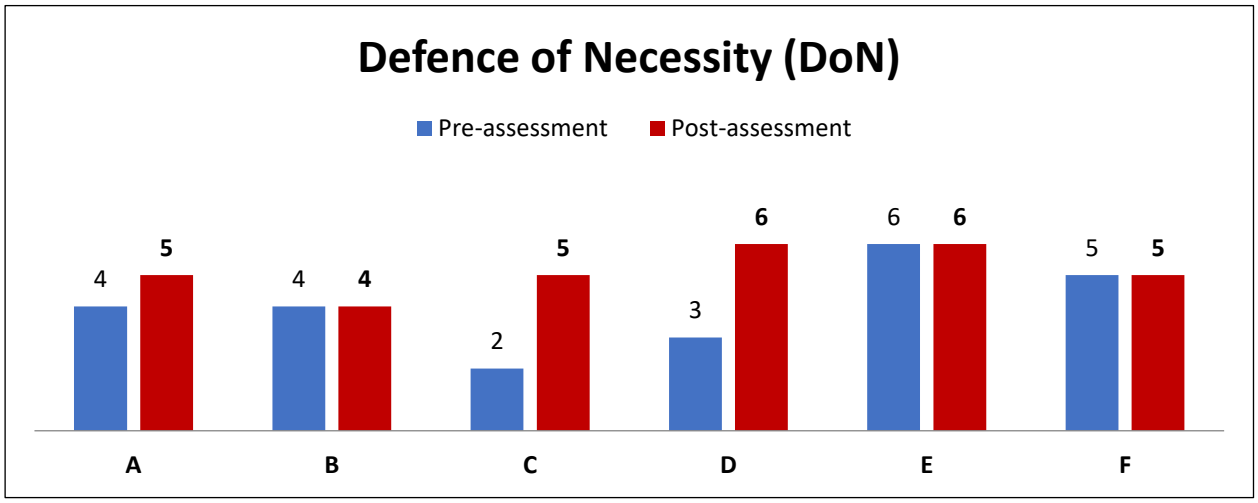


Figure 6.9 Medians Comparison Between All Groups For Defence Of Necessity (DoN)

- **Pre-assessment evaluation:**

Table 6.2 outlines the pre-evaluation of the current password policy regarding the use of DoN as an excuse for policy violation. Data from participants (N = 24) was collected via an online survey. The result from the pre-assessment showed that two participants (8 %) revealed a neutral perception of the original password policy to counter DoN, while eight participants (34 %) reported that the password policy in its current state was somewhat ineffective (N = 4), ineffective (N = 3) or strongly ineffective (N = 1) to mitigate employee tendency to adopt DoN claims. However, the rest of the participants (N=14, 58%) reported that the original password policy was somewhat effective (N=6), effective (N=5), or strongly effective (N=3), respectively.

Also, as shown in Table 6.3, the overall median of pre-assessment across all groups was (Mdn = 5, Stdev= 1.77, and IQR3-IQR1 = 3), which indicated a consensus between all group members that the original password policy is somewhat effective to counter the end users' disposition to justify the policy violation via DoN.

- **During the collaborative writing:**

The groups' perception was analysed by their argument for adopting such a justification. In particular, how do the surrounding circumstances affect an employee's tendency, in the presence of the current password policy, to share a password or account of their systems then claim that such a breach is a necessary act to complete the work? Also, the approach that the participants in each group would update the existing password policy to reduce an employees' tendency to adopt DoN and relate these modifications to SCP strategies. The following scenario was projected on the screen:

"Sarah is an employee at ABC University, and she has access to the ABC University systems. To ensure that University systems information is pre-served securely, the university has a firm password policy that all employees must keep their password confidential. One day, Sarah was approached by another employee named Tony, who asked Sarah to share her password to allow him to edit and review student records as Tony's password has difficulties to login. Sarah knew that Tony was a trustworthy colleague. ***So, she felt that they were working in a busy department, and it was essential action to share her password in order to improve work performance. Thus, Sarah gives Tony her password to let him edit the required student information using her account****."*

It was noted that all groups, participants agreed that this scenario is more likely to occur in the department that requires direct interaction with a lot of students, such as student services. Thus, having difficulties in accessing the university systems might negatively impact work activities and cause disruption for providing the university services to the students. In general, the groups updated the password policy with 12 modifications that aimed to counter the employee tendency of violating the policy via DoN. According to Freilich and Newman [301], "if you block opportunities, offenders will simply displace their criminal activity somewhere else". Hence participants reported that an intervention that focuses on manipulating the perpetrator's environment by "providing opportunities" to do something else could work positively to manipulate the perpetrator's behaviour and encourage them to undertake non-criminal acts or less serious crimes. In the same direction, most of the groups during the collaborative writing activity viewed this concept as a better way to deal with employee justification via the DoN.

As shown on Figure 6.8, most groups decided that providing opportunity by facilitating compliance and offering alternative solutions (6 out of 12 targeted DoN) are appropriate strategies to reduce an employee's claim that business necessity requires violating the password policy. For example, groups (A, E, and F) shared a common notion that an employee may believe that password/account sharing is essential to maintain efficiency and maximum performance at work. These groups believed that it must be explicitly stated in the policy that password sharing is a violation and not a necessary action. Thus, providing clear guidelines for dealing with such a situation can improve an employee's tendency to comply with the password policy and, at the same time, reduce the possible excuses needed for violating the password policy as a way to maintain productivity. More specifically, these groups chose to adjust policy by focusing on the capabilities of the IT department to handle and support all employees' IT-related issues when they are in a situation requiring urgent solutions and are unable to attend to their workload. For instance, group (A) added the following statement:

Group A:" *If you don't have access to your account due to — for example — an expired password, email IT support@lib.gla.ac.uk for a password reset link, which will be sent directly to your university email account."*

Similarly, group (E) added the following:
Group E: *"In case of emergency or a need for an instant response, please call 12345. We will be available to assist you 24/7."*

Also, group (F) modified the password policy by adding a short statement to encounter the necessity scenario by reminding the employee to contact the IT department in such a situation, like the following:

Group F: "*Refer to IT helpdesk if there is any issue with email/system access."*
Offering an alternative is the second strategy under the concept of providing opportunity. This strategy aims to target the illegal behaviour of the criminal at an early stage by providing alternative solutions to persuade the perpetrator to convert (displace) to a less risky or harmful behaviour [13]. This strategy was discussed by group D members only to counter the DoN scenario. Participants believed that if the rationale for sharing a password is to keep the business performing, the policy may provide an exception to deal with the situation. Thus, they suggested that the employee (the account holder) could authorise his/her colleague to conduct the work on his/her behalf without sharing a password. In this way, the policy can provide alternative and professional assistance to every employee instead of violating the policy by sharing the password. They also assumed that providing such an exception in a password policy would

preserve work performance and make justification via DoN more difficult. This assumption is similar to the "target hardening" in conventional SCPT 25 strategies [12]. Thus, they updated the policy with the following:

Group D: "*If a colleague needs to perform work at your account level, review the request and perform the task for them. If this is too demanding, refer them to the IT Help desk and inform your duty line manager to enquire about temporary or permanent access."*

Additionally, removing excuses was the third strategy that research participants recommended during the collaborative writing process to counter employee justification via DoN. According to DuPreez [13], simplifying regulation requirements can facilitate individual compliance with laws. Simplification can play a fundamental role in removing the excuse that can drive an individual to violate laws due to the complexity or ambiguity of law requirements. In an IT context, for example, providing an employee with a simple and easy way to report any suspicious activity can improve overall security compliance in the workplace [3]. This perception was reflected in groups A and D by directing the employee to do the correct behaviour if he could not access the system and needed assistance, or a co-worker was asked to share the system password, so they added the following:

Group F: *"If a colleague asks to know your password because they have no access to their own account, refuse and refer them to the IT Helpdesk for advice."*

Group D: *"Remember, you can change your password at any time — this will send an email with a password reset link. If you forget your password, use this function rather than asking any co-workers to share their password with you."*

Finally, it was observed that participants in both groups (B) and (C) focused on their argument that the employee may occasionally experience social and contextual discomfort, especially when the employee asks another co-worker to share their password should an employee be unable to access the system for any reason. Under the peer (co-worker or manager) and work pressure, such a situation can motivate the employee to share the password and justify the violation as a necessary action to resolve the situation. This argument was consistent with Wortley's [303] critique, which postulated that there are underlying circumstantial factors that can cause pressures, prompts, or provocations for individuals to commit specific criminal behaviour. Accordingly, Cornish and Clarke [238] updated their original SCPT model [8] to include neutralising peer pressure as one of the SCPT strategies to "reduce provocation" in crime settings. During the collaborative writing activity, both groups (B) and (C) reflected this

strategy to counter the DoN scenario and suggested adding a simple phrase to reduce the problem of peer pressure (provocation) as a trigger for password policy abuse. According to group (B) and (C) discussion records, the password policy should contain clear instructions about appropriate behaviour expected for one to stay in compliance with the policy; this allows the employee (account holder) to refer to the policy as a way to refuse sharing the password, which is necessary to protect IT assets of the organisation. They reflected this argument as the following:

Group B: *"Never disclose or share your password with ANYONE. Even if you think your or your team's performance may be impacted."*

Group C:" *Never disclose or share your password with ANYONE for any reason, not even a person of authority. This includes sharing your password to improve work performance or give professional help, even if it is common practice and you don't expect harm to come for it."*

- **Post-Assessment evaluation:**

According to Table 6.2, the groups' perception of the effectiveness of the updated password policy improved to counter employee justification via DoN for password sharing. This is evident by the fact that the majority of respondents (N= 16, 66%) stated that the updated password policy was somewhat effective (N = 4, 17 %), effective (N = 7, 29 %) and strongly effective (N = 5, 21 %). In contrast, only five of the 24 participants (21%) stated that the password policy resulting from collaborative writing was still ineffective (N= 4) and somewhat ineffective (N = 1) in reducing the tendency of end users' likelihood to justify password policy violation via DoN. Also, a comparison of the pre-and post- evaluations showed that the number of participants who believed the original policy was generally ineffective to counter the DoN was lower on post-evaluation (N = 5) compared to pre-evaluation (N = 8). Moreover, the overall median change improved post-assessment, as shown in Figure 6.9. Participants across all groups had a consensus that the revised password policy via collaborative writing was more effective. It could reduce, from their perception, the tendency of end-users to breach the password policy and justify this violation with the need to maintain business performance (Mdn = 6, Stdev=1.74, and IQR3-IQR = 1.5).

6.3.3 The Appeal of Higher Loyalty (AoHL)

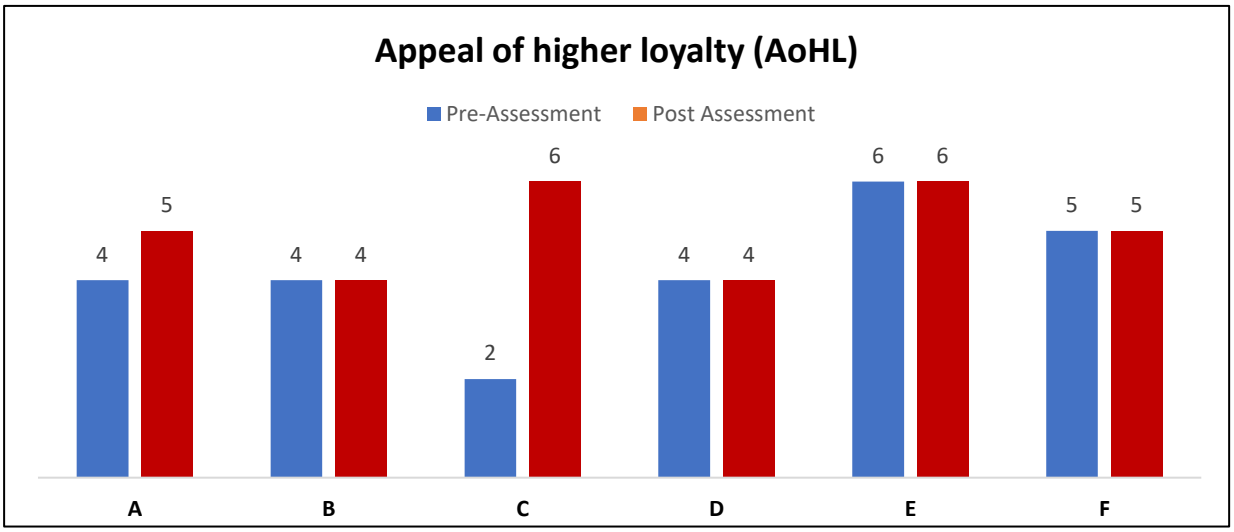


Figure 6.11 Medians Comparison Between All Groups For Appeal Of Higher Loyalty (AoHL)

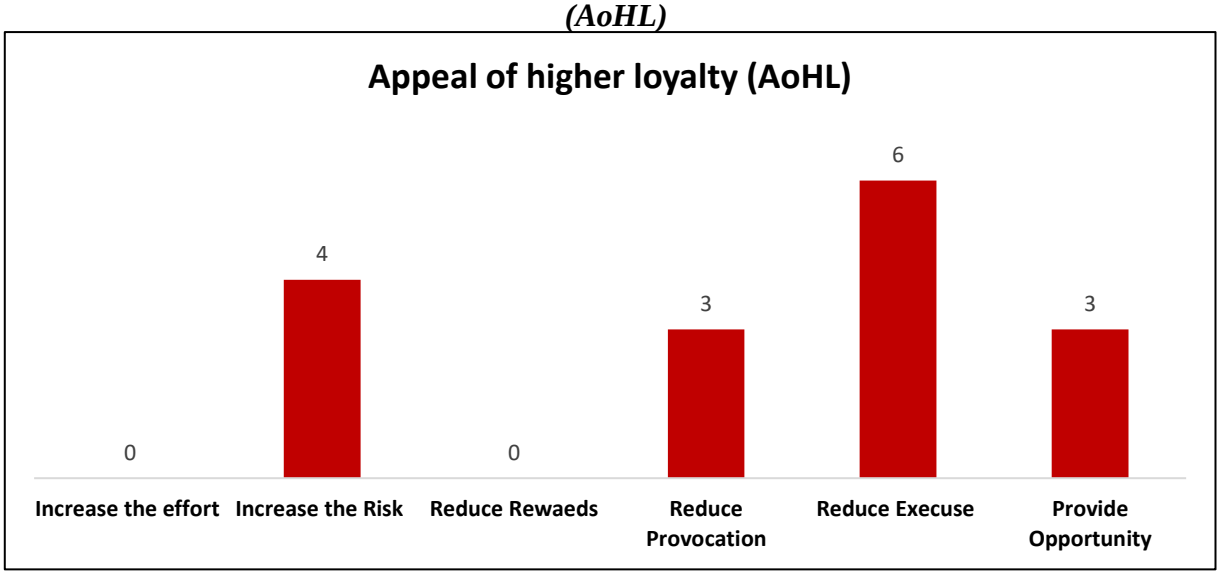


Figure 6.10 Mapping Frequency of codes between Appeal Of Higher Loyalty (AoHL)And The Situational Crime Prevention Theory

- **Pre-assessment evaluation:**

Table 6.2 illustrates participants' perception of the effectiveness of the current policy in mitigating AoHL's claims of a password policy breach. Nine out of 24 respondents (38%) believed that the original password policy was generally ineffective at mitigating an employee's claim that their breach was for "a greater good" or intention [16]. However, most respondents (N = 13, 54%) reported that the original password policy was somewhat effective (N=4), effective (N=7), and strongly effective (N=2) in alleviating an employee's tendency to justify a password policy violation via AOHL. Only two of the participants reported that the password policy was neither ineffective nor effective at reducing the tendency of an employee sharing

their password with a colleague and justifying the violation with ethical reasons such as friendship.

At the group level, the median value for each group revealed a different result. For instance, groups A, B, and D had a similar perception that the password policy in its current state was "neither effective nor ineffective". On the contrary, participants in groups E and F evaluated the policy as "effective" and "somewhat effective", while the median for group C indicated the group participants had a consensus that the policy was "ineffective" at reducing the justification of violating the password policy via the AoHL. Furthermore, the overall median (Mdn= 5, Stdev= 2.02 and IQR3-IQR1=4) across all groups' participants indicated a weak consensus between the groups regarding the effectiveness of the password policy to counter the employee policy violation justification via AoHL.

- **During the collaborative writing:**

This neutralisation technique was analysed by the group's argument and decision on how the requirements of the small group (colleagues) affected the employee's decision to share their password with a co-worker. Therefore, the employee justifies this breach by adhering to the demands of the small group and rejects compliance with the larger group (organisation) security requirements. Also, the decision-making process for each group to identify SCPT strategies that can mitigate the AOHL scenario and report their decision during the collaborative writing process password policy was analysed. At the beginning of the collaborative writing session, the following scenario was projected on the projector screen:

"Sarah knew that Tony was a trustworthy colleague and a member of her team. So, she felt that sharing password was a type of professional help to Tony. Therefore, Sarah gives Tony her password to let him write the required medical note using her account."

A total of thirteen (13) amendments were added to the university's password policy in order to mitigate the employee's tendency to violate the password policy and justify this behaviour as support for their social group's benefit or the pursuit of ideal ethical goals. In addition, an employee might justify InfoSec violation by claiming that he /she was seeking higher organisational value or order, such as helping a colleague to perform the work or task [238]. The groups introduced four main SCPT strategies to mitigate the AoHL as a noncompliance justification of the password policy. These strategies are aimed at reducing excuse, reducing provocation, providing opportunity and increasing the perceived risk.

According to Figure 6.10, across all groups, removing excuses was the most suggested SCPT to counter the AoHL excuse to violate the password policy. The main argument was that being part of a workgroup can increase the employees' tendency to adhere to the regular norms of the workgroups, which includes providing support to other members to achieve organisational goals. This support might include behavioural actions that ignore the security requirements of the password policy, which insisted on keeping the system password/account confidential. Therefore, participants suggested that there was a need to increase the awareness of the importance of password policy and enhance the employee information security sense of keeping their passwords secure. Throughout the collaborative writing process, three reducing excuse sub-strategies were recommended by the group members: post-instruction, asset compliance and alert conscience.

In addition, several groups revealed that there was a close relationship and overlap between the DoN and AOHL, as similar SCPT strategies were identified to counter both of these justifications. In particular, their argument was that if an employee was occasionally unable to perform a necessary work task, they would only ask a close colleague in the workgroup (department) for assistance. Thus, the necessity of performing the task created a situation that made the peer feel responsible for adhering to the group norms of helping each other by sharing the password and 'temporarily' ignoring the password policy.

The most recommended sub-strategy for removing the excuse for confronting an AoHL scenario was posting instructions. Groups A, D, and F focused on adding phrases that recommend an employee to act rationally if a colleague asks them to share their password. Participants in these groups (A, D and F) added the appropriate behaviour (reaction) that the employee needs to exhibit in order to escape the dilemma of adhering to social norms and violating the password policy. In particular, appropriate reactions were absolute denying of password sharing and referring the peer to the IT department for assistance. Moreover, the same groups revealed that posting these instructions that prescribe appropriate behaviour can facilitate and aid an employee's intention to comply with the password policy and, at the same time, reduce the employee's tendency to justify violation via AOHL. Therefore, adding descriptions of appropriate behaviour to the policy can free the employee from adhering to group standards, improve their position to refuse to share their password, and be consistent with the requirements of the organisation's password policy. According to Stemler [13], there is a need to provide an opportunity for conformity to individuals by facilitating and simplifying the process required to comply with the law; therefore, individuals' intention to comply can be improved by removing

their excuse for violating the law. With this in mind, during the collaborative writing process, several groups considered that posting clear instructions in policy could overlap with the conceptual meaning of the sub-strategy (facilitation) providing the opportunity. Here, all the new phrases for removing excuses by posting instructions were labelled to serve the same purpose of providing the opportunity to individuals by facilitating compliance procedures to counter AoHL scenario.

"...the importance of providing instruction clarity to guide how the employee deals with other workers in the workplace. For instance, when an employee faces such problem related to the system, your help supposed to be by directing him/her to the IT department, instead of violating the policy by sharing the password."

In response to this perception, group (A) added the following:

Group A*: "If a colleague asks to know your password because they have no access to their own account, refuse and refer them to the IT Helpdesk for advice."*

Also, members of the (D) and (F) group stated a similar point of view to reducing the excuse for justification via AoHL:

Group D*: "If someone, even a close co-worker or friend, demands to know your password, refuse and refer them to the IT Help-desk for advice."*

Group F: *"If you are asked for your password, reject the request and refer them to the IT help-desk immediately."*

In addition, alert consensus and compliance assistance from group members were proposed as sub-strategies for removing an employee's excuse to justify a password policy violation via AOHL. Here, Group B members discussed the advantage of reminding employees that the relationship with other peers should not be professionally interfering with password policy compliance; and thus, courteousness through sharing the password was the wrong behaviour of the employee. A member in group B discussed this point:

> ***Member from B:*** *"Not sharing the password makes sense, but people sometimes make mistakes until they know this behaviour is against professionalism."*

So, they reflected this perception into the policy by adding:

Group B: "*Do not do it as a professional courtesy."*

Furthermore, removing excuses by facilitating compliance was chosen by group D to mitigate employee tendency to share the password and justify their behaviour via AOHL. Members of group (D) provided additional guidance to assist (facilitate) compliance by explaining how easy it is for an employee to adhere to the password policy and resolve any password issue at any time. This requires the employee to follow a simple step to recover the password via a reset link.

Group D: "*Remember, you can change your password at any time — this will send an email with a password reset link. If you forget your password, use this function rather than asking any co-workers to share their password with you."*

Moreover, increased risk perception was suggested as the second proper SCPT strategy to discourage the end-user tendency to share the system password and justify the action via AOHL. According to Cornish and Clarke [9], an essential aspect of changing the offender's behaviour and reducing the chance of committing a crime is to raise the perception that the authorities have the capacity and power to monitor and apprehend the perpetrator during or after the crime. In our context, reducing anonymity was the sub-strategy that group B chose to counter the employee violation of the password policy and justification via AoHL. Their argument was based on the idea that any employee should be aware that any action in the system is being recorded via the IT department. Therefore, once a data or privacy breach is discovered in the system accounts, the account holder will be responsible for the related damages and consequences. This made it clear that providing support to other employees by sharing the password or account may be counterproductive to the account holder when something goes wrong. This assumption is consistent with Wortley [304], who stated that "being a member of a group or crowd can cause feelings of anonymity and induce a state of psychological disinhibition".

Reducing anonymity by demonstrating this monitoring ability provides the IT department with a perception similar to physical surveillance or field supervision by authorities and can improve the notion that nothing can be hidden from the IT department eyes. In the real world, placing CCTV inside stores and using ID cards to open designated doors aims to improve the perception of surveillance and improve individuals' belief that any misconduct will be noticed, and the perpetrator will be identified, and disciplinary action will be taken sooner or later. In the same direction, members in groups B, E and F modified the password policy by demonstrating the risk of being caught and the associated cost. For instance, a member of group B reported that:

Member from B: *"The end-user needs to understand his/her responsibility to keep the password confidential, and any miss use of the system will be detected and linked to account holder who did that regardless of who made the misuse, later, the IT department will link the action to the account holder, not to the person who actually made the action."*

Therefore, group B added the following statement:

Group B*: "Remember - Any activity taken on your account is linked back to you."*
However, other groups like E and F chose to decrease the risk of password sharing via AoHL by illustrating the negative consequences of this violation. They argued that people sometimes choose to ignore the harmful effect of their deviant behaviour when sharing a password; Hence, providing them with complete information about the expected consequences of a password policy violation can reduce their tendency to misbehave. Therefore, these groups decided that phrases to counter denial of injury could serve the purpose of discouraging justification via AOHL. Thus, they used general statements that work for both justifications DoI and AOHL like the following:

Group E*:" Just a reminder, violating this policy may result in penalties. For more information, please refer to XYZ in the university code of conduct."*

Lastly, measures to reduce provocation and opportunity for violation were suggested to counter the impact of AoHL to justify non-compliance with the university password policy. Both had a similar priority, reducing provocation by neutralising peer pressure was suggested by groups A, C and F. According to Richard Wortley [304], there are often underlying situational factors besides the opportunity of a crime that can cause discomforts such as frustration, crowding, and privacy breach, which could lead to an escalation of aggressive behaviour in locations such as prisons and bars. Cornish and Clarke [238] embraced this approach and incorporated situational attributes, particularly how to reduce peer influence on the occurrence of crime.

The influence between individuals can cause various violations such as driving under the influence of alcohol or violation of organisation policies due to encouragement from other employees. Lowry et al. [5] emphasized the vital role of peer influence in Australian beer-drinking culture. Hence, they have used some of the Australian slogans during safe driving campaigns to advocate for better decisions among friends, such as "Good mates don't let mates drink and drive". These slogans call for safe driving and encourage friends to make the right decision to prevent their peers (mates) from driving while drunk. In our context, some employees may feel uncomfortable under the pressure of colleagues' requests to share the

system password. Thus, members of groups A, C and F shared a common consensus that policy should instruct the employees about the appropriate response to deal with daily social pressure from peers. In particular, they discussed the importance of limiting circumstantial actions that require violating some of the organisation's security policies, such as sharing a password to maintain a positive relationship between employees. Social exchange theory [4] described exchange in human interaction as "*the voluntary actions of individuals that are motivated by the returns they are expected to bring and typically do in fact bring from others*." Thus, a fair and a positive relationship requires a balance between the benefit and cost between all parties.

In the workplace, an employee can demonstrate a commitment and positive attitude toward the group by acting in a way that serves the group's interests [19]. Thus, denying help to other peers by sharing passwords can trigger negative feelings of guilt, shame and can be viewed as evidence of non-commitment to the group norms. A member in the group (A) summarised this point of view as the following:

"The policy should have clear directions for the end-user about the required reaction to ensure policy compliance; these directions can help the employee to deal with social emotions such as embarrassment and guilt associated with not helping other colleagues. These instructions can make the end-user situation more solid when refusing a colleague request to share an account password."

Therefore, the groups added statements that clearly show effective ways to improve the employees' possibility of coping with peer pressure by encouraging employees to uphold primary goals consistent with the organisation's password policy. These instructions can enhance and facilitate the employees' intention to comply and provide an excellent opportunity to escape the dilemma of choosing a commitment to the group desires or organisation security goals. The following statements were added to counter employee justification via AoHL to share the password for good desires:

Group A*: "Never disclose or share your password with ANYONE, including trusted colleagues."*

Group C*: "Never disclose or share your password with ANYONE for any reason, not even a person of authority. This includes sharing your password to improve work performance or give professional help, even if it is common practice and you don't expect harm to come for it."*

Group F*: "Password is always to remain confidential, even between colleagues in a department."*

Group F*:* *"if you are asked for your password, refer them to the IT help-desk immediately."*

Group D*: "If someone, even a close co-worker, demands to know your password, refuse and refer them to the IT Help-desk for advice."*

- **Post assessment evaluation:**

Table 6.2 shows that most of the participants revealed that the updated policy was more effective at mitigating the end-user tendency to justify password policy violation via AoHL. Across the group participants (N=24), eighteen participants (75%) believed that the updated policy that considered the AOHL scenario was somewhat effective (N=3, 13%), effective (N=8, 33%) and strongly effective (N=7, 29%) at discouraging the end users' tendency of justifying sharing password as a form of support. However, four participants (20%) revealed that the modified password policy remained generally ineffective (N=2) or somewhat ineffective (N=2) against the AOHL adoption for password policy non-compliance and only one participant provided a neutral evaluation.

In the group level, the median value for four groups (B, D, E and F) revealed no change in each of the groups' perception of the policy before and after the collaborative writing process. Here, the median of participants' perception of groups B and D remained the same (Mdn=4) which indicated that the password policy before and after the modifications was still "Neither effective nor ineffective". Similarly, the median of pre-assessment and post participants for participants in groups F and E indicated no change in their perception before and after the policy modifications via the collaborative writing process, and the policy remained "Somewhat effective" for Group F members (Mdn=5) and "effective" for Group E members (Mdn=6).

However, the median for participants in group A and B post-assessments indicated an improvement in the effectiveness of the updated policy in mitigating the AOHL claim. The median comparison between the pre-assessment and post-assessment suggested an enhancement of the participants' perception. Here, the median for group A pre-assessment slightly improved from (Mdn=4, "Neither effective nor ineffective") to post-assessment (Mdn =5, "Somewhat effective"). Likewise, group C pre-assessment median of the original password policy was (Mdn= 2, "Ineffective"). The post-assessment median (Mdn=6) of the updated policy indicated that group C's perception improved and considered the updated policy effective at discouraging the end users' intention to evoke AOHL to justify password sharing. Further, table 6.2 shows that the median of participants' overall perception across all groups slightly improved and established more consensus that the revised password policy via collaborative writing was "effective". Thus, from their perception, it could reduce the tendency of end users' non-

compliance behaviour with password policy and justify this violation via AOHL (Mdn = 6, Stdev= 1.83, and IQR3-IQR1 = 2.25).

6.3.4 Everybody Else Is Doing It (EEIDI)

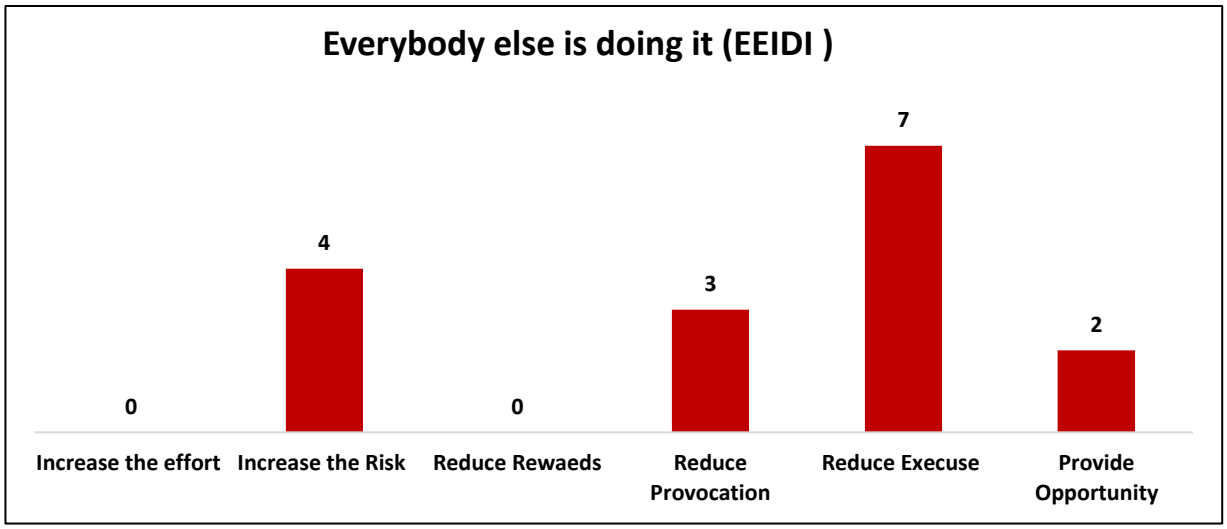


Figure 6.12 Mapping Frequency of codes between Everybody Else Is Doing It (EEIDI)And The Situational Crime Prevention Theory

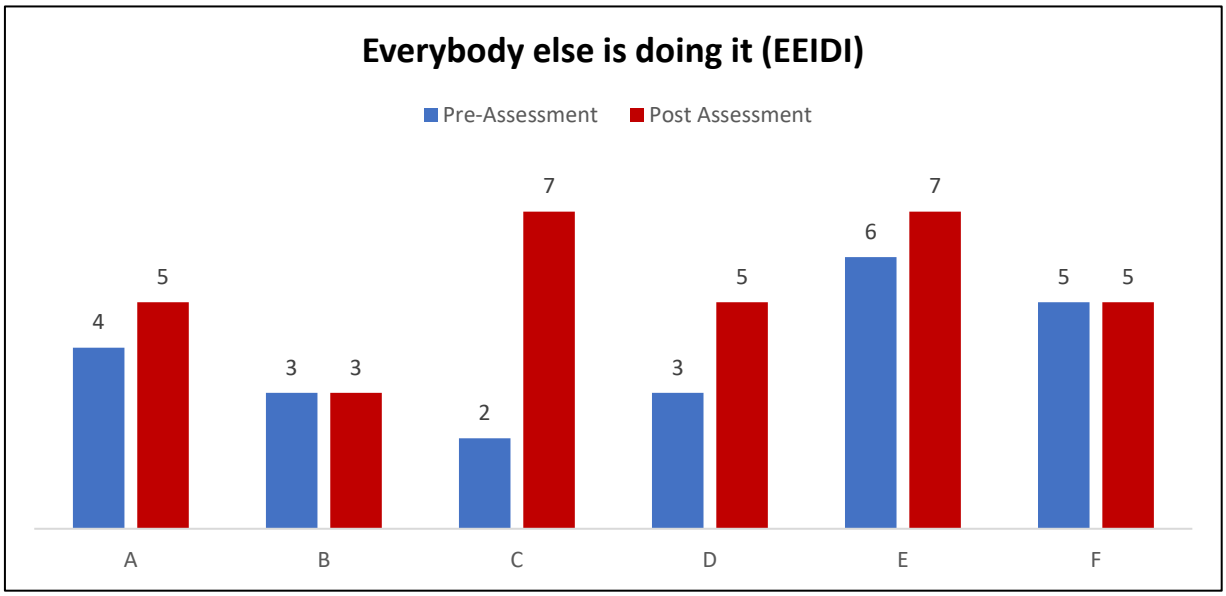


Figure 6.13 Medians Comparison Between All Groups For Everybody Else Is Doing It

- **Pre-assessment evaluation:**

Table 6.2 shows that the participant's perception of the current password policy effectiveness at discouraging end-user justification tendency via EEIDI has two sides. Eleven of 24 participants evaluated the current password policy on the effective side. In contrast, the rest of the participants (N=12 out of 24) assessed the existing password policy as strongly ineffective (N=3), ineffective (N=5) and somewhat ineffective (N=4) regarding its capability to mitigate

end-user EEIDI justification when they share their password. At the group level, as shown in Figure 6.12, the median perceptions of participants across groups B, C, and D shows that the current password policy is somewhat ineffective (B and D, Mdn =3) or ineffective (C, Mdn = 2) at mitigating the end users' tendency of sharing a password and adopting EEIDI as an excuse to justify non-compliance. Conversely, participants in groups E and F indicated that they believe that the current password policy is effective (Mdn=6) or somewhat effective (Mdn=5) at dissuading the end-users from adopting EEIDI as a valid reason to share their passwords and violate the policy. According to Table 6.2, the overall median rating across all groups for the password policy versus EEIDI indicates that the groups have a consensus that the current password policy is neither effective nor ineffective (Mdn=4, Stdev=2.07, and IQR3-IQR1= 4).

- **During the collaborative writing:**

Participants' perception of EEIDI was analysed by their arguments for accepting or rejecting such a justification, the thought process of considering adopting such a justification and the relevant decision-making process for the participants to update the current password policy to counter the end users' tendency to share the password and justify this behaviour by asserting that it is typical behaviour among colleagues, and nothing is wrong. The following scenario was projected on the screen:

"Sarah is an employee in an ABC university, and she has access to the ABC University systems. To ensure that University systems information is preserved securely, the university has a firm password policy that all employees must keep their passwords confidential. One day, Sarah was approached by another employee named Tony, who asked Sarah to share her password with him in order to edit and review student records as Tony's had difficulties to log-in the system. Sarah knew that Tony was a trustworthy colleague. ***Also, she felt that every one of her colleagues was sharing their passwords in the department. Therefore, Sarah gave Tony her password to let him edit student records using her account.*** *"*

Everybody Else is Doing It (EEIDI), according to Freilich and Newman [10], is a neutralisation technique that refers to "individual attempts to reduce guilt or to justify their behaviour by saying that the behaviour in question is common." Here, a total of sixteen password policy amendments were added to mitigate the impact of password sharing and the adoption of EEIDI to justify non-compliance behaviour. Participants in this study chose four SCPT strategies to reflect their perceptions about reducing employees' tendency to adopt EEIDI and abandon the password policy requirement to keep it confidential. According to Figure 6.11, these suggested SCPT strategies are to reduce excuse, increase risk, reduce provocation and provide

opportunities, respectively. Most group participants had a common consensus that the high level of trust among employees was a major factor in making a policy violation such as sharing password/account familiar within a group of employees. A group member explained this perception as the following:

"Everyone around you in the workplace is supposed to be a trusted one who will not do any harm to his colleagues."

It was noted that these SCPT strategies to mitigate EEIDI overlap in several aspects with the suggestions to reduce the employees' tendency to adopt AOHL. Reducing excuses was one of the most recommended SCPT strategies to reduce employees' tendency to adopt EEIDI for password policy violations. The main argument across participants was that an employee in certain situations might not be aware of correct behaviour when dealing with a colleague's request to share a password. Thus, the employee in question will evaluate the requested behaviour based on its popularity among the group members to decide whether to or not to share the password. This argument is consistent with Halbesleben et al. [305], who wrote about the negative impact of social comparison where individuals might make a wrong cognitive decision when they are confronted with an ambiguous situation related to their social environment. Individuals tend to make behavioural comparisons during the decision-making process, and often, they choose to follow the behaviour of other peers as the simplest way to escape from such a situation. For instance, a member in group D stated that:

> ***Member from D:*** *"If other people normally do this, and a colleague asks for your password, and you decline, he may be angry or upset for not helping him."*

Therefore, group D decided that the best way to mitigate the adoption of EEIDI was removing this excuse via altering the conscience of the policy reader. In particular, they added phrases that focus on the importance of keeping the passwords secure and confidential as well as concentrate on employee responsibility to report colleagues who would have shared their passwords to the management. According to Mesko et al.[306], offenders' consciences can be changed through short warning messages clarifying the responsibility and cost of an individual intending to commit an unlawful act. Thus, it can "strengthen moral condemnation" and positively influence the decision-making process. Likewise, group D had a similar perception and added the following statements:

Group D*: "Misuse of your account from a stolen or shared password is your responsibility. Remember, your co-workers might not be as aware of security procedures or careful as you."*

Group D*: "If you know of any colleagues sharing passwords or accounts, this is a significant risk to data security. It is your duty to report this to our anonymous whistle-blower team."*

In addition, the argument of groups E and F about employee propensity to adopt EEIDI was that when unacceptable behaviour such as sharing a system password is common among employees, the majority of these individuals are unaware of workplace security rules or these rules were vague. Thus, Group E and F suggested that the priority, in this case, was to mitigate the misconduct and related justifications, which required updating the password policy by establishing clear security rules and post instructions focusing on appropriate behaviour to ensure password protection. For example, Group E suggested establishing clear security rules that concentrate on sharing passwords is wrong among colleagues and highlights the negative cost of such behaviour at both the individual and the organisational levels. Likewise, Group F modified the policy by posting instructions about the appropriate response to a colleague's request to share a password/account. This was so that the policy could relieve the employee of feelings of guilt or shame for not providing support to another colleague. Here, participants in group F used a more general statement that was also used to mitigate password policy violation via AoHL.

