Alahmari, Saad (2021) *A model for describing and encouraging cyber security knowledge sharing to enhance awareness.* PhD thesis.

A Model for Describing and Encouraging Cyber Security Knowledge Sharing to Enhance Awareness

Saad Alahmari

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

August 2021

Abstract

Employees play a crucial role in enhancing information security in the workplace, and this requires everyone to have the requisite security knowledge and know-how. To maximise knowledge levels, organisations should encourage and facilitate security knowledge sharing (SKS) among employees. This thesis was based on a multi-phase study. The first and second stages were theoretical studies to investigate and mitigate the issues. The third and fourth stages involved implementing the instrument and conducting an empirical study to evaluate the effect of the SKS model. To improve sharing, ***the first stage*** is to understand the mechanisms whereby such sharing takes place and then to encourage and engender such sharing. To better understand the challenges, we conducted semi-structured interviews with two organisations. Based on the outcomes of this stage, we identified a list of barriers such as approaches to improving security awareness; these have generally been based on individualistic models (i.e., considering an individual in isolation).

To mitigate these challenges, this thesis proposes the SKS model, which includes transactive memory system (TMS) and self-determination theory (SDT). To maximise sharing security knowledge, we carried out ***second stage A*** to examine scale reliability, correlations, and relationships between the TMS scale and other constructs in the security context in order to understand SKS in organisations. Our study confirmed its applicability in this domain. ***Second stage B*** confirmed the relationships between TMS and SDT. To encourage security knowledge sharing, we propose harnessing SDT: satisfying employee needs for relatedness and a sense of competence to maximise sharing.

The third stage, based on the SKS model, describes designing and implementing a mobile game to enhance the delivery of information security training to help employees protect themselves from security attacks. ***The fourth stage,*** an empirical study (mixed method using qualitative and quantitative data), was conducted within a Saudi Arabian Fortune 100 organisation to evaluate the effect of using the app. The goals of this stage were to assess the improvement in Security Awareness for the intervention and control groups and to evaluate the model of knowledge sharing pre-test and post-test.

Overall, the results confirmed that the SKS model positively raises information security awareness for employees. Moreover, the findings confirmed the success of cooperative training by adopting intrinsic motivation via an Educational Security Game. The results demonstrated great promise for adopting and generalising this model in future studies to improve the delivery of security training.

Table of Contents

List of Tables

List of Figures

Acknowledgements

In the name of Allah, the Most Merciful, the Most Graceful.

This has been a long journey, full of both good and bad memories. However, every time I struggled, I remembered the quote: “There is no substitute for hard work. Never give up. Never stop believing. Never stop fighting.”, which was the motivation to keep going to achieve my dream.

First and foremost, I would like to thank my father and my wife’s father, who died before they could see the dream come true. They were extremely supportive during those difficult times. I really miss them at this time.

I would like to thank my supervisors, Professor Karen Renaud, and Dr Inah Omoronyia, for providing guidance and support throughout the research project and the write-up. Their insightful comments and constructive criticism have provided my work with structure and given me invaluable clarity. Karen, saying ‘thank you’ is not enough for me to express how grateful I am for your support over the years.

In addition, I would like to express my gratitude to my great mother and faithful wife, who have been tremendous inspirations in helping me achieve my goal.

Special thanks go to the former President of the Northern Border University, Professor Saeed Al Omar, for his continued faith in me. I am deeply appreciative of his support in completing my education.

Last but not least, I would want to thank the many colleagues and friends I have met during this journey, including Ibrahim and Abdillah Alghamdi, Abdullah Alkharashy, and Saad Altamimi.

Author’s Declaration

I declare that I wrote this thesis, that all of the work included herein is my own unless otherwise indicated in the text, and that this work has not been submitted for any other degree or professional qualification except as described.

Saad Alahmari
Date: 01/08/2021

Abbreviations

InfoSec	Information Security
ISA	Information Security Awareness
KM	Knowledge Management
KS	Knowledge Sharing
PMT	Protection Motivation Theory
SDT	Self-Determination Theory
SG	Security Games
SKS	Security Knowledge Sharing
STOW	A Security Knowledge Sharing System
TMS	Transactive Memory System
UK	United Kingdom

Chapter One: Introduction

Information security is crucial for the protection of data and information systems against illegal access, use, disclosure, interruption, alteration, or destruction, and to maintain confidence, integrity, and accessibility [1]. The thesis seeks to improve information security awareness (ISA) by engendering knowledge sharing (KS) among employees to enhance their security knowledge. The first study included in this thesis identifies and examines the impeding factors (or barriers) to KS. There were two types of barriers: organisational (functioning) and individual (expertise and trust) factors, as seen in Figure 1.1. The dissertation aims to mitigate those challenges by adopting transactive memory systems (TMS) and self-determination theory (SDT) to engender the SK in organisations. The role of TMS is to describe and facilitate. Part of SDT incorporates the satisfaction needs to encourage SK. SDT can deal with individual factors, such as building trust among employees through competence.

This chapter introduces the research background, thesis statement, research questions, research contribution, and thesis overview. It has five sections. Section 1.1 introduces the importance of security knowledge sharing, its associated challenges, and how to improve security awareness by facilitating and encouraging SKS in organisations. Section 1.2 defines the thesis statement. Section 1.3 provides the main research questions and sub-questions. Section 1.4 introduces the research contribution. Finally, section 1.5 provides an overview of each chapter of this dissertation.

1.1 Background

Employees play a crucial role in enhancing Information Security (InfoSec) [1]. An essential prerequisite is for employees to know what it is they must do, and how to do it; in other words, they must possess the required knowledge and skills (know-how). Knowledge sharing (SK), of all types, improves the organisation as a whole and engenders trust among employees [2]. Of particular interest in this dissertation is InfoSec knowledge sharing KS, which can improve InfoSec awareness, is important when it comes to preventing security breaches [3]. The knowledge held by an organisation’s employees is its most important asset [4]. Moreover, InfoSec can help employees see the importance of information SKS in enhancing security awareness [5]. While awareness drives and training are undeniably valuable and essential, a neglected way of ensuring that all employees gain the requisite knowledge and know-how is to encourage and facilitate SKS across the organisation [6].

The biggest challenge of SKS is gathering and sharing information and exploring the key factors that affect it [7]. However, many other factors need more investigation [8]. Previous studies explored only a handful of different theories designed to mitigate those challenges [9]. Moreover, there have been other approaches to improving security awareness which generally are based on individualistic models (considering an individual in isolation) [10-15].

A lack of provision of an environment that facilitates and motivates the process of information exchange within organisations is also common and is a powerful barrier to KS. Most of the existing studies do not propose effective solutions to mitigate such barriers [9, 15].

To facilitate access to this knowledge, many companies are introducing knowledge repositories. This makes it easier to store and distribute knowledge and has also facilitated the movement of knowledge to those outside of the organisation. While companies routinely protect their information using firewalls and filtering systems, it is crucial that they do not overlook the importance of the security knowledge held within the minds of their employees [16]. Organisations should therefore engender organisational SKS. The aim should be to make the knowledge accessible to those who need it and ultimately to improve InfoSec in the organisation. Collaborative interventions in InfoSec should encourage employees to interact with each other to share their security knowledge [9, 17], thus ensuring that all employees have access to security advice [18].

To investigate this, we ask what the challenges related to SKS are, in terms of improving security awareness. After identifying these challenges in chapter 4 [17], we consider how information security knowledge can be described and facilitated in chapter 5. Third, we explore how people can be motivated to share security knowledge in chapter 5. The aim is to maximise such sharing [17], as well as to test the validity of the transactive memory systems (TMS) theory to model the SKS within organisations. A security knowledge sharing system (STOW) application models TMS to reflect organisational factors and incorporates the satisfaction of self-determination theory (SDT) needs [19, 20] at the individual level to maximise SKS within organisations, and to improve and enhance organisational security awareness in Chapter 6 and 7.

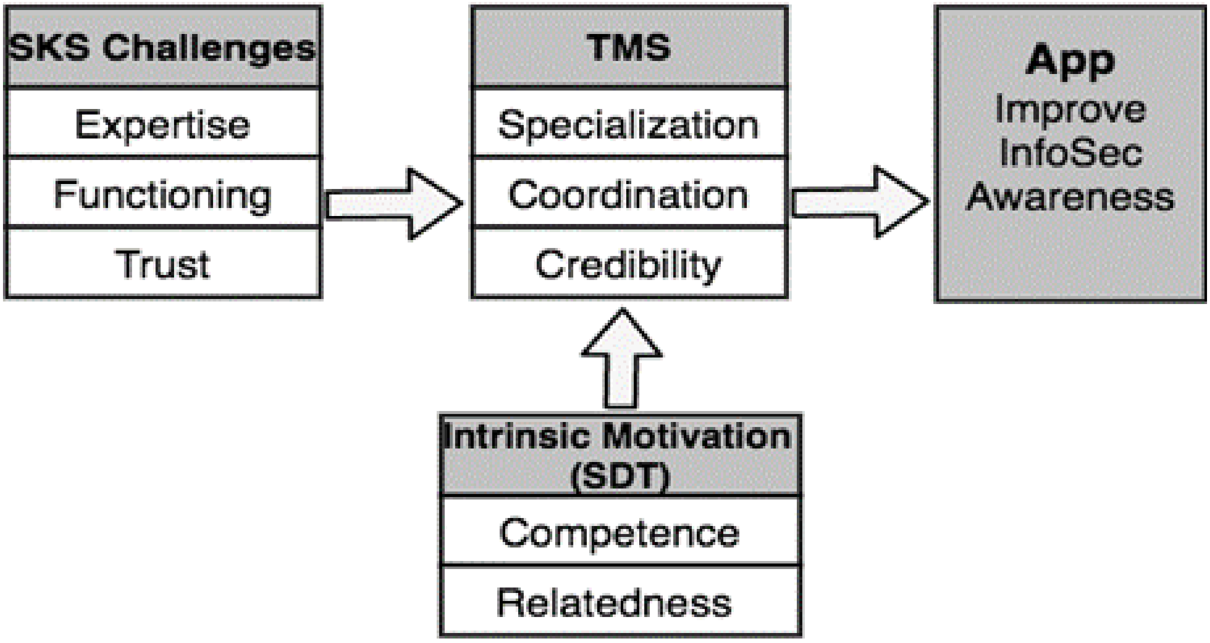


Figure 1.1 Proposed research model

1.2 Thesis Statement

There are several approaches to improving security awareness, most of which have been based on individualistic models. Still, these do not scale to organisations and neglect social aspects of security awareness.

The thesis statement is thus:

It is possible to model organisational security knowledge sharing behaviours using transaction memory system theory and encourage such sharing through the satisfaction of self-determination needs. As a consequence, security knowledge sharing will improve and enhance employee security awareness within organisations.

1.3 Research Questions

Given the foundation and overview of the problem, this dissertation addresses the following questions as shown in the proposed research model (Figure 1.1):

Main Question: How can knowledge sharing improve security awareness in organisations?

Sub-question 1*:* What are the challenges of SKS is improving security awareness?

Sub-question 2: How can information security knowledge sharing be modelled by transactive memory system (TMS) theory?

Sub-question 3: Can security knowledge sharing be modelled using TMS and sharing encouraged by satisfying the self-determination needs of employees?

1.4 Thesis Contributions and Publications

The main contributions of this work are as follows:

Developing an understanding of the challenges (Chapter 4): The study revealed several factors that deter Knowledge Sharing in organisations. To better understand these factors, the research adopted a qualitative approach, with semi-structured interviews carried out in Saudi and British organisations in different geographical locations. Interviewing is the most powerful technique for delivering comprehensive insights that allow for the best understanding of knowledge-sharing in natural environments. The information obtained was used to devise practical solutions.

Examination of the scale reliability and relationships between the TMS at an organisational level (Chapter 5): We examined scale reliability, correlations, and relationships between the TMS scale and other constructs in the security context in order to understand and facilitate SKS in organisations. This is a new finding in the security context.

Developing a model for describing and maximising Security Knowledge Sharing to enhance security awareness (Chapter 5): We proposed a model that incorporates the factors that could maximise SKS within organisations. The model emerged from the study's findings and incorporates two theories: one at the organisational level and the other at the individual level. TMS theory describes how organisational knowledge is held and how sharing is facilitated at the organisational level, with SDT encouraging sharing at an individual level.

Implementation and design of a system application based on SKS model (Chapter 6): The study led to the design of a system and implementation based on the first and second experiments' findings to mitigate the challenges identified in the literature review. Then we developed and tested the app via Android Studio and CSS.

Implications for designers and developers (Chapter 6): The thesis provides practical implications for system designers and developers who seek to improve employee security awareness within organisations via a collaborative model. Moreover, the study encourages employees to engage in prosocial behaviour through educational security games.

Empirical experiment involving a security knowledge sharing app (Chapter 7): The experiment evaluates the effect of using the app in the real world to enhance training and improve employees' security awareness in organisations. The experiment contributed to the knowledge by examining how the app can identify how SKS can be enhanced, and also how the app can be facilitated and encouraged among employees to improve their knowledge.

Autonomy as intrinsic motivation and Relatedness (Chapter 7): This study extends how to deliver security training by exploring the positive effects of including autonomy as intrinsic motivation and relatedness into training (STOW). Both encouraged the employees to complete the training without any external influence, which led to enhancing the employees' security knowledge.

Finally, significant portions of the research carried out in this thesis have been peer-reviewed and published:

- Al-Ahmari, S., Renaud, K. and Omoronyia, I., 2018, September. A Systematic Review of Information Security Knowledge-Sharing Research. In *HAISA* (pp. 101-110).
- Alahmari, S., Renaud, K. and Omoronyia, I., 2019, December. A model for describing and maximising security knowledge sharing to enhance security awareness. In *European, Mediterranean, and Middle Eastern Conference on Information Systems* (pp. 376-390). Springer, Cham.
- Alahmari, S., 2019. *Enhancing Knowledge Sharing in Information Security by Transactive Memory System*. SICSA DemoFest 2019: Bringing Research To Life, Edinburgh, UK, 04 Nov 2019.
- Alahmari, S., Renaud, K. and Omoronyia, I., 2020, December. Implement a Model for Describing and Maximising Security Knowledge Sharing. In *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 1-4). IEEE.

1.5 Thesis Overview

Chapter Two reviews related work on InfoSec awareness and how to mitigate risk in organisations through collaboration.

Chapter Three describes the research methods we used to achieve the aim of the study. The research methods include the research philosophy, justification of the research approach, and the methodology of the research study.

Chapter Four presents an exploratory study of SKS challenges in the organisations that answered the research questions (sub-question 1). The study identifies the challenges that prevent SKS within an organisation. The chapter includes an introduction, research methodology, data analysis, findings, and discussion.

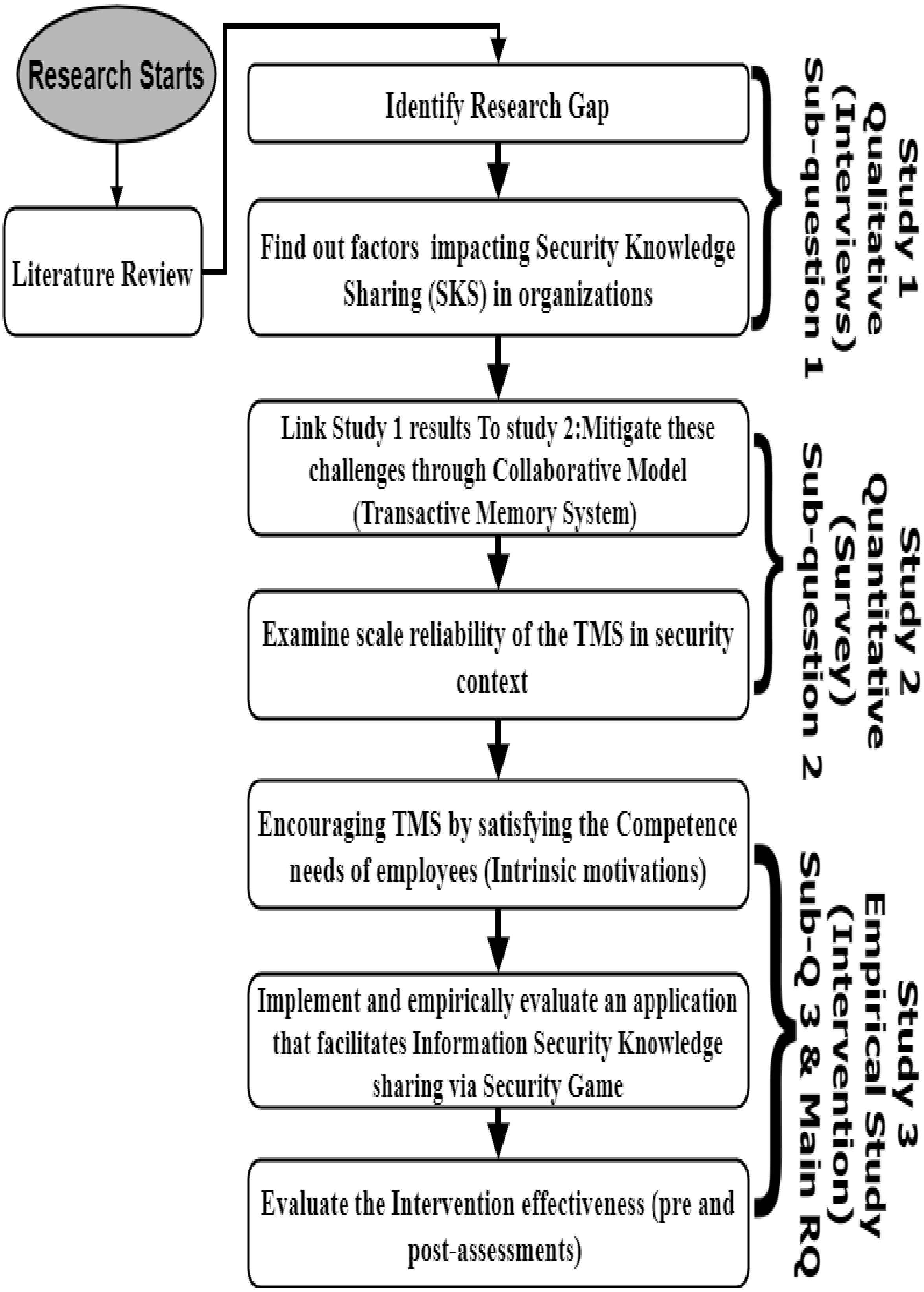
Chapter Five examines the scale reliability and relationships between the TMS and other constructs at an organisational level. We examined scale reliability, correlations, and relationships between the TMS scale and other constructs in the security context in order to understand and facilitate SKS in organisations. This answers the research question (sub-question 2). The chapter includes an introduction, research methodology, data analysis, findings, and discussion.

Chapter Six proposes a model that incorporates the factors that could maximise SKS within organisations. The model emerged from the study's findings and incorporates TMS and SDT, encouraging sharing. This answers the research question (sub-question 3 and the main question). The chapter includes an introduction, exploration of the relationship between TMS and SDT, implementation of the SKS model into the STOW app, research methodology, data analysis, findings, and discussion.

Chapter Seven presents a general discussion, discussion of study one, discussion of study two, discussion of study three, and a summary.

Chapter Eight presents the conclusions. The chapter includes research objectives and contributions, a summary of the results, interconnection of experiments, and limitations. We also discuss some possible future directions for research.

Thesis Framework


Research Starts
Literature Review
Identify Research Gap
Find out factors impacting Security Knowledge Sharing (SKS) in organizations
Link Study 1 results To study 2:Mitigate these challenges through Collaborative Model (Transactive Memory System)
Examine scale reliability of the TMS in security context
Encouraging TMS by satisfying the Competence needs of employees (Intrinsic motivations)
Implement and empirically evaluate an application that facilitates Information Security Knowledge sharing via Security Game
Evaluate the Intervention effectiveness (pre and post-assessments)
Study 1
Qualitative
(Interviews)
Sub-question 1
Study 2
Quantitative
(Survey)
Sub-question 2
Study 3
Empirical Study
(Intervention)
Sub-Q 3 & Main RQ

Chapter Two: Review of the Literature

This chapter presents a literature review and establishes the theoretical foundations for the thesis. The chapter is structured as follows: Section 2.1 defines InfoSec to include security risks, vulnerabilities, and countermeasures. Section 2.2 introduces information security awareness (ISA) and the most effective method to improve ISA in an enterprise. Section 2.3 proposes that cooperative theory enables practical information sharing as a method to deliver security training. Section 2.4 presents an overview of SKS factors, including previous studies that connect the theories, the geographic scope of prior studies, and methodologies. Section 2.5 presents information security collaboration in organisations, including offering TMS as an organisational theory to mitigate the barriers of the SKS. Section 2.6 discusses intrinsic motivation, which is an issue of human motivation theory that involves SDT and encourages human behaviours. Section 2.7 discusses educational games in the virtual environment to enhance the delivery method for security awareness. In particular, gamification includes the overall conceptualisation of gamification. Section 2.8 summarises the theoretical approaches that drove the remainder of this research.

2.1 Information Security

2.1.1 Definition of Information Security

Information security refers to the protection of data and information systems against illegal access, use, disclosure, interruption, alteration, or destruction in order to maintain confidence, integrity, and accessibility [1]. Additionally, information and system security refers to the protection of data and systems against unauthorised access, use, disclosure, interruption, alteration, or destruction in order to maintain confidentiality, integrity, and availability. InfoSec measures must be implemented carefully to safeguard an organisation's information resources, as well as its reputation, legal status, staff, and other tangible or intangible assets [2, 1]. Organisations must consider all of these elements when devising countermeasures to protect the security of their data assets. On the other hand, achieving this is difficult, as security breaches occur via various sources and channels. These include negligence or ignorance, out-of-date security measures, malware, spyware, phishing, unauthorised access, spam, and cyber assaults [2].