Group E*:" Never disclose or share your password with ANYONE, especially with your colleagues. Previous password sharing between trustworthy colleagues resulted in harming the university, and offenders may be reprimanded, especially with your colleagues."*

Group F*: "If you are asked for your password, refer them to the IT helpdesk immediately."*

Increasing risk perception was the second strategy recommended by the SCPT to improve the password policy to overcome non-compliance and justify this misbehaviour by saying that everyone else does. Participants in three groups (A, E and F) argued that when bad behaviour such as sharing a password was common among employees, it was an indication of poor enforcement of the policy.

Hence, there is a need for the management to properly enforce the password policy and assure that the violation would lead to consequences for the violator. Knapp et al.[94] reported that two factors could improve the effectiveness of an information security policy. The two factors are namely the relevance of the policy and its enforcement. To improve enforcement, the management of the organisation needs to ensure that deterrence measures are in place, and any abusive act that violated the security policy could be monitored and reported. Therefore, any violation of the security policy could be detected, and the violator could be sanctioned; and thus,

without proper enforcement, the effectiveness of information security policy requirements would be useless [6]. Group F emphasised extending guardianship by calling for any suspicious action between colleagues to be reported if it could lead to a password policy violation. A member in group F explained this point as the following:

> ***Member from F:*** *"They should also explain in the policy that he must inform the IT department of any behaviour that could compromise the password policy such as sharing the password between the employees in the department."*

While participants in groups E and A decided, for example, that the previous phrases that have been added to reflect expected injuries or consequences from password sharing against in the first scenario (DoI) could serve the same purpose to reflect the enforcement perspective of a password policy to mitigate employees' tendency to adopt EEIDI for non-compliance with the password policy. This is consistent with Bandura's [154] explanation of the impact of reinforcement and punishment on the individuals' behaviour in social learning theory. He stated that people tend to repeat others' behaviour which they would have learnt via observation. The observer may choose to repeat specific behavioural actions depending on whether people will be rewarded or punished for their actions and the outcome of this behaviour. Therefore, during collaborative writing, several groups reflected these different perceptions as the following:

Group A*:* *"Just a reminder, violating this policy may result in penalties. For more information, please refer to XYZ in the university code of conduct."*

Group E: *"Never disclose or share your password with ANYONE, especially with your colleagues. Previous password sharing between trustworthy colleagues resulted in harming the university, and offenders may be reprimanded, especially with your colleagues."*

Group F*: "If you have suspicions that your department is sharing passwords, you should immediately contact your IT helpdesk."*

Reducing provocation was the third suggested SCPT strategy to mitigate the password policy violation via EEIDI. It was noted that three groups (A, B and C) adopted this SCPT strategy. Among the groups, the common perception was that when sharing a password is a common behaviour with the team, it will cause frustration for the employee who wants to comply with the security policy, specifically if the policy does not provide the correct reaction to neutralise the peer pressure. So, these groups suggested that organisations can overcome these teamwork issues and relevant justifications for violating the password policy by providing and clarifying the decision and the correct procedures to deal with peer pressure. Thus, the employee can

neutralise the refusal to share the password when a colleague requests for their password. For instance, these groups modified the original password policy that discouraged sharing passwords by adding the term "never", which indicates an explicit prohibition from sharing the password. For instance, they added "even with a trusted colleague" or "even if everybody else is doing it"; thus, it could help from their perception, the organisation in the long term to discourage the employees from imitating each other in such undesirable behaviour. Groups added the following:

Group A: *"Never disclose or share your password with ANYONE, including trusted colleagues."*

Group B*: "Never disclose or share your password with ANYONE, Even if "Everybody else is doing it."*

Group C*: "Never disclose or share your password with ANYONE for any reason, not even a person of authority. This includes sharing your password to improve work performance or give professional help, even if it is common practice and you don't expect harm to come for it."*

Lastly, providing opportunity was the least suggested strategy to reduce justifying password sharing via "Everybody else is doing it". Only two groups (B and F) suggested such an approach, and they believed that the IT department needs to show its commitment and responsibility by assisting any employee who could be having difficulties accessing the system, by so doing, it will support the employees and reduce peer pressure through providing the employees with a chance to solve the conflict between the team norm and security requirements. A member in group B explained such variance:

> ***Member from B:*** *"If my colleague requests my password, I will help him by contacting the IT department or teaching him how to reset the password. I will not share my password."*

Thus, they update the policy by adding the following:
Group F: *"If you are asked for your password, refer them to the IT helpdesk immediately."*

Group B: *"Never disclose or share your password with ANYONE. If they demand to know your password - refuse and direct them to management."*

- **Post-Assessment evaluation EEIDI:**

As shown in Table 6.2, the respondent's evaluation of the university password policy (N=24) shows an improvement in the post-assessment of the password policy after the engagement of the end users' perception to counter EEIDI.

The majority of the respondents' perception (N=17, 70%) reported that the updated password policy is effective (N= 5, 21%), somewhat effective (N= 4, 17%), or strongly effective (N=8, 33%) at discouraging the EEIDI security claims to share the password. In contrast, five participants of the 24 believed that the updated password policy was still generally ineffective at mitigating the employees' tendency to adopt the EEIDI claim and share the password. At the group level, according to Figure 6.12, members in groups A, C, D and E reported an improvement in their perception of the updated password policy after the collaborative writing as the medians varied from (4, 2, 3, 6, and 5) in the pre-assessment to (5, 7,5, and 7) in the post-assessment. While groups B and F members reported that there were no differences from their perception between the pre-and post-assessments, which means that the updated password policy was still considered ineffective at mitigating the individuals' tendency to evoke EEIDI to justify sharing passwords. In addition, across all groups' members, the overall perception indicated that the participants generally showed more consensus that the updated password policy, considering the updated password policy was effective at confronting the employees' tendency to adopt EEIDI as a justification for policy violation (Mdn=6, Stdev= 1.8, and IQR3-IQR1=3).

6.4 Descriptive Analysis of All Participants

Table 6.3 reveals the descriptive results of all participants' pre-and post-assessment surveys for dependent variables: denial of responsibility, denial of injury, defence of necessity, Everybody else is doing it, appeal to higher loyalty, overall effectiveness, self-efficacy and work Impediment. All of them relied on ordinal data and were measured using seven points Likert scale (1=Strongly Ineffective, 2= ineffective 3= somewhat ineffective 4= neither effective nor ineffective 5= somewhat effective, 6= effective, and 7=Strongly effective). It shows the median difference in the participants' perception of the password policy's effectiveness before and after integrating the neutralisation techniques via a collaborative writing process. Table 6.3 shows that the median differences between the pre-and post-assessment surveys were slightly decreased for self-efficacy as the median value for the pre-assessment was (Mdn=7) and decreased in post-assessments to (Mdn=6), which indicated that many participants believed that they were less competent to fulfil the security requirements of the updated password policy.

Table 6.3 Descriptive Statistics for all participants

Dependent Variables	N	Median (Mdn)		Standard Deviation (stdev)		Interquartile Range (IQR)					
		Pre-assessment	Post-assessment	Pre-assessment	Post-assessment	Pre-assessment			Post-assessment		
						IQR3	IQR 1	IQR 3- IQR 1	IQR 3	IQR 1	IQR 3 - IQR 1
Denial of Responsibility	24	5	6	2.10	1.56	6	2	4	7	4	3
Denial of injury	24	5	6	1.99	2.07	6.25	3	3.25	7	4.5	2.5
defence of necessity	24	5	6	1.77	1.74	6	3	3	6	4.5	1.5
Everybody else is doing it	24	4	6	2.07	1.80	6	2	4	7	4	3
Appeal to higher loyalty	24	5	6	2.02	1.83	6	2	4	7	4.75	2.25
Overall Policy effectiveness	24	5	6	1.86	1.64	6	2	4	6	4.75	1.25
Self-efficacy	24	7	6	1.40	0.79	7	6	1	7	6	1
Work impediment	24	3	3	1.77	1.72	5	2	3	3.25	2	1.25

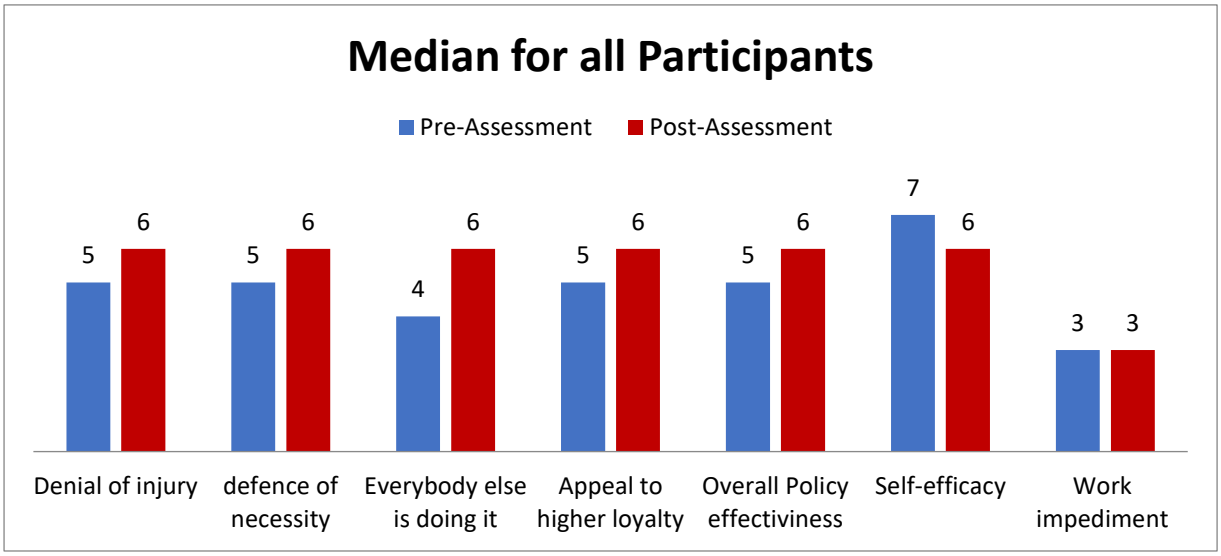


Figure 6.14 Median Across All Groups' Participants

Also, the median values for all neutralisation techniques used in this study, DoR, DoI, DoN, EEIDI and AOHL, slightly increased from (5, 5, 5, 4 and 5) to (6, 6, 6,5 and 6) respectively. Participants were asked a single question about the overall effectiveness of password policy before and after the integration of the neutralisation techniques. This revealed a slight improvement in the participants' perception as the median increased from (5) to (6). Therefore, the difference in the medians points out an improvement in the participants' perception of post-assessment when they evaluate the updated policy. The differences between pre-and post-

assessment medians indicate that the updated password policy is more effective from the participants' perspective after the collaborative writing to counter the study justification scenarios. Last, the ability for the password policy to impede the work activities for the end-users remained the same from the pre-assessment (3) to post-assessment (3). This revealed that the updated password policy after incorporating the neutralisation techniques via the collaborative writing session did not add complexity to the password policy from users' perception.

However, it is difficult to presume that the engagement of the end users' perception via a collaborative writing session caused a statistically significant enhancement in the security policy's effectiveness without testing the differences via a significance test. Therefore, the Wilcoxon signed-rank test was adopted to measure the end users' perception changes toward the password policy's effectiveness from the same individuals before and after the collaborative writing session.

6.5 Overall Statistical Significance Test for All Participants

Table 6.4 Overall Hypothesis Test for All participants

Dependent Variables	Null Hypothesis	Z-value	Sig,P value	Decision
DOR	**The median of differences between DoR Before ISP Collaborative writing and DoR *After ISP Collaborative* writing equals 0.**	**1.006**	**0.315**	**Retain the null hypothesis.**
DOI	**The median of differences between DoI Before ISP Collaborative writing and DoI After ISP Collaborative writing equals 0.**	**1.795**	**0.073**	**Retain the null hypothesis.**
DON	**The median of differences between DoN Before ISP Collaborative writing and DoN After ISP Collaborative writing equals 0.**	**2.009**	**0.045**	**Reject the null hypothesis.**
EEIDI	**The median of differences between EEIDI Before ISP Collaborative writing and EEIDI After ISP Collaborative writing equals 0.**	**2.858**	**0.004**	**Reject the null hypothesis.**
AOHL	**The median of differences between AOHL Before ISP Collaborative writing and AOHL After ISP Collaborative writing equals 0.**	**2.291**	**0.022**	**Reject the null hypothesis.**
Overall Effectiveness	**The median of differences between Overall Effectiveness Before ISP Collaborative writing and Over All Effectiveness After ISP Collaborative writing equals 0.**	**1.755**	**0.079**	**Retain the null hypothesis.**
Self-Efficacy	**The median of differences between Self-Efficacy before ISP Collaborative writing and Self Efficacy after ISP Collaborative writing equals 0.**	**0.209**	**0.835**	**Retain the null hypothesis.**
Work impediment	**The median of differences between Work impediment before ISP Collaborative writing and Work impediment after ISP Collaborative writing equals 0.**	**-0.522**	**0.601**	**Retain the null hypothesis.**

Table in (Appendix C.2) presents the Wilcoxon signed-rank test result for all participants. In this study, we checked the impact of integrating the Neutralisation techniques on the InfoSec effectiveness via pre- and post-assessments. Through this way, we found that the P-value for both DoR (Z=1.006, P=0.315) and DoI (Z=1.795 p=0.073) are bigger than 0.05. These results indicate that the post-assessment result of the participants' evaluation of the ISP effectiveness is not statistically significant; thus, the null hypothesis should be retained. However, the DoI in Table in (Appendix C.2) shows a trend towards significance as fourteen (N=14) of the participants revealed positive improvement in their post-assessment ranking after the collaborative writing process of the InfoSec policy.

In contrast, the P-value for other neutralisation techniques DoN, EEIDI and AOHL shows a statistically significant difference between the pre-and post-assessments of the participants' perception about the ISP effectiveness before and after the intervention. Table 6.3 illustrates the P-value for DoN (z= 2.009, P=0.045), EEIDI (Z=2.858, P=0.045) and AOHL (Z=2.291, P=0.022), which are less than (0.05). Therefore, our analysis confirms the participants' perception of policy effectiveness to counter DoN, EEIDI and AOHL significantly improved after the collaborative writing activity. Thus, we have enough evidence to reject the null hypotheses here.

Also, as illustrated in Table (Appendix C.2), the P-value for self-efficacy is (Z=209, P=0.835). It means that the median difference between Self Efficacy before and after ISP collaborative writing is equal to 0. Thus, there is no statistically significant difference in the participants' self-efficacy, so we retain the null hypotheses. This result indicates that participants' confidence in implementing the updated password policy requirements compared to the original policy remains the same. Thus, it provides evidence that the end-users can produce an updated policy that does not require additional skills or efforts to comply.

In addition, the P-value for the ISP work impediment on the participants' daily activities is (Z=-0.522, P=0.601). In this context, we evaluate how the existing password policy complicates the work and how integrating the neutralisation techniques via collaborative writing can reduce the password policy's complexity perception. The result reveals that the rejection of the null hypotheses is not possible. This is because findings show no statistically significant difference in the complexity of the password policy between the pre-and post-assessments after modifying the ISP. This result is consistent with the data in Table 6.3; it implies that the updated password policy does not add security requirements that can impact the end-users productivities. In general, the participants perceive that both the original and updated password policies still

hinder their work activities. However, we did not directly ask the participants during the collaborative writing process to make the password policy easier.

6.6 Chapter Summary

This chapter contributes to the thesis by analysing and describing the research intervention through a security policy's collaborative writing process to mitigate the end users' tendency of justifying a policy violation (password sharing). This chapter collected data via three consecutive steps: a Pre-assessment survey to evaluate the giving policy overall effectiveness against four hypothetical scenarios related to neutralisation techniques, observations during the collaborative writing process and the group argument and decision-making process to mitigate each of the justification in the scenarios. The third step was a post-assessment survey of the modified security policy's overall effectiveness after a focus group collaborative writing process. This empirical study makes an essential contribution to the thesis by providing evidence that the engagement of the end users' perception via a collaborative writing process could play a crucial role in developing effective security policies that better fit the work environment. Thus, it can reinforce behavioural compliance by reducing the end users' tendency to justify non-compliance with InfoSec policies.

This chapter explains the quantitative and qualitative approaches of collecting and analysing data and the statistical methods of interpreting the pre-assessment and post-assessment results. The results showed that integrating the end-user perception via a collaborative writing process improves the password policy's effectiveness at mitigating some of the neutralisation hypothetical scenarios to share the password with others. Also, engaging the perception of end-users by incorporating neutralisation techniques provides the IT department with a better understanding of the factors that stimulate the behavioural justifications of individuals and the mitigation approach that end-users adopt to confront this behaviour based on their understanding of business needs and the social context. The next chapter aims to generalise this study result by repeating in a different context at one of the biggest academic hospitals in Saudi Arabia.

Chapter 7 : Enhancing Infosec Policy Effectiveness Against Neutralisation Techniques Via The Engagement Of End Users In Policy Development (The KSA Hospital).

The previous chapter demonstrated that the engagement of end user perception via a collaborative writing activity could improve the effectiveness of password policies to mitigate some of the end users' justifications to share a password between colleagues. This chapter introduces the 4th and final phase of the research study, as shown in Figure 7.1. This phase repeats the chapter 7 intervention in one of the biggest hospitals in Saudi Arabia, the results in two different contexts (academic and healthcare) and between two different countries (the UK and Saudi Arabia) could improve the generalisation purposes.

Phase 1	Phase 2	Phase 3	Phase 4
Determine the role of Neutralisation techniques to predict medical practitioner intention to violate InfoSec policies. A quantitative study using a questionnaire in Saudi Arabia.	Investigate the motivations of medical practitioners to evoke neutralisation techniques to justify InfoSec violations. A qualitative study using semi-structured interviews in a Saudi Arabian hospital.	Enhancing InfoSec policies effectiveness against neutralisation techniques via the engagement end-user perception. An action research study using focus groups and pre and post questionnaires in the UK, University of Glasgow.	Enhancing InfoSec policies effectiveness against neutralisation techniques via the engagement end-user perception. An action research study using focus groups and pre and post questionnaires in a Saudi Arabian Hospital.

Figure 7.1 Phase Four Of The Research Study

This chapter contains the following sections. Section 7.1 explains the study's aim and purpose, while Section 7.2 provides details about the study's methodology. Section 7.3 explains data and outcome analysis and provides comprehensive information about the study's analysis procedure and the qualitative analysis of neutralisation techniques and mitigation strategies to improve the current hospital password policy in Saudi Arabia. Section 7.4 introduces the descriptive analysis, and Sections 7.5 and 7.6 provide a statistical significance test result. Section 7.7 summarises the contribution of the chapter to this thesis.

7.1 Purpose of The Study

This empirical study used a collaborative writing process to enhance the information policy effectiveness to reduce the tendency of end-users to justify policy non-compliance. In

particular, it seeks to determine whether the engagement of the end users' perception in a complex environment such as healthcare can enhance Infosec policies to be more user-centric and increase the alignment between the security requirements and medical practitioners' work duties. Thus, it can reduce an individual's tendency to adopt neutralisation techniques to justify password violation.

Only a few security scholars have attempted to counter neutralisation techniques, and all of those conducted studies attempting to change InfoSec non-compliance behaviour via various structured and unstructured Security Education, Training, and Awareness (SETA) programs. None took a close look at the security policy usability and its role on individual justifications (see chapter 2, section 2.7.3 for more details). The previous chapter provides evidence that engaging end-users in modifying password policy through collaborative writing can increase user-centred policy design and enhance its effectiveness in mitigating some neutralisation techniques. Consistent with our findings in chapter 5, environmental factors exert pressure on individuals. One of the main pillars of this pressure is employees' realisation that security policies are incompatible with their primary tasks. This misalignment of the security requirements increases individuals' likelihood to justify their security breach and endanger the organisation's security objectives. Likewise, in chapter 6, we argue that organisations need to revaluate their information security policies that disrupt work productivity and increase social pressure, inducing justifications to violate the existing security policies. Thus, the engagement of the InfoSec end-users to enhance the security policies via collaborative writing can be a promising approach to reduce the individual tendency to justify the non-compliance behaviour, primarily because it can improve the balance between security requirements and work objectives. Forty-two medical interns participated in this study from one of the largest academic hospitals in Saudi Arabia. We will refer to this hospital in this study as the "ABC hospital" for confidentiality purposes.

7.2 Study Methodology

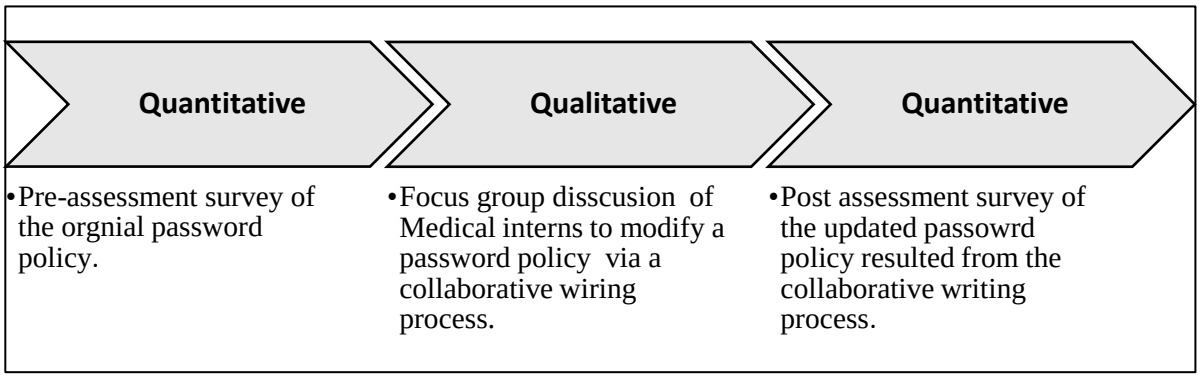


Figure 7.2 Study Methodology and Data collection for phase four study

- **Data Collection Method**

Pre- and post-assessment surveys included several security claims representing five neutralisation techniques—Denial of Responsibility (DoR), Denial of Injury (DoI), Defence of Necessity (DoN), Everybody else is doing it (EEIDI), and Appeal of Higher loyalty (AoHL).

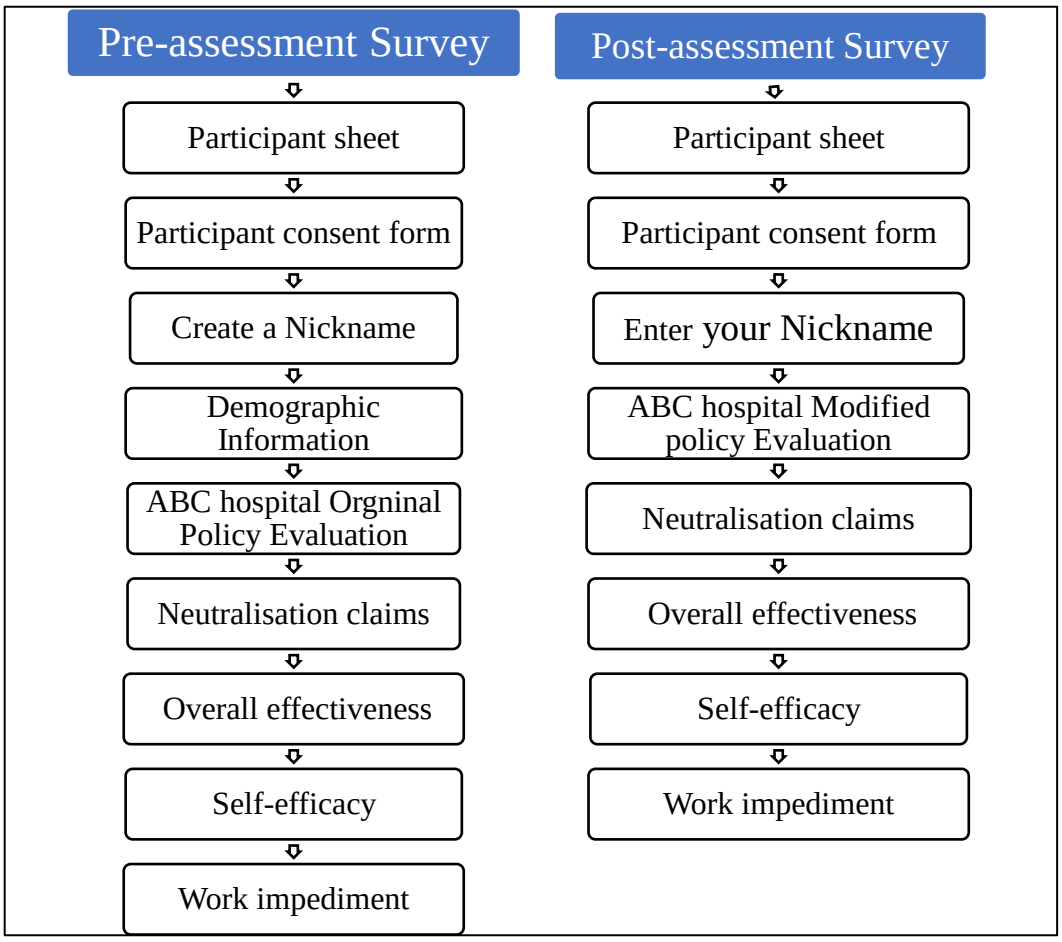


Figure 7.3 Pre And Post Assessments' Sections Follow.

Both surveys included additional constructs regarding self-efficacy, work impediment, and the overall security policy effectiveness. These surveys aimed to discover whether there was a significant improvement in password policy effectiveness to reduce the use of neutralisation techniques to violate the password policy. The study method described in the previous chapter was identical to the method used to conduct this study (see chapter 6, section 6.2 for more details). The only difference in the current study was that both the pre-and post-assessment surveys included the hospital password policy instead of the University of Glasgow password policy used in chapter 6, as shown in Figure 7.3. Also, all security scenarios that reflect four neutralisation techniques—Denial of Injury, Defence of Necessity, Everybody else is doing it, and Appeal of Higher loyalty—were revised to represent working in the hospital context. (Appendix D.1 for pre and post-assessment questions and Appendix D.4 for a security scenarios list). The researcher obtained ethical approval to conduct this study under application number 300190037 (Appendices D.5 Ethical approval and D.6 participants' sheets).

- **Study Sample**

The study sample was the medical interns in one of the largest academic hospitals in Saudi Arabia. All medical schools in Saudi Arabia require their students to study a total of seven years; the Medical Internship Program (MIP) comes after the sixth year of mandatory medical courses. The medical internship programs and materials are essential components in increasing the knowledge base and practical experience of these future doctors [307]. (chapter 4, section 4.3.3 provides more information about the study sample.) Each medical intern (MI) works under close supervision of senior physicians at the ABC hospital as they rotate through various clinics. The job duties of the medical interns are similar to the primary roles of senior physicians, which include interacting with patients, examining and diagnosing them, reviewing medical records, providing patient care, and so forth. The IT department creates an EMR account for each MI once a medical student is assigned to the hospital to start their MIP year. Unlike senior physicians, the medical interns are limited to reviewing patient records and writing medical notes; they are not privileged to issue such medical orders as lab tests, medications, X-rays, and so forth.

The researcher communicated with both the IT department and the ABC hospital's College of Medicine for approval and support in conducting the study. The ABC hospital's IT department assigned a secretary to provide logistic support. In addition, the dean's office of the College of Medicine at the hospital provided the names and emails of all the medical interns and sent the

first invitation email for the study to all medical interns during the 2019–2020 MIP year. The Dean's office also appointed a medical intern as a coordinator between the researcher and the medical interns; this individual was responsible for sending reminders about the study to the participants and communicating with them about the venue of the meetings. The invitation email included a link to a scheduling website (doodle.com) that the participants used to register their personal information and select the time and dates of their involvement in the study.

- **Study procedures**

Once five participants formed a group based on their choice of the available time and date slots, the researcher contacted them by email and provided them with the meeting time for the focus group's collaborative writing activity. So, each MI participant was assigned randomly to a group based on their choices of available date and time slots without any interference from the researcher. After each participant read the participant sheet and accepted the terms and conditions of the consent form, they received the online link for the pre-assessment survey one day before the collaborative writing activity that encouraged them to complete the survey ahead of the meeting time. As illustrated in Figure 7.3, the pre-assessment and post-assessment sections were designed as follows:

1. **Preassessment survey (21 questions):** (Appendix D.1 provides a list of the survey measurement items for both preassessment and post-assessment)**.**
   1.1. **Create a Nickname:** After reading the participant sheet and accepting the consent form, the survey starts by asking the respondent to create a nickname for the purpose of confidentiality. The nickname was used to connect each respondent's answers from the pre-assessment to the post-assessment to identify any changes between the two.
   1.2. **Demographic information:** After crating the nickname, the respondent completed three demographic questions about gender, level of education and the ability to access the hospital's EMR system. If the respondent answered "NO" to the last item, which indicates that the MI does not have access, a thank you message appeared, and the survey ended.
   1.3. **ABC hospital original policy evaluation:** The respondent read the hospital's current password policy, then proceeded directly to the neutralisation techniques section.
   1.4. **Neutralisation claims**: This section aimed to measure end-user perception regarding the effectiveness of the hospital password policy to counter several claims that end users might adopt to justify their behavioural violation of policy. This section required

the respondents to answer a total of 11 questions derived from the InfoSec literature and represented five neutralisation techniques, Denial of Responsibility, Denial of Injury, Defence of Necessity, Everybody else is doing it, and Appeal of Higher loyalty. For example, a Denial of Responsibility claim is, *"From your perspective, how effective do you think is the above policy in countering the following claim: it is not my fault that the hospital provides complex password management procedures that are inefficient. Thus, I will share my password with a trusted colleague."*

1.5. **Overall policy effectiveness:** This is a single question following the neutralisation claims section intended to determine the respondent's evaluation of the hospital current password policy effectiveness to counter all previous neutralisation claims.

1.6. **Self-efficacy:** This section was measured via three items using a 7-point Likert scale from 1, Strongly Disagree, to 7, Strongly Agree. These items are intended to capture the respondent's confidence to meet all the password policy requirements. For example, *"I have the necessary skills to fulfil the requirements of this policy."*

1.7. **Work impediment:** This section was measured via four items using the same 7-point scale as in the previous section. These questions aimed to identify the MI's perception of the complexity that the hospital password policy requirements added to the work productivity. For instance, *"Following the requirements of the given password policy distracts me from doing my actual work duties."*

2. **Post-assessment survey (18 questions):** This is identical to the pre-assessment survey, except for two sections. The demographic information section was eliminated, and the password policy evaluation section was changed to include the updated content of password policy resulting from another group's collaborative writing. The survey aims to evaluate any change of perception after the collaborative writing process modified the hospital password policy.

Unlike the study in chapter 6, the post-assessment was sent two weeks after the group discussion for the collaborative writing process due to the difficulties of forming two groups in one week and the slow participation rate from MIs. Thus, the total days to conduct this study was approximately 110 days, and the study successful recruited 42 participants forming ten groups. Eight groups (A, B, C, D, E, F, J, and G) contained four participants per group, while two groups (I and J) had five participants each. Figure 7.3 illustrates the overall data collection process for this study:

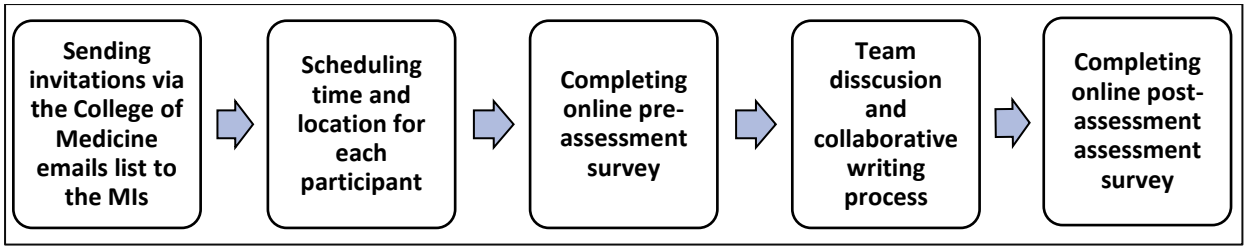


Figure 7.4 Data Collection procedures

As Figure 7.4 illustrates, the collaborative writing activity started after group members completed the pre-assessment survey. At a specific time and location, each group met face-to-face for the collaborative writing process. The current study was a group effort to discuss and modify the hospital password policy to counter a set of neutralisation scenarios that led to the violation of the password policy (see chapter 3, section 3.3.6.2 for more details about CW). At the beginning of this activity, the researcher distributed a document that included the hospital's current password policy and a list of neutralisation scenarios. Then the researcher applied the CW strategy called "a group single-author writing" and asked the group to choose an editor responsible for writing the group changes directly to the hospital password policy document. This CW strategy was appropriate because the group was small and interacting face-to-face. The CW started when each member read the policy, discussed how to counter each neutralisation scenario, and reviewed the hospital's password policy to address these scenarios. The group members coded each of their modifications (solutions) with the corresponding neutralisation technique. Once consensus was reached on all changes for each scenario, the CW session was ended.

Each CW session lasted between 60–120 minutes, and the majority of the collaborative writing sessions were audio-recorded. The researcher was present in the meeting room during these sessions, taking notes and observing without interference. All the collaborative writing discussions were mainly in English. After each session, all audio records were encrypted in a USB device, and the researcher notes were securely stored. The last part of the research methodology was the post-assessment survey, which aimed to determine any variation of the MI's perception of the updated password policy effectiveness to mitigate neutralisation claims to share the password. Most of the MIs received an online link to the post-assessment survey two weeks after the CW. Both the pre-and post-assessments were developed using a user-friendly online service (surveymonkey.com) that can be accessed via PCs or portable devices. The approximate time was 15–20 minutes to complete each of the pre-and post-assessments.

7.3 Analysis and Results

As in the previous chapter, we used qualitative and quantitative approaches to collect and analyse data. In this study, we repeated all the data collection and analysis procedures stated in chapter 6 (see section 6.3 for more details). In summary, first, the researcher used content analysis to examine all the password policy documents resulting from the CW process of the ten groups. Then we grounded the content analysis based on a prior coding approach [242] by using the Situational Crime Prevention Theory (SCPT) to generate meaningful codes and themes. Thus, all the modified documents of the hospital password policy were analysed following Krippendorff's [195] content analysis procedure, as shown in Figure 7.4.

Second, the researcher created an MS-Excel sheet that included all the added or modified sentences from the modified password policy documents—ten documents from ten MI groups. Each modified or added statement was identified and exported to the MS-Excel sheet (Unitizing). When a complete list of all the added or altered statements was generated, three copies of the MS-excel sheet were distributed to three independent researchers for the coding phase based on the SCPT codes and themes. Once those three independent researchers finished the coding phase, a focus group discussion was conducted to seek consensus for each code. This stage was completed when each added or modified statement was assigned to at least one code under a specific theme, as illustrated in Figure 7.5. Then, the researcher statistically and qualitatively analysed and reported the result.

The following subsections provide more details about the quantitative survey (pre-and post-assessments) results along with qualitative content analysis of modified password policies via the CW process. Each subsection addresses one of the neutralisation techniques in the study scope—Denial of Injury, Defence of Necessity, Appeal of Higher Loyalty, and Everybody else is doing it. The analysis includes three steps:

- **Pre-assessment:** This step was essential to capture perceptions of the hospital's existing password policy before modifying it via the collaborative writing process. An online survey includes several neutralisation claims (See Appendix 7. A) that an individual might use to violate password policy. Thus, we measured the effectiveness of the current password policy against these claims based on the calculation of medians of the participant answers. Later, an overall significant test was performed to calculate the variation of the participants' evaluation of the password policy effectiveness before and after the CW process.

- **The collaborative writing process:** We observed the discussion to counter each of the justification scenarios to understand their behavioural intention to accept or reject each justification. Therefore, we can evaluate their understanding of the importance of security compliance during their daily activities indirectly. Moreover, we were keen to understand how each group provided a solution to mitigate the consequences of each neutralisation technique under the lens of SCPT theory, which can be reflected as a text by modifying a given security policy.
- **Post-assessment:** The post-assessment survey was used to measure any change of evaluation of the modified password policy produced via the collaborative writing process. The median difference between the pre- and post-assessments can reveal whether the effectiveness of the revised password policy improved or not.