2.1.2 Security Risks, Vulnerabilities, and Countermeasures

Security risk is described as the potential to cause damage to computer systems and organisations. The source could be physical, such as a computer with critical data being stolen. Non-physical causes, such as virus infection, are also possible [3].

Human errors are the biggest weakness that information technology faces. Parsons et al. concluded that the primary source of InfoSec breaches is human error caused by a lack of security awareness and knowledge [4]. Additionally, it is believed that over half of all security breaches are triggered indirectly or directly by employee noncompliance with InfoSec procedures [5]. This necessitates a rethinking of existing techniques for employee education to address human error, which is the primary source of security breaches in companies. Recent catastrophic password breaches were discovered months after the fact, as seen in Table 2.1.

Table 2.1 Compromised passwords attacks [6]

Target	Attack Date	Passwords Revealed Date	No. of Passwords Compromised
Yahoo	2013	October 2017	3 billion
Weebly	February 2016	October 2016	43 million
Dropbox	2012	May 2016	68 million
MySpace	2008	May 2016	360 million

2.1.3 Information Security in Organisations

Employees play a crucial role in enhancing InfoSec [7]. Their understanding of risk can have a positive influence on the improvement of InfoSec behaviours [8]. The term ‘security is critical’ is one that all computer users should be familiar with. Due to the rapid development of internet technology, computer users play a critical role in making cyberspace a safer environment for everyone.

Yet, an essential prerequisite for secure behaviour is that people know what it is they have to do and how to do it; in other words, they possess the required *knowledge* and *skills* (know-how). While awareness drives and training are undeniably valuable and essential, the most powerful way to ensure that all employees gain the requisite knowledge and know-how is to encourage and facilitate KS across the organisation [9]. Moreover, today, internet technology is so ubiquitous that it serves as the backbone of contemporary life, allowing regular employees to buy, socialise, and be amused through their personal or work computers. As employees' dependence on the internet rises, so does the likelihood of hacking and other security breaches.

KS, of all types, improves the organisation as a whole. It facilitates trust between employees [10-12]. Of particular interest in this paper is *information security* knowledge sharing. KS improves information security awareness, which is important when it comes to preventing security breaches [13]. Organisations should therefore facilitate and engender KS. The aim is to make the knowledge accessible to all of those who need it and ultimately to improve InfoSec across the organisation.

We now review the core concept of 'knowledge' and discuss the kinds of knowledge that could be shared in the InfoSec context. We then report on the systematic literature review we carried out in order to gain insight into the research conducted on KS in the InfoSec context (Section 3). Section 4 presents the findings, Section 5 reflects, and Section 6 concludes.

2.2 Information Security Awareness (ISA)

ISA can be described as "a state where users in an organisation are aware of ideally committed to their security mission" [14]. According to Abawajy, ISA may be described as users' understanding of the critical nature of information security best practices [15]. Employees, in general, have different degrees of security knowledge within an organisation [15]. Several studies have contended that employees' ISA is among the most significant elements for achieving the objectives of information security in organisations [16, 17, 14]. It offers significant insights into how to enhance employees' awareness of security policies to mitigate risk [14, 18]. There have been multiple approaches to increasing employees' awareness through traditional training programmes [19]. According to Thomson and von Solms, programmes are most commonly delivered via presentations, workshops, and multimedia packages, email reminders and screen savers [14]. Moreover, Bauer and Bernroider implemented an action programme to raise ISA associated with phishing, password security and clear screen policies [16]. Consequently, Puhakainen and Siponen argued that there are two requirements to ensure a security training programme is effective [20]. The first must provide theoretical clarification of why and who the programme works for. The second requirement, the theory, must deliver guidelines for how effective training is to be delivered in the workplace [20]. Bada et al. agreed that considering how employees perceive risks is critical to inspiring effective awareness [21].

Enhancing employees' technology expertise is a significant precursor of ISA [22]. Information knowledge refers to understanding the fundamental information technology applications used in daily business, such as computers, email systems, and the internet. The level of general IT knowledge of employees positively affects their ISA [22]. Employees who are more knowledgeable about information security and information technology will be more aware of information security issues [23]. Thus, organisations are recommended to improve their employees' IT skills to avoid them from engaging in unintentional non-secure behaviour. Mejias confirmed this, stating that the constructs of technical expertise, organisational influence, and attacker assessment all had significant connections with ISA [24]. Intriguingly, corporate influence and attacker evaluation were associated with ISA more strongly than technical knowledge [24].

There is strong evidence that security awareness training is the most cost-effective method of securing an organisation [25]. Many experiments have sought to determine the degree of awareness of a phishing assault after training. The findings indicated that the training was successful since the number of individuals falling for the phishing scam decreased. These findings demonstrate that interactive material may be used to improve levels of awareness. It also implies that the channel through which awareness information is distributed is critical [15].

Puhakainen and Siponen showed that public awareness initiatives may help reduce security risks [20]. After completing a security awareness training session, the researchers discovered that users' use of weak passwords dropped substantially, and their knowledge and compliance with rules continued to increase. Because ISA lowers the frequency and severity of data security breaches, it also reduces the direct and indirect expenses associated with such breaches [15]. Puhakainen and Siponen summarised the extent of IS security training studies from 1985 to 2002 based on the findings, theory, and theoretical orientation of the training [20]. Additionally, as demonstrated in our literature evaluation, we expanded the most successful study based on contributions to the security area, as seen in Table 2.2.

Table 2.2 Review of the IS security training literature

Study	Approaches	Key Findings	Theory Base
Puhakainen and Siponen [20] 2010	Empirical Research	Puhakainen and Siponen argued that there are two requirements to meet the needs of effective security training programmes. The first must give theoretical clarification of why and who the programme is for. The second requirement is that any theory must give guidelines to clarify how effective training is to be delivered in the workplace	Theory of Reasoned Action; Neutralisation Theory
Bauer and Bernroider [26] 2017	Security Awareness Programme Approaches	The bank implemented a programme to raise ISA, which included "phishing, social engineering, password security, secure internet use, and clear screen policies". Then the bank evaluated the intervention via pre- and post-assessment	Universal Constructive Instructional Theory
Bada, et al. [21] 2019	Literature Review: UK and Africa	Considered these challenges from a psychological perspective, determining that how employees perceive risks is critical to inspiring effective awareness	
Safa, et al. [27] 2017	Theoretical Research Model	Identified information security collaboration as a powerful, efficient approach to reducing the risks to information security. Moreover, the researchers confirmed that limited studies have been conducted collaboratively in the information security field within organisations	Theory of Planned Behaviour and Triandis model
Tsohou, at al. [28] 2015	Action Research	According to Tsohou et al., the training and practices for information security awareness programmes focus on content and procedures without considering how the employees interact with the programme in order to make correct security-related decisions	Theory of Planned Behaviour and Triandis model
Vance, at al. [29] 2012	Empirical Test	Observed that many behavioural approaches have overlooked the importance of Protection Motivation Theory (PMT). PMT has a strong effect on employees' intentions to follow information security policies	Protection Motivation Theory and Habit Theory
Mejias, at al. [30] 2014	Theoretical Research Model	This research aimed to establish an information security risk model that aids the comprehension of ISA and the evaluation of ISS risk. According to the researchers, technical expertise, organisational influence, and attacker evaluation contribute significantly to the favourable path coefficients associated with ISA.	Risk assessment model
Choi, at al. [31] 2018	Qualitative Case Study	This research examined the behaviour of organisational insiders, a group responsible for preventing, responding to, and mitigating information security incidents. The researchers identified a collection of perceived components of	Organisational mission statement; knowledge of information

		adequate information security practices among organisational insiders, such as training, awareness of information security events, routines, and policy, to build more successful information security strategies	security incidents.
Ki-Aries, at al. [32] 2017	Empirical Data	This article discusses a method for detecting security-related human factors by integrating personas into the design and execution of information security awareness. The researchers concluded that a persona-centred approach to information security awareness is adaptable to the time and resources needed to execute it in the company and may contribute positively to lowering or mitigating information security risks via security awareness	Persona-centred information security awareness methodology cycle.
Furnell at al. [33] 2018	Empirical Research	This article examines the many types of assistance available and attempts to determine the impact of such support in practice. It provides results from two experimental experiments investigating how differences in password metre use and feedback may have a beneficial effect on the resultant password selections. It is shown that by giving users more detailed information (e.g., the time needed to break a password, relative ranking against other options, or the likelihood of it being broken), users are more encouraged to choose strong password selections and change previously poor ones	Based on theoretical supports from the literature and the practicality of real-world implementation.
Abawajy [15] 2014	Empirical Research	The purpose of this research is to ascertain the most effective technique for delivering security awareness. The researchers used text-based, game-based, and video-based delivery techniques to assess user preferences for information security awareness. According to the research, a combination of distribution techniques is preferable over an individual delivery method for security awareness	They used text-based, game-based, and video-based delivery methods with the aim of determining user preferences. (non-based on theory)

People can gain security knowledge from training programmes [26, 19, 34], from personal experience [11] or from other employees in the workplace [35]. However, approaches of this type of carry with them a variety of well-known limitations, such as the difficulty in determining the effectiveness of such training [35].

One mechanism for improving ISA is for employees to transfer security-related knowledge to other employees [14]. Organisations should implement suitable incentive schemes to foster employee cooperation and promote sharing, it is claimed. Several studies examined the impact of KS processes and discovered that a well-developed cooperative theory enables effective information sharing, knowledge application, and informal KS [36, 37]. In the following sections, we will discuss information SKS and its role in general terms.

2.3 Knowledge Sharing

Employees collaborate in many ways to facilitate KS [38, 39]. Safa et al. [27] identified information security collaboration as a powerful and efficient approach to reducing the risks associated with managing information security. Moreover, the researchers confirmed that limited studies have been conducted collaboratively in the information security field as it pertains to organisations. Tsohou et al. [27] observed that several studies have explored the organisational and individual aspects to enhance ISA.

As KS gains strategic importance within companies and institutions, these firms have begun implementing a variety of KM initiatives [40]. Several basic elements in KS activities have been identified, including knowledge acquisition, collection, selection, organisation, implementation, sharing, and creation [41]. KS is seen as a key component of effective knowledge management [42].

2.3.1 Knowledge and Information Security

Knowledge is gained when meaning is added to information. People can gain knowledge from their environment [43] or from personal experience [44]. In the information security context, people can gain knowledge from training drives, but are more likely to gain the knowledge they need from other employees in the workplace.

Knowledge can be either tacit or explicit [10]. The former refers to skills that cannot easily be recorded or expressed, which makes it difficult to share and retain [45]. It is important for employees to transfer tacit security-related knowledge to other employees – to externalise it [46]. Explicit knowledge can be expressed in numbers and words [47] and can be recorded. Knowledge delivers the most value when it is linked to other relevant and pertinent knowledge, thereby conveying new knowledge, a process called ‘combination’ [46].

2.3.2 Information Security Knowledge

Bartnes et al. (2016) define information security as a set of strategic management processes, policies and tools necessary for preventing, detecting, documenting and countering threats that subject non-digital and digital information systems to risks that cause damage such as loss of information and information theft [48]. Flores et al. (2014) define KS as the explicit or tacit transfer of values, experience, expert insight and contextual information from one person to another which helps that person to incorporate and evaluate new information and experience [46]. Stanton et al. suggest a two-dimensional model of end-user security behaviours [49]. The first is expertise and the second is intention. We focus on benevolent intentions. In this category, people without knowledge make naïve mistakes, but knowledge leads to awareness and security assurance. Parsons et al. conclude that human errors attributable to lack of security awareness and knowledge are the principal sources of information security breaches [4]. Using HAIS-Questionnaires and incorporating a sample of 500 employees, the authors gauged employees' awareness levels and came to the conclusion that employees with poorer security awareness subjected their organisation to security breach risks [4]. As a recommendation, the authors identified a holistic approach to employee training that emphasises knowledge and attitude as the way forward towards counteracting this problem. However, Zhang argued that knowledge expires in this field, and needs to be renewed [50]. Moreover, Junger et al. showed that warnings, by themselves, do not necessarily make that much of a difference to susceptibility to social-engineering attacks [51]. Gcaza and von Solms argued that cultivating a cyber security culture, which implies that KS has become *de rigueur*, is the best approach for addressing human factors in information security [52].

2.3.3 Information Security Knowledge Sharing

Kim and Kim showed that social pressure influences compliance intention, and that compliant behaviour is influenced by knowledge [53]. KS is crucial in the information security arena [53].

Safa and von Solms explored the process of information security knowledge sharing in organisations [54]. They discovered that "earning a reputation and gaining promotion" and "external motivations" had a positive influence on KS. Mermoud et al. reported that people would share knowledge if they expected to get something valuable in return; reciprocity was deemed to be important [9]. They suggest that organisations incentivise rather than mandate sharing.

Safa et al. aimed to deliver an insight into the phenomenon of information security knowledge sharing [27]. They combined Motivation Theory and the Theory of Planned Behaviour to deliver a knowledge sharing module [54]. Dixon discovered that trust was a barrier to KS [13]. Dang-Pham et al. aimed to find out why people provided information security advice to others [10]. They discovered that the primary barriers to sharing security knowledge were behaviour and trust. Rocha Flores et al. examined the impact of cultural factors on SKS [55]. The results show that national and cultural factors are worth considering when it comes to the nature of sharing [55]. They concluded that the most critical barrier to sharing security knowledge was cultural. Feledi et al. examined the efficiency of cooperation between participants during the process of KS [43]. They identified the primary barrier to sharing security knowledge as a lack of motivation on the part of employees.

2.4 Overview of Factors Influencing SKS

The first publication, which was a systematic review, focused on factors affecting SKS, the theory in this field, geographic scope, and methodologies utilised in previous studies.

2.4.1 Factors Affecting SKS

Several studies addressed the advantages of KS in the organisation, especially in the security awareness domain. Hawryszkiewycz and Binsawad described barriers impeding KS [56]. They identified more than 160 barriers and determined that the most significant barriers are: lack of a motivation, lack of trust, lack of incentive and reward systems, lack of organisational culture, lack of leadership, lack of technical support, and insufficient technology infrastructure [56], as seen in Table 2.3 and Figure 2.1.

Table 2.3 Factors influencing knowledge sharing

Factors	Tested and evaluated	Key Findings
Trust	[57], [58], [13], [56], [59], [60], [61], [51], [62].	The recurring theme in these studies is a lack of trust among employees due to a lack of experience, qualifications, and relationships to foster trust. The significance of trust is that it is built on expertise. Competence-based trust refers to a relationship in which one person feels the other is knowledgeable about a particular area.
Attitude	, [58], [59], [60], [53], [63].	Employee attitudes toward information sharing are favourably influenced by knowledge self-efficacy and feedback, but losing face has a negative impact. Furthermore, it has been discovered that one's attitude toward information sharing influences one's willingness to share knowledge, influencing one's knowledge sharing behaviour.
Culture	[57], [59], [63], [53].	Several studies looked at the behaviour of those studying KS to disseminate knowledge. Most of the studies adopted the theory of planned behaviour to predict and understand human behaviour. Therefore, employee cohesiveness enhances their propensity to collaborate, making it critical for collaborative behaviour to occur during the workday.
Motivation	[13], [57], [60], [63], [64], [9] [62].	There are two types of motivation: extrinsic and intrinsic. ***Extrinsic***: many results indicate that incentives have a limited influence on 'engagement' (present activity) and a negative impact on 're-engagement' (persistence). ***Intrinsic:*** changing human behaviour without external influence. There are limited studies focusing on intrinsic motivation to change the actual behaviour of humans.
IT Application	[57], [63], [64], [65], [62].	Most of the findings agreed with the need to offer an effective system to facilitate communication in the workplace. The provision of an electronic knowledge repository to record information security incidents that offer high-quality knowledge is advised to manage and reuse the knowledge.
Organisational Leaders	[57], [63], [64].	In managing knowledge throughout businesses, leadership is critical. Knowledge management initiatives might fail if top managers provide insufficient or incompetent assistance. Generally, leadership studies have not focused on leadership as a knowledge management facilitator. On the other hand, recent research has stressed the relevance of leaders in knowledge management.

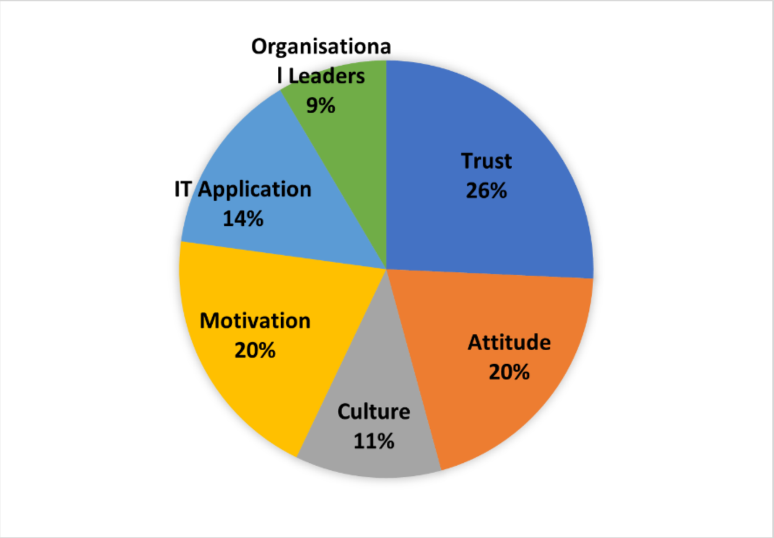


Figure 2.1 Factors impacting knowledge sharing in the reviewed papers

2.4.2 Theories mitigating the barriers of SKS

Different theories have been proposed to explain KS in information security. However, the Theory of Planned Behaviour has proved to be the most influential. The theory revolves around the idea that an individual's attitude is a predictor of their intentions and behaviour, as seen in Figure 2.2.

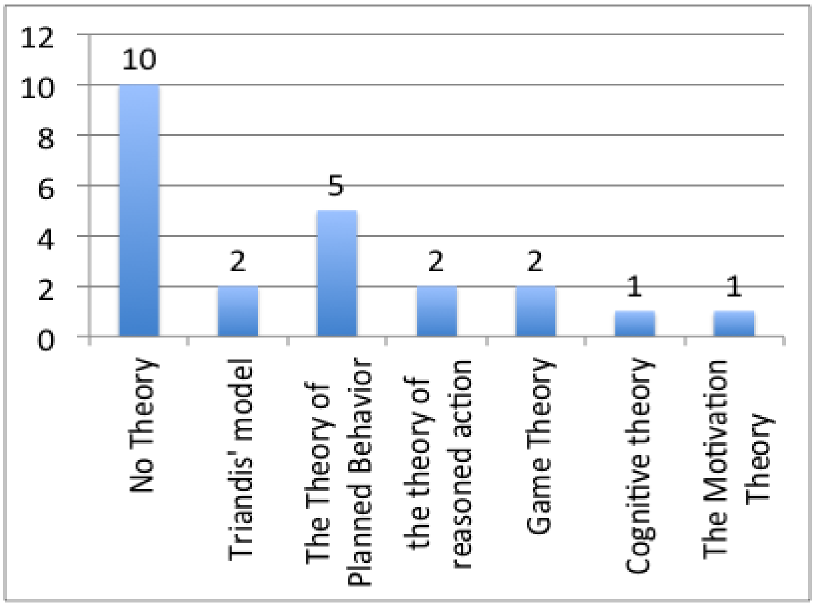


Figure 2.2 Theories used in the reviewed papers

2.4.3 Geographic Scope

Different investigations into KS in information security have been conducted in various parts of the world. The Asian continent, with 41%, coverage, has experienced the highest number of studies. Europe comes in second with 27% of studies. The North American region comes in third with 18% coverage; both Australia and Africa benefitted the least from studies related to KS in information security. Australia gained coverage of 9%, while the African continent only had 5% coverage.

2.4.4 Methodologies

In the methodology section, it was noted that survey and literature review conceptual models were the most common techniques for examining KS in information security. The survey technique involved questioning participants and obtaining their views on the topic. Some surveys were structured, with others being unstructured. Participants would choose either self- or group-administered questionnaires. The literature review conceptual model entailed investigating existing theoretical studies into KS in information security, as seen in Figure 2.3.

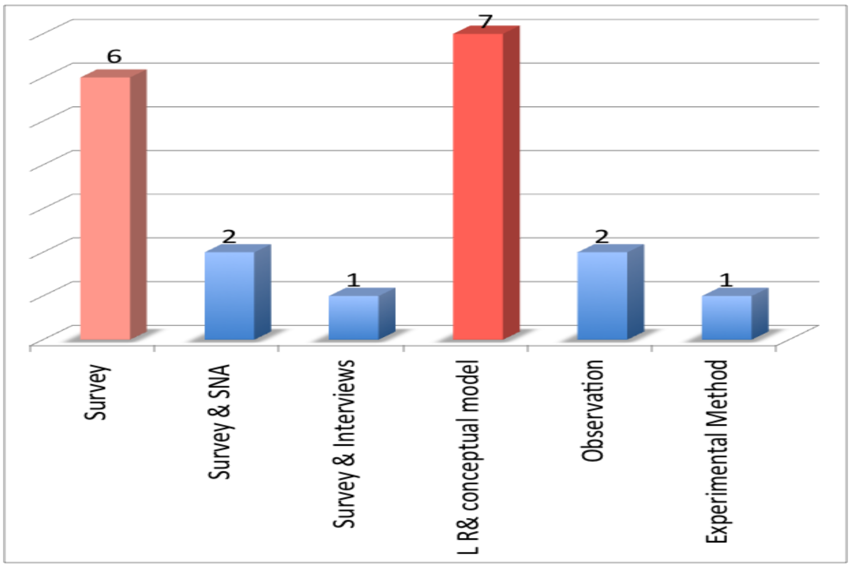


Figure 2.3 Deployed methodologies used in reviewed papers

2.4.5 Summary of Knowledge Sharing Barriers

KS has a proven positive influence on security awareness among employees. We wanted to confirm the importance of SKS and show how its influence on employees in the workplace led to enhancing resilience to cyber-attacks.

The current study identified advantages of KS in an organisational setting, especially in terms of individual security awareness. Hawryszkiewycz and Binsawad described the impact of barriers deterring KS [56]. The results of our study indicate that trust, motivation and culture are powerful barriers to KS. Most of the studies did not propose effective solutions to mitigate these barriers.

Another important finding was that the studies we reviewed used only a handful of different theories. In discussing its significance to KS, the theory proved to be more comprehensive in providing logical reasoning. Ideally, it could be argued that an employee’s cognitive state would influence them in deciding whether to participate in knowledge sharing or not. This result may be explained by the fact that the researchers focused on the theories related to the individual, such as the Theory of Planned Behaviour. The researchers neglected theories that address barriers, such as Trust Theory.

Additionally, what is surprising is that the Asian continent, with 41% coverage, has experienced the highest number of studies investigating how KS is achieved in the corporate sector. A possible explanation for this might be that the Asian continent has high levels of security risk which leads to more consideration of security and attempts to enhance employee awareness.

The most interesting finding was that, in the methodology section, survey and literature reviews dominated the literature. The survey method does not deliver in-depth analyses of human behaviours. Surprisingly, only one study was found that used interviews or focus groups to understand the barriers affecting SKS. This is surprising, since observation, surveys, and interviews are the most powerful techniques for delivering comprehensive insights that would allow for the best understanding of KS in natural environments. Such methods have the advantage of allowing more transparency in noting down real-time data based on direct or indirect interaction between the researcher and the participants.

Safa et al. set out to investigate an effective model that can reduce the negative impact of the human factor in information security [66]. In the end, the outcomes of the analysis reveal that information security knowledge sharing, experience, and collaboration have a positive impact on employees' will to comply with information security guidelines.

The previous discussion identified the importance of the organisation's incentive processes in encouraging KS in the information security context. Moreover, the role of trust was highlighted, which suggests that an organisation that suffers from a lack of trust might well experience more security incidents because employees do not share knowledge. When we consider the fact that hackers extensively and actively share knowledge [50], we have to pay attention to fostering and encouraging sharing within organisations.

Based on this, it is essential to find a new way to expand the literature review by applying the collaboration model to enhance the sharing knowledge in organisations. There are many steps to prove the efficacy of the model in the security field, before testing the model as a theoretical framework and empirical evaluation.

In the above sections, we reviewed studies that focused on the impact of SKS, the relationship between KS and information security, and barriers to SKS. We confirmed that SKS increases employee awareness, mitigates risks, improves decision-making, and improves efficiency in the workplace [4, 67]. However, many factors affect SKS, such as trust, motivation, and attitude. Researchers should investigate how a more effective sharing mechanism can be formulated, specifically to address those factors and thereby achieve improved KS across organisations. Based on the recent study reported by Mermoud et al., the role of incentivisation should also be explored [9].

In the next section, we will focus on collaboration theory, mitigating those challenges and improving the SKS in the enterprise.

2.5 Information Security Collaboration

Collaboration involves working together to achieve an objective. In particular, the goal is to facilitate and motivate mechanisms of KS to promote such sharing [38, 27]. Safa et al. identified information security collaboration as a powerful and efficient approach to reducing the risks associated with managing information security [27]. Moreover, the researchers confirmed that limited studies have been conducted collaboratively in the information security field as it pertains to organisations. Tsohou et al. observed that several studies have explored the organisational and individual aspects to enhance ISA [28].

According to the literature review, organisational culture has a significant role in shaping formal and informal knowledge processes. However, research indicates that informal networking is not a preferred mode of coordination compared to more formal coordination methods [68]. Newell and Galliers emphasise the importance of social networks and informal conversation in transmission and learning regarding knowledge in practice [69, 70]. Thus, networks within organisations must be fostered to develop a culture of sharing [69, 70].

2.5.1 Transactive Memory System (TMS)

TMS has been described as "a set of individual memory systems in combination with the communication that takes place between individuals" [71]. A TMS determines the specific division of cognitive labour within a group of people, as a means to facilitate encoding, storage, and retrieval of knowledge pertaining to various domains. When a TMS is being utilised, each group member is aware of "who knows what, and who knows who knows what" [36]. Simply put, the characteristics of a TMS mean that three crucial qualities, common to other types of socially shared cognition, are absent – i.e., differentiated knowledge; processes of transactive encoding, storage and retrieval; and the dynamic nature of TMS functions [72]. Thus, an alternative and more suitable approach might involve a shift of focus away from repositories towards processes [73]. Lehner and Maier summarised the current status of the relationship of TMS-related terms to each other [74], as seen in Figure 2.4. Additionally, they developed a conceptual model of TMS development in an intragroup context: consideration of team identification mechanism [75], as seen in Figure 2.5.

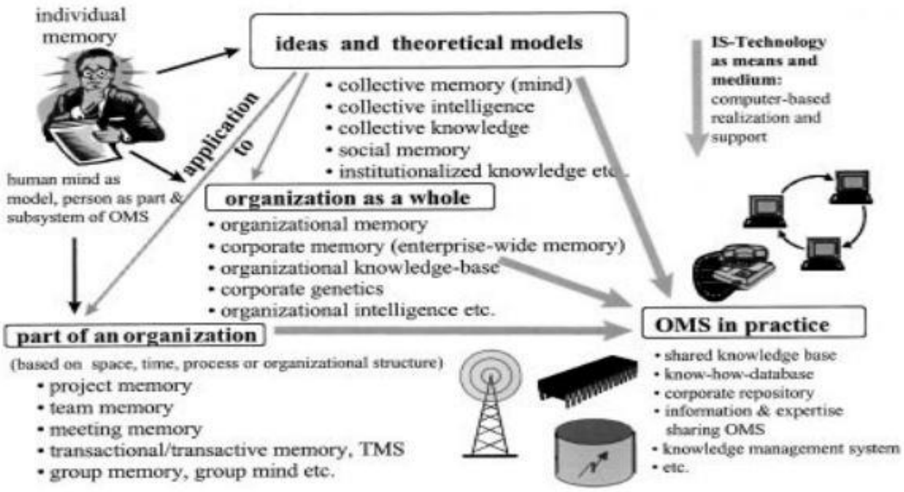

individual memory
ideas and theoretical models
• collective memory (mind)
• collective intelligence
• collective knowledge
• social memory
• institutionalized knowledge etc.
IS-Technology as means and medium: computer-based realization and support
application to
human mind as model, person as part & subsystem of OMS
organization as a whole
• organizational memory
• corporate memory (enterprise-wide memory)
• organizational knowledge-base
• corporate genetics
• organizational intelligence etc.
part of an organization
(based on space, time, process or organizational structure)
• project memory
• team memory
• meeting memory
• transactional/transactive memory, TMS
• group memory, group mind etc.
OMS in practice
• shared knowledge base
• know-how-database
• corporate repository
• information & expertise sharing OMS
• knowledge management system
• etc.

Figure 2.4 Relationship between TMS-related terms [74, p.294]

Liang, Moreland, and Argote described three aspects of TMS: specialisation, coordination, and credibility [76]. Moreover, Argote et al. identified four distinct stages of organisational learning: search, knowledge production, knowledge retention, and knowledge transfer; they provide studies on experience and corporate environment factors on learning processes and results for each function [77]. Additionally, task assignment is enhanced as when members are aware of the tasks, they excel in them. Problem resolution is also facilitated as members are aware of whom to contact for assistance [77].

2.5.1.1 Specialisation

Specialisation is the term used to describe the degree of differentiation of the knowledge held by team members [76]. Specialisation reduces the cognitive burden on community participants by allowing each to focus on his or her own area of expertise. It urges members to prioritise information integration through different domains in order to maximise team knowledge use [78]. Moreover, differentiated group knowledge results in specialisation within the team, resulting from the team's knowledge duties being divided. While expertise variety is a feature of the original team composition, specialisation occurs when team members collaborate and relates to task-specific knowledge obligations. Expertise diversity is different from the knowledge specialisation components of TMS structures in that it represents the breadth of each team member's abilities, knowledge, and training before their collaboration [79].

2.5.1.2 Coordination

This describes the efficiency of the team in terms of knowledge processing while working together to enhance the coordination of information within teams [80]. Moreover, coordination is a team process that entails the coordination, behaviour patterns, and skills among team members in order to achieve shared objectives [81]. Zhong et al. confirmed that improved coordination and collaboration would increase task performance [82].

2.5.1.3 Credibility

Credibility is the way in which individual team members perceive the reliability of the knowledge held by the other members of the team [83, 76].

As Lewis asserts, these three variables "reflect transactive memory itself, as well as the cooperative processes illustrative of transactive memory use" [78, 84]. Davison et al. [37] argue that TMS facilitates KS, leading to improved team creative performance via team creative efficacy. Our premise is that organisations should facilitate and engender SKS by removing the challenges that prevent SKS, i.e., "specialisation, credibility and coordination" [83]. The aim is to make security knowledge accessible to all of those who need it and ultimately to improve security awareness across the organisation. Our first qualitative study delivered insights about which factors impact SKS, and we are able to align these factors to the core tenets of TMS theory.

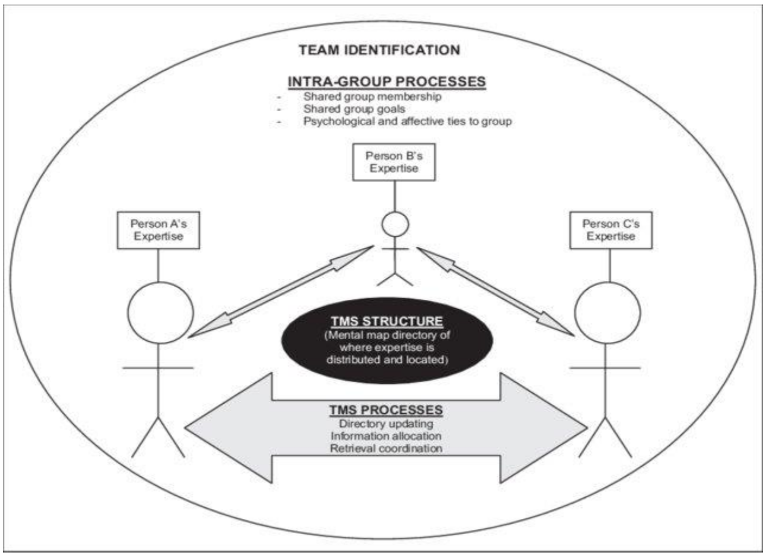


Figure 2.5 A conceptual model of TMS development in an intragroup context: Consideration of team identification mechanism [75, p.211]

2.6 Intrinsic Motivation

Motivation is the most autonomous type of motivation. It refers to an innate need shared by all humans to seek novelty and challenges, expand, and exercise their skills, and explore and discover [85]. Regarding the area's significance of theory, there are several academic fields in which reward management may be theorised, for example, economics [86], password manager [87], and information security policy compliance [88]. However, the study of psychology has probably had the most effect. This effect results from motivation's essential role in assisting in the understanding of employee performance and reward. Indeed, the basis is one of psychology's oldest ideas, and we depend on established theories to help us understand how it appears in the workplace [89]. Thus, examining a theory of human motivation seems to be an appropriate place to address the present study goals.

There are two types of motivation: extrinsic and intrinsic. Many results indicate that incentives have a limited influence on 'engagement' (present activity) and a negative impact on 're-engagement' (persistence). Intrinsic motivation changes human behaviour without an external force, such as SDT. Extrinsic motivation is the pursuit of a specific goal, such as a reward system; for instance, assume that an employee who enjoys reading for pleasure is rewarded for completing the reading in a certain amount of time. An example of extrinsic motivation is protection motivation theory (PMT), which describes the risk and response evaluation and cognitive resolution process of behavioural change.

One of the essential theories used in the previous study is PMT. Vance et al. [29] observed that many behavioural approaches have overlooked the importance of PMT. Moreover, PMT indicates that one's previous behaviour significantly affects how one evaluates dangers and one's ability to respond to them. PMT is composed of three components that describe how threats are perceived: these components are referred to as threat appraisal elements. These include rewards or benefits (any extrinsic motive for growing or maintaining an undesirable behaviour), severity (the threat's size), and vulnerability (the extent to which the individual is perceived to be susceptible to the threat) [29].

Previous research has recognised the significance of studying the human motivating factors that promote or inhibit information sharing behaviours, and many studies have conducted in-depth examinations of these problems in a variety of settings [90]. The core of SDT is that individuals may be motivated to perform certain behaviours both externally and internally.

Deci, a social psychologist, and Ryan, a clinical psychologist, have spent the last three decades pioneering the creation of SDT, a theory of human motivation and development that elucidates the fundamental principles underpinning sustained motivation [91].

According to de Charms [92] and Deci and Ryan [91], intrinsic motivation works by motivating an individual through their own natural interest in activities that are new or challenging. With intrinsic motivation, there is no need for the individual to be rewarded for their behaviour [93, 91]. In fact, there is a natural desire to learn; people have an innate wish to master something, learn something new through interest, or to explore, and this is the driver to learn throughout life [93, 91].

Self-determination theory utilises traditional empirical methods to describe human personality and motivations through in-depth examinations of these problems in a variety of settings [90]. The core of SDT is that individuals may be motivated to perform certain behaviours both externally [85, 90]. Despite many developmental phases, the dynamic connection between the individual and the social environment in the context of psychological need satisfaction has been a primary emphasis of the theory throughout its history [94, 95].

In SDT, three key human needs must be met: autonomy, competence, and relatedness [95]. Studies have shown that when these three core needs are satisfied, individuals are more likely to take part in and exhibit better performance on an activity [62, 96].

2.6.1 Autonomy

Autonomy refers to when individuals act in their own interests and ideals; the feeling of having choice over behaviour [97]; and feeling like the initiator of one’s own activities. There is a need for autonomy, which is a person’s wish to organise their own actions [85]. According to Deci et al., autonomy support is when a person in a position of power considers the viewpoint of others, recognises their emotions, and gives relevant information, reasoning, and opportunities for choice [98].

2.6.2 Competence

Competence is the knowledge of how to engage effectively with one’s surroundings and the conviction that one can affect significant outcomes [97], and the need for a sense of competence, which is when a person desires self-efficacy [85]. According to Deci and Ryan, individuals with a desire to engage successfully with the environment feel competent in generating desired results, and in order to avoid undesirable occurrences, competence is needed [95].

2.6.3 Relatedness

The need for relatedness encompasses the following: creating a sense of mutual respect and dependence [97], and the need for relatedness, i.e., a person's wish for the support and feelings of connection with others around them [99]. Deci and Ryan asserted that relatedness entails a feeling of belonging or a sense of connection to a particular social environment [95].

Overall, SDT proposes that the most self-determined kinds of regulation will drive behaviour when needs are met. In comparison, poor self-determination is a result of the three fundamental requirements being violated [98]. Additionally, SDT states that differing levels of psychological demand satisfaction within a field will have various cognitive, emotional, and behavioural impacts [95]. Moreover, Frank and Ament (2021) conducted empirical research on implementing methods to increase people's awareness of possible cybersecurity threats via sharing information security incident experiences among employees. According to the findings of a study of 385 respondents, intrinsic motivators such as increasing cooperation with colleagues increase employees' sharing behaviour. Extrinsic motivators, on the other hand, such as monetary incentives or promotion possibilities, have the reverse effect [100].

As a consequence, the thesis adopted the SDT as an intrinsic motivation to change human behaviour. To apply SDT to empirical research, the idea was to implement education games that use gamification elements. Moreover, we applied SDT dimensions to the gamification elements.

2.7 Educational Games

Educational games have become recognised as a powerful teaching tool with the potential to result in an "instructional revolution" [101]. The principal reason for this is that game-based education enables employees to learn through experience and the utilisation of a virtual environment while motivating them to think critically and problem-solve [93, 101]. Moreover, Security Games (SGs) give employees the opportunity to enjoy learning and to collaborate, as the games comprise a form of intrinsic motivation [102]. According to Dixon et al., SGs have led employees to engage with and enjoy learning, as they anticipate a smooth, agreeable and straightforward experience [103]. Recent evidence suggests that one of the primary causes seems to be a lack of user awareness about phishing risks. Our study indicates that user security education may be accomplished via both theoretical and practical knowledge. Future studies should combine procedural and conceptual understanding to create a well-designed strategy for user security education. For instance, the interaction impact of procedural and conceptual knowledge may be addressed via the development of educational games, web-based training materials, contextual training, and embedded training to enhance users' capacity to detect and avoid phishing assaults [104]. Moreover, Aladawy et al. agreed that creating a serious game that teaches individuals how to defend themselves against social engineering by utilising the defence mechanisms of social psychology is a useful strategy [105, 106]. An empirical evaluation of the game reveals that it can enjoyably boost awareness of social engineering. These studies further support the idea of using text-based, game-based, and video-based delivery techniques to assess user preferences for information security awareness. According to the researchers, a combination of distribution techniques is more preferable than an individual delivery method for security awareness [105, 106].

2.7.1 Gamification

Gamification is a term that refers to the process of creating systems, services, organisations, and activities in such a way that they may replicate the experiences and motivations found in games, with the additional aim of influencing employees' behaviour [107]. Games are particularly well known for their capacity to engage and excite. When individuals play games, they often feel mastery, competence, pleasure, immersion, or flow, all of which define characteristics of intrinsically driven human behaviour [108, 109].

Due to high-frequency communication, idea sharing, and reciprocity, gamification elements such as groups, messages, blogs, links to social networks, and chat may provide players with a stronger level of connectivity and connection [110, 111]. Moreover, on a structural level, gamification consists of three major components [112]. The affordances added to a system or service result in psychological outcomes; these exciting experiences result in behavioural outcomes – i.e., the activities and behaviours that gamification attempts to support and motivate [108], as seen in Figure 2.6.

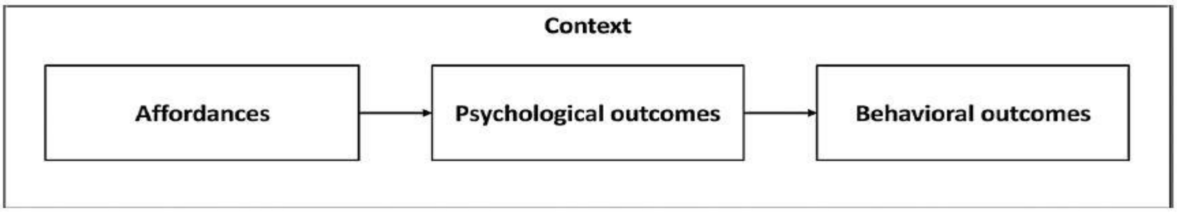


Figure 2.6 Overall conceptualisation of gamification [112, 108]

Game-based delivery techniques may be a helpful complement to or substitute for more conventional forms of awareness. To produce engaging training experiences, the online games integrate visuals, gameplay, and training ideas. The advantage of using a game-based approach for delivering attention is that it may challenge, motivate, and engage players. Gamification is a highly interactive delivery technique that may promote organisational security awareness goals while engaging ordinary users [113].

Several approaches for delivering security awareness via games have been tried in the past. Cone et al. described CyberCIEGE, defined as a flexible, highly interactive video game that may meet corporate security training goals while engaging ordinary users in an exciting security adventure [101]. Preliminary findings suggest that the game may be a helpful supplement to programmes teaching essential information awareness to general computer users [101]. Moreover, Hart et al. evaluated the game Riskio and found that it can help raise players' awareness of cybersecurity concepts [106].

Table 2.4 provides a summary of recent publications on cybersecurity awareness training based on games, showing the positive impact of those games.

Table 2.4 Summary of cybersecurity awareness training based on games

Study	Approaches	Key Findings	Theory Base
Aladawy, et al. [105] 2018	Empirical Research	The researchers developed a serious game that teaches individuals how to defend themselves against social engineering by using social psychology's defensive mechanisms. Empirical assessment of the game indicates that it is capable of entertainingly raising awareness of social engineering.	Non
Hart, et al., [106] 2020	Empirical Research	This article presents Riskio, a tabletop game aimed at increasing cybersecurity awareness among non-technical employees in organisations. Riskio creates	Constructivism learning theory

		an active learning environment in which users gain information about cybersecurity assaults and defences by taking on both attacker and defender of fictional organisation’s vital assets. Evaluation revealed that Riskio might help raise players’ awareness of cyber security concepts.	
Arachchilage and Love [104] 2014	Empirical Research	One of the primary causes seems to be a lack of user awareness about phishing risks. Our study indicates that user security education may be accomplished via both theoretical and practical knowledge. Future studies should combine procedural and conceptual understanding to create a well-designed strategy for user security education. For instance, the interaction impact of procedural and conceptual knowledge may be addressed via the development of educational games, web-based training materials, contextual training, and embedded training to enhance users’ capacity to detect and avoid phishing assaults.	Technology Threat Avoidance Theory
Cone et al., [101] 2007	Empirical Research	Numerous training methods fail because they are repetitive and do not push users to consider and apply security principles. CyberCIEGE is defined as a flexible, highly interactive video game that may meet corporate security training goals while engaging ordinary users in an exciting security adventure. Preliminary findings suggest that the game may be a helpful supplement to programmes teaching essential information awareness to general computer users.	Non
Info Secure Ghazvini and Shukur 2018 [114]	Empirical Research	The aim to improve ISA in the healthcare sector. The game covers various subjects, including phishing, online use, harmful programming, and password security. Employees found the game to be engaging and enjoyed playing it. The assessment indicates that employees' ISA levels rose significantly as a result of playing the game. Additionally, employees demonstrated a desire to engage in ISA training due to their enjoyment of the game.	Non
Lindberg 2016	Literature Analysis	The goal was to investigate the relationship between game components, users, and	Non

[115]		risky behaviour (context) to determine whether game aspects had a good or bad impact on users in different situations. The researchers achieved this via a literature review and the collection of research that used a gamified approach. This study discovered limited study and empirical research on gamification and security.	
Gjertsen et al. 2017 [116]	Empirical Research	Investigated the possibility of using gamification mechanics to improve motivation and learning results in this setting via SDT. Based on interviews with security experts and a workshop with ordinary workers at two companies, the researchers created an interactive ISA prototype application. The findings showed that gamification has promise for application in SAT training, particularly in regions where existing ISA initiatives are ineffective. Additionally, the researchers highlighted the lack of high-quality studies on the actual impacts of gamification at the moment.	Self-Determination Theory
Aladawy et al 2018 [105]	Empirical Research	The researchers created a serious game that uses social psychology defensive mechanisms to teach individuals how to protect themselves against social engineering. According to our game's empirical assessment findings, the game can enjoyably raise social engineering awareness.	Social Psychology
Puzzle game Alotaibi et al. 2018 [117]	Empirical Research	The paper discusses the design of two mobile games being created to raise awareness about cybersecurity. Two critical elements of cybersecurity are included in the games created in this study: strong password generation and virus prevention. Both the Password Protector and Malware Guardian games are well-designed, with an emphasis on usability. The pre-and post-study survey analysis for both games revealed substantial increases in the participants' knowledge of password and malware awareness.	Non

2.8 Summary of the Related Work

Firstly, the thesis sought to improve the ISA among employees. We observed that there have been other approaches to improving security awareness. These have generally been based on individualistic models (considering an individual in isolation). Our proposal is to use a more collaborative model to improve security awareness, such as KS. As seen in Table 2.3, we found several factors that prevent KS [122, 123, 66]. Moreover, our literature review revealed that information security KS generally uses a specific limited number of theories, such as the Theory of Planned Behaviour and Theory of Reasoned Action, as seen in Figure 2.2 [121].