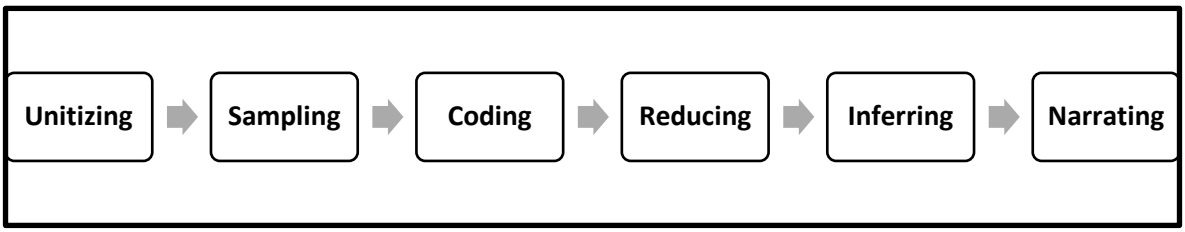


Figure 7.5 Krippendorff's Procedure For Content Analysis

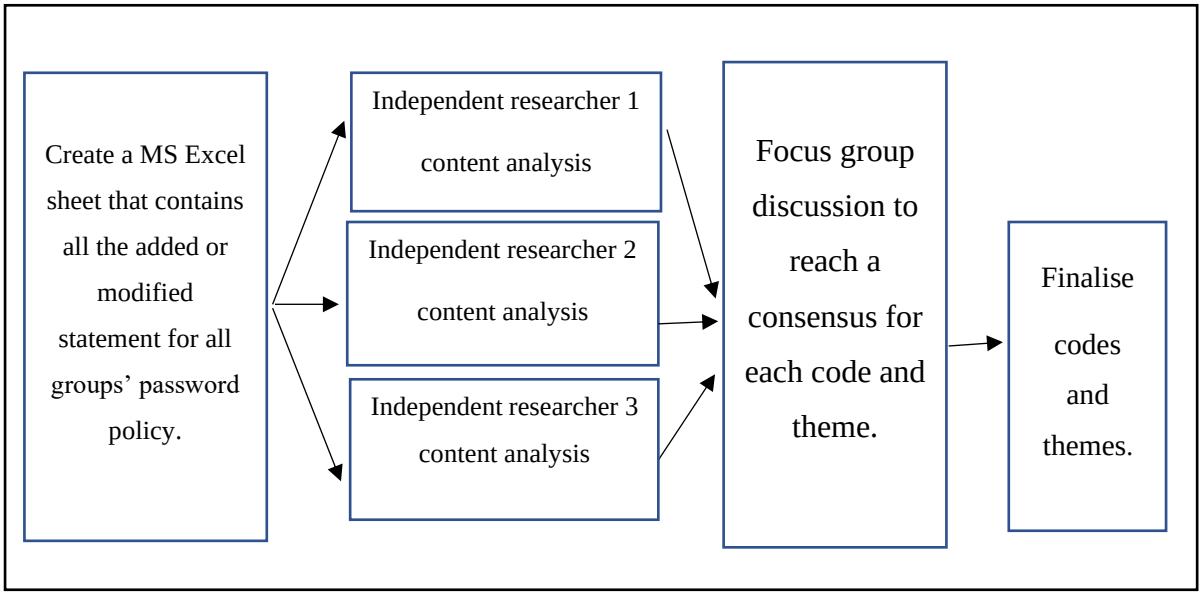


Figure 7.6 Independent Researchers Content Analysis and Focus Group Processes

Table 7.1 The Overall Pre-Assessment and Post-Assessment Frequency (%) Of Neutralisation Techniques

Pre assessment	**Denial Of Injury**	**Defence of Necessity**	**Everybody else is doing it**	**Appeal to higher loyalty**	**Policy Overall effectiveness**		**Self-efficacy**	**Work Impediment**
7 points Likert Scale	**Frequency (%)**	**Frequency (%)**	**Frequency (%)**	**Frequency (%)**	**Frequency (%)**	**7 points Likert Scale**	**Frequency (%)**	**Frequency (%)**
Strongly Ineffective (1)	**3 (7%)**	**1 (2%)**	**5 (12%)**	**4 (10%)**	**3 (7%)**	Strongly Agree	**1 (2%)**	**0 (0%)**
Ineffective (2)	**15 (36%)**	**17 (40%)**	**11 (26%)**	**12 (29%)**	**21 (50%)**	Agree	**0 (0%)**	**5 (12%)**
Somewhat Ineffective (3)	**8 (19%)**	**12 (29%)**	**12 (29%)**	**9 (21%)**	**12 (29%)**	Somewhat Agree	**1 (2%)**	**6 (14%)**
Neither effective nor ineffective (4)	**3 (7%)**	**6 (14%)**	**3 (7%)**	**7 (17%)**	**5 (12%)**	Neither Agree nor Disagree	**6 (14%)**	**5 (12%)**
Somewhat effective (5)	**5 (12%)**	**5 (12%)**	**8 (19%)**	**9 (21%)**	**1 (2%)**	Somewhat Disagree	**13 (31%)**	**14 (33%)**
Effective (6)	**7 (17%)**	**1 (2%)**	**3 (7%)**	**0 (0%)**	**0 (0%)**	Disagree	**14 (33%)**	**6 (14%)**
Strongly effective (7)	**1 (2%)**	**0 (0%)**	**0 (0%)**	**1 (2%)**	**0 (0%)**	Strongly Disagree	**7 (17%)**	**6 (14%)**
Total # of Participants	**42 (100%)**	**42 (100%)**	**42 (100%)**	**42 (100%)**	**42 (100%)**		**42 (100%)**	**42 (100%)**
post assessment	**Denial Of Injury**	**Defence of Necessity**	**Everybody else is doing it**	**Appeal to higher loyalty**	**Policy Overall effectiveness**		**Self-efficacy**	**Work Impediment**
7 points Likert Scale	**Frequency (%)**	**Frequency (%)**	**Frequency (%)**	**Frequency (%)**	**Frequency (%)**	**7 points Likert Scale**	**Frequency (%)**	**Frequency (%)**
Strongly Ineffective (1)	**0 (0%)**	**0 (0%)**	**2 (5%)**	**1 (2%)**	**0 (0%)**	Strongly Agree	**0 (0%)**	**0 (0%)**
Ineffective (2)	**6 (14%)**	**3 (7%)**	**2 (5%)**	**1 (2%)**	**5 (12%)**	Agree	**0 (0%)**	**9 (21%)**
Somewhat Ineffective (3)	**6 (14%)**	**5 (12%)**	**8 (19%)**	**7 (17%)**	**4 (10%)**	Somewhat Agree	**1 (2%)**	**6 (14%)**
Neither effective nor ineffective (4)	**1 (2%)**	**6 (14%)**	**4 (10%)**	**3 (7%)**	**6 (14%)**	Neither Agree nor Disagree	**0 (0%)**	**3 (7%)**
Somewhat effective (5)	**11 (26%)**	**9 (21%)**	**5 (12%)**	**10 (24%)**	**15 (36%)**	Somewhat Disagree	**10 (24%)**	**11 (26%)**
Effective (6)	**9 (21%)**	**8 (19%)**	**14 (33%)**	**9 (21%)**	**9 (21%)**	Disagree	**23 (55%)**	**8 (19%)**
Strongly effective (7)	**9 (21%)**	**11 (26%)**	**7 (17%)**	**11 (26%)**	**3 (7%)**	Strongly Disagree	**8 (19%)**	**5 (12%)**
Total # of Participants	**42 (100%)**	**42 (100%)**	**42 (100%)**	**42 (100%**	**42 (100%)**		**42 (100%)**	**42 (100%)**

The following subsections of this chapter (7.3.1 to 7.3.4) describe the content analysis results and the focus group of independent researchers, as mentioned above. Descriptive statistics across pre-and post-assessments captured the change in participants' perception of password policy before and after the collaborative writing process. Also, we conducted a qualitative content analysis of all updated password documents based on SCPT to identify suggested solutions that participants added to the password policy. The four neutralisation techniques were analysed using pre-assessment, during the collaborative writing process, and post-assessment as described in section 7.3.

7.3.1 Denial of Injury (DoI)

The following section provides the statistical analysis of the perception of the effectiveness of the updated password policy before and after the collaborative writing process, as well as the qualitative analysis of the updated password policy during collaborative writing. Each of these subsections was described in more detail above.

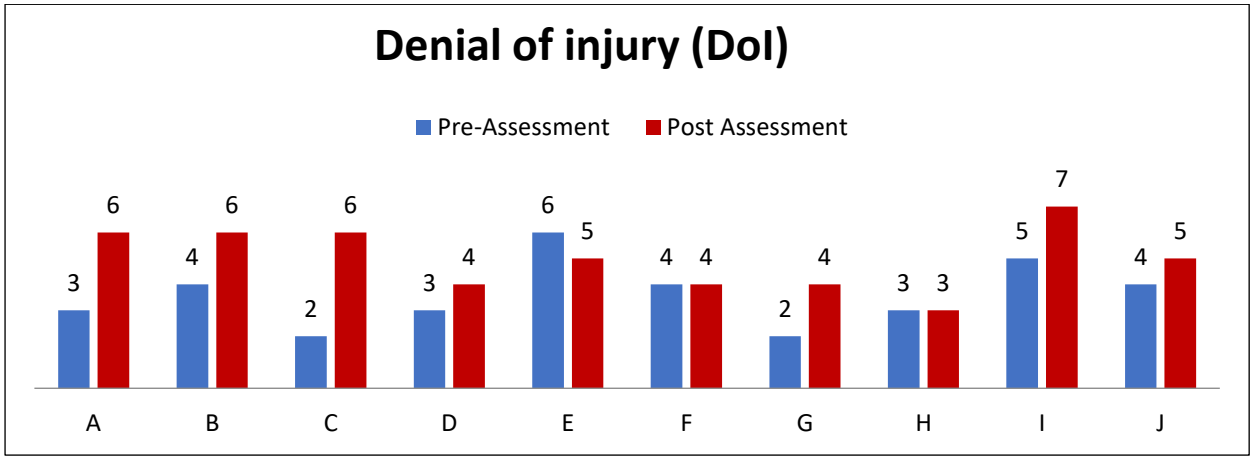


Figure 7.7 Median Comparison Between All Groups For Denial Of Injury (DoI)

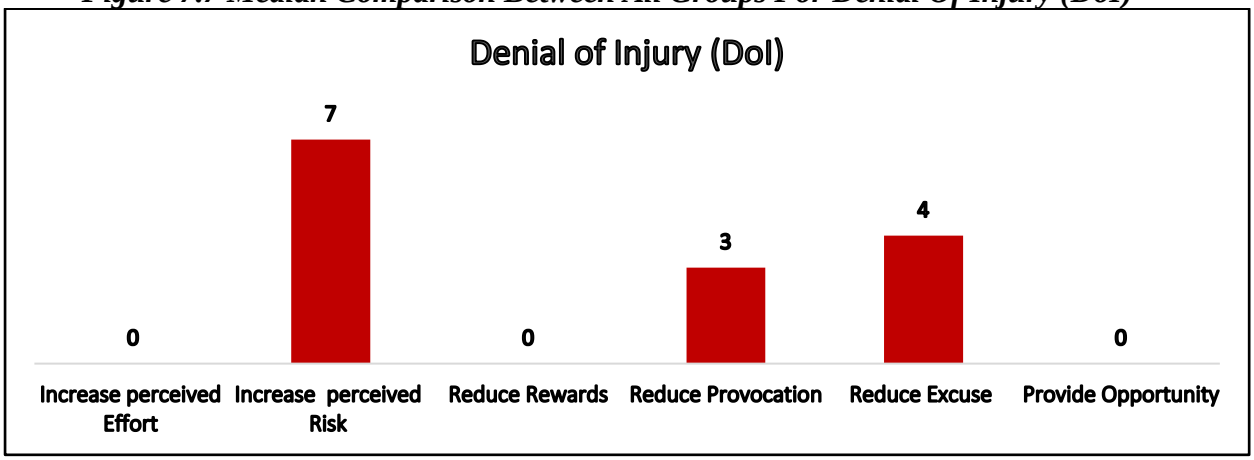


Figure 7.8 Mapping Frequency of codes between Denial Of Injury And The Situational Crime Prevention Theory

- **Pre-assessment evaluation**

Table 7.1 shows the MI's evaluation of the hospital's current password policy effectiveness to counter DoI claims to justify password sharing. The majority of the MIs in our sample (N=42) evaluated the password policy and placed it generally on the ineffective side (N=26, 62%) as the following; *"ineffective"* (N=15, 36%), *"somewhat ineffective"* (N=8, 19%) and *"strongly ineffective"* (N=3, 7%). On the other hand, only thirteen of the MIs (30%) assessed the current password policy as *"effective"* (N=7, 17%), *"somewhat effective"* (N=5, 12%), and only one MI evaluated the password policy as *"strongly effective"* (2%) to mitigate the tendency to violate password policy via DoI claims. In addition, three of the MIs (7%) shared a neutral position on the password policy, assessing it as *"neither effective nor ineffective."* According to Table 7.1, the median of the DoI in preassessment was Mdn=3, which indicated that the policy in its current state was *"ineffective"* (IQR=3).

- **During the collaborative writing:**

The MI's perception of the DoI was analysed through their arguments to accept or reject that such justifications would occur, along with their understanding of the consequences of sharing a password. Also, their decision-making process attempted to update the current password policy to represent better the expected harm of violating password policy by the medical practitioners. Then, they proposed revisions to the policy to mitigate the end-users propensity to adopt such a justification. The following scenario was projected on the screen:

"Sarah is a Medical Intern in a public large-sized hospital, and she has access to the hospital Electronic Medical Records system (EMRs). To ensure that patient information is preserved securely, the hospital has a firm password management policy that all medical staff must keep their EMRs account password confidential. One day, Sarah was approached by another medical intern named Tony, who asked Sarah to share her EMR account password to allow him to write a medical note and view patients' records as Tony's password is expired. ***Sarah knew that Tony was a trustworthy colleague, and he was a member of her team. So, she felt that nobody would get harmed if she shared her password with Tony. Therefore, Sarah gives Tony her password to let him write the medical note order using her account****."*

Denial of injury, in our context, referred to the individual justification that sharing an EMR account password with another colleague is harmless. It was noted that the MIs were very open in their discussion style. Each MI read the neutralisation scenarios silently, then started to discuss each of them. It was noted that the MIs read the DoI scenario and immediately wondered if there is any cost for non-compliance with the password policy on the patients or doctors. Unlike participants in chapter 6, the medical interns searched for any laws or regulations that

stated any legal consequences of the violation and asked if IT could detect the password violations. Also, most of the MIs mainly perceived harm as anything that can cause damages to the patient's health without careful attention to the security and privacy risks associated with sharing the password. For instance, members of groups B and D stated during their groups' discussion that:

> ***Member from* B:** "*Most of the time, no harm from sharing password.*"
>
> ***Member from* D**: "*To be honest, we always care more about the consequences on patient health more than security, so when I share my password or account, I will be more afraid of wrong drug prescriptions than thinking about patient privacy."*

As shown in Figure 7.7, all groups reached a consensus that three strategies of SCPT can discourage the end-user willingness to deny the harmful consequences of sharing a password or the EMR account. In addition, the groups added 17 (out of 89) modifications to the password policy to mitigate the DoI scenario. These modifications were coded based on the SCPT strategies for reducing the opportunity to conduct undesirable behaviour (see section 6.3 for more details). The SCPT strategies proposed by the groups were to increase perceived risk, reduce excuses, and reduce provocations.

Increased perceived risk was the most recommended strategy against the DoI scenario. This strategy aims to influence the individual decision-making process by clarifying the cost of non-compliance on both the organisational and personal levels. For instance, several members of groups G, E, and H argued that the current password policy lacks any mention of the negative consequences of sharing passwords:

> ***Member from* G: *"****The document does not state any harm to patients or doctors. There are no penalties for sharing a password between doctors, so there is no harm in doing so for both parties."***
>
> ***Member from* E:** *"The policy has not mentioned any consequences or legal action for sharing the password; I think we need to focus on this point to counter DoI's claim."*
>
> ***Member from* H:** *"We need to say why this policy is important by stating the result of violations."*

Consequently, several groups added sentences intended to reveal that password sharing was a malicious action and that conducting such behaviour would negatively affect the privacy of the patient and both the EMR account holder and account user. For example, a member in group I explained this argument by stating :

> ***Member from* I:** *"We need to make sure that who signed the medical order will be responsible for any leagl or security consequences; this includes if you allow someone to give order using your account."*

Five groups (A), (B), (I) and (J) focused on increasing the risks of password sharing by focusing on the consequences of medical error—such as "double medical order"—on patient health, security violations that could compromise patient data, and the legal liability associated with these behaviours. Their argument was based on the concept that the mindset of medical practitioners prepared them to comply with a medical oath to serve patients and not cause harm. Also, they argued that Denial of Injury could be discouraged by making the EMR account holder responsible for any harmful actions associated with the account due to sharing the EMR password with a colleague. This is consistent with Helo and Moulto[308] stating that every member of the healthcare team was responsible for making decisions that ensure the safety of the healthcare environment for the patient and healthcare workers. Therefore, amendments to password policy warned medical practitioners of the magnitude of legal harm if they were apprehended for password sharing rather than punishment such as salary reduction. Thus, they added:

Group A: "*Sharing your password might result in harm to patient or physician (e.g. Double orders, Medication errors, etc.), and you will be legally responsible."*

Group B: *"The account owner will be involved in any legal issue if sharing password led to any harmful event to the patient."*

Group F: *"A formal warning will be issued to a staff member if sharing of login credentials is found."*

Group I: *"EMRS users will be instructed that sharing their accounts might compromise system security, patient care and subject the original account user for legal consequences."*

Group J: *"Responsibility: You will be legally responsible for any action/written info/order/input/documentation that is done by your account. If sharing password/account has been confirmed: legal consequences will be taken."*

Excuses removal was the SCPT's second strategy to reduce medical practitioners' opportunities to justify a password policy violation using DoI. Excuse removal aims to neutralise the justifications that the offender used to commit a crime and includes five sub-strategies: (1) set rules, (2) post instructions, (3) alert awareness, (4) assist compliance, and (5) control drugs and alcohol [238]. During collaborative writing, a member in group D referred to the necessity of posting instructions that remind the medical practitioners to keep their EMR

passwords confidential. Thus, he argued that giving such instructions would leave no room for excuses:

> ***Member from* D:** *"We need the system to prompt a reminder message for every EMR user saying that sharing the account password or the account itself is not allowed."*

The main argument was based on the criticism that many MIs and other medical practitioners started their medical internship program or medical duty in the clinics without an active EMR account. This situation forced the MIs to ask others to share their accounts until they got an active account (see chapter 5, section 5.5.1 for more details about this situation). They emphasised the need to establish a rule that preserved the employee's right to access the hospital system before officially beginning work. Thus, putting such a rule in the policy would reduce the chance of justifying password sharing as harmless action due to no active account, and at the same time, encourage the IT department to make sure this employee right is fulfilled. Thus, group D added the following:

Group D: *"The IT department must ensure that any employee must have active access to the hospital system before the first day of his/her job."*

Additionally, group J suggested that the posting of the instructions could remove the excuse of sharing the password and guide medical practitioners on how to protect their EMR passwords. They argued that medical practitioners might create security misconceptions due to inconsistent information about what is allowed or prohibited in the password policy. In addition, clarifying these instructions would make the practitioner aware of risky behaviours, including dealing with colleagues requests to share a password. Thus, it might discourage that person from justifying password sharing with colleagues as harmless. As a result, group J added :

Group J: *"Password must not be shared, written down or stored in locations where it can be found, regardless of whether you think it is beneficial, professional, or not. and that it will be immediately changed if compromised."*

The last SCPT strategy proposed by the groups to mitigate individual justification was reducing provocations. This SCPT strategy includes five sub-strategies: (1) reduce frustrations and stress, (2) avoid disputes, (3) reduce emotional arousal, (4) neutralise peer pressure, and (5) discourage imitation. According to Padayachee [309], reducing provocation aims to decrease "the emotional triggers that may precipitate a motivated criminal to commit an offence," and she suggested that "reduce precipitators" was an alternative in the information security domain. Wortley [304] argued that two situational forces influence individual behaviour: "those which

are responsible for precipitating action and those which regulate behaviour by the opportunities they present" [238]. Thus, successful management of these situational precipitators could play an essential role in regulating an opportunity that could be exploited to offend [238].

Social pressure is a crucial situational factor that could motivate individuals to offend. According to Wortley [304], compliance with orders and instructions from authorised personnel and compliance with group norms are significant sources of social pressure in organisations. In our context, group D members discussed the importance of reducing peer pressure by giving the group member a reason to justify their refusal to share a password. This group adopted reducing provocation via neutralising peer pressure as a suitable SCPT strategy to mitigate the individual tendency to justify sharing passwords via DoI. Their main argument was that every medical team member should feel responsible for protecting their password, even from their peers. One way to do this was to expand the risk magnitude of security and privacy breaches due to password sharing. Thus, group D added the following:

Group D: "*If someone shared a password or account, the whole department/team should be held the responsibilities and consequences of any security or privacy breaches."*

- **Post-assessment Evaluation:**

The lower part of Table 7.1 illustrates the post-assessment of the participants' perception about the effectiveness of the updated policy via the collaborative writing process to mitigate MI justification that password sharing was harmless. The post-assessment of the updated policy showed that only 12 out of 42 participants (28%) evaluated the updated policy that considered the DoI scenario during the collaborative writing process was "*somewhat ineffective"* (N=6) and "*ineffective"* (N=6), respectively. Also, only one participant (2%) provided a neutral evaluation and perceived the modified policy as *"neither effective nor ineffective"* to mitigate the DoI.

However, most of the MIs (N=29; 69%) evaluated that the updated policy as *"strongly effective"* (N=9), *"effective"* (N=9), or *"somewhat effective"* (N=11) to mitigate the tendency to adopt the DoI and violate the password policy. Also, Figure 7.6 Median Comparison between all groups for Denial of Injury (DoI) showed that the median of the post-assessment for the updated policy in 7 groups (A, B, C, D, G, I, and J) had been strongly improved, while the perceptions in groups F and H remained without change: Group F evaluated the updated policy as "*neither effective nor ineffective,"* and Group H evaluated the updated policy as "*somewhat ineffective."* However, only group E post-assessments median declined as the participant

evaluated the updated policy from *"effective"* to *"somewhat effective."* Last, the change of overall median value in the participants' perception revealed more agreement that the updated policy was more effective in reducing the medical practitioners' tendency to justify the consequences of sharing policy between colleagues as harmless (Mdn=5, Stdev= 2.07, and IQR3-IQR1= 3).

7.3.2 Defence of Necessity (DoN)

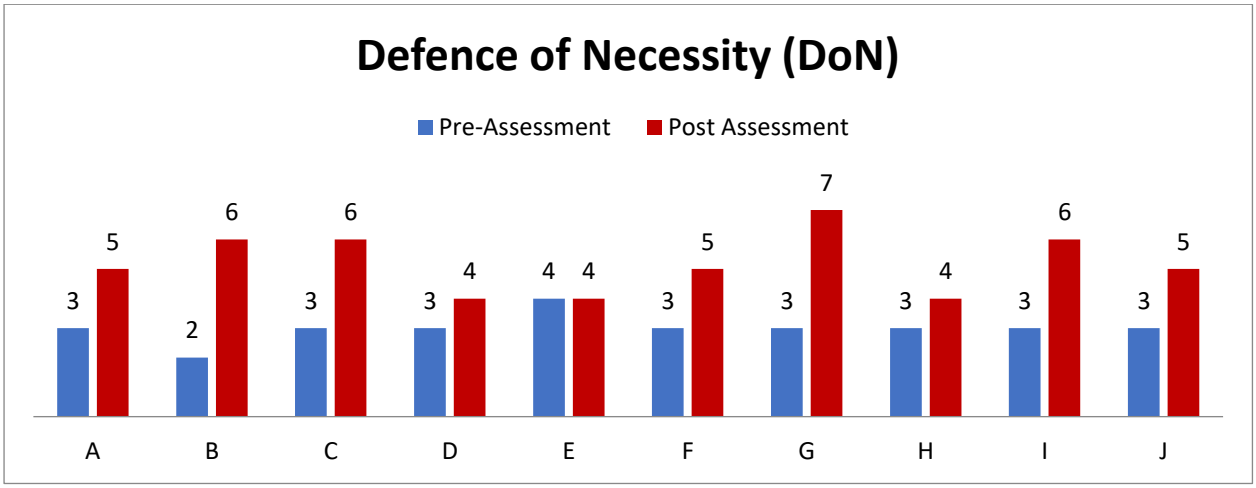


Figure 7.9 Median Comparison Between All Groups For Defence Of Necessity

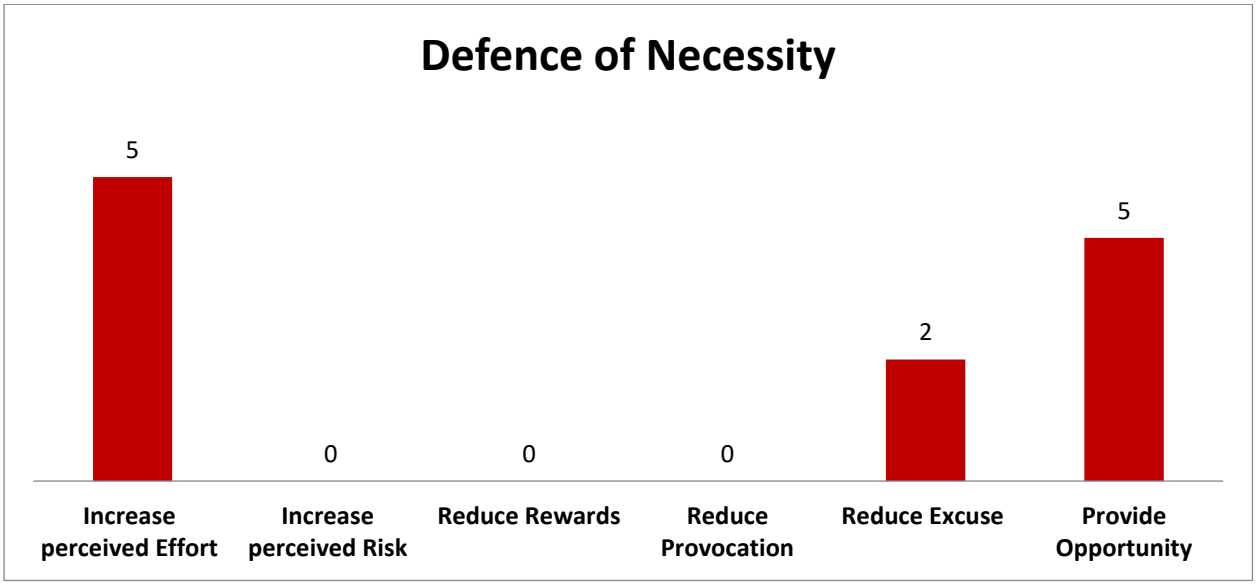


Figure 7.10 Mapping Frequency of codes between Defence of Necessity (DoN) and The Situational Crime Prevention Theory

- **Pre-assessment evaluation:**

Table 7.1 outlines the pre-evaluation of the current password policy regarding the use of DoN as an excuse for policy violation. The pre-assessment gathered data from a total of 42 medical interns. The result from the pre-assessment showed that the majority of the MIs perceived the current password policy as *"ineffective"* (N=30, 70%). Twelve participants (34%) reported that the password policy in its current state was "*somewhat ineffective"* (N=12, 29%), "*ineffective"* (N=17, 40%) or "*strongly ineffective"* (N=1, 2%) to mitigate medical practitioners' propensity to adopt DoN claims. However, a few participants (N=6, 28%) reported that the original password policy was either *"somewhat effective"* (N=5) or *"effective"* (N=1). Also, six participants (14 %) revealed a *neutral* perception of the original password policy to counter DoN. The overall median of pre-assessment across all groups was (Mdn=3, IQR=2), which indicated a consensus between all group members that the original password policy is somewhat ineffective to counter the end-users likelihood to justify the policy violation via DoN.

- **During the collaborative writing:**

The groups' perceptions were analysed in terms of their justification for accepting or rejecting the DoN, which addressed how surrounding conditions affect an employee's tendency, in the existence of the current hospital password policy, to share a password or account for their EMR systems and then claim that such a breach was necessary to finish the work. Additionally, the participants' approaches and the relevant arguments in each group to modify the original password policy in order to decrease employees' propensity to embrace DoN claim and the relationship between these alterations and reducing opportunity based on the SCPT strategies was discussed. The following scenario was projected on the screen:

"*Sarah is a Medical Intern in a public large-sized hospital, and she has access to the hospital Electronic Medical Records system (EMRs).To ensure that patient information is preserved securely, the hospital has a firm password management policy that all medical staff must keep their EMRs account password confidential. One day, Sarah was approached by another medical intern named Tony, who asked Sarah to share her EMR account password to allow him to write a medical note and view patients' records as Tony's password is expired.* ***Sarah knew that Tony was a trustworthy colleague and a member of her team. So, she felt that they were working in a busy clinic, and it was essential action to share her password in order to improve work performance. Thus, Sarah gives Tony her password to let him write the required medical note order using her account.***"

Most groups believed that this scenario was more likely to occur in clinics that require emergency responses to treat patients, such as emergency rooms, or clinics that typically interact with a large number of patients, such as outpatient clinics. They stated that the medical practitioners in these clinics were under significant workloads that could reach lifesaving situations. Thus, they cannot deal with an extra burden, such as being unable to access the EMR system to conduct the required medical orders.

A total of 11 modifications in the original password policy aimed to reduce the medical practitioner's tendency to evoke DoN and share the passwords/accounts. Thus, the groups suggested three situational crime prevention techniques that could reduce the opportunity for the medical practitioners to adopt the DoN claim and violate the password as a necessity for the work progress. According to Figure.7.9, several medical intern groups during the collaborative writing decided that "increased efforts," "provide opportunities," and "remove excuses" were suitable strategies to mitigate the medical practitioners' justification for using DoN.

"Increase efforts" involve strategies that make conducting undesirable behaviour challenging to carry out, such as violating a security policy [310]. According to Safa et al. [310], an authentication is a traditional approach for access control of IT assets, which can increase the difficulty to conduct misbehaviour. In our case, most participants agreed that controlling access to IT facilities (EMR system) would be an appropriate strategy to reduce password sharing for the greater benefit, such as increased work productivity. They argued that many clinicians would always find sharing passwords out of necessity a valid reason for violating password policy even in situations where password sharing is not actually required; as a participant in the group I stated:

> ***Member from* I:** "*Yes, there is a good cause for the doctors to share the password to serve a patient, but we agree that such behaviour can open a hole in the password policy that can be compromised system. Also, we all know some of the doctors share their passwords as a courtesy to their fellow doctors.*"

Thus, five groups (B, C, D, G, and H) added five modifications to the original policy to counter the DoN claim. They claimed that the current configuration of the EMR system allowed multiple sessions to be opened in different places, which motivated the medical practitioners to share their passwords without careful attention because these multiple sessions would not impact their work. Thus, they suggested that configuring EMR login privileges by limiting EMR sessions to just one would be an appropriate strategy to reduce their tendency to share passwords. They also

emphasised that it was challenging to prevent medical practitioners from arguing that password sharing was necessary to perform their work, which is valid on many occasions. Thus, reducing password/account sharing due to business necessity to a minimum level was the aim, which would be a positive change for the work environment and security.

According to Freilich and Neumann [10], the primary goal of the SCPT was to control and maintain crime rather than the traditional approach of trying to eradicate crime. Also, the SCPT encouraged maintaining a certain level of crime and focused more on reducing expected harm. Thus, allowing only one EMR session would affect the rational decision-making process of medical practitioners, who routinely shared their passwords, in a way to reconsider the decision of sharing the password and reassess the situation whether "worthwhile" to share the password with a colleague and freeze their work until the colleague exit from the shared EMR account. This is consistent with Safa et al. [310], who stated that "rationalisation and available opportunities for offending play vital roles in the aetiology. It is argued that if offending is difficult, as a consequence, the propensity to offend will be reduced." Thus, the groups added five statements that reflected the need for increased effort as an SCPT strategy:

Group B: "*The system will permit one account running at the moment*."

Group C: "*No two devices are allowed to log in at the same time.*"

Group D: "*the account should be login in on one computer; if two computers log in to the same account at the same time, one will be forced to log off*."

Group G: "*The account cannot be accessed by two devices at the same time, and it will log out automatically if logged in through another computer*."

Group H: "*An account cannot be accessed in more than one computer at a specific time.*"

The second SCPT strategy to counter the tendency to evoke DoN for password policy violation was to "provide opportunity." Four groups (C, J, F, and E) incorporated statements that reflected two strategies under providing opportunity: (1) facilitated compliance and (2) legalisation.

The hospital is a complex environment that requires high collaboration and coordination between the medical teams. Being unable to access the EMR system could cause significant disruption to inpatient services. It would be a challenge for the team to balance the password requirements and the work needs in such a situation. In our case, several groups during the collaborative writing discussed the poor password resetting procedure in the ABC hospital and

its effect on work efficiency. For instance, if a medical practitioner's password expired, then they would not be allowed to access the EMR system until they wrote an official email to the IT department asking for a resetting link. From the medical practitioners' perspective, this was considered an excessive amount of time to reset a password and regain access to the EMR system, so the quickest path in this situation would be asking a colleague to share their password until the IT department replied with the resetting link. Thus, in this situation, the justification for such sharing passwords would be the urgency of work. A member of a group J discussed a similar idea:

> ***Member from* J:** *"I agree that account sharing is wrong regardless of the justifications, but still, give me a solution that addresses the underlying reasons for my justifications. As a doctor, I see my justification as valid, and I have not done it arbitrarily."*

Freilich and Newman [311] claimed that providing an opportunity for the offender could encourage them "to displace the less serious offence." In our case, it implied that the organisation should accept that eliminating password sharing was an impractical idea, and there was a need to reconsider such an assumption by legalising such behaviour to ensure it was conducted at least under close monitoring from the IT department. In criminology, there was successful evidence that the legalisation of some undesirable behaviour could contribute to less harmful consequences. For instance, the legalisation of prostitution in New Zealand led to a reduction of aggressive behaviour against women who worked in this field and enhanced working conditions for them, as it ran under government regulations [301].

In our case, group C believed that implementing strict security requirements for passwords could lead indirectly to a security violation. Thus, there was a need to accept the idea of giving exceptions to circumventing the password policy under emergency conditions. A group member in group C explained this perspective as follows:

> ***Member from* C:** "*I think the system privileges should be reviewed and re-evaluated again; password sharing is an exception that needs to understand why they are doing it. Preventing password sharing using the policy without understanding the motives is just keeping the problem unresolved. There is a conflict between real work activities and policy. The policy only forbids actions or add more controls without sometimes considering the need for exceptions.*"

Thus, participants in group C agreed that there was a need to make some exceptions to the password policy regarding system privileges. Also, the group suggested that supervising doctors

could give their junior doctors some privileges to perform their routine duties such as ordering lab tests, writing documents, or discharging patients. Therefore, MIs could prepare medical orders in a consultant's EMR account for validation. This solution can provide an alternative and official method to the problem of password sharing and improve work performance without violating the policy, and the group considered this exception as a kind of privileged escalation. Thus, the group added the following:

Group C: "*A prompt system request be made available to allow at least three people in the department to use the account of a senior physician for 48 hours (providing the name and badge number of each user).*"

In addition, three groups perceived that providing such an opportunity could reduce the medical practitioner's justification via DoN by facilitating compliance with the password policy. Participants in these groups agreed that there was a need to improve the current policy by improving password generation procedures. They stated that the current password policy required changing the password for the EMR system every three months. If the password expired, the practitioner needed to complete an official form and send it to the IT department by email to receive a password reset link. This process could take at least 24 to 48 hours. Thus, it would put the practitioners under work pressure to deal with the clinic duties. Therefore, the IT department gave no room to the practitioners other than violating the password policy by temporarily asking a colleague to share their EMR password. Three groups (J, E, and F) suggested that the practitioner needed to have an opportunity to resolve such a situation by providing them with an instant method to reset the password or providing them with the ability to temporarily access the EMR using their fingerprint. Thus, providing these alternative methods could improve password policy compliance and reduce the password expiration issue and relevant justification. According to Nandakumar et al. [312], using biometric authentication to access the IT systems might overcome security issues such as password guessed, stolen, lost, forgotten, and shared between colleagues. Thus, the three groups added the following:

Group J: "*The system allows instant regenerating password using the reset link in the login page.*"

Group F: "*The system can be accessed using biometric measures, i.e. fingerprints, without requiring the input of a password.*"

Group E: "*You must log in by your fingerprint, if not possible, to use your password.*"

The last SCPT strategy to counter the tendency of the medical practitioners to evoke DoN and share the password was "removing excuses." Two groups (G and I) proposed this approach, mainly removing excuses by addressing the awareness of the medical practitioners. They argued that altering their awareness of the existing password policy requirement could enhance their compliance with the policy. According to Padayachee [109], several methods could improve the end-users awareness of security controls, such as code of ethics, acceptable use policy, and copyright protection. In our case, participants in groups I and G stated that it was critical to precisely define acceptable and unacceptable behaviour through setting clear rules to provide practitioners with a standard of behaviour. Also, they suggested that it was critical to obtain employees' signatures and confirm their knowledge of the regulations and their commitment to follow them at the beginning of their employment. This is consistent with Hinduja [313], who stated that altering awareness of the rule could "serve the purpose of demonstrating the unacceptability of specific behaviours in specific circumstances" [313]. Thus, they added the following statement to reduce the excuse as a way of dissuading medical practitioners from evoking DoN and sharing the password:

Group I: "*Each individual will be instructed not to share their password or their accounts to another colleague under any circumstances or write down and store in locations where it can be found, and that the password should be immediately changed if compromised.*"

Group G: "*Before an individual is granted access to the electronic system, an agreement form to this policy should be signed*."

- **Post-Assessment evaluation:**

According to Table 7.1, the groups' perception of the effectiveness of the updated password policy improved to counter employee justification via DoN for password sharing. This is evident by the fact that the majority of respondents (N=28 out of 42, 66%) stated that the updated password policy was "*strongly effective*" (N=11, Mdn=7), "*somewhat effective*" (N=9, Mdn=5), or "*effective*" (N=8, Mdn=6). In contrast, only eight of the 42 participants (19%) stated that the password policy resulting from collaborative writing was still "*somewhat ineffective*" (N=5, Mdn=3) or "*ineffective*" (N=3, Mdn=2) in reducing the tendency of end-users likelihood to justify password policy violation via DoN. Also, a comparison of the pre-and post-evaluations showed that the number of participants who had a neutral perception remained unchanged (N=6, Mdn=4). Moreover, the overall median change improved in post-assessment, as shown in Table 7.2. Thus, this implies that participants across all groups agreed that the

modified password policy via collaborative writing was "*somewhat effective*" (Mdn=5). It could reduce, from their perception, the tendency of medical practitioners to violate the password policy and justify this behaviour as necessary to maintain work performance (Mdn=5, IQR=3).

7.3.3 Appeal of Higher Loyalty (AoHL)

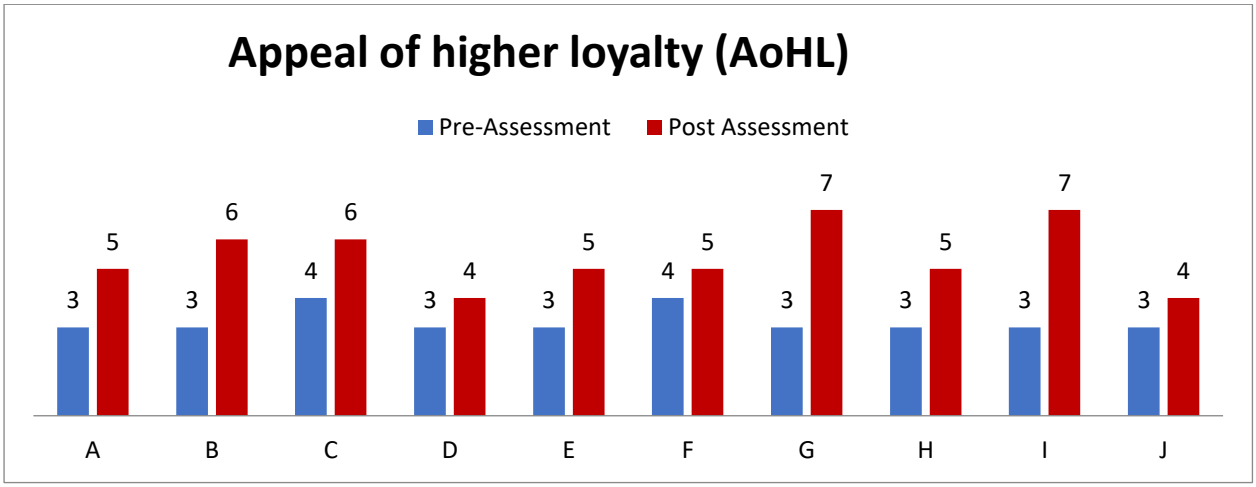


Figure 7.11 Median's Comparison Between All Groups For Appeal Of Higher Loyalty (AoHL)

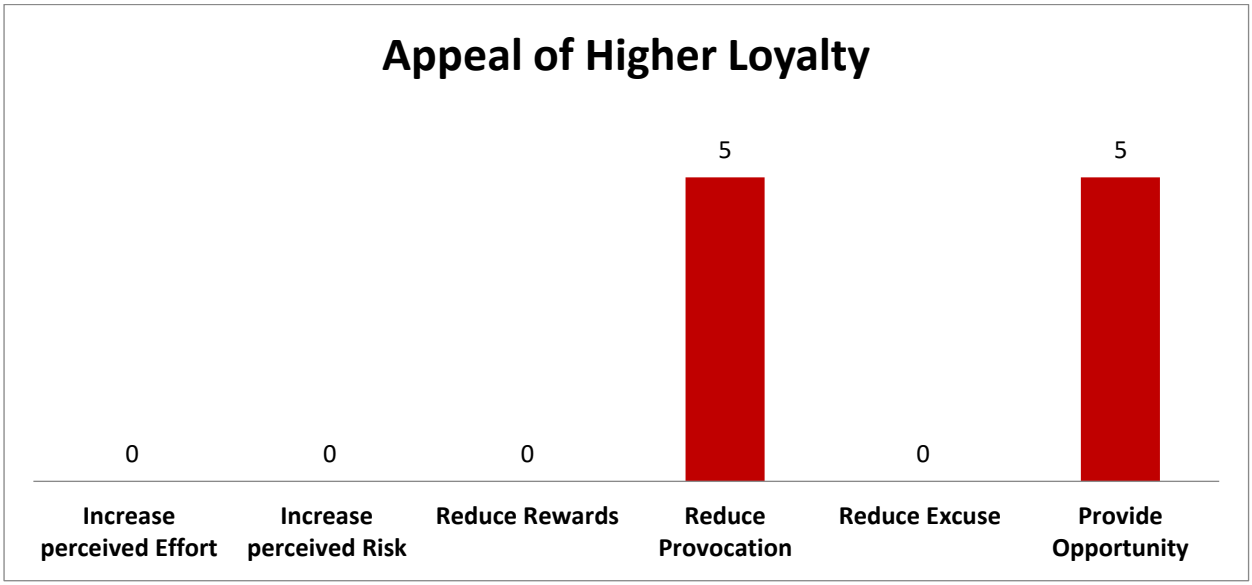


Figure 7.12Mapping Frequency of codes between Appeal of higher loyalty (AoHL)and the Situational Crime Prevention Theory

- **Pre-assessment evaluation:**

Table 7.1 shows the participants' perception of the current password policy effectiveness at discouraging end-user justification via appeal to higher loyalty (AoHL). Twenty-five (59%) of 42 participants evaluated the current password policy as *"ineffective."* In particular, the majority of the participants assessed the existing password policy as *"ineffective"* (N=12, Mdn=2), "*somewhat ineffective"* (N=9, Mdn=3), or *"strongly ineffective"* (N=4, Mdn=1) regarding the original password effectiveness to mitigate end-user AoHL justification when they share their password. In contrast, the rest of the participants (N=10 out of 42, 23%) evaluated the original password policy as *"effective"* to counter the medical practitioners' justification to violate password policy via AoHL. At the group level, as shown in Figure 7.10, the median perceptions of participants across all groups except C and F show that the original password policy is "*ineffective*" (A, B, D, E, G, H, I, and J, Mdn =3) or "*neither effective nor ineffective"* (C and F, Mdn=4) in dissuading the use of AoHL as a valid justification to share their passwords. According to Table 7.2, the overall median assessment across all groups for the original password policy using AoHL indicates that the groups agree that the current password policy is "*ineffective*" (Mdn=3, IQR3-IQR1= 2).

- **During the collaborative writing process:**

This neutralisation technique was analysed by the group regarding how the requirements and standards of a tightly knit group could affect the employee's decision-making to violate the password policy. The employee justifies the violation of the password policy by refusing the organisation's security requirements in favour of complying with the demands of the small group of coworkers. Also, the updated policy of each group was analysed to identify SCPT strategies that were suggested during collaborative writing to mitigate the AoHL scenario. At the beginning of the collaborative writing session, the following scenario was shown on the monitor screen:

"Sarah is a Medical Intern in a public large-sized hospital, and she has access to the hospital Electronic Medical Records system (EMRs).To ensure that patient information is preserved securely, the hospital has a firm password management policy that all medical staff must keep their EMRs account password confidential. One day, Sarah was approached by another medical intern named Tony, who asked Sarah to share her EMR account password to allow him to write a medical note and view patients' records as Tony's password is expired. ***Sarah knew that Tony was a trustworthy colleague and a member of her team. So, she felt that sharing her***

password was a type of professional help to Tony. Therefore, Sarah gives Tony her password to let him write the required medical note/order using her account."

Forty-two participants comprised ten groups that conducted a total of ten modifications to the original password policy to reduce medical practitioners tendency to justify password sharing. Brewer et al. [33] stated that AoHL is " a neutralization technique whereby the offender sacrifices the demands of the larger society for the needs of a smaller, alternative social group such as familial or peer groups" [33]. So, an individual might justify undesirable behaviour in the organisation's perception as support for the benefits of their social groups or the pursuit of ideal moral goals. Figure 7.11 shows that the participants of the ten groups proposed two SCPT strategies to deal with password sharing and the relevant justification via AoHL. The content analysis of ten updated password policies identifies two SCPT strategies: "providing opportunity" and "reducing provocation."

It was noted that many groups considered the AoHL scenario as an overlap with the DoN scenario. They argued that the necessity of work (DoN) motivated the medical practitioners in certain situations to provide the professional assistance required to preserve the work progress. For instance, during their work, the medical interns had limited privileges such as reviewing the medical records and writing routine documentation without the ability to conduct medical orders when using the hospital EMR system. The clinical seniors were the only ones who had full privileges to perform any medical orders relevant to their medical speciality in the EMR. So, because of trust, those seniors thought that a part of the learning process was giving their medical interns the chance to conduct medical orders. A member in group H discussed this point (see more details in chapter five, section 5.5.1.6).

***Member from* H**: "*If you notice the scenario that mentions professional help, on many occasions when I deal with senior residents, they share their EMR account with me to learn how to use the system and generate medical orders. So the justification makes sense to me as an MI because using the system with higher privileges would add to me."*

However, several examples were provided to explain and justify "professional help." In our context, the IT department needs to consider the close work relationship between medical interns and their seniors. So, group H proposed that the IT department could offer an alternative EMR account limited for department usage with specific privileges under the primary consultant's responsibility. Thus, each consultant would assign duties to their medical interns and ensure that they use their badge information to access it. Thus they added the following:

Group H: "*MRP (Main Responsible Physician) will be responsible for assigning which*

member is responsible for documentation and order in the department EMR account."

Other groups shared the same idea of creating an " Emergency account" for each department that could be used if one of the primary medical practitioners had difficulties accessing their account due to expiration or the delay of account activation for new employees. Thus, they suggested that the department consultant could grant emergency access to this account until the IT department resolves the technical issue. So, participants in groups A, C, H and B had the same perception of such a solution to mitigate sharing passwords and justify this policy violation via AoHL. They added the following:

Group A: *"If you have any difficulties accessing the system, you might use temporary alternative access by using departmental account."*

Group B: *"Use the emergency account if any technical issue happens."*

Group C: *"Each department will have their own account that requires the user's complete information with each use for the practising doctors whose own account has been delayed. With monthly password changes."*

Group H: "*Each department can access temporary accounts which can be given to Physicians with difficulties accessing their accounts, and these accounts show users' information."*

Lastly, reduce provocation was suggested as an SCPT strategy to counter the impact of AoHL on the medical practitioners to justify non-compliance with the hospital password policy. Several groups built their argument to update the password policy by reducing provocation resulting from stress or frustration. Safa et al. [310] explained that "Reducing provocation aims to decrease the emotional triggers that may precipitate a motivated criminal to commit an offence" [310]. According to Kim et al. [314], in an information security context, some of the basic emotions such as anger, joy, fear, or shame can play an essential role in the behavioural abuse of IT assets. Thus, the IT department should minimize any provocations that pose a danger to information security [310]. In some cases, employees may want to mitigate the negative repercussions of technology-induced stress and may feel justified in engaging in deviant behaviours [315], such as sharing a password with a colleague as a way of support. Thus, participants in groups H, J, D, G, and F believed that the IT department needs to show that it can solve the access issues to the EMR system. As mentioned in section 7.3.2, many medical interns stated that the hospital had a poor password resting procedure and EMR account activation that provoked medical practitioners to seek assistance from their colleagues, which caused a password policy violation.

A member in group G explained that the medical practitioners preferred their colleague's support to deal with the password reset or account activation because of the IT's department inefficient reset or activation procedures:

> ***Member from* G:** *"We usually work in the same department and know each other. If a colleague is having difficulties with their account and needs access, he will ask his colleague without hesitation before contacting the IT department."*

Thus, those five groups proposed that IT needs to review the current password setting and account activation procedure and implement a hot-line to the IT help disk. Each medical practitioner needs to be aware that the IT department is ready to provide immediate support and resolve any technical issue related to system access. Suppose an employee knew that their technical problem would be solved via a simple telephone call. According to these groups, this would reduce frustration and stress. The groups added the following:

Group H: *"24/7 Hot-line will be available to fix and manage account issues."*

Group J: *"IT Hot-line number/ direct chat support will be provided to fix technical problems as soon as possible."*

Group D: *"If you have any difficulties, use a hot-line xxxxx for the IT help desk immediate support."*

Group G: *"The system user is responsible for contacting CIMS through 27/7 hotline number: xxxxxx, for any technical issues in the account (logging in, changing password, etc.)."*

Additionally, group F suggested that two-factor authentication is a reasonable way to reset a password or activate an EMR account to reduce password sharing and the tendency of medical practitioners to neutralize this behaviour as support for their peers. Participants mentioned that they often use this method to access their bank accounts, which is an effective way to generate a new password quickly. Therefore, implementing such a common and well-known method would eliminate the burden and stress of not being able to access the EMR system, especially on night shifts. This might reduce the tendency to ask others to share their passwords because of the access problem. The group modified the original policy with the following statement.

Group F: *"Password could reset through any computer in the vicinity of the hospital using 2-factor authentication. The old password and a code sent via text message to the staff member to allow instantaneous password change."*

- **Post-Assessment evaluation:**

According to Table 7.1, most of the medical interns (N=30 out of 42) evaluated the modified password policy as more effective to reduce the tendency to justify sharing passwords via AoHL compared with the pre-assessment of the original policy (N=10). Across the ten groups, ten participants (24%) believed that the updated policy that considered the AoHL scenario was *"somewhat effective," "effective"* (N=9, 21%) or *"strongly effective"* (N=11, 26%) at discouraging the medical practitioners' tendency of justifying sharing password as a kind of assistance or professional support. In contrast, nine of the participants (21%) revealed that the updated password policy via collaborative writing remained "*somewhat ineffective"* (N=7, Mdn=3), "*ineffective"* (N=1, Mdn=2) or "*strongly ineffective"* (N=1, Mdn=1). However, only three participants evaluated that the updated password policy as neither "*effective nor ineffective"* to dissuade the medical practitioners from password violation and justify their non-compliance via the AoHL

At the group level (see Figure 7.11), the median value variation between the pre- and post-assessments shows an improvement across all ten groups. The median value for all the groups except F and C was (Mdn=3), which indicated that these eight groups (A, B, D, E, G, H, I, and J) evaluated the original password policy in the hospital as "*ineffective"* in reducing medical workers justification via AoHl to share their passwords. The post-assessment for these groups indicated an improvement in the medical interns' perception of the effectiveness of the updated password policy. For instance, the variation in pre-and post-assessments of groups A, E, and H was increased from "*somewhat ineffective*" (Mdn=3) to *"somewhat effective"* (Mdn=5). Similarly, a slight improvement was seen in groups D and J from "*somewhat ineffective"* (Mdn=3) to *"neither effective nor ineffective"* (Mdn=4).

In addition, the change in median assessments from participants in groups B, G, and I between the pre-and post-assessment was significantly improved. For example, the pre-assessment medians of groups G and I were "*somewhat ineffective"* (Mdn=3), and it has been significantly improved in the post-assessment to "*strongly effective*" (Mdn=7). Likewise, in group B, the change in the assessment of the updated policy effectiveness to counter AoHL was improved from "*somewhat ineffective"* (Mdn=3) to *"effective"* (Mdn=6). Also, groups C and F perceived the updated policy as "somewhat effective" in the post-assessment compared with their neutral evaluation (Mdn=4) in the preassessment.

Further, Table 7.2 shows that the median of overall perception across all groups slightly improved from "*somewhat ineffective*" (Mdn=3) and established consensus that the revised

password policy via collaborative writing was improved to *"effective"* (Mdn=5, IQR3-IQR1=2). Thus, from their perception, the changes could reduce the tendency of end users non-compliance with password policy and justifying this violation via AoHL.

7.3.4 Everybody Else Is Doing It (EEIDI)

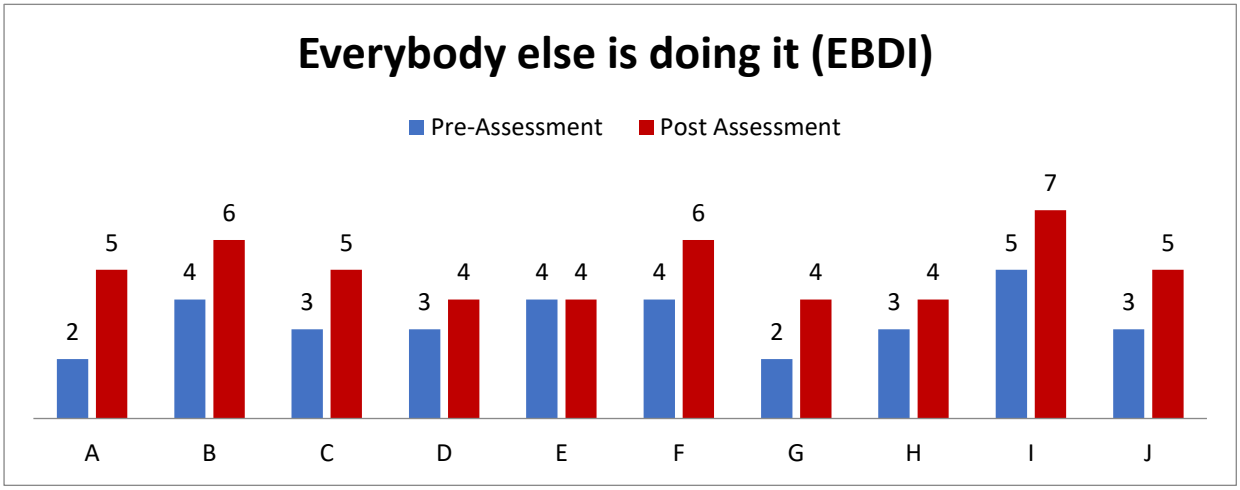


Figure 7.14 Medians Comparison Between All Groups For Everybody Else Is Doing It

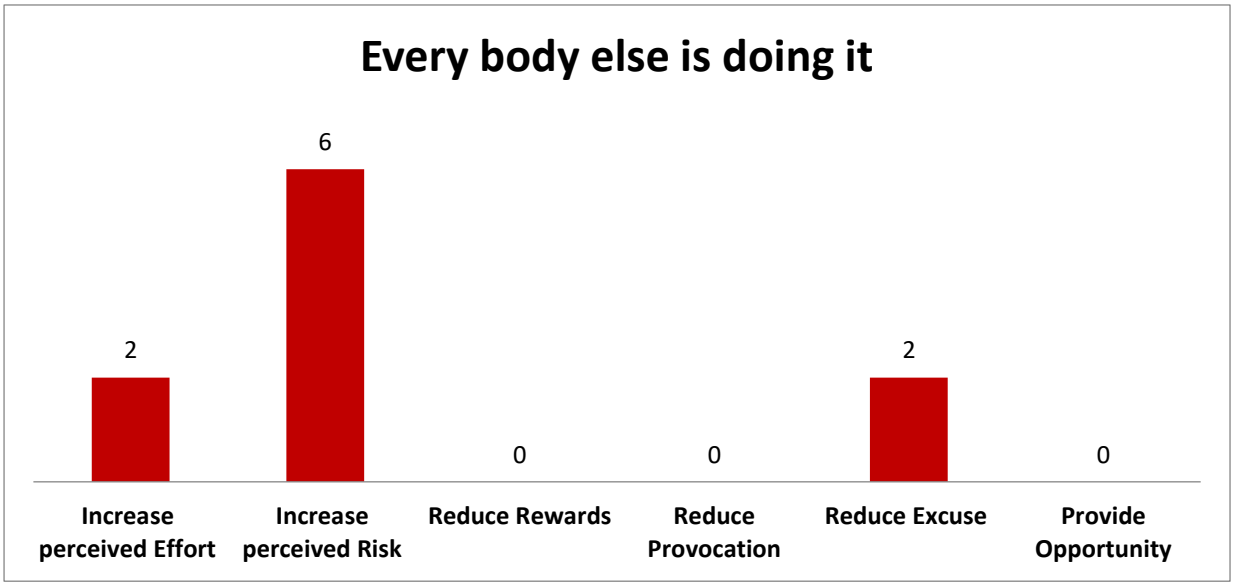


Figure 7.13 Mapping Frequency of codes between Everybody Else Is Doing It (EEIDI) And Situational Crimes Prevention theory

- **Pre-assessment evaluation:**

Table 7.1 illustrates participants' perception of the effectiveness of the current policy in mitigating EEIDI claims of password policy breaches. Twenty-eight out of 42 participants (67%) believed that the original password policy was generally ineffective at mitigating an employee's claim that their breach was justified because the behaviour in question was

performed by everybody in the group. In particular, most respondents reported that the original password policy was *"somewhat ineffective"* (N=12, Mdn=3), *"ineffective"* (N=11, Mdn=2), or *"strongly ineffective"* (N=5) in alleviating an employee's tendency to justify a password policy violation via EEIDI. Only three of the participants reported that the given password policy was *"neither ineffective nor effective"* at reducing the tendency of an employee sharing their password with a colleague and justifying the violation as normal behaviour in the work context.

At the group level, the median value for each group revealed different results. For instance, groups B, E, and F had a similar perception that the hospital password policy in its current state was *"neither effective nor ineffective*" (Mdn=4) to mitigate the use of EEIDI. Also, participants in groups C, D, H, and J evaluated the policy as "*somewhat ineffective*" (Mdn=3), while the median for groups A and G indicated the group participants agreed that the policy was "*ineffective*" at reducing the justification for violating the password policy via the EEIDI. In contrast, the only group I assessed the current password policy as *"somewhat effective."* Furthermore, the overall policy effectiveness median (Mdn= 2, IQR3-IQR1=1) across all groups indicated that there was strong agreement that the current password policy was *"ineffective"* to counter policy violation and the relevant justification via EEIDI.

- **During the collaborative writing process:**

EEIDI was examined in terms of participants' arguments for accepting or rejecting such justification. Also, their motivations when they used EEIDI were considered, as was the relevant decision-making process of participants to update the current password policy in order to counteract the tendency of other medical practitioners to share passwords and to assert that it was some sort of normal behaviour. The following scenario was projected on the screen:

"*Sarah is a Medical Intern in a public large-sized hospital, and she has access to the hospital Electronic Medical Records system (EMRs).To ensure that patient information is preserved securely, the hospital has a firm password management policy that all medical staff must keep their EMRs account password confidential. One day, Sarah was approached by another medical intern named Tony, who asked Sarah to share her EMR account password to allow him to write a medical note and view patients' records as Tony's password is expired.* ***Sarah knew that Tony was a trustworthy colleague and a member of her team. Also, she felt that everyone in her team was sharing their passwords in the clinic. Therefore, Sarah gives Tony her password to let him write the required medical note/order using her account."***

According to Renfrow and Rollo [316], individuals tend to reduce guilt and shame via a claim of normalcy, which "refutes the notion that an act is deviant by reframing it as something that

‘everyone is doing” [316]. Here, a total of ten password policy changes were added to mitigate the impact of password sharing and the use of EEIDI. Medical interns in this study proposed three SCPT strategies to reflect their perceptions for reducing employees’ tendency to adopt EEIDI and break the password policy requirement to keep it confidential: These SCPT strategies were to “increase the perceived risk,” “increase effort,” and “remove excuses.”

The most recommended SCPT strategy was to increase the perceived risk, which refers to “the consequences of crimes such as detection by management or termination” [310]. According to Tunley et al. [317], sometimes insiders develop new techniques to work around security controls and procedures. By assessing the control circumvention risks associated with job roles, organisations may design situation-specific strategies that enhance protection and improve the chance of a security breach being detected and action taken. For instance, ongoing monitoring and reporting procedures, such as spot audits, employee and system safety checks, whistleblowing, data analysis, and communications monitoring increase detection risks. In our context, it was noted that groups E, D, G, and I proposed that clarifying the cost of non-compliance with the password policy could discourage password sharing via EEIDI. The main argument behind explaining the penalties or consequences of non-compliance was the close relationship between the medical team members and the level of trust that allowed them to educate each other about any anticipated harm to personal and organisational levels. As a member in group D explained this perception:

> ***Member from* D**: *“I remembered when I started medical training, everyone in the team was a mentor to me, even the nurses. From day one, you can feel that you are part of the team spirit and everyone trying to support you.”*

Therefore, Group D said, if the consequences of non-compliance were clearly defined in the security policy and imposed in practice, members of the medical team would protect each other from harmful costs and make everyone aware of the consequences of violating the password policy. Also, they assumed this would indirectly prevent password sharing from being a typical behaviour. Therefore, such an argument revealed the impact of a medical group’s decision on the individual decision-making process to assess whether or not password sharing was acceptable, which could motivate the individual to evoke the EEIDI. This argument was consistent with Snyman et al. [318], who defined the influence of the group on individual decision-making as a “behavioural threshold.” They stated that each member of a group had an internal decision-making process for adhering to the group’s behaviour. This mechanism

evaluates the personal cost against the benefit of participating in group behaviour, taking into account the number of other group members who are already behaving in a particular way. In the information security context, Snyman et al. [318] explained behavioural threshold by writing that, "if enough members of a group share their passwords with other members and the number exceeds an individual's threshold for participation, the individual will also share their password with others even when they know that they are not supposed to" [318].

In addition, groups E, D, G, and I discussed the overlap between the DoI and EEDI, as both required modifications to the password policy, demonstrating the risk associated with non-compliance. So, they added more specific statements that illuminate the dangers of password sharing by illustrating several types of penalties or consequences, which included suspension of access to EMR accounts, legal responsibilities, and monetary fines:

Group D: "*Suspension of the account and it can reach temporary suspension of the medical licence if the password is shared multiple times or cause a massive Privacy breach."*

Group E: "*Team password sharing is prohibited, and the account that is used in sharing will be deactivated and considered compromised from the legal point of view."*

Group G: "*Sharing accounts/ passwords, writing it down or storing it in locations where it can be found, is unprofessional and that is prohibited. If compromised, will subject the individual to the following:*

- *The password of the account will be changed immediately.*
- *At the first attempt of violation, the user will get a warning letter and will be subjected to enquiry.*
- *In each future violation, the individual will be obligated to pay a penalty of 500SR.*
- *Using others' accounts is prohibited and will subject the individual to enquiry and penalty of 1000SR."*

Group I: "*EMRS users will be instructed that sharing their accounts might compromise system security, patient care and subject the original account user for legal consequences."*

In addition, two groups (J and C) agreed that the password policy could increase the perceived risk by improving the sense of natural surveillance and ensuring that the medical practitioners report any password sharing. In the SCPT, a whistleblower is an important strategy of neutral

surveillance. In criminology, a whistleblower is “the person who ‘speaks out about illegal or unethical behaviour within his or her organisation’” [319].

In information security, Pacella [320] defined a “Cybersecurity whistleblower” as the individual who is volunteering responsibly for ensuring compliance with the information security policies and controls by reporting any security threats, vulnerabilities, or breaches to management or the IT department. Their efforts play an essential role in filling the gaps in the security infrastructure [320]. Thus, two groups (C and L) modified the password policy by adding statements indicating that any password abuse should be reported in an attempt to change awareness of the consequences of a password breach. For example, conducting a surprise security audit may increase the detection possibility of any password sharing and could discourage the individual from sharing the password via EEIDI. They added:

Group J: *“If any password abuse happens, it must be reported to the chairman of the department.”*

Group C: *“Regular auditing to each department in rounds like fashion to see the non-compliant departments.”*

The second recommended SCPT strategy was to increase effort. According to Padayachee [309], “the increase the effort category involves ensuring criminal opportunities are difficult to execute which may discourage offenders.” It includes five subcategories: (1) target hardens, (2) control access to facilities, (3) screen exits, (4) deflect offenders, and (5) control tools/weapons. According to Clarke and Cornish [238], an effort escalation is a form of “hard” or traditional crime reduction method, which is based on the assumption that making crime impossible or difficult to execute by modifying environmental variables can negatively affect the offender's rational decision and reduce the risk of crime from occurring.

Two groups (A and J) suggested increasing the effort via controlling access to the EMR system. These groups agreed that relying on the psychological method, such as training, to change password sharing would be not enough if this behaviour was common among the medical team members. So they suggested that increased information security awareness should be aided with physical security controls to make sharing passwords challenging. A member in group J stated that

> *“You literally can't stop them from sharing the account or password, but at least we can make this process difficult.”*

Several groups suggested that the IT department should prevent multiple login sessions to the electronic medical records system (EMRs), which implied that each EMR account holder could only open one EMR at a time. If another session were detected, the oldest session would be automatically logged out. According to group discussions, preventing double login could provide two benefits. First, it could improve security compliance efforts to reduce password policy abuse. The second was that it could enhance IT resources management by assisting medical practitioners in finding more vacant computers to use in clinics. A member of group D discussed the resource availability issue indirectly during their argument on how to reduce EEIDI adoption by stating the following: "*Leaving an EMR account open as a way to reserve a computer causes another issue in addition to security because I need to use the computer, but if an account is opened, it means that I need to find another computer to use. If I log out from the open account, my colleague will get angry. This is really annoying because it always happens on the ward*."

This approach was proposed by different groups to discourage individuals justification via DoI for password sharing (see section 7.3.1), but here, other groups suggested increased effort via control access to the EMR as an SCPT method to discourage violating the password via EEIDI. Thus, they added the following:

Group A: *"Double log in policy, when the same username is logged in in 2 different computers, security information reminder and an instruction message will appear to remind the user, and it will require the account holder to log out from the initial session."*

Group J: *"If more than one computer is already logging in to the same account, log of from the other computer immediately."*

The last suggested SCPT to reduce medical practitioners tendency to justify password sharing via EEID was removing the excuse that everybody was sharing their passwords by altering the medical practitioner's awareness. According to Padayachee [309], integrating awareness of insider threats into regular security training would be sufficient to increase their awareness. In our context, several groups asserted that they had not been made aware of acceptable and unacceptable behaviours when they started their internship year, which is consistent with the findings of interviews (see chapter 5, section 5.4.3.1). Two members from two different groups (G and D) pointed to the lack of security awareness among the medical practitioners. As the member from group D put it,

"I feel that the sharing password is wrong, but I never knew that there is an official document in the hospital called policy prohibited it; nobody told us about it at all."

Thus, groups D and C believed that each medical clinic should support the IT department and enforce information security compliance with the password policy by educating medical practitioners and advocating password confidentiality among members of their teams. According to these two groups, changing the MI's awareness and making it clear that sharing passwords was a security breach could reduce this behaviour and the associated justification via EEIDI. As a member of group G stated:

"I read the policy twice, and I have not read any indication targeting prohibiting sharing passwords specifically between colleagues."

In addition, several MIs were surprised when they read in the original password policy the "Audit Control" section; they even suggested that this section was "terrifying" and that they were unaware of the IT department's technological capabilities to monitor any suspicious activities in the EMR system, including sharing passwords. Thus groups D and C added the following:

Group D: *"Each Department will be responsible for educating its workers regarding the importance of not sharing passwords and the consequences of this practice by the annual meeting."*

Group C: "*Regular lectures given to each department on the importance of security policies compliance."*

- **Post-Assessment evaluation:**

Table 7.1 shows that most of the participants revealed that the updated policy was more effective at mitigating the tendency to justify password policy violation via EEIDI. Across the group participants, a total of twenty-six participants perceived the updated policy as effective. Fourteen participants (33%) believed that the updated password policy that considered the EEIDI scenario was *"effective," "strongly effective"* (N=7, 17%) and *"somewhat effective"* (N=5, 12%) at discouraging justifying sharing passwords as normal behaviour. In contrast, twelve participants (29%) out of 42 revealed that the modified password policy generally remained *"somewhat ineffective,"* (N=8, Mdn=3), "*ineffective"* (N=2, Mdn=2), or "*strongly ineffective"* (N=2) against the EEIDI justification for password policy non-compliance. Only a

few of the participants (N=4, 10%) had a neutral perception of the updated password policy to mitigate the EEIDI claims.

At the group level, according to Figure 7.12, the overall median values for all groups revealed an improvement in their perception of the policy before and after the collaborative writing process to counter EEIDI. The only exception was that the perception of group E remained the same (Mdn=4), which indicated that the password policy before and after the modifications was still seen as *"neither effective nor ineffective*" to mitigate the use of EEIDI. In addition, the median variance for groups D and H indicated a minor change in their perception from *"somewhat ineffective*" (Mdn=3) before the policy modifications via the collaborative writing process to *"neither effective nor ineffective*" for both groups (Mdn=4). The median values for participants in the rest of the groups (A, G, C, J, F, B, and I) post-assessments indicated an improvement in the effectiveness of the updated policy in mitigating the EEIDI claim. The median comparison between the pre-assessment and post-assessment suggested an enhancement of the participants' perception. Here, the median for groups A and G pre-assessment significantly improved for both from *"ineffective*" (Mdn=2,) to *"somewhat effective*" (Mdn=5) for group A and *"neither effective nor ineffective*" (Mdn=4) for group G. Likewise, groups C and J pre-assessment median value of the original password policy was *"somewhat ineffective*" (Mdn= 3), while the post-assessment median for both groups was (Mdn=5) of the updated policy. Thus, the difference in the median values indicated that the perceptions of groups C and J improved and now considered the updated policy as *"somewhat effective*" at discouraging the use of EEIDI to justify password sharing. Also, the medical value comparison between groups F and B indicated substantial changes in participant evaluation from "*neutral*" evaluation in the preassessment (Mdn=4) to "*effective*" (Mdn=5) in the post-assessment. The only group I evaluated the original password policy as *"somewhat effective*" (Mdn=5), which increased after the modification of the password policy to "*strongly effective*" (Mdn=7).

Further, Table 7.2 shows that the median of participants' overall perception across all groups significantly improved and established an agreement that the revised password policy via collaborative writing was "*effective*" (Mdn=6) compared to the pre-assessment of *"somewhat ineffective*" (Mdn=3). Thus, their perception was that the changes could affect the tendency of medical practitioners' non-compliance behaviour with password policy via EEIDI (Mdn=6, IQR3-IQR1=3).

7.3.5 The Overall Effectiveness Of Password Policy Via The CW Process

In this study, the effectiveness of the updated password policy was assessed based on pre-and post-assessment tests and during the collaborative writing process. In the pre-and post-evaluation tests, we added a single question after the neutralisation claims section to measure participants' evaluation of the overall effectiveness of the given password policy to mitigate the given neutralisation claims based on a 7-point Likert scale. The following subsections illustrate the variation of the MI's perception between the original password policy and the updated password policy via collaborative writing to mitigate the intention to justify password sharing.

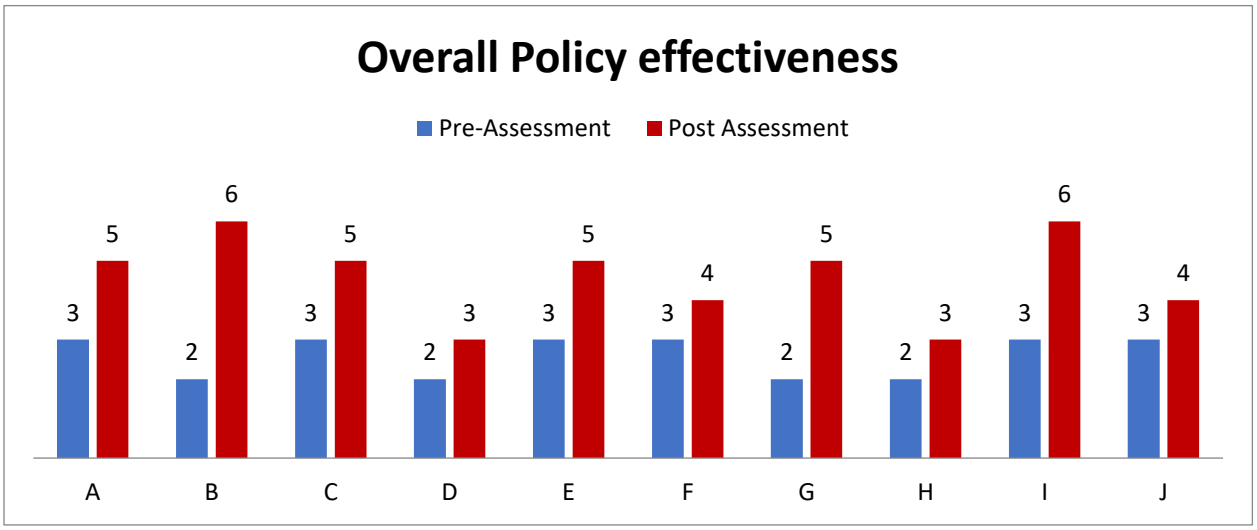


Figure 7.15 Medians Comparison Between All Groups For Overall Password Policy Effectiveness To Counter Neutralisation Claims

- **Pre-assessment evaluation**

According to Table 7.1, most of the medical interns (N=36 out of 42) evaluated the original password policy generally on the ineffective side to mitigate the various justification claims. In particular, half of the medical interns assessed the current policy as "ineffective" (N=21, Mdn=2). At the same time, twelve of them evaluated the policy as "somewhat ineffective" (N=12, Mdn=3), and three of them as "strongly ineffective" to counter the different justification claims to violate the password policy. In addition, five medical interns had a neutral perception of the current policy (Mdn=4), and only one medical intern assessed the password policy in its current state as "somewhat effective" (Mdn=5).

At the group level, Figure 7.14 shows that the groups had two perceptions of the effectiveness of the original password policy. A total of six groups perceived the original password policy in its current state as *"somewhat ineffective*"(Mdn=3), while four groups evaluated the original policy before the collaborative writing process as *"ineffective"* (Mdn=2)

- **During the collaborative writing process:**

During the collaborative writing process, the researcher was an observer of the group discussions without intervening since any intervention might influence the participant's decisions. When each group had finished recording their modifications to the password policy, the researcher asked them the following question:

"***What you have learned from this activity (the collaborative writing), and have you enjoyed it?***"

The participants provided several different perceptions of collaborative writing as an activity. Many participants asserted that they had personally seen at least one of the given scenarios to share the EMR account or password during their internship. Thus, using the collaborative writing process, the group participants would put themself in the IT department shoes and interact with each other to find solutions that could mitigate the medical worker's tendency to adopt any of the given justifications. Thus, this approach could influence the behaviour of the participants via the psychological concept of cognitive dissonance, which asserted that individuals feel discomfort when there is a contradiction between their behaviour and their cognitions such as beliefs, ideas, and values [192].

Many participants stated that the discussion and interactive writing with others based on the concept of letting participants play the role of the IT department in redesigning the password policy and reducing password breaches was both informative and enjoyable. Thus, this is consistent with Brewer et al. [33], who stated that effective behavioural intervention includes experiential and interactive elements such as discussion and role-playing and that these elements are important in reinforcing desirable behaviours and establishing prosocial habits. Many participants stated that collaborative writing increased their security awareness of the importance of the password policy and the information security threats associated with non-compliance. For instance, members in groups B and C explained the benefits of collaborative writing discussion to mitigate the password sharing justifications:

***Member from* B**: *"The discussion during the collaborative writing helps me to understand why some features are prohibited because I put myself in the IT department shoes."*

***Member from* C:** "*When I first read the policy, I thought it is 'wow,' but these justifications let me reconsider my thoughts as I did brainstorming with the group, then I found the policy do not prevent these justifications that I know they are common in our workplace. It is practical."*

Participants also mentioned the importance of "hearing their voices." They believed that such a collaborative approach could enhance the alignment of work duties with IT information security requirements and increase their security awareness in an enjoyable manner. This confirmed an essential motivation concept of "doing something because it is inherently interesting or enjoyable" [321]. Many participants described similar enjoyable feelings of being a part of a collaborative writing group to enhance a security policy:

***Member from* D**: "*There is a need to hear the practitioner voice because they are the end-users of these policies. When the policy is rigid, then there is a high chance that people will not comply."*

***Member from* E**: "*It is good to reflect our thoughts using this method; it is the first time I think about a security thing. I think I understand why we need this password policy because I'm trying to solve certain problems; I enjoyed it more than the lectures*."