We thus consider using the lens offered by TMS in order to understand and encourage SKS. TMS has been used in other contexts to model KS between employees [84]. Moreover, researchers in information retrieval have adopted the individual experience directory of TMS to gain access to the data usage of IT-based expertise information [125]. Thus, this study selected the TMS to model the dissemination of security knowledge in organisations. Choi et al. argued that KS activities have features that support specific communication and collaboration practices to facilitate team-related TMS [36]. Yet TMS only describes existing KS within organisations; our interest is also in encouraging such sharing. We thus propose incorporating the core tenets of SDT into our model as well, in order to enhance SKS. Furthermore, Tsohouet al. confirmed that there are limited studies examining security awareness at both levels (organisational and individual level) in terms of having effective information security awareness programmes [28]. Moreover, it is claimed that organisations should implement suitable incentive schemes to foster employee cooperation and promote sharing [36]. Several studies examined the impact of TMS on knowledge processes and discovered that a well-developed TMS enables effective information sharing, knowledge application, and informal KS [36, 37]. According to Vance et al., prior work in an organisational setting has focused on employees' compliance with security procedures [29].

Moreover, the most recent studies reviewed show positive results for using gamification techniques as a tool for training. Sharif and Ameen have shown an increased interest in-game as security training among organisations. Inherently, technological solutions cannot provide real self-defence. Improved employee knowledge of the company's security policy is critical to the effective execution of these rules. Offering training to their employees is a vital job for managers [126]. Furthermore, in recent years, the quantity of computer games has exploded, and game development has risen in importance. Over the past decade, games have grown in popularity for training because they motivate, inspire, and engage players. Additionally, a highly interactive environment may assist organisations in achieving their security awareness objectives by engaging everyday users [103, 127, 126]. However, Gjertsen et al. investigated the possibility of using gamification mechanics to improve motivation and learning results in this setting via SDT. Based on interviews with security experts and a workshop with ordinary workers at two companies, the researchers created an interactive ISA prototype application. The findings showed that gamification has promise for application in SAT training, particularly in regions where existing ISA initiatives are ineffective. Additionally, the researchers highlighted the lack of high-quality studies on the actual impacts of gamification at the moment [116]. The next chapter discusses the research methodology, which describes the research technique and strategies used to achieve the research aim and objectives.

We propose a collaborative model to consider organisational and individual factors to mitigate the challenges. We test and validate the model in the following chapters.

Chapter Three: Methodology

This chapter presents the research approach and strategies and clarifies the reasons for selecting these to achieve the study objectives. The chapter begins by describing the different broad methodological approaches which help to meet the objectives of the research.

3.1 Research Philosophy

Research philosophy is characterised as the creation of new knowledge and the essence of knowledge [128]. A research technique is a methodical approach to answering questions, solving problems, finding solutions, or gaining experience [129]. Research is a consistent attempt to collect, analyse, and interpret evidence and provide a resolution to a query, solve a problem, and provide evidence [130]. According to Rajasekar et al., study methodology relates to the methods that researchers use to explain and forecast phenomena [130]. The two main information system research philosophies are positivistic and phenomenological [131]. The research used both quantitative and qualitative assessment methods that have become increasingly common in recent studies.

3.1.1 Quantitative Research

According to Goertzen, approaches to quantitative analysis are concerned with gathering and analysing complex data that can be interpreted numerically in the simplest terms. One of the main objectives is to develop precise and consistent metrics that can be analysed statistically [132].

Quantitative analysis enables researchers to understand more about a population's dynamics, determine how many patrons use a programme or commodity, analyse perceptions and habits, record patterns, and clarify what is understood anecdotally [133, 134]. Frequencies (i.e., counts), ratios, proportions, and relationships are examples of metrics that can be used to calculate and provide proof for the variables listed above [132, 134]. Marczyk et al. assert that quantitative science requires experiments that focus on mathematical data to arrive at their conclusions. Formal and standardised calculations, as well as the use of data, are valuable aspects quantitative study [135].

3.1.2 Qualitative Research

This review provides a brief guide to qualitative studies in social science by illustrating how various forms of qualitative research may theoretically enhance our existing knowledge of social experience via a set of instances. The aim is to demonstrate the advantages of utilising a wider variety of testing methodologies and paying more attention to which methodologies are better suited to providing knowledge about a specific subject [136].

Qualitative study is described as research that does not seek to measure its findings using statistical analysis or description. Interviews and assumptions are popular in qualitative analysis, but no standardised measures are taken. A case study is a type of qualitative analysis that requires an in-depth analysis of one subject. Qualitative analysis is often used to generate hypotheses for a quantitative study [135].

3.2 Methodology Research Approach

To achieve the aims of the research study, as clarified above, there are three different broad methodological approaches to select from: a qualitative approach, a quantitative approach, and empirical research (using qualitative and quantitative methods) as seen in Table 3.1.

Table 3.1 Objectives of the study

Chapter	Stage/Activity	Research Objectives
Chapter 4	**One:** Understanding of challenges: Qualitative semi-structured interviews	What are the challenges of security knowledge sharing to improve security awareness?
Chapter 5	**Two A:** Examination of the scale reliability for TMS (Quantitative survey)	How can information security knowledge be facilitated through the understanding of a TMS?
Chapter 5	**Two B:** Confirm the relationships between the TMS and SDT (qualitative analysis)	How can Credibility and Coordination in a TMS be encouraged via competence and relatedness in SDT?
Chapter 6	**Three:** Implement the instrument: implementation and design	Can security knowledge sharing be modelled using TMS and sharing encouraged by satisfying the SDT needs of employees?
Chapter 7	**Four**: Action research: evaluates the effect of using the app (Mixed method using qualitative and quantitative).	How can knowledge sharing improve security awareness in organisations?

	Four A: Measure the improvement in Security Awareness level pre- and post-intervention (quantitative). **Four B**: Measure the KS pre- and post-intervention (qualitative).	

3.3 Stage One: Understanding Challenges

The first stage is divided into two parts: the interview technique overview, and the justifications for the method. In addition, the methodological approach taken is presented in this stage.

3.3.1 Interview Technique Overview

Semi-structured and *in-depth* qualitative interviews are the most important classifications. The above can only cover one or two subjects in depth. Both forms of interview allow for the exploration of knowledge on topics that the interviewer might have overlooked [137]. Semi-structured interviews “are flexible and versatile, making them a popular choice for collecting qualitative data” [138]. They involve a discussion wherein the researcher understands what she/he needs to cover and has a set of questions and other information to help guide the exchange [139]. The objective is to create a safe space where the participant feels comfortable thinking about and discussing their own encounters and experiences [139]. This approach gives the researcher a much more rich and detailed comprehension of the specific topic of interest [140]. Semi-structured interviews require the researcher to consider reciprocity with the participant, accomplished through both predefined open-ended questions and further extemporised questioning [141, 140].

3.3.2 Methodological Approach

Semi-Structured Interview

The methodological approach taken in this study is a qualitative research method. Semi-structured interviews were conducted with participants from a Saudi and a British organisation to elicit information regarding employees’ knowledge and beliefs of SKS [11]. The study attempted to illuminate SKS-related challenges [10]. The study consists of two stages due to surveys and literature reviews dominating the existing research. The survey method does not deliver in-depth analyses of human behaviours. Remarkably, only one previous study was found to use interviews or focus groups to understand SKS barriers. This is surprising, as observation, surveys and interviews are the most powerful techniques for delivering comprehensive insights that enable the best understanding of SKS in natural environments [26, 2].

3.3.3 Data Analysis

All of the audio recordings (n=28) were professionally transcribed. All transcripts were read through by the researchers while listening to the audio recordings to make sure the transcripts were as accurate as possible. Transcripts were anonymised and imported into NVivo 12.0 (QSR, Doncaster, Victoria). A thematic analysis approach was used to analyse the transcripts [62].

Codes were derived and categorised, with researchers using detailed and rich descriptions to present the findings in as realistic a way as possible [8]. The consistency of the coding was verified by matching the transcripts with their recording, as well as by the researcher repeatedly reading and reflecting on the transcripts after coding to ensure that the definition or meaning of the codes remained the same throughout the process [9]. Lastly, a senior colleague unrelated to the research was asked to objectively assess the study, looking at such areas as the relationship between the data and the research questions, the interpretation, and the level of analysis [8].

3.4 Stage Two A: Examination of Scale Reliability for TMS

The first stage is divided into two parts: the survey technique overview and the justifications for the method. In addition, the methodological approach taken is presented in this stage.

3.4.1 Quantitative Survey Technique Overview

This stage aimed to examine scale reliability, correlations, and relationships between the TMS scale (part of the SKS model) and other constructs in the security context to understand SKS in organisations.

3.4.2 Measurement of Constructs

A questionnaire was used to collect empirical data to support the research model and hypotheses developed from the prior literature review, as presented in Table 3.2. For each of the hypotheses, metrics were derived from the prior research and the probes were rephrased as necessary, as the majority of the existing studies did not focus specifically on the security context. To measure the constructs of the research model, five-point Likert scales were created with options ranging from 1 – strongly disagree to 5 – strongly agree.

3.4.3 Pre-test and Refinement of Measurement Items

A pilot test was carried out among a small group of computing science PhD students. The feedback received from the students was used to make improvements to the design of the instrument. Four independent researchers were then asked to carry out a final validation before the questions were distributed.

3.4.4 Data Collection Procedure

A link to the questionnaire was sent to a Saudi and a British organisation to collect information from a sample of employees. Each organisation’s information technology department was asked to send an email containing the questionnaire link and the study objectives to employees across all departments in order to obtain a diverse sample population. Participants were asked to provide basic demographic information, but not their name or email address. 204 people responded to the email request, with eight responses being disregarded due to incompleteness. A total of 196 were retained for analysis.

3.5 Stage Two B: Relationships between TMS and SDT

The aim of this part of the study was to confirm the relationship between SDT (Competence and Relatedness) and TMS (Credibility and Coordination) based on the analysis and observation.

3.5.1 Methodological Approach

A qualitative meta-analysis was conducted to synthesise the definitions and findings of both qualitative and quantitative inquiries of the relationship between TMS and SDT (Competence and Credibility, Relatedness and Coordination). Qualitative meta-analysis adopted a closer, more reproducible method than quantitative meta-analysis, but was more interpretative in nature rather than aggregative. The researcher reviewed textual records rather than mathematical evidence, resulting in new interpretations throughout the study phase [142].

3.6 Stage Three: Implementing the Instrument

The aim of this section is to look at the reasoning behind the development of the STOW app, as well as the theoretical foundation upon which it was built. This part also describes the steps taken in the implementation of the intervention, and the pilot study which was undertaken to improve the app and resolve any issues.

3.6.1 Application Development Process

Many instructional concept models are available for use in developing an effective e-learning course. Every researcher uses a different method. The ADDIE model is the most traditional model for instructional design, and all others are based on it. The model's name is an acronym of the five phases that are involved in the process: Analyse, Design, Development, Implementation, and Evaluation [143], as seen in Figure 3.1.

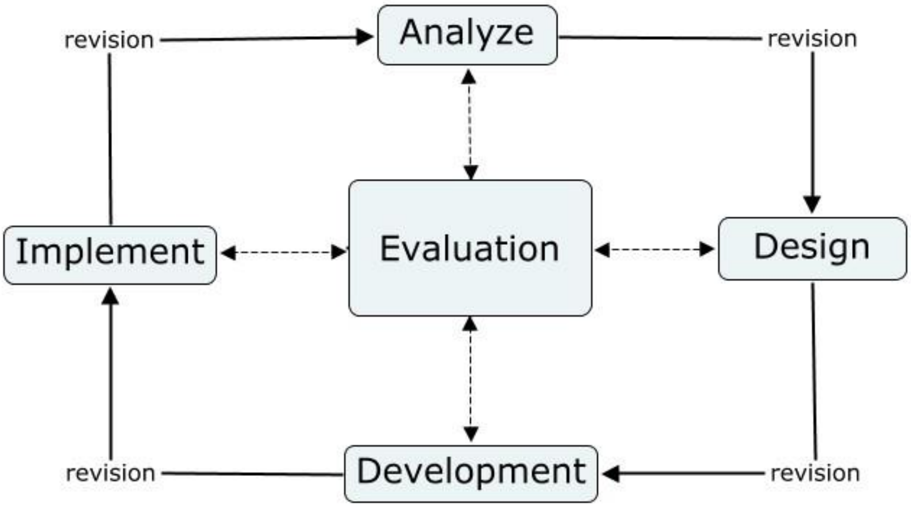


Figure 3.1 The five processes of the ADDIE model [143]

- **Analyse**: assess instructional objectives and assignments by evaluating learner characteristics.
- **Design**: establish learning objectives, choose an instructional methodology, identify success goals, create evaluation tools, and devise an instructional plan.
- **Development**: designers and engineers begin the development and testing of the project's methodology.

- **Implementation**: involves providing educational content, carrying out instructional exercises, and conducting formative tests.
- **Evaluation**: to test and improve the application [143].

3.7 Stage Four: Action Research

It is important to acknowledge that action research is only one type of action investigation. Any method that follows a loop, in which techniques are changed by systematically oscillating between taking action in the area of practice and inquiring into it, is referred to as 'action inquiry'. When planning, implementing, describing, evaluating, and improving one's work, more is learnt about both the practice and the intervention [144].

The majority of improvement methods adopt a similar pattern. Identifying the problem, preparing a response, executing it, measuring, and assessing its efficacy, for example, are all phases of problem-solving. Hospital care follows a similar pattern: signs are monitored, a condition is diagnosed, medication is prescribed, the patient is treated, and the patient's outcomes are monitored and evaluated. Whether it is for personal or career advancement, a programme or a strategy, most growth cycles follow the same process. Different applications and innovations in the simple action investigation cycle necessitate different activities in each step and begin at various points [144]. The four-phase representation of the basic action cycle is shown in Figure 3.2.

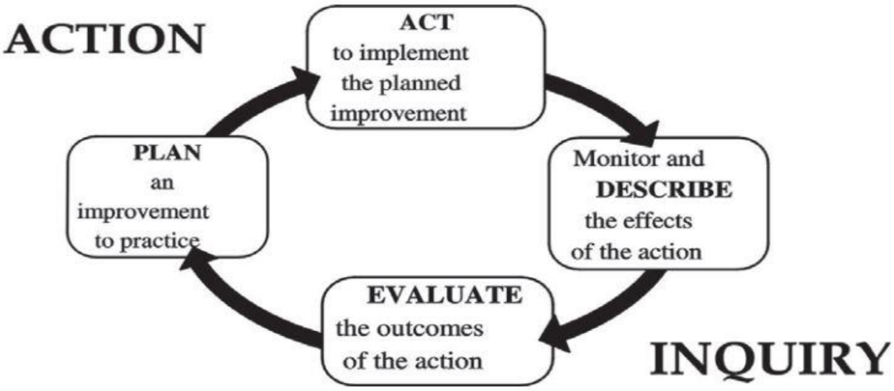


Figure 3.2 The four-phase representation of the basic action cycle [144]

Action research is essential to the scientific process and relies on experimentation and evaluation to obtain new insights [145]. Through evaluation and experimentation, decisions in the observational and theoretical realms are made. Most judgements are based on experience instead of data, in contrast with science. Furthermore, actions are focused on emotions or ‘gut instinct’. Additionally, judgements or decisions can be made based on views, thoughts, projections, assumptions, and attitudes. [135].

At this point, our research implemented and empirically evaluate an application that facilitates information security knowledge sharing based on the SKS model, which was published in our previous work [1]. The empirical evaluation is depicted in Figure 3.3.

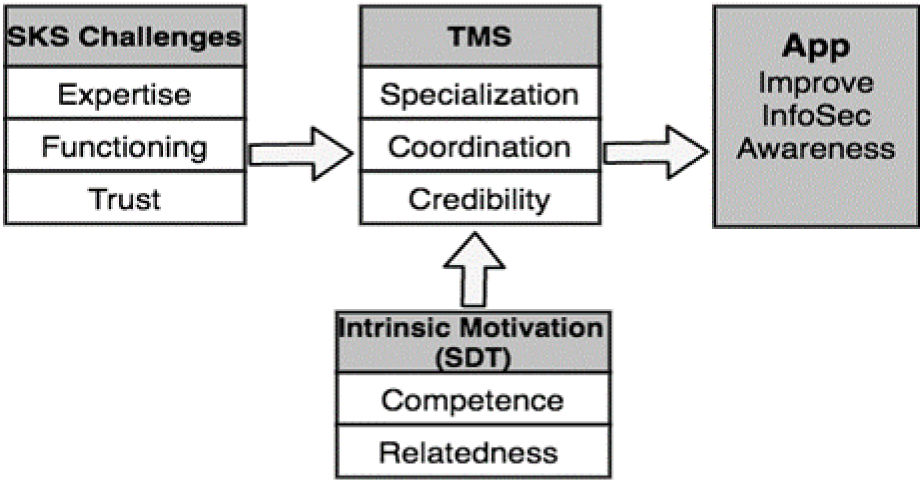


Figure 3.3 The proposed research model

3.7.1 Overview of STOW Game

The Security Knowledge Sharing System (STOW) is intended to be played by employees as a group. The security game is presented as a mobile app (e-learning scenarios to encourage reflection and discovery among employees), and includes multiple-choice questions via a virtual connection. The scenarios were based on the Global Information Security Policy and common human errors. Several features are included in the game to help employees with interactions, such as giving them scenarios to encourage them to think about the correct answers based on their experience. The experts can share their knowledge by adding the reason for choosing this answer via the ‘Check Your Answer’ button, then the ‘Add a New Answer’ button if they are not satisfied with the current best answer. The STOW system lets the employees look at the new solution by posting the new response and evaluating it. Moreover, the STOW provides the ‘Best Answer’ button based on the evaluations of the employees and department, who validate it.

3.7.2 The Importance of Games as an Approach

Security games are powerful teaching tools that can result in an ‘instructional revolution’. They enable employees to learn through experience and utilise a virtual environment while motivating them to think critically. An empirical evaluation of the game reveals that it can boost social engineering awareness in an enjoyable way. Several approaches for delivering security awareness via games have been tried in the past. CyberCIEGE is an interactive video game that may meet corporate security training goals while engaging ordinary users in an exciting security adventure. Preliminary findings suggest that the game may be a helpful supplement to programmes teaching information awareness to general computer users. Game-based delivery techniques may be a useful complement to or substitute for more conventional forms of understanding. To produce engaging training experiences, the online games integrate visuals, gameplay, and training ideas. The advantage of using a game-based approach for delivering attention is that it may challenge, motivate, and engage players. Gamification is a highly interactive delivery technique that may promote organisational security awareness goals while engaging ordinary users [113]. Moreover, the importance of the game as an approach to improving ISA is known from looking at recent publications based on games and their results, as seen in Table 2.4.

3.7.3 Data Collection Procedure

Data generation, according to Oates [30], is the “method of producing analytical data or facts, which may be quantitative or qualitative”. During the exploratory case analysis, three data generation approaches were used, which are outlined in Table 3.2.

Table 3.2 Data generation methods

Generation Method	Description
Survey (Questionnaire)	This included two sections: quantitative survey questions and qualitative open questions. Surveys are a method whereby a researcher poses a set of predetermined questions to an entire group, or sample, of people to assist in the planning of a more oriented, in-depth analysis that may involve time-consuming approaches such as in-depth interviews or field studies. In this scenario, a survey may assist a researcher in determining persons or locations from which to obtain additional details, and defining and measuring concepts.
Documents	Documents that existed prior to the study and documents created specifically for the benefit of the research mission. In addition, documents were obtained from the app which documented players' interactions during the game.
Observation	Observing and paying attention to what individuals actually do over what they say they do [146]. Furthermore, the extra time spent observing provides information that may not have been obtained through the Survey and Documents approaches [136].

Group A: Intervention Group

Employees will be given a pre-questionnaire (Information Security Assessment). They will then be given the game application which will provide users with knowledge about how their security awareness can be improved (two-week intervention). Following this, participants will be given a post-questionnaire (Information Security Assessment).