***Member from* F**: "*Even I don't know that much about security things, but I enjoyed how we as a group can enhance a policy."*

Member from I: *"If the policy is vague and practitioners are not discussed about it, they may not comply with it because the policy is not practical or effective for them."*

- **Post-assessment evaluation:**

According to Table 7.1, group perception of the overall effectiveness of the updated password policy improved to counter the given justification claims for password sharing. This is evident by the fact that the majority of respondents (N=27 out of 42, 65%) stated that the updated password policy was "somewhat effective" (N=15, Mdn=5), "effective" (N=9, Mdn=6), or "strongly effective" (N=3, Mdn=7). In contrast, only nine of the 42 participants (22%) stated that the overall effectiveness of the updated password policy resulting from collaborative writing was still "ineffective" (N=5, Mdn=2) or "somewhat ineffective" (N=4, Mdn=3) in reducing the tendency to justify password policy violation via the given neutralisation claims. Also, a comparison of the pre-and post- evaluations showed that the number of participants who had a neutral perception that the effectiveness of the updated password policy increased slightly (N=6, Mdn=4) compared with the pre-assessment (N=5). Moreover, the overall median change improved in post-assessment, as showed in Table 7.2, from "ineffective" (Mdn=2) to "somewhat effective" in the post-assessment (Mdn=5). Thus, this implies that participants across all groups agreed that the modified password policy via collaborative writing was overall improved and could reduce, from their perception, the

tendency of medical practitioners to violate the password policy and justify this behaviour using various justifications.

At the group level, Figure 7.14 shows an improvement in participants' evaluation of the effectiveness of the updated password policy across all the groups. Groups B and I provided the most significant variation in the updated password perception as they both revaluated the original policy as "ineffective" (Mdn=2) and "somewhat ineffective" (Mdn=3) respectively, while their perception transformed to "effective" (Mdn=6) for both groups in the post-assessment. The medians variation in four groups (A, C, and E) improved from "somewhat ineffective" (Mdn=3) to "somewhat effective" (Mdn=5) in the post-assessment. Similarly, group G evaluated the overall effectiveness of the modified policy to be "somewhat effective" (Mdn=5). Groups F and J showed slight improvement, and the members of these groups perception improved from "somewhat ineffective" (Mdn=3) to neutral (Mdn=4) for the overall effectiveness of the updated policy. The effectiveness perception of groups D and H remain on the ineffective side in the post-assessment evaluation.

An interesting part of the analysis of groups D and H was that their post-assessment of the password policies resulted from the collaborative writing process of groups B and E. Group D evaluated the updated policy from group B, while group H was responding to the updated policy developed by group E. The content analysis of groups B and H revealed that these two groups used generic sentences to counter all neutralisation scenarios and did not target each of the neutralisation scenarios with a specific statement. This probably influenced the judgment of groups D and H and implied that the collaborative writing that addressed specific neutralisation techniques could generate more effective approaches to counter the risk of behavioural justification than less specific generic writing.

7.4 Descriptive Analysis of All Participants

Table 7.2 Descriptive Statistics For All Participants

Dependent Variables	N	Median (Mdn)		Standard Deviation (stdev)		Interquartile Range (IQR)					
		Pre-assessment	Post-assessment	Pre-assessment	Post-assessment	Pre-assessment			Post-assessment		
						IQR3	IQR 1	IQR 3- IQR 1	IQR 3	IQR 1	IQR 3 - IQR 1
Denial of Responsibility	42	4	6	1.72	1.49	6	5	1	6	5	1
Denial of injury	42	3	5	1.73	1.74	5	2	3	6	3	3
defence of necessity	42	3	5	1.17	1.60	4	2	2	7	4	3
Everybody elseis doing it	42	3	6	1.50	1.76	5	2	3	6	3	3
Appeal to higher loyalty	42	3	5	1.44	1.62	4	2	2	7	4	3
Overall Policy effectiveness	42	2	5	0.89	1.43	3	2	1	6	4	2
Self-efficacy	42	5	6	1.23	0.80	6	5	1	6	5	1
Work impediment	42	5	5	1.56	1.73	6	3	3	6	3	3

Table 7.2 shows the descriptive results of the pre-and post-assessment surveys of all participants for the dependent variables Denial of Responsibility (DoR), Denial of Injury (DoI), Defence of Necessity (DoN), Everybody Else Is Doing It (EEIDI), and Appeal of Higher loyalty (AoHL) in terms of overall effectiveness, self-efficacy, and work impediment. These dependent variables relied on ordinal data and were measured using two 7-point Likert scales. The difference in the median values indicated that perception of the hospital's password policy varied before and after the policy modification.

All the medians of the neutralisation techniques illustrated in Table 7.2, showed an improvement trend in the respondents' evaluation for the updated password policy between the pre- and the post-assessment from (4, 3, 3, 3, and 3) to (6, 5, 5, 6, and 5) respectively. This implies that the neutralisation technique scenarios via collaborative writing produced, from the respondents' perspective, *"somewhat effective"* (MDn=5) and *"effective"* (Mdn=6) updated password policies. Likewise, the comparison between the pre- and post-assessment median values of the overall policy effectiveness construct revealed substantially improved evaluations, as the median increased from *"ineffective"* (Mdn=2) in the pre-assessment to *"somewhat effective"* (Mdn=5) in the post-assessment.

According to Table 7.2 , the median values of respondents perception about their self-efficacy was slightly improved. This implied that their confidence to conduct the security requirements of the modified policy was increased. Group members shared a common awareness of the security requirements after thoroughly discussing the original password policy. Lastly, the work impediment variable referred to a problem that occurred when the security requirements were incongruent with the employee work goals. The median variation between the pre- and post-assessments in Table 7.2. reveals that the respondents' perception about the modified password policy did not add more complication to their work duties. Thus, their median variation of the work impediment between the pre- and post-assessments remain the same at *"somewhat agree"* (Mdn=5).

However, a statistical measure is needed to calculate the group's perception of the effectiveness of the updated policy to counter all neutralisation scenarios. Thus, the Statistical Significance test was performed to account for this difference. However, the data collected was based on two Likert scales that use ordinal data. We, therefore, used a non-parametric test called the Wilcoxon signed-rank test to measure changes in the perception of MIs toward the effectiveness of the hospital password policy from the same individuals before and after the collaborative writing session as discussed in the following section.

7.5 Statistical Significance Test

The Wilcoxon signed-rank test is nonparametric that was used to assess the significance of median differences of the MI's perception about the effectiveness of password policy to mitigate the neutralisation techniques before and after the collaborative writing activity. This test is an alternative to the paired samples t-test to calculate whether the median differences differ from zero in the population. Ko and Dorantes [322] stated that the Wilcoxon signed-rank test "is adequate when comparing before-and-after observations on the same subjects." According to Laerd statistics [323], the Wilcoxon signed-rank test requires three criteria to decide whether to use it as an alternative to the parametric tests. First, the dependent variables are measured based on either continuous or ordinal data. In our case, this criterion is satisfied, as all the dependent variables are measured based on two 7-points Likert ordinal scales (see section 7.2). The second criterion for the Wilcoxon signed-rank test is that the study includes two related groups, which means the same participants are being tested on two occasions. In our context, this criterion was assured as the MI perception of the password policy effectiveness

to counter neutralisation techniques was measured before and after the collaborative writing process via the pre and post-assessment surveys.

Finally, the third criterion states that the Wilcoxon signed-rank test is only used when the data of variables are not normally distributed [324]. Therefore, the Shapiro-Wilk test is an important test to check the normality of the data of the dependent variables. The normality test results of the Shapiro-Wilk test indicate that data is not normally distributed for all the dependent variables as the P-value < (0.05) (See Appendix D.3 for the test of normality). Therefore, it violated the assumption that any parametric test (e.g., a paired T-test) can be applied to compute the statistical significance of the difference between two related samples (pre-and post-assessments).

Based on the above, the Wilcoxon signed-rank test can be used to decide whether there was a significant median difference between paired observations of participants' perception at two-time points. If the P-value resulting from the Wilcoxon signed-rank test is more significant than 0.05 (P> 0.05), we can conclude no statistically significant difference between the two related groups. Thus, we do not have enough evidence to reject the Null hypothesis. In contrast, we can consider that the result is statistically significant if the P-value is less than 0.05 (P<0.05), which indicates that the median variance is statistically significant. Thus, this test can detect any change in the participant evaluation of the effectiveness of the updated password policy against neutralisation techniques before and after the collaborative writing process. The Wilcoxon sign rank test was performed using the Statistical Package for the Social Sciences (SPSS) V.26.0 (IBM Crop) to calculate the difference between two related groups based on the following hypothesis:

- **Null hypothesis (H0):** The median difference for medical interns perception (evaluation) of the updated password policy effectiveness to counter neutralisation techniques between the pre-and post-assessments is equal to Zero.
- **The alternative hypothesis (H1):** The median difference for medical interns perception (evaluation) of the updated password policy effectiveness to counter neutralisation techniques between the pre and post-assessments is not equal to Zero.

7.6 Overall Statistical Significance Test For All Participants

Table 7.3 Overall Hypothesis Test Via Related-Samples Wilcoxon Signed Rank Test For All Participants

Hypothesis Test Summary				
	Null Hypothesis	**Z-value**	**Sig. P-value**	**Decision**
DOR	**The median of differences between DoR before ISP collaborative writing and DoR after ISP Collaborative writing equals 0.**	3.185	0.001	**Reject the null hypothesis.**
DOI	**The median of differences between DoI before ISP collaborative writing and DoI after ISP collaborative writing equals 0.**	3.981	0.000	**Reject the null hypothesis.**
DON	**The median of differences between DoN before ISP collaborative writing and DoN after ISP collaborative writing equals 0.**	4.56	0.000	**Reject the null hypothesis.**
EEIDI	**The median of differences between EEIDI before ISP collaborative writing and EEIDI after ISP collaborative writing equals 0.**	4.555	0.000	**Reject the null hypothesis.**
AOHL	**The median of differences between AOHL before ISP collaborative writing and AOHL after ISP collaborative writing equals 0.**	4.728	0.000	**Reject the null hypothesis.**
Overall policy Effectiveness	**The median of differences between Over All Effectiveness before ISP collaborative writing and Over All Effectiveness after ISP collaborative writing equals 0.**	5.278	0.000	**Reject the null hypothesis.**
Self-Efficacy	**The median of differences between Self-Efficacy before ISP collaborative writing and Self-Efficacy after ISP collaborative writing equals 0.**	2.742	0.006	**Reject the null hypothesis.**
Work impediment	**The median of differences between Work impediment before ISP Collaborative writing and Work Impediment after ISP collaborative writing equals 0.**	-0.868	0.385	**Retain the null hypothesis.**
Asymptotic significances are displayed. The significance level is .050.				

Table 7.3 presents the Wilcoxon signed-rank test result for all participants. In this study, we used pre-and post-assessments to measure the impact of integrating the neutralisation scenarios on the infosec effectiveness via the collaborative writing process. Thus, we find a significant improvement in the MI's perception of the updated password policy before and after the CW activity. Table 7.3 shows that P-values for all of the neutralisation techniques (DoR, DoI, DoN, AoHL, and EEIDI) are less than 0.05 ($P<0.05$). These results indicate that the post-assessment of the effectiveness of the modified password policy to counter the neutralisation claimes are statistically significant. Thus, we have enough evidence to reject the null hypotheses.

Also, as illustrated in Table 7.3, the P-value for self-efficacy is ($z=2.742$, $P=0.006$), which means that the median difference between Self Efficacy before and after ISP collaborative writing is not equalled to Zero. Thus, there is a statistically significant difference in the

participant self-efficacy, so we accept the alternative hypothesis that there is an improvement in medical practitioner self-efficacy. According to Bandura's social cognitive theory [160], self-efficacy is defined as "individuals' judgments of their capabilities to organise and execute courses of action required to attain designated types of performances." In information security, self-efficacy is defined as an individual's judgment of their capacity (e.g., skills and competence) to adhere to security policies to safeguard organisational information and systems [325]. In our context, a significant positive difference in the self-efficacy of medical interns indicates that they feel more competent to meet the security requirements and objectives of the updated password policy via the CW than the original password policy. Thus, such positive self-efficacy from the medical interns could improve their intent to comply with the modified password policy. It also implies that engaging the end-user of the policy during the security policy development process can lead to the creation of a new policy that is more likely to suit the end users' existing skills and does not increase the IT burden on the employee to comply with the security policies.

In addition, the P-value for the InfoSec policies work impediment (hindrance) on the medical interns' daily activities is Z=-0.868, P-value=0.385. In information security literature, work impediment is referred to as "a detriment to an employee's daily job-related tasks and activities resulting from compliance with the requirements of the ISP" [42]. We draw a similar concept in our context as we evaluate how the hospital's existing password policy obscures the primary tasks and how integrating the SCPT to mitigate the neutralisation techniques via CW could increase or reduce the password policy's complexity perception.

The result reveals that the rejection of the null hypotheses is not possible. It shows no statistically significant difference in the complexity of the password policy between the pre- and post-assessments after modifying the hospital password policy. However, it offers a negative association relationship between the pre-and post-assessment, which implies that both the updated and the original password policy still interferes with the medical practitioners' daily tasks as a cost of compliance. Several groups have suggested several SCPT strategies to improve password policy, such as using a fingerprint instead of a password when the account is inaccessible due to password expiration. Still, these modifications remain without actual implementation in the real world, which may bias their post-evaluation because they haven't seen them in practice. Also, the work impediment has been added as a construct within the pre- and post-assessments to evaluate whether end-user participation in security policy development can produce a security policy that balances security requirements and business activities.

However, we did not expect medical interns during CW to improve the password policy to make it simpler; we evaluated their perceptions based on the proposed SCPT solutions to mitigate the four neutralisation techniques scenarios that could lead to a password policy violation.

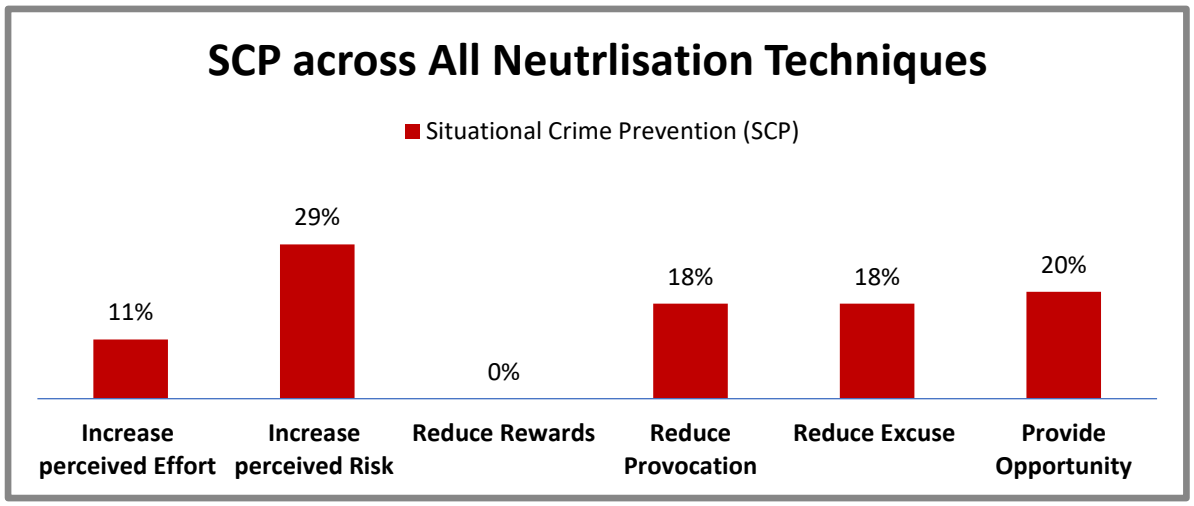


Figure 7.16 The Overall Recommended SCPT Strategies Across All Groups To Counter Neutralisation Scenarios

7.7 Chapter Summary

Like chapter 6, this chapter contributes to the thesis by analysing and describing the study intervention to decrease end users' propensity to rationalize security policy violation through a collaborative writing process for security policies (password sharing) in one of the largest hospitals in Saudi Arabia. This empirical study contributes significantly to the thesis by demonstrating that engaging end-users through a collaborative writing process can help develop more effective security policies more suited to the actual work environment. As a result, this can help reinforce behavioural compliance by decreasing end users' propensity to justify non-compliance with InfoSec policies.

IT security controls and measures may be unsatisfactory in the information security literature when the balance of information security compliance costs tilts in favour of the expected benefits for non-compliance [326][109]. Thus, according to Situational Crime Prevention Theory (SCPT), this generates an opportunity that could motivate the individual to justify the violation of security measures or procedures, which is the link between the neutralisation techniques and the SCPT concept of opportunity-reduction. This thesis demonstrates that such an imbalance exists in today's information technology security initiatives in chapters 4 and 5. The current chapter argues that more effective strategies may be developed by paying equitable, proportionate attention to individual justifications to violate information security

policies as a valuable way of improving the current security policies and controls. We asserted that user engagement, in general, would be valuable since the insider threat might be aggravated by misunderstanding security policies or controls, as well as a lack of procedural fairness [327][109]. As a result, including users throughout the information security policy lifecycle, from development to implementation, may be beneficial. Therefore, in this chapter, we encourage the involvement of end-users to assess the usability of security measures that may be the first step in reducing insider discomfort with information security safeguards and reinforcing compliance with the organisation's information security policies.

This chapter explains the quantitative and qualitative approaches to data collection and analysis and the statistical method used to evaluate the results of pre-and post-evaluation. Also, the qualitative approach includes the content analysis of the password policy document after the collaborative writing process and the focus group discussions. The results indicate that incorporating end-user perceptions through the collaborative writing process increases the effectiveness of password policies in mitigating some hypothetical neutralisation scenarios causing password sharing. Thus, the study provides new knowledge for improving information security policies using an interdisciplinary approach focused on integrating the concept of opportunity reduction via SCPT and neutralisation techniques for justifying password policy breaches.

In this chapter, the statistical results show a significant variation between the medical practitioners' evaluations of the effectiveness of the modified policy before and after the collaborative writing process. Also, the qualitative findings provide interesting and valuable knowledge of the obstacles that the password policy causes on the work performance of medical interns, which too often leads to the adoption of neutralisation techniques to share the password. Also, the collaborative writing groups provide several solutions to mitigate password sharing risks and the associated justifications using the SCPT as a baseline to code and identify these solutions from the end user's perspective. These proposed solutions could improve the IT's department understanding of the challenges resulted from complying with the current security policies and related controls.

Figure 7.15 shows the overall SCPT strategies across all groups to counter four neutralisation scenarios. Increased perceived risk of password violation is found to represent 29% of the group's total modifications to the original password policy after the CW. This is a traditional method for mitigating crime and non-compliance with information security policies and

controls in the InfoSec literature [328]. In our context, compliance depends on the increasing cost (negative consequences) of non-compliance with information security policies through formal and informal sanctions such as salary reduction, legal responsibility, termination of service, and so forth. This is consistent with the semi-structured interviews in chapter 5 that the hospital had poor enforcement of the security policies formal and informal sanctions, which create a poor security awareness that information security is not a priority matter in the hospital. Increasing the perceived risk was the most suitable approach to mitigate DoI.

According to Figure 7.15, the second strategy was providing the opportunity to the medical practitioners to improve their compliance and mitigate their justification for password sharing. This strategy represented 20% of the modifications to enhance the password policy effectiveness. The suggestions included facilitating compliance to counter the DoN and AoHL by simplifying some security procedures, using a fingerprint instead of the password, offering an alternative solution to help the medical practitioners during urgent situations by creating an emergence account for the clinic, and the legalisation of password sharing in certain conditions.

Removing excuses and reducing provocations were both of equal importance (18%) to minimise the given scenarios, especially the EEIDI and DOI to share the password. Based on the SCPT, the groups proposed removing excuses by changing the medical practitioners' awareness by providing the medical practitioners with the proper security awareness education and training.

Setting clear and consistent rules in the security policies or imposing a code of ethics as part of the security compliance initiatives could discourage the medical practitioners from justifying the password violations. This includes posting instructions of acceptable and unacceptable behaviour to ensure information security compliance. Furthermore, the groups suggested reducing provocation, which refers to the emotional triggers that motivate medical practitioners to rationalize password sharing via the following methods: (1) refining an information security culture by leveraging the solid social bond between medical teams to convey and raise awareness of information security; (2) employee acknowledgement of security policies; (3) tasks computerisation such as resetting the password on the spot; (4) employees signature on information security policies; and (5) Crime Prevention Through Environmental Design (CPTED). According to Wortley [329], precipitator controls in the "reduce provocations" category represent a softer approach than the other four categories in the SCPT. Thus, implementing these SCPT strategies can reduce stress and frustration from the pressure of the

social context, facilitate work duties, and improve compliance with security needs, ultimately discouraging the tendency of medical practitioners to adopt neutralisation techniques.

The next chapter concludes this thesis and describes its limitations and potential future work direction.

Chapter 8 : Conclusion

This thesis proposed that the effectiveness of information security (InfoSec) policies to mitigate an individual's tendency to justify security non-compliance could be improved through the engagement of the end-user in the development phase of security policies via a collaborative writing process. In the healthcare context, four empirical studies presented in Chapters 4–7 were used to investigate in-depth the role of neutralisation techniques on individual information security violations, to identify the environmental factors that trigger behavioural justifications, and conduct action research to evaluate the efficiency of the collaborative writing process to balance security policy requirements with the medical practitioners' work goals. Sections 8.1 to 8.3 address the research questions presented in Chapter one. Section 8.4 introduces the research contribution for the thesis. Next, section 8.5 presents the thesis limitations for each of the thesis phases and future work. Finally, Section 8.6 presents a summary of the thesis.

8.1 Thesis Research Question 1

The first research question for this thesis is RQ1: "***What is the association between neutralisation techniques and the intention of medical interns to violate information security policies?***"

The answer to this question is covered in Chapter 4, the first phase of this research. In that chapter, a quantitative study was conducted to understand better the research problem—the role of neutralisation techniques in violating information security policies and patient privacy in hospitals. A quantitative study was conducted based on a theoretical model to test the hypothesis of the relationship between neutralisation theory and the intent behind a medical intern's behavioural violation of InfoSec policies. The theoretical model had one proposition:

Hypothesis one (H1): "***Neutralisation directly and positively affects the intention of Medical Interns (MI) to violate the hospital's information security policies intended to protect patient privacy."***

An online research questionnaire was used to collect data from medical interns in four academic hospitals in three different regions of Saudi Arabia. Each of these universities has an academic hospital that offers a Medical Internship Program (MIP) for medical students. The data collection process successfully identified a total of 66 medical intern participants. The result found that neutralisation theory via the defence of necessity (DoN), denial of injury (DoI), the metaphor of ledger (MoL), condemnation of condemners (CoC), denial of responsibility (DoR), and appeal to higher loyalties (AoHL) predicted and influenced positively the medical interns' intention to violate InfoSec policies. This positive relationship established the basis of the thesis to investigate

the environmental motivations that led the medical practitioners to evoke neutralisation techniques to violate the security policies, sometimes placing the privacy of patients at risk.

8.2 Thesis Research Question 2

The second research question of this thesis is **RQ2**: "***What drives behavioural justifications among medical practitioners to violate information security policies in healthcare organisations?***"

The answer to the second research question was addressed in Chapter 5, which constituted phase two in the research methodology. The purpose of this phase was to examine the effect of environmental factors on medical practitioners' motives to not comply with a hospital's information security policy. Thus, we adopted a qualitative approach by conducting a series of semi-structured interviews to explore the factors that contribute to behavioural justifications for violating security policies designed to protect patient privacy. Semi-structured interviews were performed in one of the largest hospitals in Saudi Arabia. This hospital has about 1,400 beds in various specialities and many medical facilities and research centres across the country. The hospital receives about 30,000 patients each year and serves more than 250,000 registered patients.

We argued that adherence to information security policies could not be taken for granted. Medical Interns (MIs) sometimes drift into non-compliance and adopt neutralisation techniques to ease their consciences when they decide not to comply with InfoSec policy dictates. On the other hand, sometimes the environment and social norms explicitly encourage non-compliance: people follow the descriptive norms (what others are doing) rather than injunctive norms (what the policies tell them to do).

We interviewed 28 participants in total, including twenty Medical Interns and eight IT staff. Using in-depth thematic analysis, we identified several social, emotional, and organisational factors that motivated the medical interns to justify their violations of hospital InfoSec policies. Sometimes the environment and social norms explicitly encourage non-compliance: people follow the descriptive norms rather than injunctive norms. In particular, the social factors influencing the MIs to evoke neutralisation techniques fell into two main themes: (1) influences from peers and superordinates and (2) emotional facilitators, primarily those of trust and empathy. At the same time, poor awareness of the existing information security policies and poor awareness of the consequences of InfoSec violation and corresponding deterrence mechanisms were organisational factors that motivated the medical interns to justify security non-compliance. In conclusion, the results of the study indicated that there is a need to develop information security policies that take into account specific environmental factors that stimulate behavioural justifications for

information security non-compliance and improve the usability of policies to reduce work disruption.

8.3 Thesis Research Question 3

The third research question of this thesis is RQ3: "***To what extent does the engagement of the perception of end-user during information security policy development via a collaborative writing process increase the effectiveness of the information security policies to mitigate the role of neutralisation techniques?"***

The answer to this research question was addressed in Chapters 6 and 7, which constituted phases three and four in the research methodology. Two similar studies were conducted to discover whether involving end-users of information security policies in the policy development stage could produce a more effective policy that aligns security requirements with business needs, thus alleviating the tendency of individuals to justify non-compliance.

In Chapter Six, the involvement of twenty-four graduate students from the University of Glasgow to participate in a collaborative writing process was discussed. The results from the pre-assessment and post-assessment confirmed that the revised password policy produced by the collaborative writing process was effective, from the student's perspective, in mitigating some of the neutralisation techniques claims. In particular, the statistically significant results revealed that the variation of the password policy effectiveness before and after the collaborative writing process was enough to reject the null hypothesis for Don and EEIDI. However, the statistical significance using the Wilcoxon signed-rank test for the overall effectiveness of the updated password policy was insignificant in reducing the overall individual tendency to justify password sharing. Therefore, based on the findings from Chapter six, the answer to the third question is that the findings partly support the intervention goal of improving security policy through end-user engagement, which in turn results in better security policy that can discourage individual behavioural justifications for security non-compliance.

Chapter seven repeated the study in chapter six but in a different country and work environment to generalise the previous results. Forty-two medical interns, who were working full-time in one of the biggest hospitals in Saudi Arabia, were invited to participate in this study. The study result confirmed that the engagement of the end-users of InfoSec policies via a collaborative writing process improved the effectiveness of the security policy and produced an updated policy that reduced the intention of medical practitioners to rationalise password and account sharing. The Wilcoxon signed-rank test was used to compute the statistical significance of the difference between the password policy effectiveness before and after the collaborative writing process. The

results reveal sufficient evidence to reject the null hypotheses because the P-value of all neutralisation techniques (DoR, DoI, DoN, AoHL and EEIDI) was significant. Thus, we found a significant improvement in MI's perception of the updated password policy after CW activity. Also, the difference in the overall effectiveness of the updated password policy to counter neutralisation claims was statistically significant. This means that engaging end-users in the development phase of the security policy lifecycle has been a promising approach to improving the effectiveness of an information security policy to counter individual behavioural justifications for non-compliance with security policies. Therefore, based on the results of chapter 7, the third research question has been addressed.

Direct comparisons between the results of the UK study (Chapter 6) and the Saudi Hospital study (Chapter 8) are problematic since the two sample groups may differ in terms of culture, education level, working experience, and IT expertise. However, as shown, the approach appears to work for these two quite different user samples.

8.4 Research Contributions

The main objective of this thesis was to investigate the role of neutralisation techniques and their environmental factors that affect the behavioural justifications of individuals to violate information security policies. Next, we proposed an intervention to reduce the tendency of these behavioural justifications by engaging the end-user in the information security policy development stage using a collaborative writing process, thus improving the effectiveness of security policy by balancing security requirements with business needs. The significant contributions of this thesis (outlined in Chapter 1, Section 1.5) can be summarised as follows:

- **Chapter 2** provides a comprehensive overview of the role of information security policies in protecting information and IT assets in organisations. This chapter explained why individual behavioural non-compliance is a serious internal threat to organisations, specifically in the healthcare industry, and identified the high cost of information security breaches to both organisations and individuals. It also describes the theoretical foundation of neutralisation theory and its applications in criminology and digital and information security. In addition, this chapter discussed several criminal and psychological theories related to neutralisation theory. Finally, the chapter reviews the limited attempts of information systems scholars to mitigate the impact of neutralisation techniques and promote compliance with information security policies.
- **Chapter 4** contributes to the first phase of this thesis. This chapter answered the first research question (RQ1) by extending the InfoSec literature on neutralisation theory's role in a

healthcare setting to predict a medical practitioner's violation of the security policies that protect patient privacy. This study is centred on a theoretical model that acts as a foundation for collecting data on the relationship between neutralisation theory and its function in predicting employee justifications for non-compliance with information security policies. This study makes three important contributions: first, it investigates the impact of neutralisation techniques on an individual's violation of information security policies within a healthcare environment. Thus, it is the first study based on our best knowledge that explores such a security threat in the healthcare industry to predict cognitive justification strategies that may lead to intent to breach information security policies. Second, this study extends the work of Park et al. [78] and Siponen and Vance [1] in the information security literature beyond North America and Europe [17] and investigates the influence of the neutralisation techniques on the information security policy violation in the Middle East, specifically Saudi Arabia. Third, the study provides evidence to information technology decision-makers in healthcare organisations, especially in Saudi Arabia, to consider the impact of neutralisation techniques on non-compliance with security requirements to help them improve their efforts to enhance information security policies and privacy awareness programs.

- **Chapter 5** contributes to the second phase of the thesis and addresses the second research question. The purpose is to investigate and identify the healthcare environmental factors that motivate medical practitioners to justify their violations of the information security policies in one of the biggest hospitals in Saudi Arabia. It contributes to the body of knowledge by exploring the different problems associated with information security management in a healthcare setting. A set of semi-structured interviews with twenty-eight medical interns and eight IT department staff was analysed in detail. This chapter employed a thematic analysis to generate a list of textual codes and themes. The findings indicated that various social, organisational, and emotional variables contribute to the adoption of neutralisation strategies to alleviate emotions of guilt or shame associated with breaking information security policies and potentially compromising patient privacy. Based on the chapter results, it was decided to focus on the influence of peer pressure as social factors, trust as an emotional facilitator, and password sharing as a common security threat to develop four neutralisation scenarios to investigate the effectiveness of the password policy to mitigate these scenarios and a set of relevant justification claims in chapters 6 and 7.
- **Chapter 6** contributes to the third phase of the thesis. This chapter addressed research question three (RQ3) by conducting an action research study that included twenty-four students at the University of Glasgow divided into six groups. The purpose of this experiment was to discover if the effectiveness of InfoSec policies could be improved by integrating the perceptions of

end-users to mitigate neutralisation techniques via a collaborative writing process. The chapter empirically analysed the data in three steps: (1) before the collaborative writing process, (2) during the collaborative writing process, and (3) after the collaborative writing process. Before the collaborative writing process, a self-developed pre-assessment survey was conducted regarding the effectiveness of the original password policy to counter neutralisation claims. The qualitative analysis was conducted to examine both the group discussion and a content analysis of the produced document from the collaborative writing activity. Then, a post-assessment survey of the updated password policy was conducted to determine any change of the password policy's effectiveness to counter the neutralisation claims. The findings showed that such engagement would create more user-centred policies, which can support the IT department's efforts to produce and implement more effective InfoSec policies and controls. Therefore, this process could play an essential role in countering end user tendencies to justify non-compliance behaviour.

- **Chapter 7** contributes to the fourth and last stage of the thesis. The purpose was to increase the generalizability of the research on the outcome of the intervention by replicating the experiment described in Chapter 6 in one of the largest hospitals in Saudi Arabia. This chapter addressed the third research question (RQ3) by providing evidence for improving the effectiveness of password policy after engaging medical practitioners in efforts to develop password policy to reduce the tendency to adopt neutralisation techniques for password sharing. Again, this chapter includes three data collection methods: (1) pre-assessment survey of the perceived effectiveness of the hospital's current password policy to counter justifications claims to share the password between medical practitioners, (2) during the collaborative writing process, and (3) post-assessment survey to evaluate the effectiveness of the resulted updated password policy to reduce justifications of password violation.

  The chapter's analysis of pre-and post-assessment tests aimed to determine the variance, if any, of the medical practitioners' evaluation between the original and the updated password policy and whether there was a positive statistically significant difference. Also, this chapter used a qualitative analysis for the group discussions during the collaborative writing activity and content analysis to examine the password policy after the modifications of the collaborative writing. The findings of the chapter provide evidence that the engagement of end-users in the development stage of the security policy could positively influence its effectiveness to counter the propensity to evoke neutralisation techniques for non-compliance. The outcome of this chapter also provides evidence for the IT department that the alignment of IT security requirements with business needs can be achieved by "hearing the voice of end

users" by involving them in the security policy development process. This engagement through collaborative writing can combine the end user's understanding of their work environment with IT security expertise, which can produce more balanced security policies that could discourage end users from justifying violations of the security policies and enhance security compliance.

8.5 Practical implications

The current study has numerous essential management ramifications. The practical contribution is made by information security departments being able to build and deploy better information security policies inside their organisations. By gaining a better understanding of the impact of environmental and social factors that trigger behavioural justifications for non-compliance, the information security managers may be better equipped to develop and implement information security policies inside their organisations. Below is a summary of the practical implications of developing the information security policies via a collaborative writing activity to mitigate the role of neutralisation techniques. Therefore, it can improve the individuals' compliance with the information security policies:

- This research indicates that information security policies need to be tailored to target the logic of neutralisation that is often claimed as a justification for policy violations. According to Chapters 6 and 7, this approach attempts to directly oppose the use of neutralisation techniques to violate the security policy by tailoring different messages via a collaborative writing activity in the security policy based on the end users' understanding of their work context and the common justifications among co-workers. Thus, it can provide the IT department with a better opportunity to understand the deficiencies in their security policy requirements and enhance its contents.
- Involve the end-user in a focus group to discuss and develop information security policies based on a set of common workplace justifications (scenarios) and have end-users play the role of the IT department in protecting the organizations' IT assets. This approach presented in this thesis provides the end-user with the knowledge to shape appropriate behaviour when there is a conflict between business priorities and information security requirements. Thus, it can indirectly improve their information security awareness and understanding of the factors behind having these security requirements in policy and the related risks of non-compliance.
- The researcher believes that the intention of individuals to adopt neutralisation techniques to justify non-compliance with information security policies is a common security issue facing many organizations in different industries in the world. Thus, the results of the

current study that is based on modifying the security policies via a collaborative writing process show that the involvement of the end-user in the development of information security policies and controls can produce more efficient policies to counter the security risks resulting from this undesirable behaviour. Thus, providing the IT department with an additional and cost-effective preventive strategy instead of relying on the traditional approach to maintaining compliance, such as formal and informal sanctions.

8.6 Limitations And Directions For Future Work

This study was organised into four phases to investigate the role of neutralisation techniques on individual non-compliance. Each phase encountered many constraints that impacted the study design, data collecting, and analysis. This section discusses the research constraints associated with each phase, as seen in Figure 8.1 as well as potential directions for future investigation.

Phase 1	Phase 2	Phase 3	Phase 4
Determine the role of Neutralisation techniques to predict medical practitioner intention to violate InfoSec policies. A quantitative study using a questionnaire in Saudi Arabia.	Investigate the motivations of medical practitioners to evoke neutralisation techniques to justify InfoSec violations. A qualitative study using semi-structured interviews in a Saudi Arabian hospital.	Enhancing InfoSec policies effectiveness against neutralisation techniques via the engagement end-user perception. An action research study using focus groups and pre and post questionnaires in the UK, University of Glasgow.	Enhancing InfoSec policies effectiveness against neutralisation techniques via the engagement end-user perception. An action research study using focus groups and pre and post questionnaires in a Saudi Arabian Hospital.

Figure 8.1 The Four Phases of The Research

8.6.1 Limitations in Phase 1

This empirical study has three significant limitations that should be acknowledged: first, the study sample was limited in size (66 medical interns) and was drawn from just four academic hospitals in Saudi Arabia; thus, caution should be exercised when generalising the study results. As a result, future studies should include a qualitative method and a bigger sample size. Second, all survey respondents (MIs) were Saudi citizens; hence, when generalising our findings, the effect of national cultural variations should be considered. Also, this study was conducted in the context of healthcare, which is a very complex environment with a huge workload and high levels of stress. Thus, future researchers need to expect a low response rate as many medical practitioners may feel unmotivated to participate in a research study unrelated to the field of health care. Therefore, future information security research should consider investing more time, communication, and effort to encourage medical practitioners to participate. In this study, the

researcher had previous practical experience in the field of health care, which facilitated communications and logistics support obstacles to reach the target sample.

Third, this study relied on a self-reported technique that collected MI intentions to violate the security policies that protect patient privacy via hypothesised scenarios; hence, the degree of realism of the scenarios had a significant effect on the intention but not on the actual behaviour.

Future work should consider conducting comparative studies in other healthcare organisations using Hofstede's cultural dimensions model [186] located in a different country with similar cultural indexes such as Power distance or Collectivism to confirm and generalise the results.

8.6.2 Limitations in Phase 2

This study has limitations relating to the sample chosen for the interviews. Here, all the collected data was limited to a single academic hospital in Saudi Arabia with a relatively high degree of homogeneity in the demographic in terms of the Saudi culture. Thus, caution is suggested when generalising the study findings in other contexts. Another limitation is the Social Desirability Response Bias (SDRB) during face-to-face interviews, where the participants answer the interviewer's questions in such a way as to present a favourable self-image. We attempted to overcome this research issue by asking the participants to report their colleagues' behaviour to violate InfoSec policies and related justifications instead of asking them to describe their own behaviour. Also, additional caution should be taken when developing the interview questions by considering the differences between the organisation's context in terms of cyber security expertise and IT security resources.

Future work could include interviewing team leaders or immediate managers of the medical teams, the chief of clinics. or senior physicians to explore their views on the impact of information security policies on job duties, their awareness of information security policies, and their level of acceptance of neutralisation techniques to violate the security policies. Thus, it would be useful to investigate the influence of these people as an important social factor that can motivate their subordinates to justify security policy violations. In addition, future work could investigate the critical role of the middle or immediate managers in establishing a solid information security culture among employees and the advantages of their involvement in the enforcement efforts of the information security policies compliance. According to several interviewees in phase 2, the position of the superordinate, particularly that of the immediate manager, had a significant impact on information security compliance behaviour. In our case, the medical practitioners are more likely to agree to activities that they believe are approved by immediate managers and superordinates, which may significantly impact negatively or positively their information security

behavioural compliance. Finally, we found that individual emotions, such as trust and empathy, play an important role in facilitating behavioural justifications. Future work could explore more emotional facilitators that could play a role in motivating the behavioural justifications for InfoSec policies non-compliance.

8.6.3 Limitations in Phase 3

The participants in this phase were graduate students from the University of Glasgow. This phase was approached as a pilot study to measure the intervention's applicability, test its research measurements, and get a deeper understanding of its complexity. One limitation in this study was the level of work experience of most of the participants, as some students participated only marginally in the discussions because they felt that they were less experienced to suggest modifications to the security policy. In addition, most of the participants were from the School of Engineering, and students outside this school were less active during the discussion as those participants with IT knowledge dominated the discussion. Future work may consider undertaking the study with current employees working in different departments at a different university. Also, another limitation of the study was due to the spread of the Covid-19 pandemic in the UK and the implementation of social distance restrictions across the country, which hindered getting feedback using a focus group from the university's IT department. Future work may consider getting feedback using the focus group method from IT departments for the feasibility of these proposed solutions and make an assessment at the level of abstraction of similarities and differences between security best practices and proposed security solutions in modified information security policy documents via a collaborative writing process.

8.6.4 Limitations in Phase 4

This phase faced many limitations as it was conducted in a real working environment in one of the largest hospitals in Saudi Arabia. In this study, it was difficult to obtain a large sample due to the reasons mentioned above, as well as large patient loads, a strict work schedule between clinics, emergency calls from different clinics requiring personal attendance, and so forth. Thus, over three months, we obtained only 42 medically trained participants. Also, the researcher had to interrupt the experiment on several occasions as the hospital called a blue code, which required some participants to leave the collaborative writing session immediately. Furthermore, pre- and post-evaluation tests were developed based on the finding in Chapter 5, which reflected the influence of peer pressure and trust on password and account sharing. Thus, future work may consider the effect of the superordinate pressure on subordinates to develop neutralisation scenarios and claims that reflect this social factor to motivate risky behaviour, such as sharing

EMR patient screen images via social media applications. Another limitation was that the IT department at the ABC Hospital had not empirically evaluated the outcome of this phase.

Like the UK, Saudi Arabia still applies strict social distancing rules to protect its citizens from the Covid-19 virus. For six months, the researcher tried to get feedback from the ABC hospital security department, and they all apologised that they were too busy dealing with the workload. Also, the ABC Hospital was a victim of excessive cyber attacks attempting to gain cyber advantages from the critical situation of the pandemic. Future work may consider engaging IT department security personnel in a focus group to evaluate proposed solutions from end-users to mitigate neutralisation techniques via the collaborative writing process. Also, future work may consider providing the participants with information about the concept of situational crime prevention techniques (SCPT) before they are involved in the collaborative writing process. This could improve the quality of the discussion and may make it more focused on the purpose of the study. In addition, future work may evaluate using the collaborative writing activity as an interactive approach to increase the individual information security awareness of the information security policies and controls. This may require the development of pre-and post-assessment tests that can evaluate the participants' security awareness using behavioural justifications as triggering ideas to lead the discussion. Also, this study was conducted in a single hospital in Saudi Arabia. Thus, caution should be taken to generalise the findings, which could provide an opportunity to perform a similar study in another healthcare organisation and compare the result.

8.7 Summary

The research presented in this thesis examined the role of neutralisation techniques in individuals violating information security policies in a healthcare organisation. This research is divided into four main studies. It begins with a quantitative study that tests a theoretical model for establishing the relationship between neutralisation techniques and the intent of medical interns to violate information security policies that protect patient privacy. The result demonstrated that there is a positive and meaningful relationship between neutrality and information security non-compliance. The second study is a qualitative study that aims to identify the environmental factors that motivate medical practitioners to adopt behavioural justifications for violating information security policies.

The results of the third and fourth studies, however, confirmed the single most important finding of this research: involving end-users in the IT department's efforts to develop information security policies through a collaborative writing process would develop policies that reflect both the technical and security needs of the IT department—and thus the organization as a whole—and the real world medical and business needs of front line medical practitioners. Thus, this study

can improve the effectiveness of information security policies and enhance security compliance while at the same time reducing the tendency of individuals to justify violations of InfoSec policies—and thus risk violating patient privacy and even health—by invoking neutralisation techniques.

Appendix A
(Appendix to Chapter 4)

A.1 Hypothetical security scenarios

Table A. 1 Hypothetical Security Scenarios for Phase 1

#	Violation	Security Scenario
1	Information Handling	Ahmad is a medical intern in a medium-sized public hospital where he was recently hired. He has access to the hospital Electronic Medical Records system (EMRs) to perform his duties. To ensure that patient information is preserved securely, the hospital has a firm information security policy that any document that contains partial or complete information of a patient's EMR must be kept in secure drawers. Recently, he was contacted by a physician colleague named Emma, who asked Ahmad to access four patients' Electronic Medical Records (EMR) in order to print their medical history, including patients' names, medications and diagnoses. Afterwards, she told Ahmad to put those files at the nurses' shared desk in the clinic reception. Emma's plan was to collect those files the next day afternoon. Thus, Ahmad has expected that printing medications and treatments history and dropping them in the nurses' shared desk would save his colleague's time. He also knows that printing patient EMR information is a common practice in the hospital, and recently an employee was blamed for printing documents, which included sensitive patient information as patient name, diagnosis history, and left them at a shared desk surface. Ahmad printed the requested patients EMR information for Emma and left them at the nurses' shared desk surface in the clinic reception.
2	Use of Social Media Apps	Sara is a medical intern in a public large -sized hospital where she has worked for several months, and she has access to the hospital Electronic Medical Records system (EMRs). To ensure that patient information is preserved securely, the hospital has a firm information security policy that all medical staff must not share any type or format of information related to patient electronic medical records via social media websites or applications. One day, Sara was approached by a physician co-worker named Muhammad, who asked her to access a specific patient Electronic Medical Records system (EMRs) and take pictures of the patient EMR screen. Then, she sent those pictures back to him via a mobile WhatsApp application, which would give Tony a quick overview of the patient emergency case. Sara has expected that sending those pictures of the patient information via WhatsApp could save Muhammad's time to deal faster with an emergency case. Although Sara believes sending sensitive patient information via social media application (WhatsApp) may be a violation of the hospital information security policy. Sara took several pictures of the patient EMR information screen and shared them with Muhammad via WhatsApp.

A.2 Measurement Items

Table A. 2 independent variables Measurements Items And Sources For Phase 1

Constructs	Item		Source
MI Intention to violate InfoSec policies that protect the security	Int_1	How likely that you would do what Ahmad did in the described scenario?	Adopted from D'Arcy et al. [330]
	Int_1	How likely that you would do what Sara did in the described scenario?	
Denial of Responsibility	DoR-1	It is OK to violate the hospital information security policy if you aren't sure what the policy is.	Adapted from Thurman [252] and Siponen and Vance[1]
	DoR-2	It is OK to violate the hospital's information security policy if the policy is not advertised.	Adapted from Siponen and Vance [1]
	DoR-3	It is OK to violate the hospital's information security policy if you do not understand it.	
Denial of injury	DoI-1	It is OK to violate the hospital's information security policy if no harm is done.	Adapted from Siponen and Vance [1]
	DoI-2	It is OK to violate the hospital's information security policy if no one gets hurt.	Adapted from Thurman [252] and Siponen and Vance[1]
	DoI3	It is OK to violate the hospital's information security policy if no damage is done to the hospital.	Adapted from Siponen and Vance[1]
Condemnation of condemners	CoC-1	It is not wrong to violate the hospital's information security policy when the policy is unreasonable.	Adapted from Thurman [252] and Siponen and Vance[1]
	CoC-2	It is not wrong to violate a hospital's information security policy that requires too much time to comply with	Adapted from Siponen and Vance [1]
	CoC-3	It is not wrong to violate a hospital's information security policy that is too restrictive.	
Appeal to higher loyalties	AHL1	It is all right to violate a hospital's information security policy to get a job done.	Adapted from Thurman [252] and Siponen and Vance[1]
	AHL2	It is all right to violate the hospital's information security policy if you get your work done	Adapted from Siponen and Vance[1]
	AHL3	It is all right to violate the hospital's information security policy if you complete the task given by management	
Defence of necessity	DoN1	It is all right to violate the hospital's information security policy under circumstances where it seems like you have little other choices	Adapted from Thurman[252] and Siponen and Vance[1]
	DoN2	It is all right to violate the hospital's information security policy when you are under a tight deadline	Adapted from Siponen and Vance[1]

	DoN3	It is all right to violate the hospital's information security policy when you are in a hurry	
Metaphor of the ledger	MoL1	feel my general adherence to the hospital's information security policies compensates for occasionally violating an information security policy.	Adapted from Siponen and Vance [1]
	MoL2	I feel my good job performance compensates for occasionally violating the information security policy.	
	MoL3	I feel my hard work in the hospital compensates for occasionally violating an information security policy	

A.3 Descriptive Statistics in Tabulation Format

Table A. 3 Demographic Characteristics of the Sample for phase 1

Variable	Frequency	Percentages (%)
Gender		
Female	24	36.4
Male	42	63.6
Age		
18 - 23 yrs	2	3.0
24 - 29 yrs	60	90.9
30 - 35 yrs	4	6.1
Have you been informed about the security procedures defined by the hospital to protect patient information privacy and confidentiality		
Yes	34	51.5
No	32	48.5
In a typical day, how many hours do you spend using Electronic Medical Records System (EMRs) for your work		
Less than 1 hours	5	7.6
1 - 2 hours	26	39.4
3 - 4 hours	25	37.9
5 - 6 hours	7	10.6
More than 6 hours	3	4.5
In a typical day, how many total hours of internet usage do you consume per day in your workplace		
Less than 1 hours	22	33.3
1 - 2 hours	28	42.4
3 - 4 hours	12	18.2
5 - 6 hours	3	4.5
More than 6 hours	1	1.5

A.4 Ethical Approval

A.5 Participant's Information Sheet

University of Glasgow | College of Science & Engineering

Participant Information Sheet

The title of study: **Investigating the Role and the Relationship of Humans' Neutralisation Techniques and**

Organisational Factors that Drive the Problem of Information Security Violation.

Name of Researchers: Dr Tim Storer & Mr.Saad Altamimi

You are being invited to take part in a research study. Before you deciding to participate, it is important for you to understand why the research is conducted and what it will involve. Please take time to read the following information carefully and discuss it with others if you wish. Ask us if there is anything that is not clear or if you would like more information. Take time to decide whether or not you want to participate. Participation is entirely voluntary and can be stopped at any time.

Research purpose and structure

They are two main objectives of this study:

- Investigating why employee in healthcare organisations may violate information security policies and the role of human's Neutralisation techniques to drive such a problem.
- Understanding the psychological factors that may impact the effectiveness of both information security policies and the information security and security awareness programmes in the healthcare context.

This study is a web - based survey which will be conducted approximately in 10-20 minutes. Medical interns will be asked to read two security scenarios and based on the scenarios; he/she will fill out of the study questionnaire as the following steps:

1. Demographic information.
2. Participants' behavioural intention toward doing the same actions that one of the scenario characters did.
3. Participants' neutralisation techniques that will may be used to justify the violation of the patient security.

Risks

Similar to most of the research studies, the researchers should consider any kind of risks that may affect the participants. However, based on our knowledge, there are no foreseeable risks associated with this survey.

Benefits

You will not directly benefit from participating in this research, but benefits to academia and society include extending the body of knowledge in healthcare settings. Thus, this study is developed to enhance our understanding in information security field, specifically in the protection of patient information security.

Confidentiality

Your identity will not be captured in this survey, nor will the data provided be available to deduce individual respondents. Both you and your healthcare organisation will remain anonymous. Data will be encrypted in process, transfer and storage and can only be accessed by this research conductors.. This data might be used as part of research publications. However, all data will be anonymised and once the survey is submitted even the investigator cannot identify individual respondents.

Participation

Completing this survey is totally voluntary, and you can withdraw at any time without providing any reasons

Contact

If you have any further questions, please do not hesitate to contact:

Mr.Saad Altamimi, Email: s.altamimi.1@research.gla.ac.uk

Dr Tim Storer , Email: timothy.storer@glasgow.ac.uk

School of Computing Science, University of Glasgow

Appendix B
(Appendix to Chapter 5)

B.1 Participants Consent Form

Consent Form

Title of Project: Improving security policies quality by integrating user perspective via collaborative writing process.

Name of Researchers: : Mr.Saad Altamimi and Dr.Tim Storer

Basic details

☐ I confirm that I have read and understood the Participant Information Sheet for the above study.

☐The study has been explained to me, and I understand the explanation given and what my participation will involve.

☐I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.

Confidentiality/anonymity clauses

☐I acknowledge that participants will not be personally identified.

Consent on method clause

☐ I consent to interviews being audio-recorded

Clauses relating to data usage and storage

All names and other material likely to identify individuals will be anonymised.
The material will be treated as confidential and kept in secure storage at all times.
The material may be retained in secure storage for use in future academic research.
The material may be used in future publications, both print and online.
☐I agree to waive my copyright to any data collected as part of this project.

Basic consent clause

☐I have initialled the above boxes myself, and I agree to take part in the study.

Name of Participant	Date	Signature
…….	…….	……
Researcher	Date	Signature
…….	…….	…….

B.2 Participant Information Sheet

University of Glasgow | College of Science & Engineering

PARTICIPANT INFORMATION SHEET

- **Study title**: Understanding the motivation of behavioural justifications that lead to information security non-compliance in a healthcare context
- **Invitation paragraph**
  You are being invited to take part in a research study. Before you decide to participate, it is essential for you to understand why the research is conducted. Please take time to read the following information carefully and discuss it with others if you wish. Ask us if there is anything that is not clear or if you would like more information. Take time to decide whether or not you want to participate. Participation is entirely voluntary, and you can withdraw at any time.
- **What are the objectives of the study?**
  In the information security policies context, the employees' non-compliance behaviour considers one of the greatest risks as they use the digital hospital infrastructure to accomplish their routine work. The aim of this study is to extend the current research work in the information security field and its relationship to humans' behaviour. Specifically, we want to understand the internal and the external factors that influence the audience (end users) of the information security policies to violate them as well as the IT management perspective to develop and implement such security policies and its actual impact on the end-users. Under the lenses of Neutralisation theory, this study will gather and analyse the end users' responses and justifications (Medical interns as a research sample in Saudi Arabia) to violate the hospital security policies. Thus, this study output will help the researcher to get a deeper understanding of the end users' behaviour toward information security policies in a complex and dynamic environment such as a hospital. Also, it will help the hospital's IT management to consider some important factors during the development and the implementation of information security policies. Thus, this study will help the researcher to identify and integrate those factors to develop a security policies development framework that focus on designing those security policies collaboratively to reflect the end-users perception as a proposed solution to reduce end-users violation/non-compliance behaviour.
- **Why have I been chosen?**
  The study focuses on the medical individuals' behaviour (Medical Interns MI) who are regulated by a list of information security policies in their work environment and required to comply with these policies to protect the hospital IT assets. Also, this study examines the IT experts point of view in the hospitals about the internal and external factors that impact the process of information security policies development and implementation as well as the impact of those factors on end-users security policies violations.
- **Do I have to take part?**
  Participating in this study is voluntary, and it is up to you to decide whether or not to take part of the interview. If you do choose to join, you can withdraw at any time without giving a reason.

- **What do I have to do?**
  A list of semi-structure questions will be asked during the interview to each participant in order to fulfil the study purpose. Each question will obtain specific details that will serve the study investigation. Each participant has the right to accept or refuse answering any question.

- **What are the possible disadvantages and risks of taking part?**
  This study is expected to be risk-free, and it will not involve any risk on the physical and mental level.

- **What are the possible benefits of taking part?**
  You will not directly benefit from participating in this study, but benefits to academia and society include extending the body of knowledge in an information security policies development and implementation contexts. However, the information that is collected during this study will provide us to form a better understanding of the hospital information security environment and the hidden reasons behind the medical intern's non-compliance behaviour as well as their justifications for such risky behaviour. Thus, this study can escalate our understanding of the importance of end-user involvement in the security policy development and implementation process with the IT department.

- **Will my taking part in this study be kept confidential?**
  1. All participants' names will be fully anonymised.
  2. Every piece of information/ document in any format (digital or physical) gathered during this study will be encrypted and securely stored in a cabinet.
  3. All data/ documents only are accessed by the researcher for use in future academic research.
  4. No reference will be made in any form or shape that could associate participants to this study.
  5. Data/documents collected during this study will be securely stored in a safe cabinet for a maximum duration of three years; after this period, this data will be securely destroyed.

- **What will happen to the results of the research study?**
  Results will likely be published after the analysis of the results of the study. You will not be identified in any report/publication. You can request a copy of the publication on the condition that you will use it for academic purposes.

- **Who has reviewed the study?**
  The project has been reviewed by the College of Science and Engineering Ethics Committee in the University of Glasgow.

- **Contact for Further Information**
  Name: Mr.Saad Altamimi, Dr.Timothy Storer
  Emails: (*s.altamimi.1@research.gla.ac.uk*, *Timothy.Storer@glasgow.ac.uk*

B.3 List of the interview questions for it staff and medical interns

General Questions:

1. What is your Job Description?
    a. What does your job involve?
2. How long have you been doing this job?
    a. How long you've been at the hospital?
3. How does security engage to your day?
4. What is your information security background (Courses/training)?

- **Security policies development**
    1. How much would you say you know in general about the hospital security policies?
    2. Are people in the hospital consulted about the information security policy, to what extent? (Probe for: who and how).
    3. In general, what do you think of the security policies? Do you think they are too strict, too soft, or about right?
- **Security policies awareness /Training:**
    1. Have you had any training about security policies recently?
    2. Was it new information or just a refresher?
    3. How long was the security policies training? Was that a day or less than a day? Was it online-based or face to face? (Describe).
    4. Was it more actually training or just information delivery?
- **Security policies implementation:**
    1. Would you say the people follow all of the rules all the time in terms of security policies? Or most people follow them most of the time? Or somewhere in between?
    2. Can you think of a reason in your work environment why somebody might not follow one of them (such as password or encryption policies)?
    3. Are there any policies or procedures that people routinely don't comply with?
        a. Why do they do this? (Neutralisation question about the motivation)
- **Security policies enforcement:**
    1. Would people get reprimanded for not complying with security policies, for example if somebody was in the habit of not putting the lock on the screen when they left their desk?
    2. Does the hospital check whether employees comply with security policies? How?
    3. How would someone get caught if they did not follow those security policies?
    4. What sanctions or punishments are used against people that get caught?
        b. Do you think these are appropriate?
- **Security incidents reporting**
    1. What would you do if someone doesn't follow the security policy?
    2. Have you ever come across something that you consider to be a security vulnerability that the hospital IT management hasn't thought of?
    3. What do you think about the security culture in your hospital in general?

- **Closing question:**

How would you say that the hospital's information security compares with other issues, such as budget reduction or patient safety, that the hospital also cares about?

Appendix C
(Appendix to Chapter 6)

C.1 Pre And Post Assessment Survey Items For The Password Policy

Table C. 1 Measurements Items and references for Phase 3

Neutralisation Techniques	**How effective is the given policy in countering the following claim:**	**Measurement** 7 Point Likert scale	**Source**
Denial of responsibility	It is not my fault that the Universit provides complex password procedures that are inefficient. Thus, I will share my password with a trusted colleague.	1- Strongly Ineffective 2- Somewhat Ineffective 3- Ineffective 4- Not effective or ineffective 5- Somewhat effective 6- Effective 7- Strongly effective	Adapted from Silic et al. [151] and Siponen and Vnce [1]
	It is OK to share my password with a trusted colleague if I don't understand it.		
Denial of injury	No one got hurt if I share my password with a colleague.		
	It is OK to share my password with a trusted colleague at work if no harm is done.		
Defence of necessity	When I'm less busy, I will change my behaviour. Right now, it is necessary to share my password with a trusted colleague to complete our work faster.		
	It is all right to share my password with a trusted colleague when I'm under a tight deadline.		
Everybody else is doing it	it is OK to share my password with a trusted colleague because this is what everyone around me at work does.		
	Everybody around me is sharing their passwords with other colleagues. Thus, I will share my password with only a trusted colleague.		
Appeal to higher loyalty	I share my password with trusted colleagues to support them in their work.		
	It is all right to share my password at work if it helps my colleague to get the job done.		
Overall policy effectiveness	How do you evaluate the overall effectiveness of the given password policy in countering individuals justifications to share the password with their trusted colleagues?		
Self-efficacy	I have the necessary skills to fulfil the requirements of this policy.	1- Strongly disagree 2- Disagree 3- Somewhat disagree 4- Neither Agree nor Disagree 5- Somewhat Agree 6- Agree 7- Strongly agree	Adapted from Bulgurcu et al. [23]
	I have the necessary knowledge to fulfil the requirements of this policy.		
	I have the necessary competencies to fulfil the requirements of the policy.		
Work impediment	Following the requirements of the given password policy distract me from doing my actual work duties.		
	Following the requirements of the given password policy slows down my response time to my colleagues.		
	Following the requirements of the given password policy hinders my productivity at work.		
	Following the requirements of the given password policy reduces my efficiency at work.		

Appendix D
(Appendix to Chapter 7)

D.1 Pre And Post Assessment Survey Items For The Password Policy in the hospital

Table D. 1 Measurements Items and references for Phase 4

Neutralisation Techniques	**How effective is the given policy in countering the following claim:**	**Measurement** 7 Point Likert scale	**Source**
Denial of responsibility	It is not my fault that the hospital provides complex password procedures that are inefficient. Thus, I will share my password with a trusted colleague.	1. Strongly Ineffective 2. Somewhat Ineffective 3. Ineffective 4. Not effective or ineffective 5. Somewhat effective 6. Effective 7. Strongly effective	Adapted from Silic et al. [151] and Siponen and Vnce [1]
	It is OK to share my password with a trusted colleague if I don't understand it.		
Denial of injury	No one got hurt if I share my password with a colleague.		
	It is OK to share my password with a trusted colleague at work if no harm is done.		
Defence of necessity	When I'm less busy, I will change my behaviour. Right now, it is necessary to share my password with a trusted colleague to complete our work faster.		
	It is all right to share my password with a trusted colleague when I'm under a tight deadline.		
Everybody else is doing it	it is OK to share my password with a trusted colleague because this is what everyone around me at work does.		
	Everybody around me is sharing their passwords with other colleagues. Thus, I will share my password with only a trusted colleague.		
Appeal to higher loyalty	I share my password with trusted colleagues to support them in their work.		
	It is all right to share my password at work if it helps my colleague to get the job done.		
Overall policy effectiveness	How do you evaluate the overall effectiveness of the given password policy in countering individuals justifications to share the password with their trusted colleagues?		
Self-efficacy	I have the necessary skills to fulfil the requirements of this policy.	1. Strongly disagree 2. Disagree 3. Somewhat disagree 4. Neither Agree nor Disagree 5. Somewhat Agree 6. Agree 7. Strongly agree	Adapted from Bulgurcu et al. [23]
	I have the necessary knowledge to fulfil the requirements of this policy.		
	I have the necessary competencies to fulfil the requirements of the policy.		
Work impediment	Following the requirements of the given password policy distract me from doing my actual work duties.		
	Following the requirements of the given password policy slows down my response time to my colleagues.		
	Following the requirements of the given password policy hinders my productivity at work.		
	Following the requirements of the given password policy reduces my efficiency at work.		

D.2 Wilcoxon Signed Rank Test Results for Pre- Versus Post assessment for all participants.

Table D. 2 Wilcoxon Signed Rank Test Results for Phase 4

Post assessment minus Pre assessment	Note	Rank sign	N	Mean Rank	Sum of Ranks
DoR After Intervention - DoR Before Intervention	DoR After Intervention <DoR Before Intervention	**Negative Ranks**	8	14.06	112.50
	DoR After Intervention >DoR Before Intervention	**Positive Ranks**	26	18.56	482.50
	DoR After Intervention = DoR Before Intervention	**Ties**	**8**		
	Total		**42**		
DoI After Intervention - DoI Before Intervention	DoI After intervention <DoI Before Intervention	**Negative Ranks**	6	11.08	66.50
	DoI After intervention>DoI Before Intervention	**Positive Ranks**	28	18.88	528.50
	DoI After intervention = DoI Before Intervention	**Ties**	8		
	Total		**42**		
DoN After Intervention - DoNI Before Intervention	DoN After intervention <DoNI Before Intervention	**Negative Ranks**	6	10.83	65.00
	DoN After intervention>DoNI Before Intervention	**Positive Ranks**	33	21.67	715.00
	DoN After intervention = DoNI Before Intervention	**Ties**	3		
	Total		**42**		
EEIDI After Intervention - EEIDI Before Intervention	EEIDI After intervention <EEIDI Before Intervention	**Negative Ranks**	3	9.17	27.50
	EEIDI After intervention>EEIDI Before Intervention	**Positive Ranks**	30	17.78	533.50
	EEIDI After intervention = EEIDI Before Intervention	**Ties**	9[l]		
	Total		**42**		
AOHL After Intervention - AOHL Before Intervention	AOHL After Intervention <AOHL Before Intervention	**Negative Ranks**	4	5.75	23.00
	AOHL After intervention>AOHL Before Intervention	**Positive Ranks**	30	19.07	572.00
	AOHL After Intervention = AOHL Before Intervention	**Ties**	8		
	Total		**42**		
All Effect After Intervention - All Effect Before Intervention	All Effect After Intervention <All Effect Before Intervention	**Negative Ranks**	2	5.00	10.00
	All Effect After Intervention >All Effect Before Intervention	**Positive Ranks**	36	20.31	731.00
	All Effect After Intervention = All Effect Before Intervention	**Ties**	**4**		
	Total		**42**		
Self Effecacy after Intervention - Self Effecacy before Intervention	Self Efficacy after Intervention <Self Efficacy before Intervention	**Negative Ranks**	5	11.80	59.00
	Self Efficacy after Intervention >Self Efficacy before Intervention	**Positive Ranks**	19	12.68	241.00
	Self-Efficacy after Intervention = Self Efficacy before Intervention	**Ties**	**18**		
	Total		**42**		

Work impediment after Intervention - Work impediment before intervention	Work impediment after intervention <Work impediment before intervention	**Negative Ranks**	17	15.12	257.00
	Work impediment after intervention>Work impediment before intervention	**Positive Ranks**	12	14.83	178.00
	Work impediment after intervention = Work impediment before intervention	**Ties**	13		
	Total		42		

D.3 Test of Normality for all Independent variables

Table D. 3 Test of Normality for all Independent variables

Dependent variables	Shapiro-Wilk		
	Statistic	df	P-value.Sig.
DoR_Before_Intervention	0.924	42	0.008
DoR_After_Intervention	0.814	42	0.000
DoI_Before_Intervention	0.873	42	0.000
DoI_After_Intervention	0.874	42	0.000
DoN_Before_Intervention	0.865	42	0.000
DoN_After_Intervention	0.899	42	0.001
EBDI_Before_Intervention	0.906	42	0.002
EBDI_After_Intervention	0.890	42	0.001
APHL_Before_Intervention	0.918	42	0.005
APHL_After_Intervention	0.893	42	0.001
OverAll_Effectiveness before intervention	0.856	42	0.000
OverAll_Effectiveness after intervention	0.907	42	0.002
Self Effecacy before Intervention	0.877	42	0.000
Self Effecacy after Intervention	0.808	42	0.000
Work impeiment before Intervention	0.917	42	0.005
Work imoediment after Intervention	0.890	42	0.001

D.4 Neuralisation security scenarios list

Now, based on your understanding of your workplace environment, please read and edit the given policy in a way to better reflect your thoughts as a group to mitigate the following scenarios and their related justifications (A, B, C and D)

PI: (Clinical Recodes and documentation Policy)

Sarah is a physician in a public large -sized hospital, and she has access to the hospital Electronic Medical Records system (EMRs).

To ensure that patient information is preserved securely, the hospital has a firm **privacy and security section** that all medical staff must keep their EMRs account password confidential and secure.

One day, Sarah was approached by another medical physician named Tony, who asked Sarah to share her EMR account password in order to allow him to write a medical note/order and view patients' records as Tony has difficulties to log-in the EMR system. (*here, place one of the following actions A, B , C and D)*

a) (**DON**): Sarah knew that Tony was a trustworthy colleague and a member of her team. So, she felt that they were working in a busy clinic, and it was essential action to share her password in order to improve work performance. Thus, Sarah gives Tony her password to let him write the required medical note/order using her account.

b) (DoI): Sarah knew that Tony was a trustworthy colleague, and he was a member of her team. So, she felt that nobody would get harm if she shared her password with Tony. Therefore, Sarah gives Tony her password to let him write the medical note/order using her account.

c) (**AoHL**): Sarah knew that Tony was a trustworthy colleague and a member of her team. So, she felt that sharing her password was a type of professional help to Tony. Therefore, Sarah gives Tony her password to let him write the required medical note/order using her account.

d) (EBDI): Sarah knew that Tony was a trustworthy colleague and a member in her team. Also, she felt that everyone in her team was sharing their passwords in the clinic. Therefore, Sarah gives Tony her password to let him write the required medical note using her account.

D.5 Ethical Approval

D.6 participants' Information sheets

University of Glasgow | College of Science & Engineering

PARTICIPANT INFORMATION SHEET

- **Study title**: Improving information security policies effectiveness by integrating the end-user perspective to reduce neutralisation techniques via a collaborative writing process.
- **Invitation paragraph**

  You are being invited to take part in a research study of the application of collaborative writing to improving security policies for end-users. Before you decide to participate, you need to understand why the research is conducted. Please take time to read the following information carefully and discuss it with others if you wish. Ask us if there is anything that is not clear or if you would like more information. Take time to decide whether or not you want to participate. Participation is entirely voluntary and you can withdraw at any time.

- **What are the objectives of the study?**
  I. Investigating the impact of end-user perception on the effectiveness of information security policies.
  II. Getting a deeper understanding of the type of modifications that end-user performs on security policies to reflect his/her perspective to reduce Neutralisation techniques.
  III. Implementing collaborative writing as a strategy to integrate user perspectives to enhance the organisation security policies along with the policymakers
- **Why have I been chosen?**

  The study focuses on individuals who are regulated by a list of information security policies in their work or study environment and required to comply with these policies to protect the organisation IT assets and infrastructure.

- **Do I have to take part?**

  Participating in this study is voluntary, and it is up to you to decide whether or not to take part. If you do choose to join, you can withdraw at any time without giving a reason. Note: we will appreciate if you can notify the authors before you withdraw, to keep that in in the experiment records.

- **What do I have to do?**

  This study has five phases. All phases will be conducted **online at a specific time** and the total time of the experiment approximately (80-90 minutes)

  1. Reading a security policy (5 -7 minutes)
  2. Completing a pre-assessment survey (5 minutes).

3. Participating in collaborative writing activity with a group (60 minutes)
4. Read another group document (5-7 minutes)
5. Completing a post-assessment survey (5 minutes)

At a specific time and location , All participants in each group will meet and discus a given security policy, which they will edit it collaboratively . The pre-assessment and post-assessment questionnaires will be identical and will include: demographic information such as age, gender, qualification. Afterwards, the participant will be asked to answer a list of question to evaluate a given security policy.

- **What are the possible disadvantages and risks of taking part?**
  This study is expected to be risk-free, and it will not involve any risk on the physical and mental level.
- **What are the possible benefits of taking part?**
  You will not directly benefit from participating in this study, but benefits to academia and society include extending the body of knowledge in the context of an information security policies development. However, the information that is collected during this study will help us to form a better understanding of the importance of end-user involvement in the security policy development process to enhance the effectiveness of security policies.

- **Will my taking part in this study be kept confidential?**
  You can choose to provide or not provide information like age, qualification, gender and years of work experience. The results of the study may be published later, but general information like age, gender, etc will be anonymised. You will not be asked to provide your name; instead, an ID number and a mask name will assign to you. Please note that assurances on confidentiality will be strictly adhered to unless evidence of serious harm, is uncovered. In such cases, the University may be obliged to contact relevant statutory bodies/agencies.'

- **What will happen to the results of the research study?**
  Results will likely be published after the analysis of the study results. You can request a copy of the publication on the condition that you will use it for academic purposes.

- **Who has reviewed the study?**
  The project has been reviewed by the College of Science and Engineering Ethics Committee at the University of Glasgow.

- **How is the study funded?**
  The Saudi Arabian Ministry of Education is providing the researcher (Alta Mimi's) by a scholarship. The specific experiment does not have any additional funding.

- **Contact for Further Information**
  Name: Mr.Saad Altamimi, Dr.Timothy Storer

Emails: *s.altamimi.1@research.gla.ac.uk* , *Tim.Storer@glasgow.ac.uk*

Address: Room G103 , SAWB (Computing Science building) 18 Lilybank Gardens, Glasgow G12 8RZ.

D.7 A sample of the pre-assessment survey

Collaborative Writing for the security policies_Pre-assessment_NGHA_GroupB

Participant Consent Form

NGHA_Pre-Assessment for Group B

Consent Form

Please complete the consent form below

* 1. Basic details:

- [ ] I confirm that I have read and understood the Participant Information Sheet for the above study.
- [ ] The study has been explained to me, and I understand the explanation given and what my participation will involve
- [ ] I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.

* 2. Confidentiality/anonymity clauses:

- [ ] I acknowledge that participants will not be personally identified

* 3. Clauses relating to data usage and storage: All names and other material likely to identify individuals will be anonymised. The material will be treated as confidential and kept in secure storage at all times. The material may be retained in secure storage for use in future academic research. The material may be used in future publications, both print and online.

- [ ] I agree to waive my copyright to any data collected as part of this project.

* 4. Basic consent clause:

- [ ] I have ticked the above boxes myself, and I agree to take part in the study.

* 5. Please Create a Nickname for yourself? (This nickname you will use it for pre-assessment and post-assessment surveys. This is to ensure anonymity and confidentiality, so make sure you don't forget it)

Demographic Information

6. What is your gender?

- ◯ Male
- ◯ Female

* 7. What is your current level of education?

- ◯ Bachlor
- ◯ Master
- ◯ Other (please specify)

* 8. Have you held a job or role where you have access to the NGHA hospital Electronic Medical Records system (EMRs)?

- ◯ Yes
- ◯ No

Collaborative Writing for the security policies_Pre-assessment_NGHA_GroupB

Policy Evaluation

Thank you for participating in this study.
We are happy to get your feedback. Please read Carefully the following security policy and afterwards fill a short questionnaire. Your answers and thoughts are highly appreciated (Note: your answers will be anonymous).

6.2.3 Privacy and Security

6.2.3.1 Authorization Control

6.2.3.1.1 Before an individual is granted access to the electronic system, a request form will be submitted to the CIMS indicating the following:

6.2.3.1.1.1 Name
6.2.3.1.1.2 Badge number
6.2.3.1.1.3 Pager
6.2.3.1.1.4 Department
6.2.3.1.1.5 Position; and
6.2.3.1.1.6 Signature of the requesting individual and the Department Head

6.2.3.1.2 CIMS will assign a unique user ID for each individual. This ID will be associated with and enable tracking of the user identity on the system.

6.2.3.1.3 CIMS will be responsible for assigning the appropriate level of authorization for each individual according to position and job

responsibilities.

6.2.3.2 Password Management

6.2.3.2.1 The system will automatically generate a random password to the user upon creating an account. The user will be instructed to change the password upon the first login to the system.

6.2.3.2.2 The password will be six (6) or more characters.

6.2.3.2.3 The system will prompt a password change every six (6) months. Otherwise, the password will expire and the user will not be able to login to the system. The user will need to request reactivation of the account.

6.2.3.2.3.1 Physicians will change their password quarterly, i.e. every three (3) months.

6.2.3.2.4 Each individual will be instructed that their password must not be shared, written down or stored in locations where it can be found, and that it will be changed immediately if compromised.

6.2.3.3 Access Control

6.2.3.3.1 System users will be informed about the importance of logging off after finishing data entries or reviewing the patient or employee health record and will be made aware of subsequent security threats that may occur from acce abuse.

6.2.3.3.2 The system will automatically log off after fifteen (15) minutes of inactivity.

6.2.3.4 Audit Control

6.2.3.4.1 The following audit log will be captured on the system. Pertinent reports will be available for the following on request:

6.2.3.4.1.1 User access and account activity

6.2.3.4.1.2 Dormant account reports

6.2.3.4.1.3 Failed login reports

6.2.3.4.1.4 Attempts to guess passwords

6.2.3.4.1.5 Changes to user privileges.

6.2.4 Data Backup. In order to prevent electronic data loss, data backup will be performed on a nightly incremental basis and weekly full-system backup.

6.2.5 Downtime. This is addressed in the relevant Information Systems and Informatics Division (ISID) DPP for computerized physician order entries.

Collaborative Writing for the security policies_Pre-assessment_NGHA_GroupB

Neu_Tech

This section contains 11 questions

* 9. From your perspective, how effective do you think is the above security policy in countering the following claim: "***It is not my fault that the hospital provides complex password management procedures that are inefficient. Thus, I will share my password with a trusted colleague***".

Strongly Ineffective	Ineffective	Somewhat Ineffective	Neither effective nor Ineffective	Somewhat effective	Effective	Strongly effective
○	○	○	○	○	○	○

* 10. From your perspective, How effective do you think is the above security policy in countering the following claim: " **It is OK to share my password with a trusted colleague if I don't understand the policy** ".

Strongly Ineffective	Ineffective	Somewhat Ineffective	Neither effective nor Ineffective	Somewhat effective	Effective	Strongly effective
○	○	○	○	○	○	○

* 11. From your perspective, How effective do you think is the above security policy in countering the following claim: "***No one will get hurt if I share my password with a trusted colleague***".

Strongly Ineffective	Ineffective	Somewhat ineffective	Neither effective nor ineffective	Somewhat effective	Effective	Strongly effective
○	○	○	○	○	○	○

* 12. From your perspective, How effective do you think is the above security policy in countering the following claim: "**It is OK to share my password with a trusted colleague at the hospital if no harm is done.**".