Group B: Control Group

This group will be given a pre- and post-questionnaire (Information Security Assessment) with no intervention to maximise SKS.

3.7.4 Data Analysis

Stage Four is divided into two sections: *Stage 4 A* measured the improvement in Security Awareness levels pre- and post-intervention (quantitative); and *Stage 4 B* measured the Knowledge Sharing pre- and post-intervention (qualitative).

Four A: Measure the improvement in Security Awareness Level Pre-Post (Quantitative).

Awareness Level Measurement

The following awareness scale has been adapted from Kruger and Kearney which was used to explain the level of awareness [147], as shown in Table 3.3.

Table 3.3 Awareness level measurement

Awareness	Measurement	Actions
Good	80–100	Satisfactory: expert user and can be group leader
Average	60-79	Minor action potentially required
Poor	59 and less	Unsatisfactory: improvement required

Four B: Measuring the KS Pre- and Post-intervention (Qualitative)

Quantitative and qualitative data were used to test the applied improvements. The quantitative research included looking at a number of artefacts produced during the game, such as security investigation records and documents as well as logs generated from player interactions. The STOW app and accessible questions were used to gather qualitative data. Both quantitative and qualitative evidence was used to further validate and illustrate gaps in the findings and data obtained.

3.8 Summary

This chapter described the research methods adopted in the construction of this dissertation. The research methods used included research philosophy, methodology research approach, interviews, survey, implement model and action research to evaluate the intervention within the organisation.

Chapter Four: Understanding Challenges of Security Knowledge Sharing through Exploratory Interviews

4.1 Purpose of the Study

Semi-structured interviews were carried out with employees from two organisations to ascertain their awareness and opinions regarding SKS [148]. By so doing, we were investigating SKS-related challenges [149]. This was to expand on previous research which relied purely on either surveys or literature reviews. Surveys, on their own, do not deliver in-depth analyses of human behaviours. Only one study was found to have used interviews or focus groups to explore SKS challenges and barriers [150, 62]. This is surprising, since observation and interviews are the most powerful techniques for delivering comprehensive insights that lead to enhanced understanding of SKS in natural environments [148, 151].

4.2 Ethical Approval

This experiment adopted the BPS ethical principles for performing experiments on human subjects and was accepted by the FIMS ethics committee of the University of Glasgow (ref: 300170175) (Appendix A).

4.3 Study Methodology

This study was the first part of a sequential mixed-methods study to understand the challenges associated with SKS in organisations. Exploring the challenges of SKS and the sources can best be accomplished through in-depth discussion with employees.

Based on the importance of organisations allowing researchers to explore such challenges and seek solutions [152], we selected two organisations for evaluation of information security risks. We reached an agreement with the organisations to carry out our research. The organisations were chosen based on the information security risk in those organisations. Moreover, the author worked for one of these organisations. As per the arrangement, the organisation's identity must be protected. We decided to call this organisation Fortune 100.

4.3.1 Data Collection Procedure

The study used interviews [151] in order to facilitate an in-depth look into, and exploration of, perceptions and perspectives [153]. In 2018, interviews were conducted with participants from a Saudi university and a British university. The interviews took between 15 and 20 minutes and explored how participants would respond to a security incident in the workplace. Participants were also asked some general questions about trust, privacy, experience, and the effect of the relationship in terms of sharing security advice in the security knowledge system.

4.3.2 Semi-Structured Interview

The methodological approach taken in this study is qualitative in nature. Semi-structured interviews were conducted with participants from a Saudi and a British university to elicit information regarding employees' knowledge and beliefs of SKS [11]. The study attempted to illuminate SKS-related challenges [10]. The study consists of two stages due to surveys and literature reviews dominating the existing research. The survey method does not deliver in-depth analyses of human behaviours. Remarkably, only one previous study was found to use interviews or focus groups to understand SKS barriers. This is surprising, as observation, surveys and interviews are the most powerful techniques for delivering comprehensive insights that enable the best understanding of SKS in natural environments [26, 2].

4.3.3 Pre-Test and Refinement of Measurement Items

The interview guide was designed based on literature regarding the usage of security information sharing which included the challenges. We validated the questionnaire with an academic colleague, and it was modified accordingly, as seen in Appendix B. A pilot test was carried out among a small group of computing science PhD students. The feedback received from the students was used to simplify the terms used in order to make them more understandable to non-academic people.

4.3.4 Participants

The interview began with an explanation of the study's aim, followed by informed consent acquisition. We asked open-ended questions related to SKS challenges, such as trust, age, education, the style of the job, and exploring new factors to understand the challenges and discover effective solutions. The participation criteria used to recruit participants for this study were employees of organisations that use computers to complete their work during their working hours.

Participants were employees between the ages of 20 and 60 years of age. 28 people participated (seven females, 21 males). Eight had a high school certificate, 13 had a bachelor's degree, and seven had a master's degree, as shown in Table 4.1.

Table 4.1 Participants' characteristics of the first experiment

Categories	Sub-categories	# (n=28)
Gender	Female Male	7 21
Age	20-25 26-30 31-40 41-50	6 8 11 3
Education	High School or below Bachelor's degree Master's degree and above	8 13 7
Experience	1-3 years (Beginner) 4-9 years (Intermediate) Over 10 years (Expert)	9 11 8
Security incident	Experienced a security incident Successfully resisted an incident Have not experienced a security incident	7 10 11

4.4 Data Analysis

The transcripts were analysed by the researchers using guided content review. "The qualitative method of categorising contextual textual data into groups of related individuals, or semantic categories, in order to define consistent trends and associations between variables or themes is known as content analysis" [154]. These themes can be established *a priori*, in which case the researcher looks for proof from participants' gestures on these themes, or they may appear through review of the transcript. A content review may be done in three ways: conventional, directed, and summative [155]. As the study wanted to expand the literature's theoretical construct of SKS and its origins, a guided content review approach was adopted, which is a good way to test or broaden a philosophical hypothesis or theoretical framework [150, 156].

All of the audio recordings (n=28) were professionally transcribed. All transcripts were read through by the researchers while listening to the audio recordings to make sure the transcripts were as accurate as possible. Transcripts were de-identified and imported into NVivo 12.0 (QSR, Doncaster, Victoria). A thematic analysis approach was used to analyse the transcripts [62].

Codes were derived and categorised, with researchers using detailed and rich descriptions to present the findings in as realistic a way as possible [8]. The consistency of the coding was verified by matching the transcripts with their recording, as well as by the researchers' repeated reading and reflecting on the transcripts after coding to ensure that the definition or meaning of the codes remained the same throughout the process [9]. Lastly, a senior colleague unrelated to the research was asked to objectively assess the study, looking at such areas as the relationship between the data and the research questions, the interpretation, and the level of analysis [8].

4.5 Results

Results of Study 1: We now answer the research question: *"Which factors impact SKS in organisations?"* (Table 4.2 and Figure 4.1).

Table 4.2 Concepts and categories that emerged from the analysis

First Order Concepts	Themes
➢ Offer effective system to facilitate communication among those in the workplace. ➢ Offer an electronic knowledge repository to record information security incidents which offer high-quality knowledge.	Infrastructure
➢ Experience, qualifications and relationships with colleagues. Experience is more important than qualifications in an information security incident.	Knowledge
➢ Sensitive documents refused to anyone working outside the IT dept. ➢ Trust based on the situation such as critical problems and need for a quick solution. ➢ Lack of experience and knowledge in the security field prevents helping others.	Trust
➢ Security knowledge sharing, not violation of privacy. Those reporting would rather be anonymous. ➢ Recording a bad experience with an employee's skills by the incident reporting which show the employee's name in the knowledge repository.	Personal Factors

➢ Lack of knowledge of policies, to provide a set of strategies and explain user responsibilities	
➢ Annual evaluation. ➢ Financial incentives and moral incentives. ➢ Reward system based on their contribution to recording the incident such as attending training and conferences.	Motivation
➢ Improving decision making, reducing information security incidents. Mitigates risk through learning from previous incidents.	IT Advantage
➢ Gain knowledge by practise and learn lessons from previous incidents. ➢ Lessons learnt when knowledge sharing. ➢ Reduce the loss of know-how.	Employees' Advantages

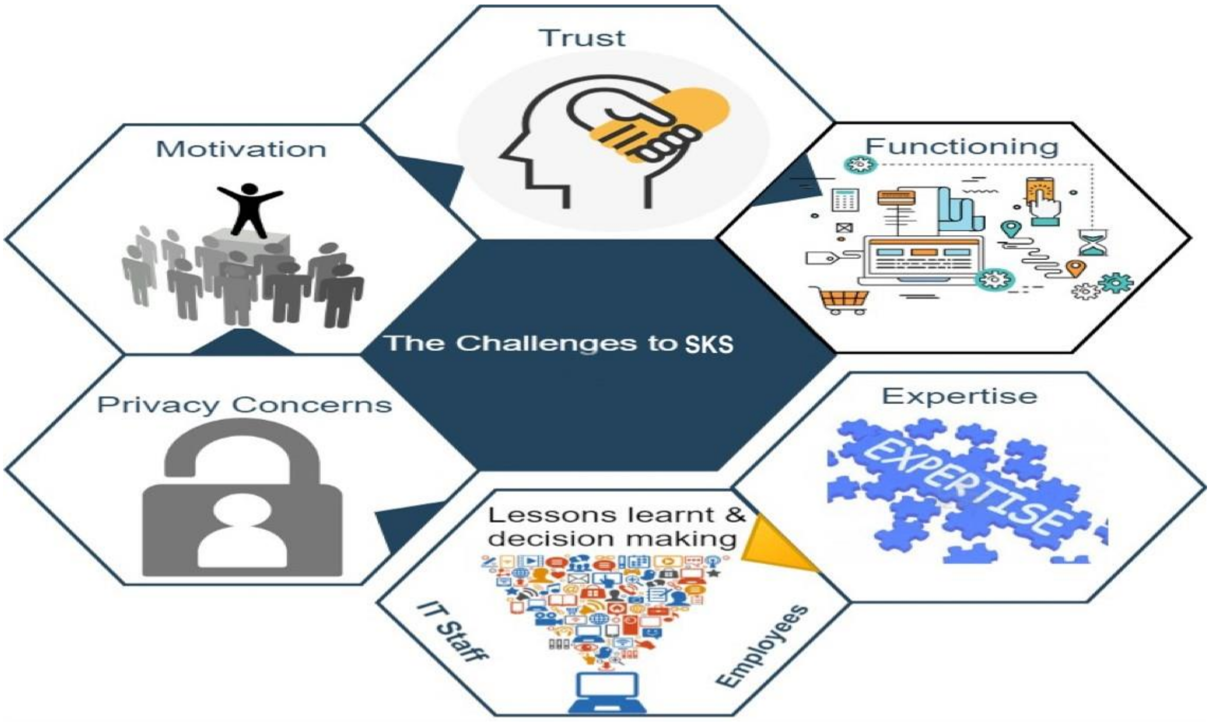


Figure 4.1 Findings of the study

4.5.1 Infrastructure

This refers to the software and hardware that facilitate dissemination of knowledge in the organisations. The participants agreed on the importance of infrastructure that facilitates communication between people during the working day and after they leave the workplace, such as offering an electronic knowledge repository to record information security incidents which offers high-quality knowledge: *"there is a need for a knowledge management process* *and database due to the ongoing risk of losing information and knowledge as people transition from one role to another and/or leave the University"* (A21). It is important to note that we found little evidence that the Universities fostered an environment that facilitates SKS.

4.5.2 Trust Building

Factors involved building enough trust to request help, which focuses on motivations including encouraging employees to trust their colleagues enough to accept their solutions or advice that is already available in the knowledge repository. When the participants were asked about it, the majority commented that experience is one of the most important factors involved in building trust in others, and the majority of respondents revealed that experience is more important than qualifications in an information security incident: *"It is based on the relationship, and I can judge if I can trust him or not. On the other hand, the experience together with an appropriate qualification is essential in building the trust before asking anyone"* (A1).

4.5.3 Trust

The third theme is trust and factors that prevent employees from trusting others in the workplace, such as sensitive documents leading to the refusal of any advice from anyone who works outside the IT department: *"I have sensitive documents which prevent me from asking anyone who works outside the IT department"* (A1). Moreover, trust is based on the situation such as critical problems and need for a quick solution.

4.5.4 Personal Factors

What is surprising is that a lack of anonymity prevents employees from sharing their incidents. Many feel that SKS can violate their privacy if they add an incident which includes personal details, such as their names. Many employees would prefer to be anonymous when reporting incidents: *"They don't have to know the personal information about me"* (A13); *"it will appear as a bad experience about me"* (A3).

4.5.5 Motivation

The current study found that a reward system affected the employees' likelihood of sharing knowledge. The most effective reward system is annual evaluation, encouraging employees with financial incentives and moral incentives a reward system based on their contribution to recording incidents.

4.5.6 The Advantage of SKS for Employees and IT Department

Enhancing the IT department’s response to cyber-attacks: An important finding was that SKS improved decision making based on recording in the knowledge repository and reducing information security incidents.

Enhancing employees’ information security to prevent cyber-attacks: The most interesting finding was that employees can gain knowledge by practising and learning lessons from previous incidents and benefit from security advice. This reduces the loss of know-how and leads to increased security awareness.

4.5.7 Knowledge

One of the main challenges was the disparity in staff experience, qualifications, and relationships with colleagues. Experience is more important than qualifications in an information security incident.

4.6 Discussion

The findings showed that the biggest challenges to SKS are (1) facilitating infrastructure, (2) trust, (3) knowledge, and (4) increasing motivation. Our results confirmed that SKS could enhance security awareness, leading to many benefits for both employees and the IT department (confirming [78, 4]).

Previous research has indicated the positive effects of trust, which increases interaction among employees in terms of SKS [157, 158]. Prior studies have noted the importance of trust as an influential factor in the security field as barriers can prevent the sharing of security knowledge advice [150, 159].

The current study is one of the first to investigate SKS in non-profit organisations. We showed that SKS mitigates risk [67] through learning from previous incidents and security advice [35]. It reduces the loss of knowhow [46], and the outcome of the study reveals that SKS can have a positive impact on employees’ willingness to comply with information security guidelines [66].

Our literature review revealed that SKS investigations use only a handful of different theories, such as the Theory of Planned Behaviour [150]. We model SKS using TMS [83, 84] (the first time this will have been used in the cyber security context). We augment this descriptive model by incorporating the tenets of SDT in order to address individual sharing motivations, and IT facilitation to address organisational factors.

We wanted to confirm the importance of SKS and show how its influence on employees in the workplace leads to enhanced security awareness [150]. The study highlighted the advantages of SKS in an organisational setting, especially in terms of individual security awareness [150]. Hawryszkiewycz and Binsawad [56] describe the impact of barriers deterring SKS. Our study indicated that trust [150, 13, 56], affording anonymity [160], facilitating infrastructure [161], and engendering motivation [157, 158] are factors affecting SKS. In particular, we found a lack of provision of an environment that specifically facilitates SKS. Such an environment could improve incident reporting and inspire employees to participate more fully in recording incidents and sharing their advice [150, 62].

4.7 Chapter Contribution

Developing an understanding of challenges: The study revealed several factors that deter KS in organisations. To better understand these factors, the research adopted a qualitative approach (semi-structured interviews). Interviewing is the most powerful technique for delivering comprehensive insights that would allow for the best understanding of KS in natural environments. The information obtained was used to devise practical solutions. Moreover, the study was carried out in Saudi and British organisations in different geographical locations.

4.8 Summary

This chapter described an exploratory interview study of SKS in two organisations. The study investigated significant challenges associated with SKS, which required improving security awareness in organisations. The interview was the most reliable source that could be obtained through in-depth discussions with employees.

In the next chapter, we propose a model that describes, facilitates, and encourages SKS in organisations. We relied on TMS theory to understand and facilitate SKS to mitigate those challenges, which we came up with in Stage One. Moreover, the model encouraged SKS by adapting intrinsic motivation (self-determination theory).

Chapter Five: Model for Describing and Optimising Security Knowledge Sharing

5.1 Purpose of the Study

The aim of this study was to examine scale reliability, correlations, and relationships between the TMS scale and other constructs in the security context in order to understand SKS in organisations, as well as to confirm the relationships between the TMS and SDT.

5.2 Ethical Approval

This experiment adopted the BPS ethical principles for performing experiments on human subjects and was accepted by the FIMS ethics committee of the University of Glasgow (300180008, 300180274) (Appendix C and D).

5.3 Study Methodology Stage Two A

This stage is to investigate the scale reliability, associations, and interactions between the TMS scale and other constructs in the security context in order to better understand SKS in organisations.

5.3.1 Measurement of Constructs

A questionnaire was used to collect empirical data to support the research model and hypotheses developed from the prior literature review, as presented in Figure 5.1. For each of the hypotheses, metrics were derived from the prior research and the probes were rephrased as necessary, as the majority of the existing studies did not focus specifically on the security context. In order to measure the constructs of the research model, five-point Likert scales were created with options ranging from 1 (strongly disagree) to 5 (strongly agree), (Appendix D2).

5.3.2 Pre-test and Refinement of Measurement Items

A pilot test was carried out among a small group of computing science PhD students. The feedback received from the students was used to make improvements to the design of the instrument. Four independent researchers were then asked to carry out a final validation before the questions were distributed.

5.3.3 Data Collection Procedure

A link to the questionnaire was sent to a Saudi and a British organisation to collect information from a sample of employees. The university's information technology department was asked to send an email containing the questionnaire link and the study objectives to employees across all departments in order to obtain a diverse sample population. Participants were asked to provide basic demographic information, but not their name or email address. 204 people responded to the email request, eight of which were disregarded due to incompleteness. 196 were retained for analysis.

5.3.4 Related Work

Collaborative interventions in information security should encourage employees to interact with each other to share their security knowledge, thus ensuring that all employees have access to security advice [150, 62]. The study tests the validity of the transactive memory system (TMS) theory to model security knowledge sharing within organisations. TMS reflects organisational factors and incorporates the satisfaction of SDT needs [91] on the individual level to maximise SKS within organisations [162].

5.3.4.1 Transactive Memory System (TMS)

TMS has been described as "*a set of individual memory systems in combination with the communication that takes place between individuals*" (p.186) [71]. A TMS determines the specific division of cognitive labour within a group of people, as a means to facilitate encoding, storage, and retrieval of knowledge pertaining to various domains. When a TMS is being utilised, each group member is aware of "*who knows what, and who knows who knows what*" (p.856) [36]. Simply put, the characteristics of a TMS mean that three crucial qualities, common to other types of socially shared cognition, are absent – i.e. differentiated knowledge; processes of transactive encoding, storage and retrieval; and the dynamic nature of TMS functions [72]. Thus, an alternative and more suitable approach might involve a shift of focus away from repositories towards processes [73].

5.3.4.2 TMS Hypothesis development

Liang, Moreland, and Argote (1995) described three aspects of TMS:

Specialisation: this is the term used to describe the degree of differentiation of the knowledge held by team members [76]. Specialisation reduces the cognitive burden on community participants by allowing each to focus on his or her own area of expertise. It urges members to prioritise information integration through different domains in order to maximise team knowledge use [78]. Hence, the first hypothesis is: **H1**: Specialisation (Employee Knowledge) is positively related to SKS transfer within the organisation.

Coordination: this describes the efficiency of the team in terms of knowledge processing while working together to enhance the coordination of information within teams [80]. Moreover, coordination is a team process that entails the coordination, behaviour patterns, and skills among team members in order to achieve shared objectives [81]. Zhong et al. confirmed that improved coordination and collaboration would increase task performance [82]. The second hypothesis is: **H2**: Coordination (Functioning) is positively related to SKS transfer within the organisation [76].

Credibility: this is the way in which individual team members perceive the reliability of the knowledge held by the other members of the team. The third hypothesis is: **H3:** Credibility (Trust) of shared knowledge is positively related to SKS transfer within the organisation. These three dimensions are considered variables that can be used to measure the degree to which a TMS has developed among the members of a group, and they have frequently been used for this purpose in empirical studies [83, 76].

As Lewis [78, 84] (2003, p.590) asserts, these three variables "*reflect transactive memory itself [78], as well as the cooperative processes illustrative of transactive memory use*" as shown in Figure 5.1.

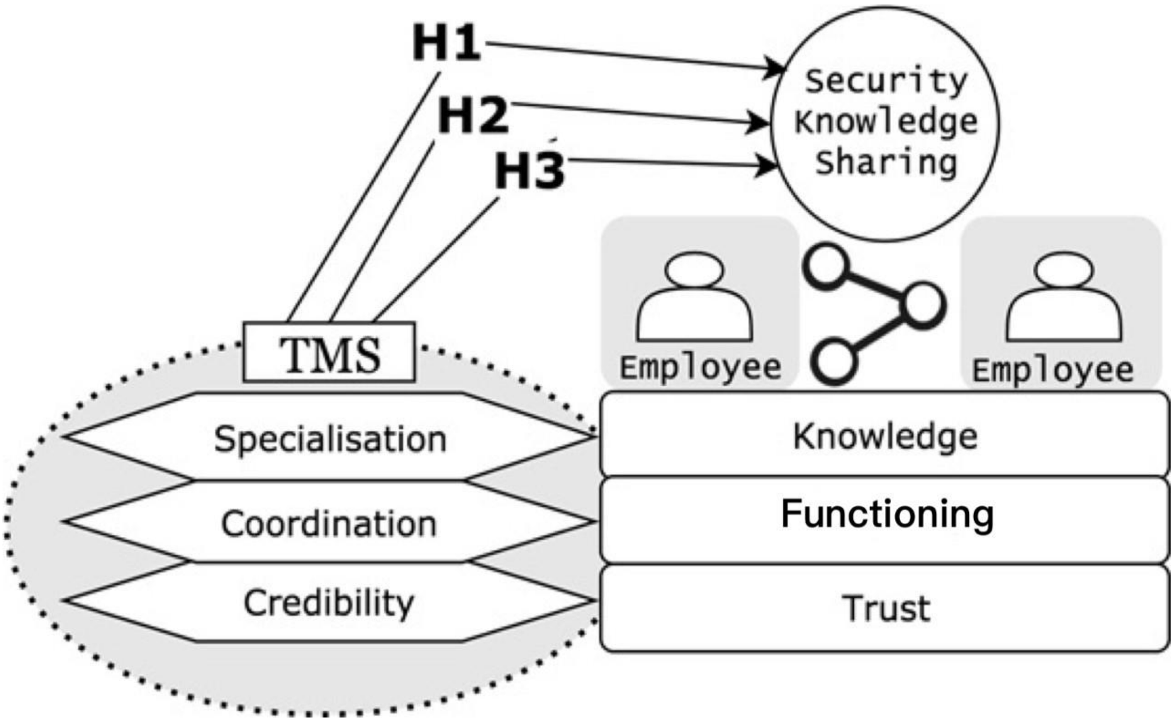


Figure 5.1 Using TMS to model organisational security knowledge sharing

Davison et al. [37] argue that TMS facilitates KS, leading to improved team creative performance via team creative efficacy. Our premise is that organisations should facilitate and engender SKS by removing the challenges that prevent SKS, i.e. "*Specialization, Credibility and Coordination*" [83]. The aim is to make security knowledge accessible to all of those who need it and ultimately to improve security awareness across the organisation. Our first qualitative study delivered insights about which factors impact SKS, and we are able to align these factors to the core tenets of TMS theory.