Strongly Ineffective	Ineffective	Somewhat ineffective	Neither effective nor ineffective	Somewhat effective	Effective	Strongly effective
○	○	○	○	○	○	○

* 13. From your perspective, How effective do you think is the above security policy in countering the following claim: "***When I'm less busy, I will change my behaviour. Right now, it is necessary to share my password with a trusted colleague to complete our work faster.***"

Strongly Ineffective	Ineffective	Somewhat ineffective	Neither effective nor ineffective	Somewhat effective	Effective	Strongly effective
○	○	○	○	○	○	○

* 14. From your perspective, How effective do you think is the above security policy in countering the following claim: **"It is all right to share my password with a trusted colleague when I'm under a tight deadline."**

Strongly Ineffective	Ineffective	Somewhat ineffective	Neither effective nor ineffective	Somewhat effective	Effective	Strongly effective
○	○	○	○	○	○	○

* 15. From your perspective, How effective do you think is the above security policy in countering the following claim: **"it is ok to share my password with a trusted colleague because this is what everyone around me at the clinic does "**

Strongly Ineffective	Ineffective	Somewhat ineffective	Neither effective nor ineffective	Somewhat effective	Effective	Strongly effective
○	○	○	○	○	○	○

* 16. From your perspective, How effective do you think is the above security policy in countering the following claim: **"Everybody around me is sharing their passwords with other colleagues. Thus, I will share my password with only a trusted colleague"**

Strongly Ineffective	Ineffective	Somewhat ineffective	Neither effective nor ineffective	Somewhat effective	Effective	Strongly effective
○	○	○	○	○	○	○

* 17. From your perspective, How effective do you think is the above security policy in countering the following claim: ***"I share my password with trusted colleagues to support them in their work"***

Strongly Ineffective	Ineffective	Somewhat ineffective	Neither effective nor ineffective	Somewhat effective	Effective	Strongly effective
○	○	○	○	○	○	○

* 18. From your perspective, How effective do you think is the above security policy in countering the following claim: ***"It is all right to share my password at the clinic if it helps my colleague to get the job done."***

Strongly Ineffective	Ineffective	Somewhat ineffective	Neither effective nor ineffective	Somewhat effective	Effective	Strongly effective
○	○	○	○	○	○	○

* 19. From your perspective, How do you evaluate the overall effectiveness of the above security policy in countering individual's justifications to share their passwords with their trusted colleagues?

Strongly Ineffective	Ineffective	Somewhat ineffective	Neither effective nor ineffective	Somewhat effective	Effective	Strongly effective
○	○	○	○	○	○	○

Collaborative Writing for the security policies_Pre-assessment_NGHA_GroupB

ISP-WS

you will answer 6 questions

* 20. I have the necessary knowledge to fulfil the requirements of the given security policy

Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

* 21. I have the necessary experience to fulfil the requirements of the given security policy

Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

* 22. I have the necessary competencies to fulfil the requirements of the given security policy

Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

* 23. Following the requirements of the given security policy distracts me from doing my actual work or study duties

Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

* 24. Following the requirements of the given security policy slows down my response time to my colleagues.

Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

* 25. Following the requirements of the given security policy hinders my productivity at work or study

Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
○	○	○	○	○	○	○

University of Glasgow | School of Computing Science

University of Glasgow

College of Science & Engineering

School of Computing Science

Statement of Originality

Name: *Saad Nasser AlTamimi*

Registration Number:

I certify that the thesis presented here for examination for my PhD degree of the University of Glasgow is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it) and that the thesis has not been edited by a third party beyond what is permitted by the University's PGR Code of Practice.

I declare that the thesis does not include work forming part of a thesis presented successfully for another degree.

I declare that this thesis has been produced in accordance with the University of Glasgow's Code of Good Practice in Research.

I acknowledge that if any issues are raised regarding good research practice based on reviewo of the thesis, the examination may be postponed pending the outcome of any investigation of the issues.

The work described in this thesis has been published in the following papers:

1. Altamimi, Saad, Karen Renaud, and Timothy Storer. "“I do it because they do it”: social-neutralisation in information security practices of Saudi medical interns." *CRiSIS 2019: 14th International Conference on risks and security of internet and systems*. Springer, 2020.

2. *S. Altamimi, T. Storer and A. Alzahrani, "The role of neutralisation techniques in violating hospitals privacy policies in Saudi Arabia," 2018 4th International Conference on Information Management (ICIM), 2018, pp. 133-140, doi: 10.1109/INFOMAN.2018.8392823.*

The author (**Saad Altamimi**) of this thesis was extensively involved in the publication of all of the above papers which included the following tasks: conceptualisation, methodology, code development, paper writing, literature review, design/development of proposed algorithms and models, review rebuttals and addressing of reviewer comments and data analysis.

Dr.Timothy Storer: Conceptualisation, Review and Supervision.

Dr.Karen Renaud: Methodology and Review.

Signature:

Date: 19/08/2021.

Bibliography

[1] M. T. Siponen and A. Vance, “Neutralization: New insights into the problem of employee information systems security policy violations,” *MIS Q. Manag. Inf. Syst.*, vol. 34, no. SPEC. ISSUE 3, pp. 487–502, 2010, doi: 10.2460/javma.228.4.578.

[2] The U.S.-Saudi Business Council, “Healthcare and Medical Sector : Overview and Commercial Prospects in Saudi Arabia and the United States,” 2017.

[3] World Health Organization, “The World health report : 2000 : Health systems : improving performance,” *World Health*, vol. 78, no. 1, pp. 1–207, 2000, [Online]. Available: http://www.who.int/whr/2000/en/whr00_en.pdf.

[4] F. Abdul Rahim, Z. Ismail, and G. N. Samy, “A Review on Influential Factors of Information Privacy Concerns in the Use of Electronic Medical Records,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 7, pp. 17–27, 2016.

[5] M. J. Culnan and C. C. Williams, “HOW ETHICS CAN ENHANCE ORGANIZATIONAL PRIVACY : LESSONS FROM THE CHOICE POINT,” *MIS Q.*, vol. 33, no. 4, pp. 673–687, 2009.

[6] G. Narayana Samy, R. Ahmad, and Z. Ismail, “Security threats categories in healthcare information systems,” *Health Informatics J.*, vol. 16, no. 3, pp. 201–209, Sep. 2010, doi: 10.1177/1460458210377468.

[7] A. Bensefia and A. Zarrad, “A Proposed Layered Architecture to Maintain Privacy Issues in Electronic Medical Records,” *E-Health Telecommun. Syst. Networks*, vol. 03, no. 04, pp. 43–49, 2014, doi: 10.4236/etsn.2014.34006.

[8] U.S. Department of Health and Human ServicesHHS, “SUMMARY OF THE HIPAA PRIVACY RULE HIPAA Compliance Assistance O C R P R I V A C Y B R I E F SUMMARY OF THE HIPAA PRIVACY RULE,” 2003, Accessed: Mar. 16, 2017. [Online]. Available: https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[9] L. A. Alsulaiman and W. A. Alrodhan, “Information Privacy Status in Saudi Arabia,” *Comput. Inf. Sci.*, vol. 7, no. 3, 2014, doi: 10.5539/cis.v7n3p102.

[10] G. N. Samy, R. Ahmad, and Z. Ismail, *Security threats categories in healthcare information systems*, vol. 16, no. 3. 2010, pp. 201–209.

[11] C. Posey, T. L. Roberts, P. B. Lowry, R. J. Bennett, and J. F. Courtney, “Insiders’ protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors,” *Mis Q.*, pp. 1189–1210, 2013.

[12] M. Silic, J. B. Barlow, and A. Back, “A new perspective on neutralization and deterrence: Predicting shadow IT usage,” *Inf. Manag.*, vol. 54, no. 8, pp. 1023–1037, Dec. 2017, doi: 10.1016/J.IM.2017.02.007.

[13] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness,” *MIS Q. Manag. Inf. Syst.*, vol. 34, no. SPEC. ISSUE 3, pp. 523–548, 2010, doi: 10.2307/25750690.

[14] M. E. Whitman, A. M. Townsend, and R. J. Aalberts, “Information systems security and the need for policy,” in *Information security management: Global challenges in the new millennium*, IGI Global, 2001, pp. 9–18.

[15] M. Choi and J. Song, “Social control through deterrence on the compliance with information security policy,” *Soft Comput.*, vol. 22, no. 20, pp. 6765–6772, 2018.

[16] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2003.

[17] M. Warkentin and R. Willison, “Behavioral and policy issues in information systems security: The insider threat,” *European Journal of Information Systems*, vol. 18, no. 2. pp. 101–105, 2009, doi: 10.1057/ejis.2009.12.

[18] R. Bray and E. Lead, “How to Secure Collaboration from Insider Threats,” *mesaonline.org*, 2019. https://www.mesaonline.org/wp-content/uploads/2019/04/How-to-Secure-Collaboration-from-Insider-Threats-LiveTiles.pdf (accessed Apr. 05, 2021).

[19] ENISA, “ENISA Threat Landscape 2020 - Insider Threat,” *Enisa*, no. April, 2020, [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat.

[20] A. H. Seh *et al.*, “Healthcare Data Breaches: Insights and Implications,” *Healthcare*, vol. 8, no. 2, p. 133, May 2020, doi: 10.3390/healthcare8020133.

[21] Verizon, “2020 Data Breach Investigations Report(DB,” 2020. [Online]. Available: https://enterprise.verizon.com/en-gb/resources/reports/dbir/2020/data-breach-statistics-by-

industry/healthcare-data-breaches-security/.
[22] C. Stokes, “The Electronic Health Revolution: How Health Information Technology Is Changing Medicine-And the Obstacles in Its Way,” *Heal. Law Policy*, vol. 7, pp. 1–30, 2012.
[23] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness,” *MIS Q. Manag. Inf. Syst.*, vol. 34, no. SPEC. ISSUE 3, pp. 523–548, 2010, doi: 10.2307/25750690.
[24] M. A. Alnatheer, “Information Security Culture Critical Success Factors,” in *2015 12th International Conference on Information Technology - New Generations*, Apr. 2015, pp. 731–735, doi: 10.1109/ITNG.2015.124.
[25] M. Chan, I. Woon, and A. Kankanhalli, “Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior,” *J. Inf. Priv. Secur.*, vol. 1, no. 3, pp. 18–41, 2005, doi: 10.1080/15536548.2005.10855772.
[26] S. Goel and I. N. Chengalur-Smith, “Metrics for characterizing the form of security policies,” *J. Strateg. Inf. Syst.*, vol. 19, no. 4, pp. 281–295, Dec. 2010, doi: 10.1016/J.JSIS.2010.10.002.
[27] S. Pahnila, M. Siponen, and A. Mahmood, “Employees’ behavior towards IS security policy compliance,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2007, pp. 156b--156b, doi: 10.1109/HICSS.2007.206.
[28] W. A. Cram, J. G. Proudfoot, and J. D’Arcy, “Organizational information security policies: A review and research framework,” *European Journal of Information Systems*, vol. 26, no. 6. pp. 605–641, 2017, doi: 10.1057/s41303-017-0059-9.
[29] W. A. Cram, J. D’Arcy, and J. G. Proudfoot, “Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance,” *MIS Q.*, vol. 34, no. 2, pp. 525–554, 2019, doi: 10.25300/MISQ/2019/15117.
[30] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis, “Don’t make excuses! Discouraging neutralization to reduce IT policy violation,” *Comput. Secur.*, vol. 39, no. PART B, pp. 145–159, Nov. 2013, doi: 10.1016/j.cose.2013.05.006.
[31] P.-L. Teh, P. K. Ahmed, and J. D’Arcy, “What Drives Information Security Policy Violations among Banking Employees? Insights from Neutralization and Social Exchange Theory,” *J. Glob. Inf. Manag.*, vol. 23, no. 1, pp. 44–64, 2015, doi: 10.4018/jgim.2015010103.
[32] S. H. Kim, K. H. Yang, and S. Park, “An integrative behavioral model of information security policy compliance,” *Sci. World J.*, vol. 2014, p. 463870, 2014, doi: 10.1155/2014/463870.
[33] R. Brewer, S. Fox, and C. Miller, “Applying the Techniques of Neutralization to the Study of Cybercrime,” in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Springer International Publishing, 2019, pp. 1–19.
[34] G. M. Sykes and D. Matza, “Techniques of Neutralization: A Theory of Delinquency,” *Source Am. Sociol. Rev.*, vol. 22, no. 6, pp. 664–670, 1957, Accessed: Nov. 09, 2017. [Online]. Available: http://www.jstor.org/stable/2089195.
[35] J. W. Rogers and M. D. Buffalo, “Neutralization techniques: Toward a simplified measurement scale,” *Sociol. Perspect.*, vol. 17, no. 3, pp. 313–331, 1974, doi: 10.2307/1388569.
[36] D. Chappell, “Book Reviews : The Professional Fence, Carl B. Klockars. Pp. 242. New York, Free Press, 1974.,” *Crime Delinq.*, vol. 21, no. 4, pp. 380–383, Oct. 1975, doi: 10.1177/001112877502100414.
[37] W. W. Minor, “Techniques of Neutralization: A Reconceptualization and Empirical Examination,” *J. Res. Crime Delinq.*, vol. 18, no. 2, pp. 295–318, Jul. 1981, doi: 10.1177/002242788101800206.
[38] J. W. Coleman, *The criminal elite: The sociology of white collar crime*. Macmillan, 2001.
[39] P. Cromwell and Q. Thurman, “the devil made me do it: use of neutralizations by shoplifters,” *Deviant Behav.*, vol. 24, no. 6, pp. 535–550, Nov. 2003, doi: 10.1080/713840271.
[40] R. Willison and M. Warkentin, “BEYOND DETERRENCE: AN EXPANDED VIEW OF EMPLOYEE COMPUTER ABUSE 1,” Accessed: Apr. 28, 2017. [Online]. Available: https://pdfs.semanticscholar.org/04ac/6e2357ee3a45272199d6cc65fa3762490324.pdf.
[41] ISO/IEC29100, “ISO/IEC 29100:2011(en), Information technology — Security techniques — Privacy framework.” https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en (accessed Mar. 27, 2017).
[42] J. D’Arcy and P. B. Lowry, “Cognitive-affective drivers of employees’ daily compliance with information security policies: A multilevel, longitudinal study,” *Inf. Syst. J.*, vol. 29, no. 1, pp. 43–69, Nov. 2019, doi: 10.1111/isj.12173.
[43] L. C. Harris and A. Dumas, “Online consumer misbehaviour: An application of neutralization

theory," *Mark. Theory*, vol. 9, no. 4, pp. 379–402, 2009, doi: 10.1177/1470593109346895.
[44] D. Dang-Pham and S. Pittayachawan, "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach," *Comput. Secur.*, vol. 48, pp. 281–297, 2015, doi: https://doi.org/10.1016/j.cose.2014.11.002.
[45] H. Arksey and L. O'Malley, "Scoping studies: Towards a methodological framework," *Int. J. Soc. Res. Methodol. Theory Pract.*, vol. 8, no. 1, pp. 19–32, 2005, doi: 10.1080/1364557032000119616.
[46] H. L. Colquhoun *et al.*, "Scoping reviews: Time for clarity in definition, methods, and reporting," *J. Clin. Epidemiol.*, vol. 67, no. 12, pp. 1291–1294, 2014, doi: 10.1016/j.jclinepi.2014.03.013.
[47] D. Levac, H. Colquhoun, and K. K. O'Brien, "Scoping studies: Advancing the methodology," *Implement. Sci.*, vol. 5, no. 1, 2010, doi: 10.1186/1748-5908-5-69.
[48] D. Gough, J. Thomas, and S. Oliver, "Clarifying differences between review designs and methods," *Syst. Rev.*, vol. 1, no. 1, pp. 1–9, 2012.
[49] T. U. S. D. of H. and H. Services HHS., "SUMMARY OF THE HIPAA PRIVACY RULE HIPAA Compliance Assistance O C R P R I V A C Y B R I E F SUMMARY OF THE HIPAA PRIVACY RULE." Accessed: Mar. 20, 2017. [Online]. Available: https://www.hhs.gov/sites/default/files/privacysummary.pdf.
[50] International Organization for Standardization(ISO), "Health informatics - Information security management in health using ISO/IEC 27002," 2016. Accessed: Mar. 10, 2017. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:27799:ed-2:v1:en.
[51] F. Y. Pai and K. I. Huang, "Applying the Technology Acceptance Model to the introduction of healthcare information systems," *Technol. Forecast. Soc. Change*, vol. 78, no. 4, pp. 650–660, 2011, doi: 10.1016/j.techfore.2010.11.007.
[52] F. Akowuah, X. Yuan, J. Xu, and H. Wang, "A survey of security standards applicable to health information systems," *Int. J. Inf. Secur. Priv.*, vol. 7, no. 4, pp. 22–36, 2013, doi: 10.4018/ijisp.2013100103.
[53] M. Care, "Annals of Internal Medicine Improving Patient Care Systematic Review : Impact of Health Information Technology on," *Most*, vol. 144, pp. 742–752, 2006, doi: 0000605-200605160-00125 [pii].
[54] F. A. Rahim, Z. Ismail, and G. N. Samy, "A Review on Influential Factors of Information Privacy Concerns in the Use of Electronic Medical Records," *IJCSIS) Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 7, 2016, Accessed: Mar. 09, 2017. [Online]. Available: http://search.proquest.com/docview/1815514566/fulltextPDF/CA216B5E5BD1429EPQ/1?accountid=142908.
[55] World Health Organization, "Global diffusion of eHealth: Making universal health coverage achievable.," 2016. [Online]. Available: http://who.int/goe/publications/global_diffusion/en/.
[56] J. J. Yang *et al.*, "Emerging information technologies for enhanced healthcare," *Comput. Ind.*, vol. 69, pp. 3–11, 2015, doi: 10.1016/j.compind.2015.01.012.
[57] P. Kierkegaard, "Electronic health record: Wiring Europe's healthcare," *Comput. Law Secur. Rev.*, vol. 27, no. 5, pp. 503–515, Sep. 2011, doi: 10.1016/j.clsr.2011.07.013.
[58] E. Deutsch, G. Duftschmid, and W. Dorda, "Critical areas of national electronic health record programs. Is our focus correct?," *Int. J. Med. Inform.*, vol. 79, pp. 211–222, 2010, doi: 10.1016/j.ijmedinf.2009.12.002.
[59] U.S. Department of Health and Human Services, "What is the difference between a Personal Health Record, an Electronic Health Record, and an Electronic Medical Record?," 2015. https://www.healthit.gov/providers-professionals/faqs/what-are-differences-between-electronic-medical-records-electronic (accessed Mar. 17, 2017).
[60] WHO, "The World Health Report 2008: Primary Health Care: Now More Than Ever," World Health Organization, 2008. Accessed: Mar. 13, 2017. [Online]. Available: http://www.who.int/whr/2008/en/.
[61] U.S. Department of Health & Human Services and O. for C. Rights, *OFFICE RIGHTS FOR CIVIL Privacy, Security, and Electronic Health Records 1 PRIVACY, SECURITY, AND ELECTRONIC HEALTH RECORDS. .*
[62] M. Choi, "Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing," 2016, doi: 10.3390/su8070638.
[63] S. Posthumus and R. Von Solms, "A framework for the governance of information security," *Comput. Secur.*, vol. 23, no. 8, pp. 638–646, 2004, doi: 10.1016/j.cose.2004.10.006.
[64] British Standards Institute BSI, "ISO27000:2016 BSI Standards Publication Information

technology — Security techniques — Information security management systems — Overview and vocabulary," 2016.

[65] R. Kissel, "Glossary of Key Information Security Terms Glossary of Key Information Security Terms," *Nist*, vol. NISTIR 729, no. Revision 2, 2013, doi: 10.6028/NIST.IR.7298r2.

[66] H. Zafar and J. G. Clark, "Current state of information security research in IS," *Commun. Assoc. Inf. Syst.*, vol. 24, no. 1, pp. 557–596, 2009, doi: 10.17705/1cais.02434.

[67] C. P. Pfleeger, S. L. Pfleeger, and J. Margulies, *Security in Computing*, 5th ed. Pearson Education India, 2009.

[68] The British Standards Institution, "ISO 27000 - Information technology — Security techniques — Information security management systems — Overview and vocabulary," 2020.

[69] ENISA, "Risk Management : Implementation principles and Inventories for Risk Management / Risk Assessment methods and tools," 2006. [Online]. Available: https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/files/deliverables/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools.

[70] C. Papoutsi, J. E. Reed, C. Marston, R. Lewis, A. Majeed, and D. Bell, "Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study.," *BMC Med. Inform. Decis. Mak.*, vol. 15, p. 86, 2015, doi: 10.1186/s12911-015-0202-2.

[71] C. L. Hsu, M. R. Lee, and C. H. Su, "The role of privacy protection in healthcare information systems adoption," *J. Med. Syst.*, vol. 37, no. 5, p. 9966, Oct. 2013, doi: 10.1007/s10916-013-9966-z.

[72] J. H. P. Eloff and M. Eloff, "Information security management: a new paradigm," in *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*, 2003, pp. 130–136, [Online]. Available: http://dl.acm.org/citation.cfm?id=954014.954028.

[73] G. I. Burke and D. G. Jarratt, "The influence of information and advice on competitive strategy definition in small-and medium-sized enterprises," *Qual. Mark. Res. An Int. J.*, 2004.

[74] W. E. Deming, *Out of the Crisis*. MIT press, 2018.

[75] ENISA, "The ISMS Framework," *Enisa.europa.eu*, 2013. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/framework (accessed Feb. 10, 2019).

[76] K. P. Andriole, "Security of electronic medical information and patient privacy: What you need to know," *J. Am. Coll. Radiol.*, vol. 11, no. 12, pp. 1212–1216, 2014, doi: 10.1016/j.jacr.2014.09.011.

[77] A. Mahfuth, J. Singh Dhillon, and S. Mohd Drus, "a Systematic Review on Data Security and Patient Privacy Issues in Electronic Medical Records," *J. Theor. Appl. Inf. Technol.*, vol. 3190, no. 2, pp. 106–116, 2016, Accessed: Mar. 09, 2017. [Online]. Available: www.jatit.org.

[78] E. H. Park, J. Kim, and Y. S. Park, "The role of information security learning and individual factors in disclosing patients' health information," *Comput. Secur.*, vol. 65, pp. 64–76, 2017, doi: http://dx.doi.org/10.1016/j.cose.2016.10.011.

[79] R. Ayyagari and N. Figueroa, "Is seeing believing? Training users on Information Security: Evidence from Java applets," *J. Inf. Syst. Educ.*, vol. 28, no. 2, pp. 115–120, 2017.

[80] Y. Lee and K. R. Larsen, "Threat or coping appraisal: Determinants of SMB executives′ decision to adopt anti-malware software," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 177–187, 2009, doi: 10.1057/ejis.2009.11.

[81] P. B. Lowry, R. E. Crossler, A. C. Johnston, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *Comput. Secur.*, vol. 32, no. JUNE, pp. 90–101, 2013, doi: 10.1016/j.cose.2012.09.010.

[82] British Standards Institute BSI, "Information technology – Security techniques Information security management systems – Overview and vocabulary ISO/IEC 27000:2020," no. March 2020, 2020.

[83] K. Höne and J. H. P. Eloff, "What makes an effective information security policy?," *Network Security*, vol. 2002, no. 6. Elsevier Advanced Technology, pp. 14–16, Jun. 01, 2002, doi: 10.1016/S1353-4858(02)06011-7.

[84] National Institute of Standards and Technology, "Security and privacy controls for federal information systems and organizations," *NIST Spec. Publ. 800-53 V5*, vol. 800, p. 53, 2013.

[85] H. Paananen, M. Lapke, and M. Siponen, "State of the art in information security policy

development," *Computers and Security*, vol. 88. Elsevier BV, p. 101608, Jan. 2020, doi: 10.1016/j.cose.2019.101608.

[86] A. Klaić, "Overview of the state and trends in the contemporary information security policy and information security management methodologies," *MIPRO 2010 - 33rd Int. Conv. Inf. Commun. Technol. Electron. Microelectron. Proc.*, pp. 1203–1208, 2010.

[87] E. Yeniman Yildirim, G. Akalp, S. Aytac, and N. Bayram, "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey," *Int. J. Inf. Manage.*, vol. 31, no. 4, pp. 360–365, 2011, doi: 10.1016/j.ijinfomgt.2010.10.006.

[88] N. F. Doherty, L. Anastasakis, and H. Fulford, "The information security policy unpacked: A critical study of the content of university policies," *Int. J. Inf. Manage.*, vol. 29, no. 6, pp. 449–457, 2009, doi: 10.1016/j.ijinfomgt.2009.05.003.

[89] P. Ward and C. L. Smith, "The development of access control policies for information technology systems," *Comput. Secur.*, vol. 21, no. 4, pp. 356–371, 2002, doi: 10.1016/S0167-4048(02)00414-5.

[90] R. Baskerville and M. Siponen, "An information security meta-policy for emergent organizations," *Logist. Inf. Manag.*, vol. 15, no. 5/6, pp. 337–346, 2002, doi: 10.1108/09576050210447019.

[91] J. Rees, S. Bandyopadhyay, and E. H. Spafford, "PFIRES: A policy framework for information security," *Commun. ACM*, vol. 46, no. 7, pp. 101–106, 2003.

[92] S. V. Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who," *Comput. Secur.*, vol. 61, pp. 169–183, 2016, doi: 10.1016/j.cose.2016.06.002.

[93] British Standards Institute BSI, "Information Technology Security Techniques. Code of Practice for Information Security Management," 2000, [Online]. Available: http://www.sabs.co.za/content/uploads/files/SANS21827(colour).pdf.

[94] K. J. Knapp, R. Franklin Morris, T. E. Marshall, and T. A. Byrd, "Information security policy: An organizational-level process model," *Comput. Secur.*, vol. 28, no. 7, pp. 493–508, 2009, doi: 10.1016/j.cose.2009.07.001.

[95] M. A. Al-Awadi, "A study of Employees' Attitudes Towards Organisational Information Security Policies in the UK and Oman," University of Glasgow, 2009.

[96] B. K. Kahn, D. M. Strong, and R. Y. Wang, "Information Quality Benchmarks: Product and Service Performance," *Commun. ACM*, vol. 45, no. 4, pp. 184–192, 2002, doi: 10.1145/505248.506007.

[97] Y. Huh, F. Keller, T. Redman, and A. Watkins, "Data quality," *Inf. Softw. Technol.*, vol. 32, no. 8, pp. 559--565, 1990, doi: 10.1016/0950-5849(90)90146-I.

[98] R. R. Nelson, P. A. Todd, and B. H. Wixom, "Antecedents of information and system quality: An empirical examination within the context of data warehousing," *J. Manag. Inf. Syst.*, vol. 21, no. 4, pp. 199–235, 2005, doi: 10.1080/07421222.2005.11045823.

[99] J. Miller and B. A. Doyle, "Measuring the effectiveness of computer-based information systems in the financial services sector," *MIS Q.*, pp. 107–124, 1987.

[100] W. X. and G. T. William J. Doll, "A confirmatory factor analysis of the EUCS Instrument," *MIS Q.*, vol. 18, no. 4, pp. 453–461, 1994.

[101] I. Kirlappos, S. Parkin, and M. A. Sasse, "'Shadow security' as a tool for the learning organization," *ACM SIGCAS Comput. Soc.*, vol. 45, no. 1, pp. 29–37, 2015, doi: 10.1145/2738210.2738216.

[102] M. Bada, A. Sasse, and J. Bada, M., Sasse, A., Nurse, "Cyber Security Awareness Campaigns: Why They Fail to Change Behavior," *Int. Conf. Cyber Secur. Sustain. Soc.*, p. 11, 2014, Accessed: Jun. 13, 2019. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf.

[103] A. Adams and M. A. Sasse, "Users Are Not The Enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, 1999, doi: 10.1145/322796.322806.

[104] Society for Information Management (U.S.), University of Minnesota. Management Information Systems Research Center., Society for Management Information Systems (U.S.), and Association for Information Systems., *MIS quarterly : management information systems.* Society for Management Information Systems, 1977.

[105] G. D. Moody, M. Siponen, and S. Pahnila, "Toward a unified model of information security policy compliance," *MIS Q. Manag. Inf. Syst.*, vol. 42, no. 1, pp. 285–311, 2018, doi: 10.25300/MISQ/2018/13853.

[106] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors,"

Comput. Secur., vol. 24, no. 2, pp. 124–133, 2005, doi: 10.1016/j.cose.2004.07.001.
[107] "Verizon 2020 Data Breach Investigation Report (DBIR)," *Verizon*, pp. 1–119, 2020, Accessed: Jul. 10, 2019. [Online]. Available: https://enterprise.verizon.com/resources/reports/2020/2020-data-breach-investigations-report.pdf.
[108] "Protecting Patients, Providers and Payers 2019 Healthcare Threat Report," 2019. [Online]. Available: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-2019-healthcare-threat-report.pdf.
[109] K. Padayachee, "An assessment of opportunity-reducing techniques in information security: An insider threat perspective," *Decis. Support Syst.*, vol. 92, pp. 47–56, Dec. 2016, doi: 10.1016/j.dss.2016.09.012.
[110] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Inf. Manag.*, vol. 51, no. 1, pp. 69–79, Jan. 2014, doi: 10.1016/j.im.2013.10.001.
[111] P. Ifinedo, "Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines?," *Inf. Syst. Manag.*, vol. 33, no. 1, pp. 30–41, 2016, doi: 10.1080/10580530.2015.1117868.
[112] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis, "Don't even think about it! the effects of antineutralization, informational, and normative communication on information security compliance," *J. Assoc. Inf. Syst.*, vol. 19, no. 8, pp. 689–715, 2018, doi: 10.17705/1jais.00506.
[113] M. Durgin, "Understanding the importance of and implementing snternal security measures," *SANS Institue: InfoSec Reading Room*, pp. 1–16, 2007.
[114] Ponemon Institute, "Cost of a data breach report," 2019. [Online]. Available: https://www.ibm.com/downloads/cas/ZBZLY7KL.
[115] Verizon, "2019 Data Breach Investigations Report," 2019. doi: 10.1016/s1361-3723(19)30060-0.
[116] T. Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 106–125, 2009, doi: 10.1057/ejis.2009.6.
[117] K. Njenga, "Information Systems Security Policy Violation : Systematic Literature Review on Behavior Threats by Internal Agents," *CONF-IRM 2016 Proc.*, no. May, pp. 1–13, 2016.
[118] C. S. G. Khoo, J. C. Na, and K. Jaidka, "Analysis of the macro-level discourse structure of literature reviews," *Online Inf. Rev.*, vol. 35, no. 2, pp. 255–271, 2011, doi: 10.1108/14684521111128032.
[119] R. Parks, C. H. Chu, and H. Xu, "Healthcare information privacy research: Issues, gaps and what next?," in *17th Americas Conference on Information Systems 2011, AMCIS 2011*, 2011, vol. 2, pp. 1589–1604, Accessed: Sep. 05, 2017. [Online]. Available: http://aisel.aisnet.org/amcis2011_submissions.
[120] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *Comput. Secur.*, vol. 32, pp. 90–101, 2013, doi: 10.1016/j.cose.2012.09.010.
[121] K. D. Loch, H. H. Carr, and M. E. Warkentin, "Systems : Reality , Today ' s Yesterday ' s Understanding," *MIS Q.*, vol. 16, no. 2, pp. 173–186, 1992.
[122] R. Willison and M. Warkentin, "Beyond deterrence: An expanded view of employee computer abuse," *MIS Q.*, vol. 37, no. 1, pp. 1–20, 2013, doi: 10.1080/01639625.2012.759048.
[123] S. Aurigemma and T. Mattson, "Do it OR ELSE! exploring the effectiveness of deterrence on employee compliance with information security policies," 2014.
[124] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *J. Manag. Inf. Syst.*, vol. 28, no. 2, pp. 203–236, 2011, doi: 10.2753/MIS0742-1222280208.
[125] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis, "Don't make excuses! Discouraging neutralization to reduce IT policy violation," *Comput. Secur.*, vol. 39, no. PART B, pp. 145–159, 2013, doi: 10.1016/j.cose.2013.05.006.
[126] D. P. T. Dang, "Predicting insider's malicious security behaviours: a General Strain Theory-based conceptual model," *2014 Int. Conf. Inf. Resour. Manag. (Conf-IRM 2014)*, no. May 2014, 2014.
[127] S. Kraemer and P. Carayon, "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists," *Appl. Ergon.*, vol. 38, no. 2, pp. 143–154, 2007, doi: 10.1016/j.apergo.2006.03.010.
[128] M. Warkentin and R. Willison, "Behavioral and policy issues in information systems security: the insider threat," *Eur. J. Inf. Syst.*, vol. 18, no. 18, pp. 101–105, 2009, doi: 10.1057/ejis.2009.12.

[129] M. Siponen and A. Vance, “Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations,” *European Journal of Information Systems*, vol. 23, no. 3. pp. 289–305, 2014, doi: 10.1057/ejis.2012.59.

[130] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, “Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory,” *Comput. Secur.*, vol. 39, no. PART B, pp. 447–459, Nov. 2013, doi: 10.1016/j.cose.2013.09.009.

[131] M. Maasberg, “Insider espionage: Recognizing ritualistic behavior by abstracting technical indicators from past cases,” *20th Am. Conf. Inf. Syst. AMCIS 2014*, no. October, 2014.

[132] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, “Prevention is better than cure! Designing information security awareness programs to overcome users’ non-compliance with information security policies in banks,” *Comput. Secur.*, vol. 68, pp. 145–159, 2017, doi: 10.1016/j.cose.2017.04.009.

[133] A. Hovav and J. D’Arcy, “Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea,” *Inf. Manag.*, vol. 49, no. 2, pp. 99–110, Mar. 2012, doi: 10.1016/j.im.2011.12.005.

[134] J. D’Arcy and A. Hovav, “Deterring internal information systems misuse,” *Commun. ACM*, vol. 50, no. 10, pp. 113–117, Oct. 2007, doi: 10.1145/1290958.1290971.

[135] P. Menard, G. J. Bott, and R. E. Crossler, “User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory,” *J. Manag. Inf. Syst.*, vol. 34, no. 4, pp. 1203–1230, 2017, doi: 10.1080/07421222.2017.1394083.

[136] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, “What Do Systems Users Have to Fear? Using Fear Appeals To Engender Threats and Fear that Motivate Protective Security Behaviours,” *MIS Q.*, vol. 39, no. 4, pp. 837–864, 2015, doi: 10.25300/MISQ/2015/39.4.5.

[137] N. S. Safa, C. Maple, T. Watson, and R. Von Solms, “Motivation and opportunity based model to reduce information security insider threats in organisations,” *J. Inf. Secur. Appl.*, vol. 40, pp. 247–257, Jun. 2018, doi: 10.1016/j.jisa.2017.11.001.

[138] I. Ajzen, “The Theory of Planned Behavior,” *Organ. Behav. Hum. Decis. Process.*, vol. 50, pp. 179–211, 1991, Accessed: Apr. 16, 2017. [Online]. Available: http://ac.els-cdn.com/074959789190020T/1-s2.0-074959789190020T-main.pdf?_tid=ff7daa44-22c9-11e7-abfd-00000aacb361&acdnat=1492363843_82a0618cd1485e8f5c92fc88294aefaf.

[139] J. Hwang, H. Lee, K. Kim, H. Zo, and A. P. Ciganek, “Cyber neutralisation and flaming,” *Behav. Inf. Technol.*, vol. 35, no. 3, pp. 210–224, 2016, doi: 10.1080/0144929X.2015.1135191.

[140] D. E. Montaño and K. Danuta, “Theory of reasoned action, theory of planned behavior, and the integrated behavioral model,” *Heal. Behav. Theory, Res. Pract.*, vol. 7, no. 4, p. 231, 2015, doi: 10.7326/0003-4819-116-4-350_1.

[141] I. Ajzen and M. Fishbein, “Attitude-behavior relations: A theoretical analysis and review of empirical research.,” *Psychol. Bull.*, vol. 84, no. 5, p. 888, 1977, doi: 10.1007/s11614-012-0060-4.

[142] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness1,” *Source MIS Q.*, vol. 34209244, no. 3, pp. 523–548, 2010, Accessed: Aug. 07, 2017. [Online]. Available: http://www.jstor.org/stable/25750690.

[143] M. Foth, “Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence,” *Eur. J. Inf. Syst.*, vol. 25, no. 2, pp. 91–109, 2016, doi: 10.1057/ejis.2015.9.

[144] Q. Hu, T. Dinev, P. Hart, and D. Cooke, “Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture,” *Decis. Sci.*, vol. 43, no. 4, pp. 615–660, 2012, doi: 10.1111/j.1540-5915.2012.00361.x.

[145] P. Ifinedo, “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory,” in *Computers and Security*, 2012, vol. 31, no. 1, pp. 83–95, doi: 10.1016/j.cose.2011.10.007.

[146] Y. A. N. Chen, K. R. A. M. Ramamurthy, and K. Wen, “Impacts od Comprehensive Information Security Programs on Information Security Culture,” *J. Comput. Inf. Syst.*, vol. 55, no. 3, p. 11, 2015, doi: 10.1080/08874417.2015.11645767.

[147] J. P. GIBBS, “Crime , Punishment , and Deterrence,” *Southwest. Soc. Sci. Q.*, vol. 48, no. 4, pp. 515–530, 1968.