5.3.5 Data Analysis and Results of Stage Two A

5.3.5.1 Data Analysis

The research model and hypotheses were tested using a component-based partial least squares (PLS) regression approach to structural equation modelling (SEM). This kind of approach is the most appropriate for the current study as it has a focus on theory development and the prediction of data [163]. SmartPLS (v.3.0) was used to test the model as it is a powerful, user-friendly instrument for graphical path modelling with latent variables.

5.3.5.2 Results

The results of a real TMS model strongly support two hypotheses, which are Coordination (t=3.840, p < 0.001), and Specialisation (t=2.241, p < 0.001).

Table 5.1 Path coefficient of the research hypotheses

Hypo	Relationship	Std. Beta	Std. Error	T-value	P-value	Decision
H1	SPE → SKS	0.189	0.075	2.521	0.012	Supported
H2	COO → SKS	0.359	0.090	4.001	0.000	Supported
H3	CRE → SKS	0.132	0.091	1.448	0.148	Unsupported

Notes SPE: Specialisation; CRE: Credibility; COO: Coordination

The path coefficient of the research hypotheses was used to determine whether SPE, COO and CRE variables predict the participants' intentions to transfer SKS within the organisation. Dependent variable: Facilities SKS; independent variables: SPE, COO and CRE, as shown in Table 5.1 and Figure 5.2. H1 and H2 are supported, but H3 is unsupported. We will, however, retain all three tenets of TMS in our model due to the smallness of our sample, and the fact that we are not at liberty to pick apart TMS. Having modelled SKS within organisations, we now turn to considering how to facilitate and encourage SKS.

Confirmatory factor analysis findings established the reflective constructs' reliability and validity, as seen in Table 5.2. Cronbach's alpha and composite reliability were more than 0.70, indicating that the construct's dependability and internal consistency were validated.

Table 5.2 The construct reliability and validity

Measures	Cronbach's Alpha	Reliability rho	Composite Reliability	Average Variance Extracted (AVE)
COO	0.741	0.798	0.823	0.49
CRE	0.812	0.84	0.876	0.64
KS	0.919	0.921	0.943	0.804
SPE	0.779	0.793	0.849	0.531

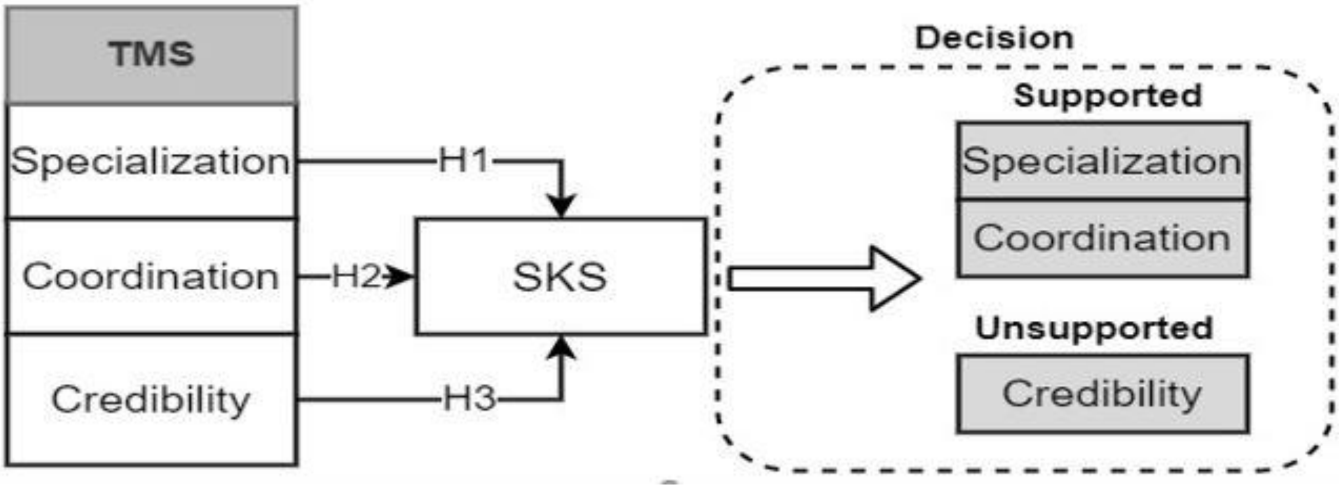


Figure 5.2 Findings of the experiment

5.3.6 Discussion of Stage Two A

The path coefficient of the research hypotheses was utilised to establish whether SPE, COO, and CRE positively affect the transfer of SKS within an organisation. In terms of employees' intention to share knowledge with others, SPE and COO were the strongest predictors here. On the other hand, CRE was not supported as employees need to know who they can trust to take information from and pass knowledge on to. Trust was found to be one of the biggest challenges in the context of SKS, mainly due to information security and sensitive issues among employees in the organisation [36]. These challenges can be mitigated through coordination of the TMS, as this can play a key role in increasing credibility among employees and achieving classification of the specialisation [164]. Moreover, Wang et al. suggest that technical systems feed into the creation of TMSs. For instance, with the help of IT-empowered collaboration platforms, colleagues may assemble a knowledge index and mutual trust in expertise to maximise effectiveness. Moreover, the researchers referred to the benefits of collective knowledge based on TMS as a useful knowledge network for employees in organisations [84].

In the next stage, based on these results, we investigated how inspired the employees were by motivating an individual through their own natural interest in activities that are new or challenging. With intrinsic motivation, there is no need for the individual to be rewarded for their behaviour by SDT.

5.4 Stage Two B

5.4.1 Intrinsic Motivation

According to de Charms [92] and Deci and Ryan [91], intrinsic motivation works by motivating an individual through their own natural interest in activities that are new or challenging. With intrinsic motivation, there is no need for the individual to be rewarded for their behaviour [3, 19]. In fact, there is a natural desire to learn; people have an innate wish to master something, learn something new through interest, or to explore, and this is the driver to learn throughout life [3, 19].

SDT utilises traditional empirical methods to describe human personality and motivations In SDT [85, 165], three key human needs must be met:

- The need for autonomy, which is a person's wish to organise their own actions.
- The need for a sense of competence, which is when a person desires self-efficacy.
- The need for relatedness, i.e. a person's wish for the support and feelings of connection with others around them [99].

Studies have shown that when these three core needs are satisfied, individuals are more likely to take part in and exhibit better performance on an activity [62, 96].

5.4.2 The Relationship between TMS and SDT

Collaboration is particularly tricky in social contexts like societal activities, for instance, which are rather abstract and cannot be perceived easily. Such activities are sometimes seen as having no relevance in people's everyday lives. However, it is widely acknowledged that games are a good way to induce collaboration between people, even when they previously did not know each other, as is frequently observed in online multiplayer games [108]. Many studies have evidenced the fact that people find enjoyment in collaborative games [62, 166, 167, 27, 168, 169]. The collaboration seen in games takes place organically and without effort. For this reason, rather than maintaining a focus on individual behaviour and motivation, research on gamification should focus more on developing a deeper understanding of ways in which collaborative and collective behaviours can be induced and maintained [108].

5.4.2.1 Competence and Credibility

As mentioned, competence is related to an individual's sense of self efficacy. If feelings of competence, developed through evaluation and feedback, are felt during a particular action then intrinsic motivation will be improved. Previous research has shown that intrinsic motivation is enhanced through positive performance feedback [91]. Recent evidence has also confirmed that users' feedback and evaluation can positively influence behavioural intention to perform secure behaviours [170]. Moreover, the result of reinforcing a person's competence in terms of computer-based activities is a rise in their confidence in their aptitude in this area [171]. The Credibility reflects the extent to which the team members believe that the relevant task knowledge possessed by any of the other team members is correct and accurate [78]. The stage is to confirm the relationship between Competence (SDT) and Credibility (TMS) before adapting it into the model. The study considers intrinsic motivation (SDT) factors which have an influence on employee attitudes toward sharing their knowledge. In particular, Competence is an important component among the intrinsic motivation (SDT) factors, and plays a key role in Credibility (TMS), as shown in Figure 5.3 [170].

5.4.2.2 Relatedness and Coordination

Our previous study has confirmed that Coordination plays vital role in enhancing communication in the virtual environment. We have also identified that 'Assuming the App' is the Coordination which is 'functioning' to facilitate SKS in organisations. In order to adapt intrinsic motivation in the app, the study considered relatedness as an important factor to encourage competence, as shown in Figure 5.3. According to Butz and Stupnisky (2017), relatedness was significantly correlated with greater self-determined motivation [172]. Recently, investigators have examined the effects of relatedness on collaboration work. Koivisto and Hamari reported that while collaboration is a natural type of human behaviour, it is a recognised challenge to induce collaboration among individuals [108].

In addition, feelings of connectedness with other researchers who have similar views is likely to increase the willingness of researchers to work together, with perceptions of competence and autonomy also being increased. When considered together, these factors provide the opportunity for scientific knowledge to be created and shared – using next-generation technological tools – in order to enhance intrinsic motivation among individuals to participate with one another [127].

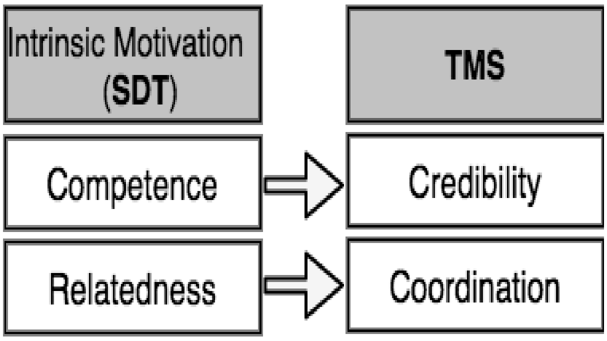


Figure 5.3 Relationship between TMS and SDT

5.5 Security Knowledge Sharing Model

We propose a model that describes SKS based on TMS constructs, encouraging SKS by using SDT constructs (Figure 5.4). TMS relies considerably on information technology for support. The model complements prior SKS models including Gagné’s [118] model of organisational knowledge use. The differences between the models, however, are in the conceptualisation of facilitation by TMS, which is multidimensional in the SKS model and also in the inclusion of psychological factors that can impact on the quality of motivation by SDT. Our model gives a detailed explanation of how and why certain HRM practices impact on engagement with SKS behaviour, thus providing solid advice for employees [118].

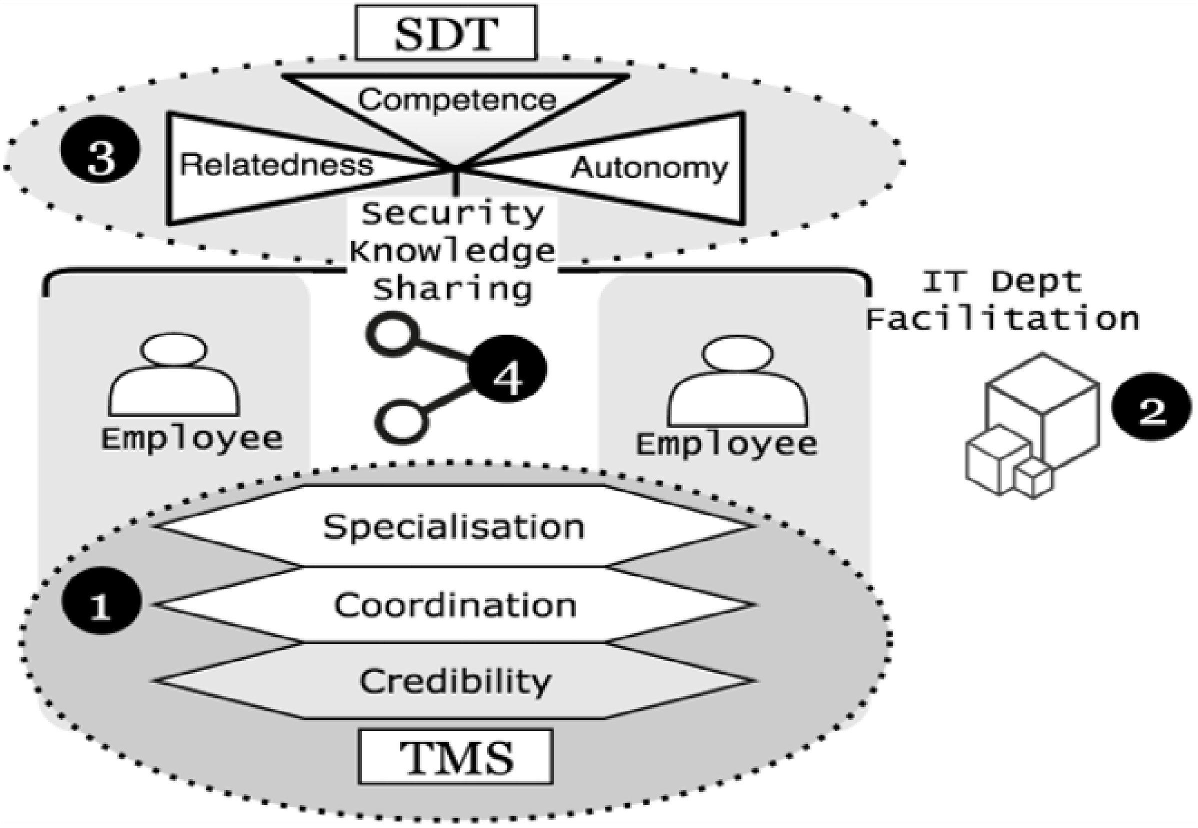


Figure 5.4 Model for describing (1), facilitating (2) and encouraging (3) security knowledge sharing, thereby enhancing sharing (4)

5.6 Chapter Contribution

Examination of the scale reliability and relationships between the TMS at an organisational level: We examined scale reliability, correlations, and relationships between the TMS scale and other constructs in the security context in order to understand and facilitate SKS in organisations (which is a new finding in the security context).

Development of a model for describing and maximising security knowledge sharing to enhance security awareness: We proposed a model that incorporates the factors that could maximise SKS within organisations. The model emerged from the study's findings and incorporated two theories: one at the organisational level and the other at the individual level. TMS theory describes how organisational knowledge is held and how sharing is facilitated at the organisational level, with SDT encouraging sharing at an individual level.

5.7 Summary

This chapter presented an experiment in order to better explain SKS in organisations, and to examine scale reliability, correlations, and interactions between the TMS scale and other constructs in the security context. In particular, we have explained the TMS and how the description of SKS in organisations can be improved. We discussed dimensions of TMS consisting of Specialisation, Coordination, and Credibility. Moreover, this chapter explored the relationship between TMS and SDT and the ways in which SDT can encourage employees by satisfying their competence needs as intrinsic motivation. The findings from this study provided strong support for two hypotheses, namely Coordination and Specialisation. Credibility was unsupported. However, our findings show that the Credibility is motivated through the Competence of SDT. Moreover, Coordination is motivated by the relatedness of SDT. Thus, we proposed an SKS model that adapts TMS at an organisational level and SDT as intrinsic motivation at the individual level. Our aim was to uncover ways to maximise knowledge sharing, both by facilitating and encouraging it.

In the next chapter, we will implement the SKS model, design a system, and test the app before release that facilitates information security knowledge sharing and mitigates SKS challenges in organisations.

Chapter Six: STOW App Implementation and Evaluation

6.1 Purpose of the Chapter

SG are powerful teaching tools that can result in an ‘instructional revolution’, enabling employees to learn through experience and utilise a virtual environment while motivating them to think critically. An empirical evaluation of the game reveals that it can boost social engineering awareness in an enjoyable way. Several approaches for delivering security awareness via games have been tried in the past. CyberCIEGE is an interactive video game that may meet corporate security training goals while engaging ordinary users in an exciting security adventure. Preliminary findings suggest that the game may be a helpful supplement to programmes teaching information awareness to general computer users. Game-based delivery techniques may be a useful complement to or substitute for more conventional forms of understanding. To produce engaging training experiences, the online games integrate visuals, gameplay, and training ideas. The advantage of using a game-based approach for delivering attention is that it may challenge, motivate, and engage players. Gamification is a highly interactive delivery technique that may promote organisational security awareness goals while engaging ordinary users [113].

The aim of this chapter is to look at the reasoning behind the development of the STOW app, as well as the theoretical foundation upon which it was built. This part also describes the steps taken in the implementation of the intervention, and the pilot study, which was undertaken to improve the app and resolve any issues.

6.2 Application Development Process

The instrument was created with the goal of allowing learners to learn and share their knowledge on the basis of the SKS model, as seen in Figure 6.1.1 [162]. As a result, the learner was given as much influence over and interaction with the learning process as possible by constant input on the information transfer process [62]. Moreover, the structuring and presentation of the instrument around critical aspects of baseline security expertise enabled them to address the challenges and validate the security knowledge [162]. The SKS model was used to build the instrument components in line with the cooperation model established in chapters 4 and 5. The instrument, named STOW SYS, reflected the primary objective of the thesis [62].

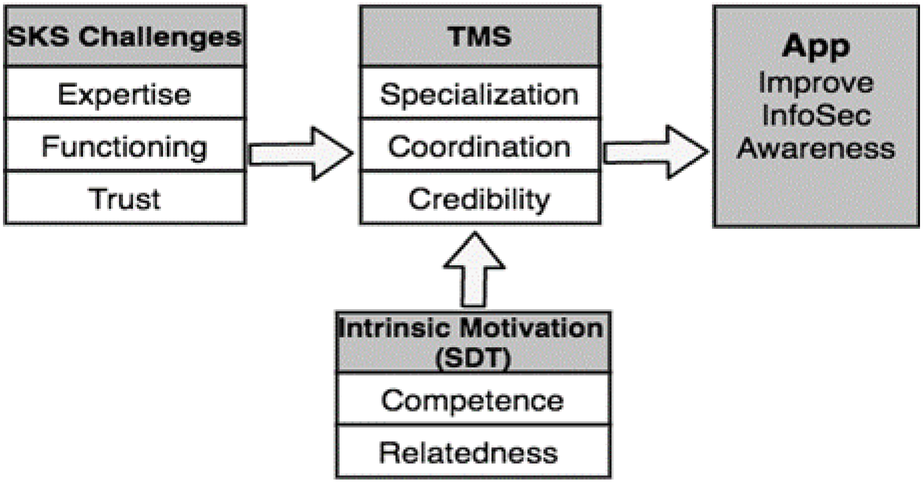


Figure 6.1 The proposed research model

When developing the instrument, the dissertation considered previous work in terms of how it tackled challenges and how the SKS model could be implemented to mitigate those challenges [150]. Further, what security knowledge issues should the employees be informed of, and how should these topics be presented? To achieve these goals, we adapted e-learning scenarios to encourage reflection and discovery among employees that involve multiple-choice questions delivered through a virtual connection [38, 103]. The scenarios are based on the Global Information Security Policy as well as basic human mistakes (in the real world) [28].

Many instructional concept models are available for use in developing effective e-learning in the workplace. Each researcher employs a unique approach, which varies based on the current aim and participants [173]. The ADDIE model is the most traditional model for instructional design, and all others are based on it. The model’s name is an acronym of the five phases that are involved in the process: Analyse, Design, Development, Implementation, and Evaluation [143], as seen in Figure 6.2.

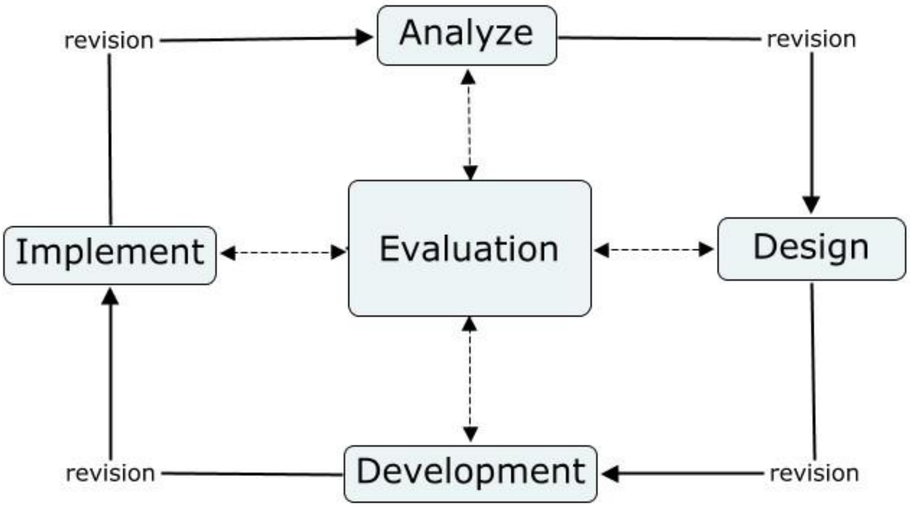


Figure 6.2 The five processes of the ADDIE model [1]

6.2.1 Analysis

In order to assess instructional objectives and assignments by evaluating learner characteristics, in this step, we attempted to understand the challenges of the previous work [174]. In addition, we interviewed 28 employees with a view to obtaining comprehensive insights that lead to enhanced understanding of SKS in natural environments [62]. Thus, this step explored the barriers and evaluated employees’ characteristics [1].