[148] R. Willison, M. Warkentin, and A. C. Johnston, “Examining employee computer abuse intentions:

insights from justice, deterrence and neutralization perspectives," *Inf. Syst. J.*, vol. 28, no. 2, pp. 266–293, 2018, doi: 10.1111/isj.12129.
[149] D. W. Straub, "Effective IS security: An empirical study," *Inf. Syst. Res.*, vol. 1, no. 3, pp. 255–276, 1990, doi: 10.1287/isre.1.3.255.
[150] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, 2009, doi: 10.1287/isre.1070.0160.
[151] M. Silic, J. B. Barlow, and A. Back, "A new perspective on neutralization and deterrence: Predicting shadow IT usage," *Inf. Manag.*, vol. 54, no. 8, pp. 1023–1037, 2017, doi: 10.1016/j.im.2017.02.007.
[152] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, 2009, doi: 10.1016/j.dss.2009.02.005.
[153] Y. Chen, K. Ramamurthy, and K.-W. Wen, "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *J. Manag. Inf. Syst.*, vol. 29, no. 3, pp. 157–188, 2012, doi: 10.2753/MIS0742-1222290305.
[154] A. Bandura and D. C. McClelland, *Social learning theory*, vol. 1. Englewood cliffs Prentice Hall, 1977.
[155] I. Hwang, R. Wakefield, S. Kim, and T. Kim, "Security Awareness: The First Step in Information Security Compliance Behavior," *J. Comput. Inf. Syst.*, vol. 0, no. 00, pp. 1–12, 2019, doi: 10.1080/08874417.2019.1650676.
[156] S. McLeod, "Bandura - social learning theory," *Simply Psychology*, 2016. https://www.simplypsychology.org/bandura.html (accessed Sep. 25, 2019).
[157] T. J. Holt, G. W. Burruss, and A. M. Bossler, "Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world," *J. Crime Justice*, vol. 33, no. 2, pp. 31–61, 2010, doi: 10.1080/0735648X.2010.9721287.
[158] M. Warkentin, A. C. Johnston, and J. Shropshire, "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *Eur. J. Inf. Syst.*, vol. 20, no. 3, pp. 267–284, May 2011, doi: 10.1057/ejis.2010.72.
[159] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Comput. Human Behav.*, vol. 24, no. 6, pp. 2799–2816, 2008, doi: 10.1016/j.chb.2008.04.005.
[160] B. Albert, "Social foundations of thought and action: A social cognitive theory," *NY Prentice-hall*, 1986.
[161] B. Y. Ng, A. Kankanhalli, and Y. (Calvin) Xu, "Studying users' computer security behavior: A health belief perspective," *Decis. Support Syst.*, vol. 46, no. 4, pp. 815–825, 2009, doi: 10.1016/j.dss.2008.11.010.
[162] H. S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Comput. Secur.*, vol. 28, no. 8, pp. 816–826, 2009, doi: 10.1016/j.cose.2009.05.008.
[163] A. Gurung, X. Luo, and Q. Liao, "Consumer motivations in taking action against spyware: an empirical investigation," *Inf. Manag. Comput. Secur.*, vol. 17, no. 3, pp. 276–289, 2009, doi: 10.1108/09685220910978112.
[164] B. James W, "Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2011, vol. 71, no. 7, p. 4483, doi: 10.1109/HICSS.2011.368.
[165] A. C. Johnston and M. Warkentin, "Information privacy compliance in the healthcare industry," *Inf. Manag. Comput. Secur.*, vol. 16, no. 1, pp. 5–19, 2008, doi: 10.1108/09685220810862715.
[166] E. H. Sutherland, "Principles of Criminology, revised by DR Cressey," *DR, Chicago*, 1955.
[167] A. Heckert and D. M. Heckert, "A new typology of deviance: Integrating normative and reactivist definitions of deviance," *Deviant Behav.*, vol. 23, no. 5, pp. 449–479, 2002.
[168] H. Copes, "Societal attachments, offending frequency, and techniques of neutralization," *Deviant Behav.*, vol. 24, no. 2, pp. 101–127, 2003.
[169] S. Zamoon, "Software Piracy: Neutralization Techniques that Circumvent Ethical Decision-Making," no. July, pp. 1–177, 2006, doi: 10.3102/00346543067001043.
[170] K. Keenan, "Rationalizing Professional Misconduct : An Examination of Techniques of Neutralization in Lawyer Discipline Proceedings by," 2019.

[171] M. J. Hindelang, “The commitment of delinquents to their misdeeds: do delinquents drift?,” *Soc. Probl.*, vol. 17, no. 4, pp. 502–509, 1970.
[172] P. Cromwell and Q. Thurman, “The devil made me do it: Use of neutralizations by shoplifters,” *Deviant Behav.*, vol. 24, no. 6, pp. 535–550, 2003, doi: 10.1080/713840271.
[173] S. Henry and R. Eaton, *Degrees of Deviance:Student accounts of their deviant behavior*. Gower Publishing Company Ltd, Hants, 1989.
[174] B. Byers, B. W. Crider, and G. K. Biggers, “Bias Crime Motivation: A study of hate crime and offender neutralization techniques used against the Amish,” *J. Contemp. Crim. Justice*, 1999, doi: 10.1177/1043986299015001006.
[175] H. Copes, “Streetlife and the rewards of auto theft,” *Deviant Behav.*, vol. 24, no. 4, pp. 309–332, 2003, doi: 10.1080/713840224.
[176] N. L. Piquero, S. G. Tibbetts, and M. B. Blankenship, “Examining the role of differential association and techniques of neutralization in explaining corporate crime,” *Deviant Behavior*, vol. 26, no. 2. pp. 159–188, 2005, doi: 10.1080/01639620590881930.
[177] A. Gannett and C. Rector, “The Rationalization of Political Corruption,” *Public Integr.*, vol. 17, no. 2, pp. 165–175, 2015, doi: 10.1080/10999922.2015.1000654.
[178] R. D. Evans and C. J. Forsyth, “Dogmen: The Rationalization of Deviance,” *Soc. Anim.*, vol. 6, no. 3, pp. 203–218, Jan. 1998, doi: 10.1163/156853098X00159.
[179] A. Bandura, “The role of selective moral disengagement in terrorism and counterterrorism.,” 2004.
[180] M. Siponen, A. Vance, and R. Willison, “New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs,” *Inf. Manag.*, vol. 49, no. 7–8, pp. 334–341, 2012, doi: 10.1016/j.im.2012.06.004.
[181] R. G. Morris and G. E. Higgins, “Neutralizing potential and self-reported digital piracy: A multitheoretical exploration among college undergraduates,” *Crim. Justice Rev.*, vol. 34, no. 2, pp. 173–195, 2009, doi: 10.1177/0734016808325034.
[182] J. R. Ingram and S. Hinduja, “Neutralizing Music Piracy: An Empirical Examination,” *Deviant Behav.*, vol. 29, no. 4, pp. 334–366, 2008, doi: 10.1080/01639620701588131.
[183] Y. T. Chua and T. J. Holt, “A Cross-National Examination of the Techniques of Neutralization to Account for Hacking Behaviors,” *Vict. Offenders*, vol. 11, no. 4, pp. 534–555, 2016, doi: 10.1080/15564886.2015.1121944.
[184] S. Hinduja, “Neutralization theory and online software piracy: An empirical analysis,” *Ethics Inf. Technol.*, vol. 9, no. 3, pp. 187–204, Nov. 2007, doi: 10.1007/s10676-007-9143-5.
[185] A. Vance, M. T. Siponen, and D. W. Straub, “Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures,” *Inf. Manag.*, vol. 57, no. 4, Jun. 2020, doi: 10.1016/j.im.2019.103212.
[186] G. Hofstede, “Dimensionalizing Cultures: The Hofstede Model in Context,” *Online Readings Psychol. Cult.*, vol. 2, no. 1, pp. 1–26, 2011, doi: 10.9707/2307-0919.1014.
[187] S. H. Kim, K. H. Yang, and S. Park, “An integrative behavioral model of information security policy compliance,” *Sci. World J.*, vol. 2014, 2014, doi: 10.1155/2014/463870.
[188] M. Siponen, P. Puhakainen, and A. Vance, “Can individuals’ neutralization techniques be overcome? A field experiment on password policy,” *Comput. Secur.*, vol. 88, p. 101617, Sep. 2020, doi: 10.1016/j.cose.2019.101617.
[189] M. T. Siponen, “A conceptual foundation for organizational information security awareness A conceptual foundation for organizational information security awareness,” 2006.
[190] R. Baskerville, P. Spagnoletti, and J. Kim, “Incident-centered information security: Managing a strategic balance between prevention and response,” *Inf. Manag.*, vol. 51, no. 1, pp. 138–151, 2014, doi: 10.1016/j.im.2013.11.004.
[191] A. Tsohou, M. Karyda, S. Kokolakis, and E. Kiountouzis, “Managing the introduction of information security awareness programmes in organisations,” *Eur. J. Inf. Syst.*, vol. 24, no. 1, pp. 38–58, 2015.
[192] M. Siponen, P. Puhakainen, and A. Vance, “Can individuals’ neutralization techniques be overcome? A field experiment on password policy,” *Comput. Secur.*, vol. 88, 2020, doi: 10.1016/j.cose.2019.101617.
[193] H. Tobi and J. K. Kampen, “Research design: the methodology for interdisciplinary research framework,” *Qual. Quant.*, vol. 52, no. 3, 2018, doi: 10.1007/s11135-017-0513-8.
[194] V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, 2006, doi: 10.1191/1478088706qp063oa.

[195] K. Krippendorff, “Emerging trends in content analysis,” *Int. Encycl. Commun.*, vol. 1, pp. 401–407, 1989, [Online]. Available: http://repository.upenn.edu/asc_papers/226.
[196] R. B. Johnson and A. J. Onwuegbuzie, “Toward a Definition of Mixed Methods Research,” *J. Mix. Methods Res.*, vol. 1, no. 2, pp. 112–133, 2007, doi: 10.1177/1558689806298224.
[197] M. J. Zyphur and D. C. Pierides, “Is Quantitative Research Ethical? Tools for Ethically Practicing, Evaluating, and Using Quantitative Research,” *J. Bus. Ethics*, vol. 143, no. 1, Jun. 2017, doi: 10.1007/s10551-017-3549-8.
[198] K. Howe and M. Eisenhart, “Standards for Qualitative (and Quantitative) Research: A Prolegomenon,” *Educ. Res.*, vol. 19, no. 4, May 1990, doi: 10.3102/0013189X019004002.
[199] M. Jokela, “Urban–Rural Residential Mobility Associated With Political Party Affiliation: The U.S. National Longitudinal Surveys of Youth and Young Adults,” *Soc. Psychol. Personal. Sci.*, Feb. 2021, doi: 10.1177/1948550621994000.
[200] H. Vance, “Nudge Communication: A Causal-Comparative Study of Interventions that Impact Persistence of Higher Education Students,” Liberty University, 2021.
[201] A. P. Rovai, J. D. Baker, and M. K. Ponton, *Social science research design and statistics: A practitioner’s guide to research methods and IBM SPSS*. Watertree Press LLC, 2013.
[202] J. R. Blakeslee, “Effects of high-fidelity simulation on the critical thinking skills of baccalaureate nursing students: A causal-comparative research study,” *Nurse Educ. Today*, vol. 92, p. 104494, Sep. 2020, doi: 10.1016/j.nedt.2020.104494.
[203] R. Libby, R. Bloomfield, and M. W. Nelson, “Experimental research in financial accounting,” *Accounting, Organ. Soc.*, vol. 27, no. 8, pp. 775–810, 2002, doi: 10.1016/S0361-3682(01)00011-3.
[204] P. Aspers and U. Corte, “What is Qualitative in Qualitative Research,” *Qual. Sociol.*, vol. 42, no. 2, Jun. 2019, doi: 10.1007/s11133-019-9413-7.
[205] K. L. Matthews, M. Baird, and G. Duchesne, “Using Online Meeting Software to Facilitate Geographically Dispersed Focus Groups for Health Workforce Research,” *Qual. Health Res.*, vol. 28, no. 10, Aug. 2018, doi: 10.1177/1049732318782167.
[206] I. Korstjens and A. Moser, “Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing,” *Eur. J. Gen. Pract.*, vol. 24, no. 1, Jan. 2018, doi: 10.1080/13814788.2017.1375092.
[207] B. M. Asenahabi, “Basics of Research Design : A Guide to selecting appropriate research design,” *Int. J. Contemp. Appl. Res.*, vol. 6, no. 5, 2019.
[208] D. Sekayi and A. Kennedy, “Qualitative Delphi Method: A Four Round Process with a Worked Example,” 2017.
[209] A. Moser and I. Korstjens, “Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis,” *Eur. J. Gen. Pract.*, vol. 24, no. 1, Jan. 2018, doi: 10.1080/13814788.2017.1375091.
[210] L. Ricci *et al.*, “Qualitative Methods Used to Generate Questionnaire Items: A Systematic Review,” *Qual. Health Res.*, vol. 29, no. 1, Jan. 2019, doi: 10.1177/1049732318783186.
[211] L. H. Toledo-Pereyra, “Research design,” *Journal of Investigative Surgery*, vol. 25, no. 5. 2012, doi: 10.3109/08941939.2012.723954.
[212] J. W. Creswell, V. L. Plano Clark, M. L. Gutmann, and W. E. Hanson, “An expanded typology for classifying mixed methods research into designs,” *A. Tashakkori y C. Teddlie, Handb. Mix. methods Soc. Behav. Res.*, pp. 209–240, 2003.
[213] N. V. Ivankova, J. W. Creswell, and S. L. Stick, “Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice,” *Field methods*, vol. 18, no. 1, pp. 3–20, 2006, doi: 10.1177/1525822X05282260.
[214] B. J. Oates, *Researching information systems and computing*. Sage, 2005.
[215] M. Rosemann and I. Vessey, “Toward improving the relevance of information systems research to practice: The role of applicability checks,” *MIS Q. Manag. Inf. Syst.*, vol. 32, no. 1, pp. 7–22, 2008, doi: 10.2307/25148826.
[216] J. Creswell, A. C. Klassen, V. Plano, and K. C. Smith, “Best Practices for Mixed Methods Research in the Health Sciences,” *Bethesda Natl. Institutes Heal.*, vol. 29, pp. 541--545, 2011, doi: 10.1002/cdq.12009.
[217] Y. Gangire, A. Da Veiga, and M. Herselman, “Information Security Behavior: Development of a Measurement Instrument Based on the Self-determination Theory,” *IFIP Adv. Inf. Commun. Technol.*, vol. 593 IFIPAI, pp. 144–157, 2020, doi: 10.1007/978-3-030-57404-8_12.

[218] A. Da Veiga, “Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study,” *Inf. Comput. Secur.*, vol. 24, no. 2, pp. 139–151, 2016, doi: 10.1108/ICS-12-2015-0048.
[219] M. Denscombe, *EBOOK: The Good Research Guide: For Small-Scale Social Research Projects*. McGraw-Hill Education (UK), 2017.
[220] C. Buschle, H. Reiter, and A. Bethmann, “The qualitative pretest interview for questionnaire development: outline of programme and practice,” *Qual. Quant.*, May 2021, doi: 10.1007/s11135-021-01156-0.
[221] J. W. Creswell and J. D. Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2017.
[222] D. Howcroft and E. M. Trauth, *Handbook of critical information systems research: Theory and application*. Edward Elgar Publishing, 2005.
[223] K. Davis *et al.*, “Beyond interviews and focus groups: a framework for integrating innovative qualitative methods into randomised controlled trials of complex public health interventions,” *Trials*, vol. 20, no. 1, Dec. 2019, doi: 10.1186/s13063-019-3439-8.
[224] E. A. McTate and J. M. Leffler, “Diagnosing disruptive mood dysregulation disorder: Integrating semi-structured and unstructured interviews,” *Clin. Child Psychol. Psychiatry*, vol. 22, no. 2, pp. 187–203, Apr. 2017, doi: 10.1177/1359104516658190.
[225] M. N. Marshall, “Sampling for qualitative research,” *Fam. Pract.*, 1996, doi: 10.1093/fampra/13.6.522.
[226] A. S. Acharya, A. Prakash, P. Saxena, and A. Nigam, “Sampling: why and how of it?,” *Indian J. Med. Spec.*, vol. 4, no. 2, Jul. 2013, doi: 10.7713/ijms.2013.0032.
[227] P. A. H. Williams, “Making research real: Is action research a suitable methodology for medical information security investigations?,” *Proc. 4th Aust. Inf. Secur. Manag. Conf.*, 2006, doi: 10.4225/75/57b66e3834779.
[228] R. M. Davison, M. G. Martinsons, and N. Kock, “Principles of canonical action research,” *Inf. Syst. J.*, vol. 14, no. 1, pp. 65–86, 2004, doi: 10.1111/j.1365-2575.2004.00162.x.
[229] R. L. Baskerville and A. T. Wood-Harper, “A critical perspective on action research as a method for information systems research,” *J. Inf. Technol.*, vol. 11, no. 3, pp. 235–246, 1996, doi: 10.1007/978-3-319-29269-4_7.
[230] G. Walsham, “The Emergence of Interpretivism in IS Research,” *Inf. Syst. Res.*, vol. 6, no. 4, pp. 376--394, 1995.
[231] A. Blackstone, “Principles of sociological inquiry: qualitative and quantitative methods,” *The Saylor Foundation*, 2012. https://2012books.lardbucket.org/books/sociological-inquiry-principles-qualitative-and-quantitative-methods/index.html.
[232] G. Guest, E. Namey, J. Taylor, N. Eley, and K. McKenna, “Comparing focus groups and individual interviews: findings from a randomized study,” *Int. J. Soc. Res. Methodol.*, vol. 20, no. 6, Nov. 2017, doi: 10.1080/13645579.2017.1281601.
[233] R. A. Krueger and M. A. Casey, “Focus groups: A practical guide for applied research 5th Edition,” *Focus Groups A Pract. Guid. Appl. Res.*, 2015.
[234] Yong Mei Fung, “Collaborative Writing Features,” *RELC J.*, vol. 41, no. 1, Apr. 2010, doi: 10.1177/0033688210362610.
[235] P. B. Lowry, A. Curtis, and M. R. Lowry, “Building a taxonomy and nomenclature of collaborative writing to improve interdisciplinary research and practice,” *J. Bus. Commun.*, vol. 41, no. 1, pp. 66–99, 2004, doi: 10.1177/0021943603259363.
[236] D. Trilling and J. G. F. Jonkman, “Scaling up Content Analysis,” *Commun. Methods Meas.*, vol. 12, no. 2–3, Apr. 2018, doi: 10.1080/19312458.2018.1447655.
[237] H. Kyngäs, M. Kääriäinen, and S. Elo, “The Trustworthiness of Content Analysis,” in *The Application of Content Analysis in Nursing Science Research*, Cham: Springer International Publishing, 2020.
[238] D. Cornish and R. Clarke, “OPPORTUNITIES, PRECIPITATORS AND CRIMINAL DECISIONS: A REPLY TO WORTLEY’S CRITIQUE OF SITUATIONAL CRIME PREVENTION,” *Crime Prev. Stud.*, vol. 32, no. 2003, pp. 41–63, 2002, [Online]. Available: http://www.popcenter.org/Responses/crime_prevention/PDFs/Cornish&Clarke.pdf.
[239] J. D. Freilich and G. R. Newman, “Situational Crime Prevention,” in *Oxford Research Encyclopedia of Criminology and Criminal Justice*, 2017.
[240] R. DuPreez, “A model for green IT strategy: a content analysis approach,” Nelson Mandela

Metropolitan University, 2010.
[241] T. Tuyikeze and S. Flowerday, “Information security policy development and implementation: A content analysis approach,” in *Proceedings of the 8th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2014*, 2014, pp. 11–20, Accessed: Nov. 22, 2017. [Online]. Available: https://pdfs.semanticscholar.org/a7ce/d6cb5e3ec3efe46b55c059d5fdc5c3828200.pdf.
[242] S. Stemler, “An overview of content analysis, Practical Assessment, Research, and Evaluation,” *Sch. Amherst*, vol. 7, no. 17, pp. 2000–2001, 2001.
[243] C. B. Jarvis, S. B. MacKenzie, and P. M. Podsakoff, “A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research,” *J. Consum. Res.*, vol. 30, no. 2, pp. 199–218, Sep. 2003, doi: 10.1086/376806.
[244] A. Petter, Stacie and Straub, Detmar and Rai, “Specifying Formative Constructs in Information Systems Research,” *MIS Q.*, vol. 31, no. December, pp. 623–656, 2007.
[245] S. B. MacKenzie, P. M. Podsakoff, and C. B. Jarvis, “The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions,” *J. Appl. Psychol.*, vol. 90, no. 4, pp. 710–730, 2005, doi: 10.1037/0021-9010.90.4.710.
[246] M. J. O’Fallon and K. D. Butterfield, “A review of the empirical ethical decision-making literature: 1996-2003,” *J. Bus. Ethics*, vol. 59, no. 4, pp. 375–413, 2005, doi: 10.1007/s10551-005-2929-7.
[247] A. C. Johnston, M. Warkentin, M. McBride, and L. Carter, “Dispositional and situational factors: Influences on information security policy violations,” *Eur. J. Inf. Syst.*, vol. 25, no. 3, pp. 231–251, 2016, doi: 10.1057/ejis.2015.15.
[248] T. T. Moores and J. C. J. Chang, “Ethical decision making in software piracy: Initial development and test of a four-component model,” *MIS Q. Manag. Inf. Syst.*, vol. 30, no. 1, pp. 167–180, 2006, doi: 10.2307/25148722.
[249] L. K. Trevino, “Experimental Approaches to Studying Ethical-Unethical Behavior in Organizations,” *Bus. Ethics Q.*, vol. 2, no. 2, pp. 121–136, 1992, doi: 10.5840/10.2307/3857567.
[250] I. Krumpal, “Determinants of social desirability bias in sensitive surveys: a literature review,” *Qual. Quant.*, vol. 47, no. 4, pp. 2025–2047, 2013.
[251] A. R. Piquero and M. Hickman, “An empirical test of tittle’s control balance theory,” *Criminology*, vol. 37, no. 2, pp. 319–342, 1999, doi: 10.1111/j.1745-9125.1999.tb00488.x.
[252] Q. C. Thurman, “Deviance and the neutralization of moral commitment: An empirical analysis,” *Deviant Behav.*, vol. 5, no. 1–4, pp. 291–304, 1984, doi: 10.1080/01639625.1984.9967646.
[253] C. M. Ringle, S. Wende, and A. Will, “SmartPLS release: 2.0 (beta),” *SmartPLS, Hamburg, Ger. URL http//www. smartpls.*, 2005.
[254] J. F. Hair Jr, G. T. M. Hult, C. Ringle, and M. Sarstedt, *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications, 2014.
[255] K. S. Taber, “The Use of Cronbach’s Alpha When Developing and Reporting Research Instruments in Science Education,” *Res. Sci. Educ.*, vol. 48, no. 6, pp. 1273–1296, 2018, doi: 10.1007/s11165-016-9602-2.
[256] R. P. Bagozzi and Y. Yi, “On the evaluation of structural equation models,” *J. Acad. Mark. Sci.*, vol. 16, no. 1, pp. 74–94, 1988, doi: 10.1007/BF02723327.
[257] M. Sarstedt, C. M. Ringle, and J. F. Hair, “Partial least squares structural equation modeling,” *Handb. Mark. Res.*, vol. 26, no. 1, pp. 1–40, 2017.
[258] J. Hulland, “Use of partial least squares (PLS) in strategic management research: A review of four recent studies,” *Strateg. Manag. J.*, vol. 20, no. 2, pp. 195–204, 1999, doi: 10.1002/(sici)1097-0266(199902)20:2<195::aid-smj13>3.0.co;2-7.
[259] D. Gefen and D. Straub, “A Practical Guide To Factorial Validity Using PLS-Graph: Tutorial And Annotated Example,” *Commun. Assoc. Inf. Syst.*, vol. 16, pp. 91–109, 2005, doi: 10.17705/1cais.01605.
[260] C. Fornell and D. F. Larcker, “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error Evaluating Structural Equation Models with,” *Source J. Mark. Res.*, vol. 18, no. 1, pp. 39–50, 1981, Accessed: Jul. 24, 2017. [Online]. Available: http://www.jstor.org/stable/3151312.
[261] H. Liang, Y. Xue, and L. Wu, “Ensuring employees’ IT compliance: Carrot or stick?,” *Inf. Syst. Res.*, vol. 24, no. 2, pp. 279–294, 2013, doi: 10.1287/isre.1120.0427.
[262] W. W. Chin, “The partial least squares approach to structural equation modelling. In Marcoulides G. A. (Ed.),” *Mod. Methods Bus. Res.*, vol. 295, no. 2, pp. 295–336, 1998.

[263] K. K. K.-K. Wong, “Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS,” *Mark. Bull.*, vol. 24, no. 1, pp. 1–32, 2013, [Online]. Available: http://marketing-bulletin.massey.ac.nz/v24/mb_v24_t1_wong.pdf%5Cnhttp://www.researchgate.net/profile/Ken_Wong10/publication/268449353_Partial_Least_Squares_Structural_Equation_Modeling_(PLS-SEM)_Techniques_Using_SmartPLS/links/54773b1b0cf293e2da25e3f3.pdf.

[264] B. BYERS, B. W. CRIDER, and G. K. BIGGERS, “Bias Crime Motivation,” *J. Contemp. Crim. Justice*, vol. 15, no. 1, pp. 78–96, Feb. 1999, doi: 10.1177/1043986299015001006.

[265] R. A. D. Stephen L. Eliason, “techniques of neutralization used by deer poachers in the western united states: a research note,” *Deviant Behav.*, vol. 20, no. 3, pp. 233–252, Jun. 1999, doi: 10.1080/016396299266489.

[266] R. Paternoster and S. Simpson, “Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime,” *Source Law Soc. Rev.*, vol. 30, no. 3, pp. 549–584, 1996, Accessed: Dec. 14, 2017. [Online]. Available: http://www.jstor.org/stable/3054128.

[267] M. Siponen, A. Vance, and R. Willison, “New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs,” *Inf. Manag.*, vol. 49, no. 7–8, pp. 334–341, 2012, doi: 10.1016/j.im.2012.06.004.

[268] J. D. Wall, P. B. Lowry, and J. B. Barlow, “Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess,” *J. Assoc. Inf. Syst.*, vol. 17, no. 1, pp. 39–76, 2016.

[269] P. B. Lowry and G. D. Moody, “Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies,” *Inf. Syst. J.*, vol. 25, no. 5, pp. 433–463, 2015, doi: 10.1111/isj.12043.

[270] I. Kirlappos, A. Beautement, and M. A. Sasse, “‘Comply or Die’ Is Dead: Long Live Security-Aware Principal Agents The Need for Information Security,” in *Financial Cryptography and Data Security*, 2013, pp. 70–82.

[271] E. Niemimaa and M. Niemimaa, “Information systems security policy implementation in practice: From best practices to situated practices,” *Eur. J. Inf. Syst.*, vol. 26, no. 1, pp. 1–20, 2017, doi: 10.1057/s41303-016-0025-y.

[272] I. Kirlappos, “Learning from " Shadow Security ": Understanding Non-Compliant Behaviours to Improve Information Security Management,” 2016.

[273] P. Biernacki and D. Waldorf, “Snowball Sampling: Problems and Techniques of Chain Referral Sampling,” *Sociol. Methods Res.*, vol. 10, no. 2, pp. 141–163, 1981, doi: 10.1177/004912418101000205.

[274] R. E. Boyatzis, *Transforming qualitative information: Thematic analysis and code development*. sage, 1998.

[275] E. H. Sutherland, D. R. Cressey, and D. F. Luckenbill, *Principles of criminology*. Altamira Press, 1992.

[276] H. R. Peikari, T. Ramayah, M. H. Shah, and M. C. Lo, “Patients’ perception of the information security management in health centers: The role of organizational and human factors 17 Psychology and Cognitive Sciences 1701 Psychology 11 Medical and Health Sciences 1117 Public Health and Health Services,” *BMC Med. Inform. Decis. Mak.*, vol. 18, no. 1, 2018, doi: 10.1186/s12911-018-0681-z.

[277] D. W. Straub, “Effective IS Security: An Empirical Study,” *Inf. Syst. Res.*, vol. 1, no. 3, pp. 255–276, Sep. 1990, doi: 10.1287/isre.1.3.255.

[278] N. S. Safa and R. Von Solms, “An information security knowledge sharing model in organizations,” *Comput. Human Behav.*, vol. 57, pp. 442–451, 2016, doi: 10.1016/j.chb.2015.12.037.

[279] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, “Information security conscious care behaviour formation in organizations,” *Comput. Secur.*, vol. 53, pp. 65–78, 2015, doi: 10.1016/j.cose.2015.05.012.

[280] A. Da Veiga and J. H. P. Eloff, “A framework and assessment instrument for information security culture,” *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, Mar. 2010, doi: 10.1016/j.cose.2009.09.002.

[281] T. Schlienger and S. Teufel, “Information security culture – from analysis to change,” *South African Comput. J.*, vol. 31, pp. 46–52, 2003, Accessed: Nov. 26, 2017. [Online]. Available: http://icsa.cs.up.ac.za/issa/2003/Publications/025.pdf.

[282] A. Nasir, R. A. Arshah, M. R. A. Hamid, and S. Fahmy, "An analysis on the dimensions of information security culture concept: A review," *J. Inf. Secur. Appl.*, vol. 44, pp. 12–22, 2019, doi: 10.1016/j.jisa.2018.11.003.
[283] B. von Solms, "Information Security - The Fourth Wave," *Comput. Secur.*, 2006, doi: 10.1016/j.cose.2006.03.004.
[284] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link' - A human/computer interaction approach to usable and effective security," *BT Technol. J.*, vol. 19, no. 3, pp. 122–131, 2001, doi: 10.1023/A:1011902718709.
[285] S. Alfawaz, K. Nelson, and K. Mohannak, "Information security culture: A behaviour compliance conceptual framework," *Conf. Res. Pract. Inf. Technol. Ser.*, vol. 105, pp. 47–55, 2010, Accessed: May 09, 2019. [Online]. Available: http://eprints.qut.edu.au/29221.
[286] K. R. Williams and R. Hawkins, "Perceptual Research on General Deterrence: A Critical Review," *Law Soc. Rev.*, vol. 20, no. 4, p. 545, 2006, doi: 10.2307/3053466.
[287] T. Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 106–125, 2009, doi: 10.1057/ejis.2009.6.
[288] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner, "Information security awareness and behavior: A theory-based literature review," *Manag. Res. Rev.*, vol. 37, no. 12, pp. 1049–1092, Nov. 2014, doi: 10.1108/MRR-04-2013-0085.
[289] N. S. Safa *et al.*, "Deterrence and prevention-based model to mitigate information security insider threats in organisations," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 587–597, 2019, doi: 10.1016/j.future.2019.03.024.
[290] M. E. Zurko and R. T. Simon, "User-centered security," in *Proceedings of the 1996 workshop on New security paradigms*, 1996, pp. 27–33.
[291] S. Clarke and C. L. Cooper, *Managing the risk of workplace stress: Health and safety hazards*. Psychology Press, 2004.
[292] J. David, "Policy enforcement in the workplace," *Computers and Security*. 2002, doi: 10.1016/S0167-4048(02)01006-4.
[293] T. Kayworth and D. Whitten, "Effective information security requires a balance of social and technology factors," *MIS Q. Exec.*, vol. 9, no. 3, pp. 163–175, 2010.
[294] I. Kirlappos, S. Parkin, and M. A. Sasse, "Learning from 'Shadow Security:' Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security," 2014, doi: 10.14722/usec.2014.23007.
[295] K. Höne and J. H. P. Eloff, "Information security policy - What do international information security standards say?," *Computers and Security*, vol. 21, no. 5. Elsevier Advanced Technology, pp. 402–409, Oct. 01, 2002, doi: 10.1016/S0167-4048(02)00504-7.
[296] L. S. M., O. D. L., and T. Silvana, "Co-innovation: convergenomics, collaboration, and co-creation for organizational values," *Manag. Decis.*, vol. 50, no. 5, pp. 817–831, Jan. 2012, doi: 10.1108/00251741211227528.
[297] C. K. Prahalad and V. Ramaswamy, "The co-creation connection," *Strateg. Bus.*, pp. 50–61, 2002.
[298] V. Prahalad, Coimbatore K and Ramaswamy, "The co-creation connection," *Strateg. Bus.*
[299] J. Jackson, B. Bradford, M. Hough, A. Myhill, P. Quinton, and T. R. Tyler, "Why do people comply with the law? Legitimacy and the influence of legal institutions," *Br. J. Criminol.*, vol. 52, no. 6, pp. 1051–1071, 2012.
[300] R. V. G. Clarke, "'SITUATIONAL' CRIME PREVENTION: THEORY AND PRACTICE," *Br. J. Criminol.*, vol. 20, no. 2, pp. 136–147, Nov. 1980, [Online]. Available: http://www.jstor.org.sdl.idm.oclc.org/stable/23636692.
[301] J. D. Freilich and G. R. Newman, "Providing opportunities: A sixth column for the techniques of situational crime prevention," in *Organized Crime, Corruption and Crime Prevention*, Springer International Publishing, 2014, pp. 33–42.
[302] P. Mackieson, A. Shlonsky, and M. Connolly, "Increasing rigor and reducing bias in qualitative research: A document analysis of parliamentary debates using applied thematic analysis," *Qual. Soc. Work*, vol. 18, no. 6, pp. 965–980, 2019.
[303] R. Wortley, "Guilt, shame and situational crime prevention," *Crime Prev. Stud.*, vol. 5, pp. 115–132, 1996, Accessed: Aug. 24, 2020. [Online]. Available: https://www.researchgate.net/publication/252780265.
[304] R. Wortley, "A Classification of Techniques for Controlling Situational Precipitators of Crime,"

in *Crime Opportunity Theories*, 2001, pp. 425–444.
[305] J. R. B. Halbesleben, A. R. Wheeler, and M. R. Buckley, “Everybody else is doing it, so why can’t we? Pluralistic ignorance and business ethics education,” *J. Bus. Ethics*, vol. 56, no. 4, pp. 385–398, 2005, doi: 10.1007/s10551-004-3897-z.
[306] G. Meško, K. Bančič, K. Eman, and C. B. Fields, “Situational crime-prevention measures to environmental threats,” in *Understanding and managing threats to the environment in South Eastern Europe*, Springer, 2011, pp. 41–67.
[307] M. S. Al-Moamary, S. Mamede, and H. G. Schmidt, “Innovations in medical internship: benchmarking and application within the King Saud bin Abdulaziz University for Health Sciences.,” *Educ. Health (Abingdon).*, vol. 23, no. 1, p. 367, 2010, doi: 367 [pii].
[308] S. Helo and C. A. E. Dd, “Complications: Acknowledging, managing, and coping with human error,” *Transl. Androl. Urol.*, vol. 6, no. 4, pp. 773–782, 2017, doi: 10.21037/tau.2017.06.28.
[309] K. Padayachee, “A framework of opportunity-reducing techniques to mitigate the insider threat,” in *2015 Information Security for South Africa - Proceedings of the ISSA 2015 Conference*, 2015, pp. 1–8, doi: 10.1109/ISSA.2015.7335064.
[310] N. S. Safa, C. Maple, T. Watson, and R. Von Solms, “Motivation and opportunity based model to reduce information security insider threats in organisations,” *J. Inf. Secur. Appl.*, vol. 40, pp. 247--257, 2018, doi: 10.1016/j.jisa.2017.11.001.
[311] J. D. Freilich and G. R. Newman, “Situational Crime Prevention : Historical Back - ground and Origins of the Idea,” *Oxford Res. Encycl. Criminol. Crim. Justice*, vol. 3, no. April 2020, pp. 1–28, 2017.
[312] K. Nandakumar, A. K. Jain, and S. Pankanti, “Fingerprint-based fuzzy vault: Implementation and performance,” *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 4, pp. 744–757, 2007, doi: 10.1109/TIFS.2007.908165.
[313] S. Hinduja and B. Kooi, “Curtailing cyber and information security vulnerabilities through situational crime prevention,” *Secur. J.*, vol. 26, no. 4, pp. 383–402, 2013, doi: 10.1057/sj.2013.25.
[314] J. Kim, E. H. Park, and R. L. Baskerville, “A model of emotion and computer abuse,” *Inf. Manag.*, vol. 53, no. 1, pp. 91–108, 2016, doi: 10.1016/j.im.2015.09.003.
[315] U. Güğerçin, “Does techno-stress justify cyberslacking? An empirical study based on the neutralisation theory,” *Behav. Inf. Technol.*, vol. 39, no. 7, pp. 824–836, 2020, doi: 10.1080/0144929X.2019.1617350.
[316] D. G. Renfrow and E. A. Rollo, “Sexting on Campus: Minimizing Perceived Risks and Neutralizing Behaviors,” *Deviant Behav.*, vol. 35, no. 11, pp. 903–920, 2014, doi: 10.1080/01639625.2014.897122.
[317] M. Tunley, M. Button, D. Shepherd, and D. Blackbourn, “Preventing occupational corruption: utilising situational crime prevention techniques and theory to enhance organisational resilience,” *Secur. J.*, vol. 31, no. 1, pp. 21--52, 2018.
[318] D. P. Snyman, H. Kruger, and W. D. Kearney, “I shall, we shall, and all others will: paradoxical information security behaviour,” *Inf. Comput. Secur.*, vol. 26, no. 3, pp. 290–305, 2018, doi: 10.1108/ICS-03-2018-0034.
[319] R. Heinrichs, Randi and Loacker, Bernadette and Weiskopf, “The ethico-politics of whistleblowing: Mediated truth-telling in digital cultures,” *Ephemer. Theory Polit. Organ.*, vol. 19, no. 3, pp. 671--969, 2019.
[320] J. M. Pacella, “The Cybersecurity Threat: Compliance and the Role of Whistleblowers,” *SSRN Electron. J.*, vol. 11, no. 1, 2016, doi: 10.2139/ssrn.2803995.
[321] R. M. Ryan and E. L. Deci, “Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions,” *Contemp. Educ. Psychol.*, vol. 25, no. 1, pp. 54–67, 2000, doi: 10.1006/ceps.1999.1020.
[322] M. Ko and C. Dorantes, “The impact of information security breaches on financial performance of the breached firms: An empirical investigation,” *J. Inf. Technol. Manag.*, vol. 17, no. 2, pp. 13–22, 2006.
[323] Laerd Statistics, “Wilcoxon signed-rank test using SPSS Statistics. Statistical tutorials and software guides,” 2015. https://www.statistics.laerd.com/ (accessed Oct. 09, 2019).
[324] S. S. Shapiro and M. B. Wilk, “An Analysis of Variance Test for Normality (Complete Samples),” *Biometrika*, vol. 52, no. 3/4, p. 591, 1965, doi: 10.2307/2333709.
[325] J. D. Wall, P. Palvia, and P. B. Lowry, “Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy,” *J. Inf. Priv. Secur.*, 2013, doi:

10.1080/15536548.2013.10845690.

[326] N. L. Beebe, S. Rao, R. Beebe, and V. S. Rao, “Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security,” in *Proceedings of the 2005 SoftWars Conference, Las Vegas, NV*, 2005, pp. 1--18, Accessed: Mar. 11, 2021. [Online]. Available: https://www.researchgate.net/publication/237264626.

[327] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Roles of information security awareness and perceived fairness in information security policy compliance,” in *15th Americas Conference on Information Systems 2009, AMCIS 2009*, 2009, vol. 5, pp. 3269–3277, Accessed: Apr. 12, 2017. [Online]. Available: http://aisel.aisnet.org/amcis2009.

[328] N. L. Beebe and S. V. Rao, “Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process,” *Commun. Assoc. Inf. Syst.*, vol. 26, no. 1, pp. 329–358, 2010, doi: 10.17705/1cais.02617.

[329] R. Wortley, “Studies on Crime and Crime Prevention, 7, 173-188.,” *Prevention*, pp. 173–188, 1998.

[330] J. D’Arcy, T. Herath, and M. K. Shoss, “Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective,” *J. Manag. Inf. Syst.*, vol. 31, no. 2, pp. 285–318, 2014, doi: 10.2753/MIS0742-1222310210.