6.2.2 Design

The design stage involves establishing learning objectives, choosing an instructional methodology, identifying success goals, creating evaluation tools, and devising an instructional plan [174]. The learning objective was to provide employees with the information they need to deal with these threats in organisations by sharing their security knowledge. The methodology adopted to develop the STOW SYS was to design the idea and create the STOW components using Adobe XD. Adobe XD is a UI/UX tool for creating designs and prototypes of web pages and mobile apps and is used to create new design ideas.

6.2.3 Development

This stage is when designers and engineers begin the development and testing of the project's methodology [174]. In this step, the main app was developed using HTML, CSS, PHP, and Android Studio System Software V3.7. Moreover, the STOW SYS was evaluated using Android Emulator, which builds an android virtual device in Android Studio to be used by the emulator to install and run the application.

6.2.4 Implementation

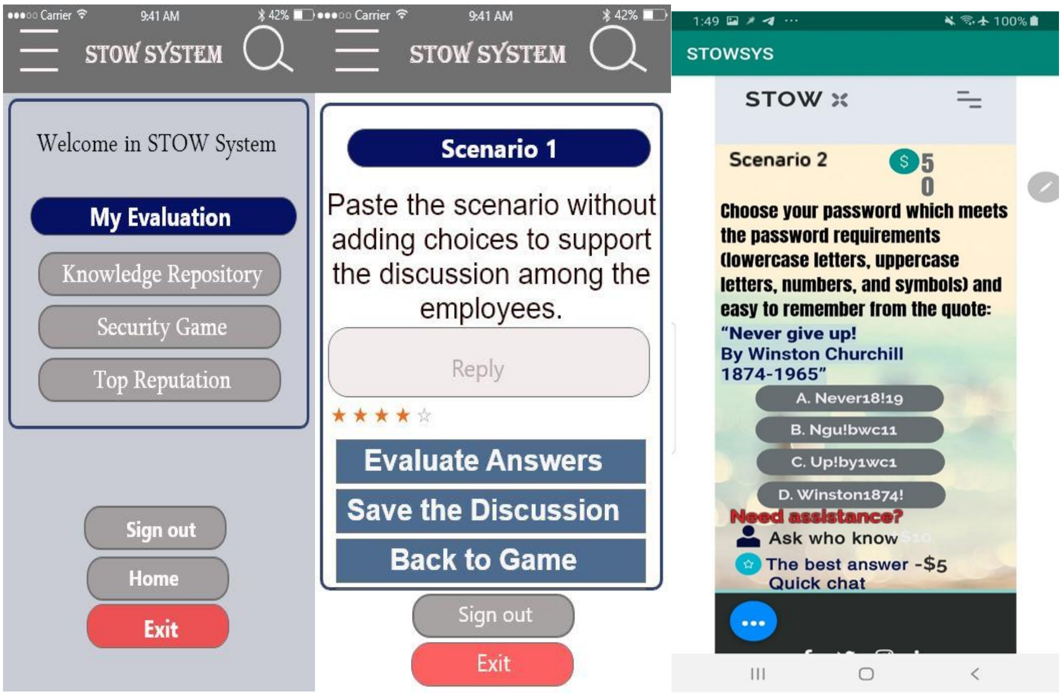
Implementation involves providing educational content, carrying out instructional exercises, and conducting formative tests [174]. The research adopted different scenarios to carry instructional material during the game. It was based on the Global Information Security Policy and common human errors. All scenarios were validated in the Literature Review. The style of the scenarios and challenges encourage employees to work together to achieve the same goal.

6.2.5 Evaluation

The last step was to test and improve the application [143, 174] . First was *UX testing*: The user experience (UX) criteria include navigation clarity, the interface's intuitiveness, the look and sound of the app's configuration, and error messages and handling. UX checking is critical to ensuring that the software is accepted by employees [175]. Second, two security experts evaluated the design of the experiment pilot studies and assisted in identifying problems that had been overlooked during the materials planning. This included the consistency of the instructions, the task's validity and sophistication, and the task's practicality in relation to the time available for the experiment. Finally, a pilot test was carried out among a small group of computing science PhD students. The feedback received from the students was used to make improvements to the design of the STOW. The first release of STOW V1.0 is as seen in Figure 6.3. STOW V1.0 was designed with a beginner user's ease of use in mind, as well as reliability in navigation and content coverage. The following best practices should be followed when developing a game's navigation features:

- A hyperlinked main menu makes navigation clear and easy.
- Employees can leave the game and restart where they left off.

- Employees can always communicate with and receive feedback on their location within the game.
- Employees can evaluate the answer and add a new answer if they believe it is superior.

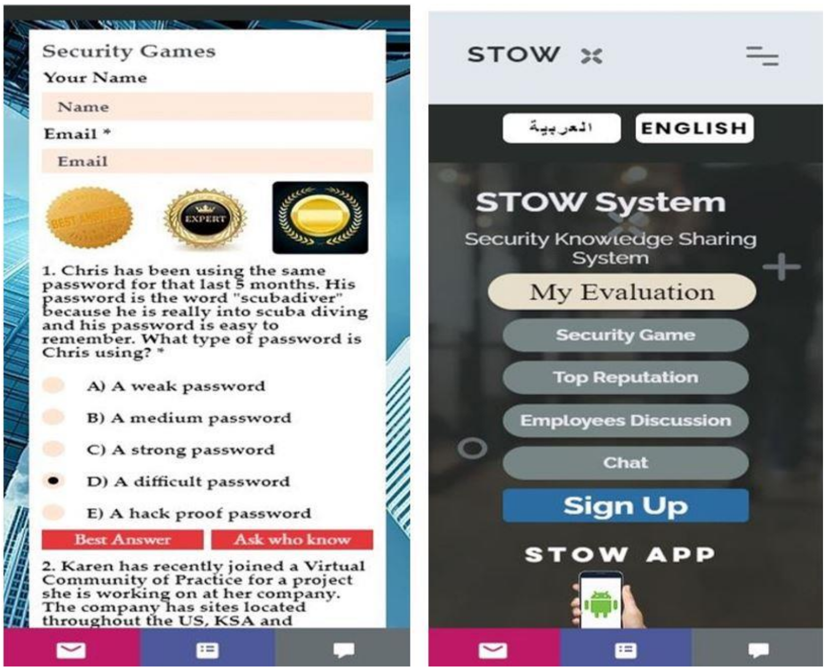


Paste the scenario without adding choices to support the discussion among the employees.

Choose your password which meets the password requirements (lowercase letters, uppercase letters, numbers, and symbols) and easy to remember from the quote: "Never give up! By Winston Churchill 1874-1965"

Figure 6.3 The first release of STOW V1.0

Following this, we received useful feedback to improve the performance of the app, such as bug fixes to optimise the user experience to make it even smoother, and certain performance improvements.



Security Games

Your Name

Name

Email *

Email

1. Chris has been using the same password for that last 5 months. His password is the word "scubadiver" because he is really into scuba diving and his password is easy to remember. What type of password is Chris using? *

○ A) A weak password

○ B) A medium password

○ C) A strong password

● D) A difficult password

○ E) A hack proof password

Best Answer | Ask who know

2. Karen has recently joined a Virtual Community of Practice for a project she is working on at her company. The company has sites located throughout the US, KSA and

STOW

العربية | ENGLISH

STOW System

Security Knowledge Sharing System

My Evaluation

Security Game

Top Reputation

Employees Discussion

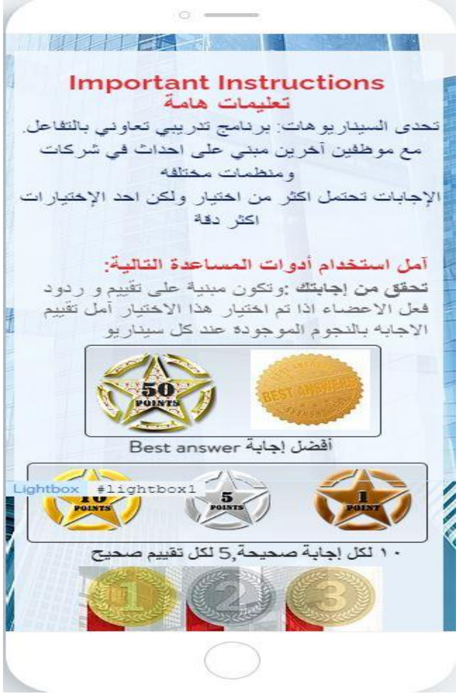
Chat

Sign Up

STOW APP

Figure 6.4 STOW Application V2

Furthermore, we noticed that employees could misunderstand the purpose of the STOW and disregard the resources that can help them determine the answer. To fix these issues, we added instructions before the game starts, as seen in Figure 6.5, to guarantee that they are made aware of the tools and tags.



Important Instructions
تعليمات هامة
تحدى السيناريوهات: برنامج تدريبي تعاوني بالتفاعل.
مع موظفين آخرين مبني على احداث في شركات
ومنظمات مختلفه
الإجابات تحتمل اكثر من اختيار ولكن احد الإختيارات
اكثر دقة

آمل استخدام أدوات المساعدة التالية:
تحقق من إجابتك :وتكون مبنية على تقييم و ردود
فعل الاعضاء اذا تم اختيار هذا الاختيار آمل تقييم
الاجابه بالنجوم الموجوده عند كل سيناريو

Best answer أفضل إجابة

١٠ لكل إجابة صحيحة,5 لكل تقييم صحيح

Figure 6.5 The STOW instructions before the game begins

6.3 The STOW Game Overview and Rules

The STOW is a security game presented as a mobile app (e-learning scenarios to encourage reflection and discovery among employees) which includes multiple choice questions via a virtual connection. The scenarios are based on the Global Information Security Policy and common human errors. STOW is designed to be played by employees as a group under the guidance of the IT department who will control the game, as shown in Figure 6.4.

Several features were included in the game to assist employees with interactions. For example, we gave them scenarios to think about, and the correct answers were theirs to decide based on their expertise. The experts can share their knowledge by adding the reason for choosing this answer via the "**Check Your Answer**" button, then the "**Add a New Answer**" button if they are not satisfied with the current best answer. The STOW system lets the employees look at the new solution by posting the new response and evaluating it. Moreover, the STWO provided the **"The Best Answer"** button based on the best evaluation by the employees and department, who validated it.

6.3.1 Design Elements for Game

Appropriate competition dynamics will help persuade employees to become more engaged in their assignments which were developed using the SKS model, as shown in Table 6.1.

Table 6.1 Design elements for game

Game dynamics	Related game elements	Description
Challenge scenarios	Points and badges	***Competence*** is an important component of intrinsic motivation and plays a key role in Credibility via Evaluation, as seen in Figure 6.7.
Leader board	Badges	***Relatedness***: Employees can trust co-workers based on the leader board, as seen in Figure 6.5 and Figure 6.8
Best answer	Reuse and Retrieve	***Competence***: Choosing the best answer based on employees' personal opinion, as seen in Figure 6.8.
Chat and ask who knows	Tracking improvement	The plan of the study was changed after Coronavirus to be online – the data will help to analyse improvements.
Badges	Badges	***Competence:*** Employees can collect badges that visually show their achievements, as shown in Figure 6.5 and .

6.3.2 The STOW Screen Design

This section details the STOW as it was applied to the employees during the experiment.

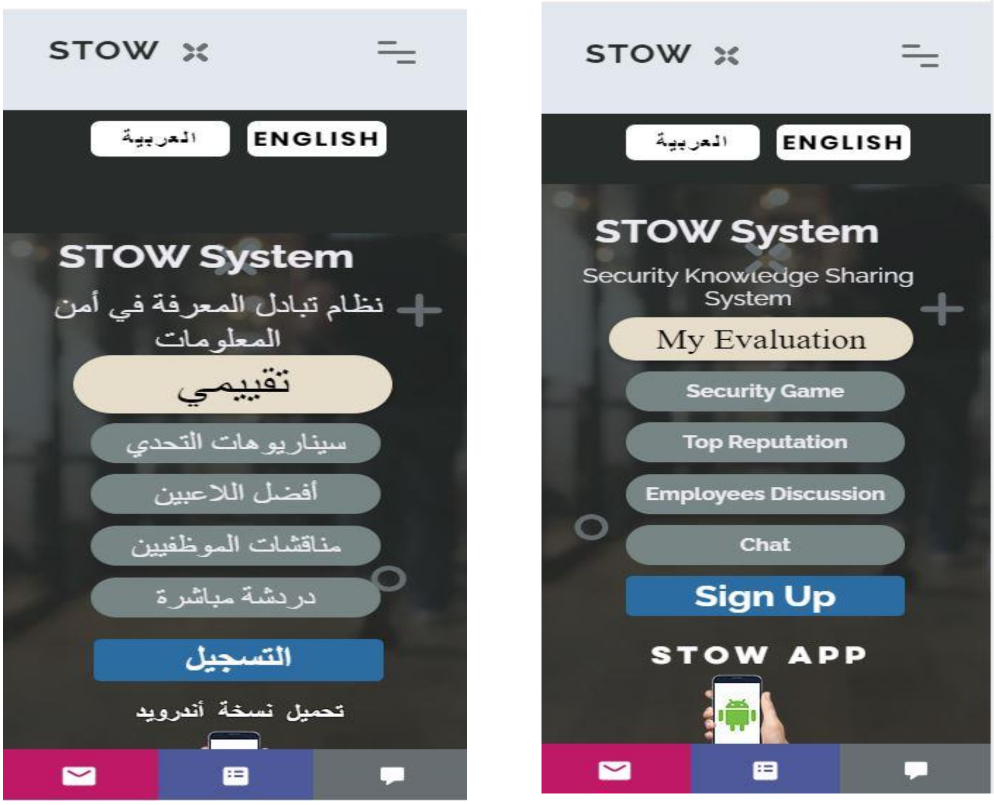
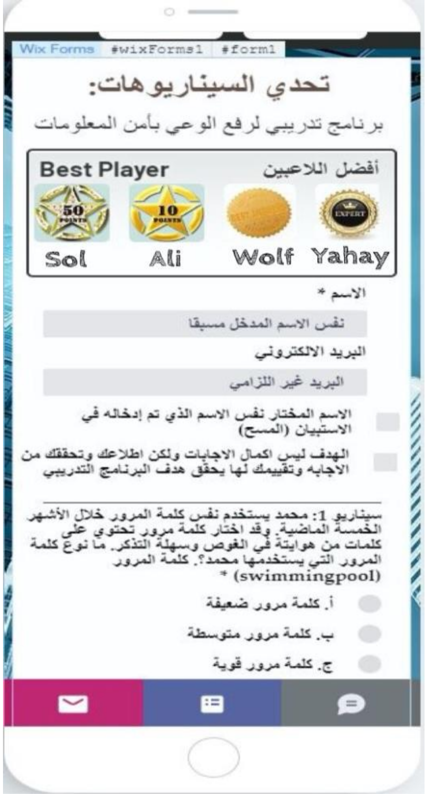


Figure 6.6 Home screen

After registering for STOW, employees received a pre-assessment evaluation. Following this, they began the game and then wrote their nickname or email to match pre- and post-assessment with the STOW players, as seen in Figures 6.7 and 6.8.



تحدي السيناريوهات:

برنامج تدريبي لرفع الوعي بأمن المعلومات

Best Player أفضل اللاعبين

Sol Ali Wolf Yahay

الاسم *

نفس الاسم المدخل مسبقا

البريد الالكتروني

البريد غير اللزامي

□ الاسم المختار نفس الاسم الذي تم إدخاله في الاستبيان (المسح)

□ الهدف ليس اكمال الاجابات ولكن اطلاعك وتحققك من الاجابه وتقييمك لها يحقق هدف البرنامج التدريبي

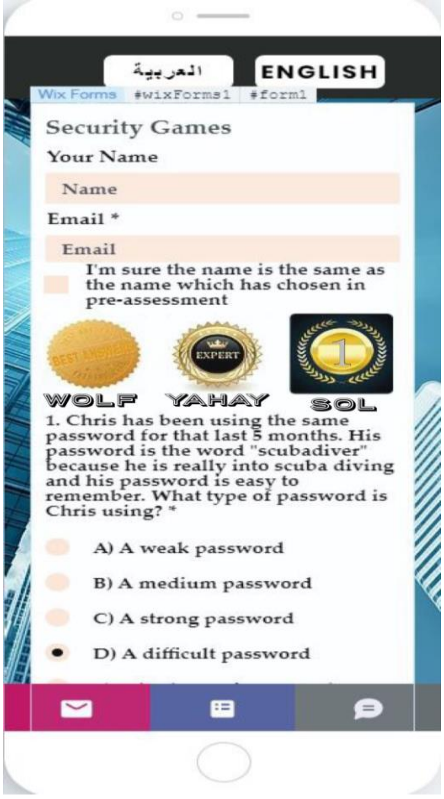
سيناريو 1: محمد يستخدم نفس كلمة المرور خلال الأشهر الخمسة الماضية. وقد اختار كلمة مرور تحتوي على كلمات من هوايتة في الغوص وسهلة التذكر. ما نوع كلمة المرور التي يستخدمها محمد؟. كلمة المرور (swimmingpool) *

○ أ. كلمة مرور ضعيفة

○ ب. كلمة مرور متوسطة

○ ج. كلمة مرور قوية

Figure 6.7 STOW game: Arabic



Security Games

Your Name

Name

Email *

Email

□ I'm sure the name is the same as the name which has chosen in pre-assessment

WOLF YAHAY SOL

1. Chris has been using the same password for that last 5 months. His password is the word "scubadiver" because he is really into scuba diving and his password is easy to remember. What type of password is Chris using? *

○ A) A weak password

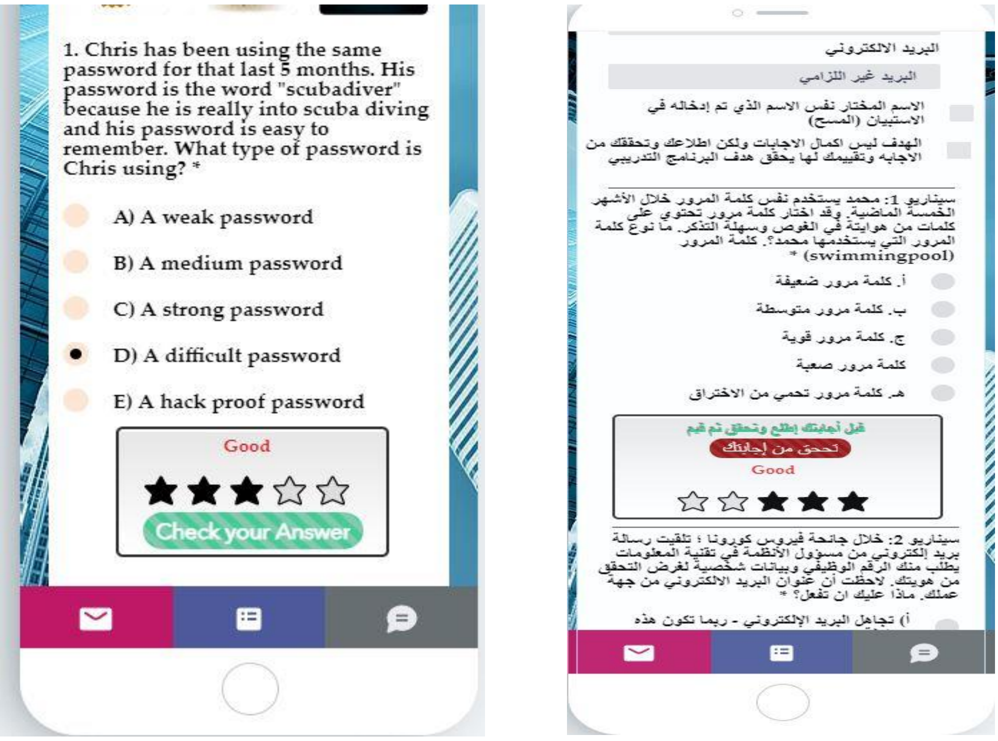
○ B) A medium password

○ C) A strong password

● D) A difficult password

Figure 6.8 STOW game: English

Several features were included in the game to assist employees with interactions, including ‘Check your Answer’ and ‘Evaluate’, as seen in Figure 6.9.



1. Chris has been using the same password for that last 5 months. His password is the word "scubadiver" because he is really into scuba diving and his password is easy to remember. What type of password is Chris using? *

○ A) A weak password

○ B) A medium password

○ C) A strong password

● D) A difficult password

○ E) A hack proof password

Good

★★★☆☆

Check your Answer

البريد الالكتروني

البريد غير اللزامي

□ الاسم المختار نفس الاسم الذي تم إدخاله في الاستبيان (المسح)

□ الهدف ليس اكمال الاجابات ولكن اطلاعك وتحققك من الاجابه وتقييمك لها يحقق هدف البرنامج التدريبي

سيناريو 1: محمد يستخدم نفس كلمة المرور خلال الأشهر الخمسة الماضية. وقد اختار كلمة مرور تحتوي على كلمات من هوايتة في الغوص وسهلة التذكر. ما نوع كلمة المرور التي يستخدمها محمد؟. كلمة المرور (swimmingpool) *

○ أ. كلمة مرور ضعيفة

○ ب. كلمة مرور متوسطة

○ ج. كلمة مرور قوية

○ كلمة مرور صعبة

○ هـ. كلمة مرور تحمي من الاختراق

قبل أجابتك إطلع وتحقق ثم قيم

تحقق من إجابتك

Good

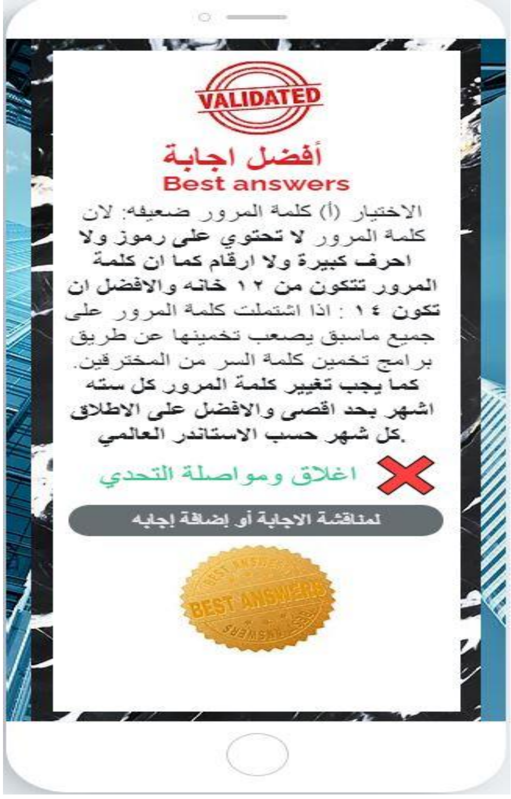
☆☆★★★

سيناريو 2: خلال جائحة فيروس كورونا ؛ تلقيت رسالة بريد إلكتروني من مسؤول الأنظمة في تقنية المعلومات يطلب منك الرقم الوظيفي وبيانات شخصية لغرض التحقق من هويتك. لاحظت أن عنوان البريد الالكتروني من جهة عملك. ماذا عليك ان تفعل؟ *

○ أ) تجاهل البريد الإلكتروني - ربما تكون هذه

Figure 6.7 STOW Evaluate and Check your Answer

Moreover, to authenticate the response, STOW allowed employees to evaluate it in the manner agreed upon by the SKS model. By pushing the same button, the best response is shown to the staff. Additionally, the information technology department developed a tag that verified the best response and awarded the best response badge, as seen in Figure 6.10.


VALIDATED

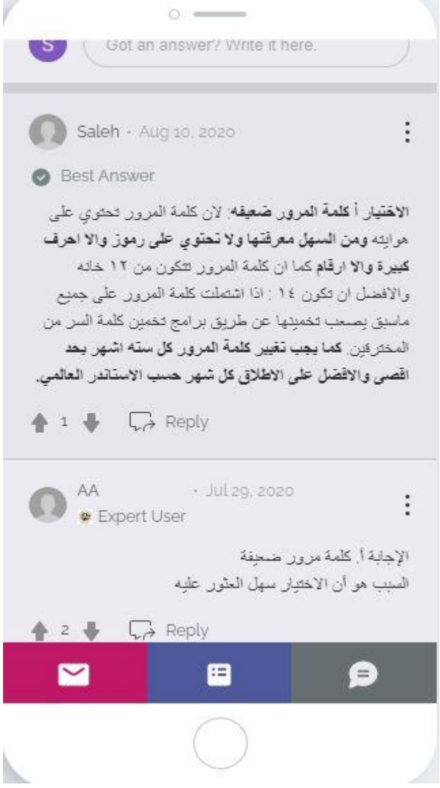
أفضل اجابة

Best answers

الاختيار (أ) كلمة المرور ضعيفه: لان كلمة المرور لا تحتوي على رموز ولا احرف كبيرة ولا ارقام كما ان كلمة المرور تتكون من ١٢ خانه والافضل ان تكون ١٤ : اذا اشتملت كلمة المرور على جميع ماسبق يصعب تخمينها عن طريق برامج تخمين كلمة السر من المخترقين. كما يجب تغيير كلمة المرور كل سته اشهر بحد اقصى والافضل على الاطلاق كل شهر حسب الاستاندر العالمي.

اغلاق ومواصلة التحدي

لمناقشة الاجابة أو إضافة إجابه


Got an answer? Write it here.

Saleh · Aug 10, 2020

Best Answer

الاختيار أ كلمة المرور ضعيفه: لان كلمة المرور تحتوي على هوايته **ومن السهل معرفتها ولا تحتوي على رموز والا احرف كبيرة والا ارقام** كما ان كلمة المرور تتكون من ١٢ خانه والافضل ان تكون ١٤ : اذا اشتملت كلمة المرور على جميع ماسبق يصعب تخمينها عن طريق برامج تخمين كلمة السر من المخترقين. **كما يجب تغيير كلمة المرور كل سته اشهر بحد اقصى والافضل على الاطلاق كل شهر حسب الاستاندر العالمي.**

1 Reply

AA · Jul 29, 2020

Expert User

الإجابة أ. كلمة مرور ضعيفة

السبب هو أن الاختيار سهل العثور عليه

2 Reply

Figure 6.8 Steps to validate the best answer

6.4 Chapter Contribution

Implementation and design of a system application based on SKS model: The study led to the design of a system and implementation based on the first and second experiments' findings to mitigate the challenges identified in the literature review. Then we developed and tested the app via Android Studio and CSS.

Implications for designers and developers: The thesis provides practical implications for system designers and developers who seek to improve employee security awareness within organisations via a collaborative model. Moreover, the study encourages employees to engage in prosocial behaviour through educational security games.

Gamification is a relatively recent concept in the field of information security. This indicates that employees may interact with and learn about information security risks and vulnerabilities via the use of a specifically designed game. Gamification has proven to be an effective method of increasing employees' ISA level since it tailors the ISA training material to their specific requirements [23].

6.5 Summary

The goal of this chapter was to look at the reasoning behind the STOW's construction as well as the theoretical foundation on which it was built. The chapter began by reviewing information security learning aspects to better grasp its meaning and process continuum, which begins with SKS and goes through security games and interaction. The STOW was built based on the SKS model to explain how security awareness could lead to inappropriate security behaviour. Moreover, this chapter described the STOW's elements, including the main page for the app. It is also explained how employees can register with STOW. The chapter concluded by explaining the STOW's structure and content categories, as well as the processes used in the intervention's implementation and the pilot study that was carried out to improve the app and address any concerns.

In the next chapter, we conduct an empirical study based on the outcome of this chapter to evaluate an application that facilitates information security knowledge sharing based on the SKS model in the real world.

Chapter Seven: Intervention Study

7.1 Purpose of the Study

The STOW was implemented based on the SKS model. The SKS model is considered in the first part of the SKS challenges. Moreover, TMS and SDT were theories to mitigate those challenges (as depicted in Figure 7.1). The study examined the impact of adopting the app in the real world to improve employee security awareness and enhance training. The experiment contributes to the existing body of knowledge by investigating how the app can improve SKS and can be used to encourage employees to learn more.

7.2 Theoretical Background of the Intervention

Collaborative interventions in information security should encourage employees to interact with each other to share their knowledge, enhancing the impact of teamwork which changes employee behaviour – thus providing solid advice for employees [62]. This study tested the effect of TMS theory to facilitate SKS. Moreover, the study encouraged TMS through intrinsic motivation, which is the SDT needs of employees within a STOW application. The STOW includes TMS to address organisational factors as well as SDT to address individual factors in the organisations. The research question for the chapter is: ‘Can security knowledge sharing be modelled using TMS and sharing encouraged by satisfying the self-determination needs of employees?’. After implementing the application, it will be empirically evaluated to answer this question, as shown in Figure 7.1.

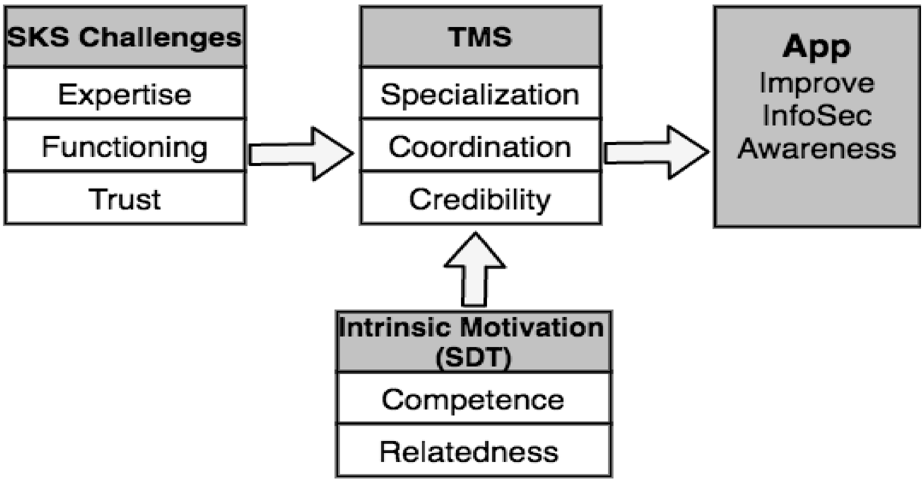


Figure 7.1 Intervention model

7.3 Ethical Approval

This experiment adopted the BPS ethical principles for performing experiments on human subjects and was accepted by the FIMS ethics committee of the University of Glasgow (300190139) (Appendix B.1).

7.4 Study Methodology

As described in Chapter 3 regarding the general methodology, this part contains additional specifics about the methods used in the experiment.

7.4.1 Data Collection Procedure

Group A – ***Intervention group***

Employees were given a pre-questionnaire (Information Security Assessment). They were then given the game application which provided users with knowledge about how their security awareness can be improved (two-week intervention). Following this, participants were given a post-questionnaire (Information Security Assessment), as seen in Figure 7.2.

Group B – ***Control group***

Participants in this group were given a pre- and post-questionnaire (Information Security Assessment) with no intervention to maximise SKS, as seen in Figure 7.2.

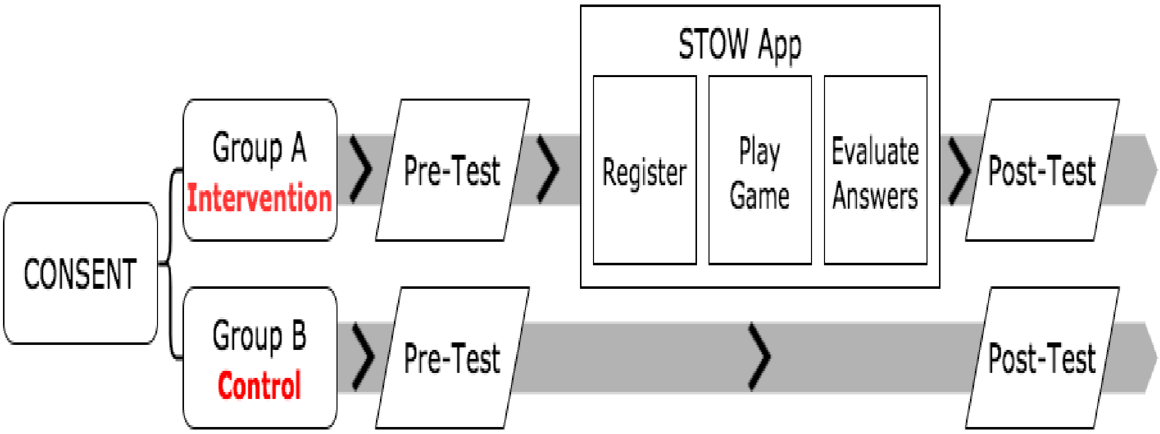


Figure 7.2 Assessment and game flow

7.4.2 Study Design and Participants

The study was conducted to whether the effects of satisfaction of SDT needs mitigate SKS challenges between the intervention and control groups. After the study was approved by the FIMS ethics committee of the University of Glasgow, three hundred employees at one university in Saudi Arabia were invited to participate in the study. The university has two campuses in two different cities. Group A was on campus (AR), and Group B was on campus (RA). One hundred and twenty-eight (43%) employees agreed to participate in the study and were divided into two groups: intervention in campus A (n=64) and control group in campus B (n=64). The study groups were not allocated to employees at random; our goal was to reduce the chance that the control group might learn about ergonomics from the other two groups. As a result, participants were divided into groups based on their buildings' geographic isolation. Participants who completed the steps are presented in Table 7.7.1, with participant statistics shown in

Table **7.7.2**.

Table 7.7.1 Demographic information

Categories	**Sub-categories Intervention Group A**	**# (n=39)**
Gender	Female Male	9 31
Age	20-30 31-40 41-50	4 27 6

	Over 51	3
Education	High School or Below	5
	Bachelor’s degree	26
	Master’s degree	6
	PhD	3
Categories	**Sub-categories Control Group B**	**# (n=40)**
Gender	Female	12
	Male	27
Age	20-30	3
	31-40	27
	41-50	5
	Over 51	3
Education	High School or Below	6
	Bachelor’s degree	19
	Master’s degree	7
	PhD	7

Table 7.7.2 Participant statistics

Group	Pre-Assessment	Games	Post-Assessment
A	64	52	39
B	64	none	40

7.4.3 Scenario and Questionnaire Component Validity

Validity was measured using a content validity expert panel consisting of two faculty members and six doctoral students experienced in quantitative analysis and quantitative research. The techniques established content validity for all scenarios (both formative and reflective) via a literature study [176]. Our target in this experiment was to improve the delivery of training in information security awareness. To put this theory to the test, scenarios and questionnaires focused on password management, email usage, and general questions about incidents that occurred during the workday. For several reasons, both the recommendations in the Literature Review and the Data Breach Investigations Report confirmed that the most common causes of security breaches in many organisations were password management and email use [177, 178]. Due to the short duration of the experiment, it was not possible to cover all aspects of information security awareness. Additionally, concentrating on specific elements aids in testing the research hypothesis and obtaining an answer.

7.4.4 Awareness Level Measurement

The following awareness scale, adopted by Kruger and Kearney, was used to explain the level of awareness as seen in Table 7.3 [179].

Table 7.3 Awareness level measurement

Awareness	Measurement (%)	Actions
Good	80–100	Satisfactory: badges as an expert user and can be group leader.
Average	60–79	Minor– action potentially required
Poor	59 and less	Unsatisfactory: needs improvement

7.5 Data Analysis

As indicated in the methodology chapter, the data for this stage came from a survey (questionnaire), documents, and observations. The experiment's approach to data analysis was divided into two phases: quantitative and qualitative.

7.5.1 Analysis of Quantitative Data

Quantitative data, taken from the pre- and post-intervention measurements were compared to see whether the intervention had made any changes to the employees' security knowledge. Quantitative data analysis was the first phase, which included information taken from a questionnaire which was collected pre- and post-assessment. First of all, normality tests were performed on the data prior to running the analysis. To fulfil normality requirements, the research tested outliers in the intervention and control groups. [180]. Engagement scores were normally distributed for the control and intervention groups, as seen in Table 7.7.4. The control group was assessed using Shapiro-Wilk's test ($p=0.552 < .05$) as shown in Table 7.7.4. This group was also assessed by visual inspection of normal Q-Q plots, as shown in Figure 7.3. Thus, as the p-value is larger than 0.05, we assume a normal distribution.

The intervention group was as assessed by Shapiro-Wilk's test ($p=0.017 < .05$) as shown in Table 7.7.4. Additionally, the participants were assessed by visual inspection of normal Q-Q plots, as shown in Figure 7.3. Therefore, if the p-value is smaller than 0.05, we do not assume a normal distribution, as seen in Table 7.7.4.

The control group was dispersed normally, whereas the intervention group was not. Thus, non-parametric tests were used in the statistical analysis [181-183].

The Wilcoxon signed-rank test was used within groups to determine the median difference between pre and post-intervention [184]. A between-group design was used in the Mann-Whitney U test to determine differences between the two groups on a continuous or ordinal dependent variable [181, 185].

Table 7.7.4 Tests of normality

Group		**Kolmogorov Smirnov**			**Shapiro Wilk**		
		Statistic	Df	P-value	Statistic	Df	P-value
Difference	Intervention	.152	39	.023	.930	39	.017
	Control	.081	40	.200	.976	40	.552

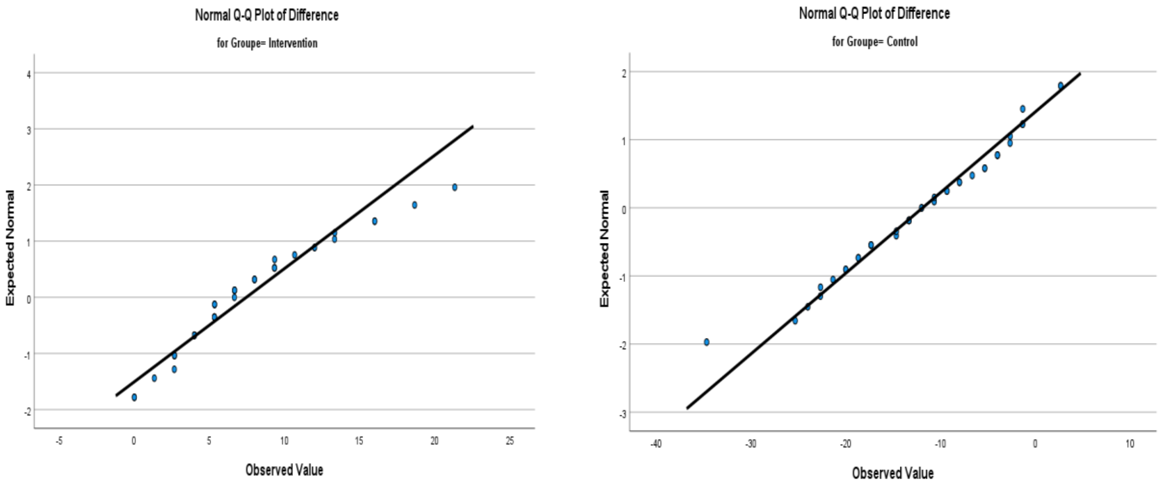


Figure 7.3 Visual inspection of normal Q-Q plots of Control Group

7.5.2 Analysis of Qualitative Data

The experiment followed three steps to analyse the qualitative data:

- Pre-assessment test: The pre-assessment test score was used to determine the players' information security awareness before the game, as well as to measure KS during work before STOW.
- During the game: we followed the requirements of the factors which we have addressed in the SKS model in the document. The document included the employees' scores before, after, and during the game. Also included are interactions during the game, such as contributions to the knowledge repository, evaluation of the players' answers, and lower players before and after the game.
- Post-assessment test: Following the game, the post-assessment test score was utilised to establish the players' level of information security awareness, as well as to determine whether the STOW improved knowledge exchange during the workday after use.

7.6 Results

After we implemented and empirically tested the application, the research question could be addressed. The results are divided into two sections: quantitative and qualitative.

7.6.1 Quantitative Results

7.6.1.1 Within-subject design

Intervention Group A

Following the intervention, there was a significant increase in the employees' level of information security awareness.

To determine whether the intervention increased employees' level of information security awareness, a Wilcoxon signed-rank test revealed a statistically significant increase in employees' security knowledge for the intervention group participants: z = -5.35, p = 0.00, with a large effect size (r = 0.72) as seen in the descriptive statistics table (Table 7.5) and Wilcoxon signed-rank test (Table 7.6). Participants' pre-test and post-test scores are presented in Figure 7.4.

Table 7.5 Descriptive statistics: Group A

Group A	N	Mean	Std. Deviation	Minimum	Maximum
Pre-test	39	78.57	8.1	48	90.7
Post-test	39	86.02	6.75	64	96

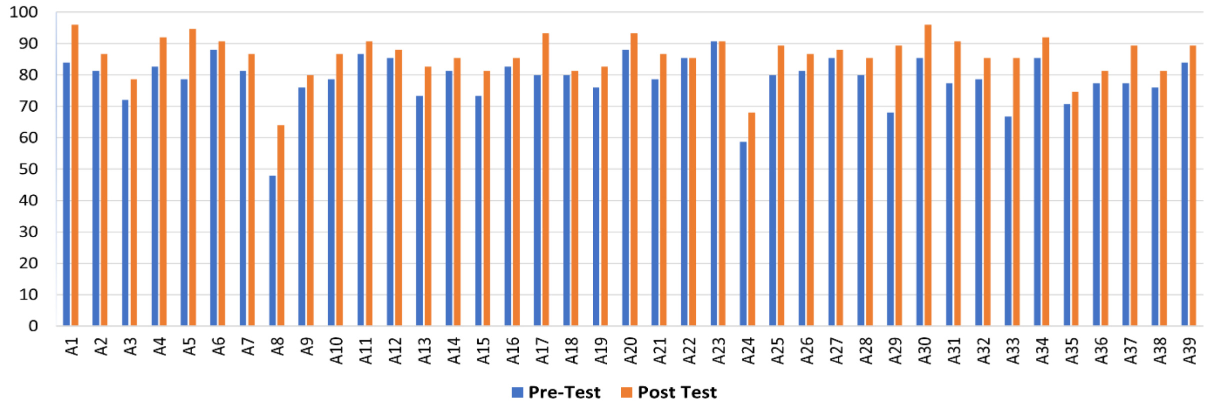


Figure 7.4 Intervention Group A before and after

Table 7.6 Wilcoxon signed ranks test: Group A

<table>
<tr><td rowspan="4"><b>Pre-test – Post-test</b></td><td><b>Ranks</b></td><td><b>N</b></td><td><b>Z-value</b></td></tr>
<tr><td>Negative Ranks</td><td>0</td><td><b>-5.35</b></td></tr>
<tr><td>Positive Ranks</td><td>37</td><td><b>P-value</b></td></tr>
<tr><td>Ties</td><td>2</td><td><b>0.00</b></td></tr>
<tr><td></td><td>Total</td><td colspan="2">39</td></tr>
</table>

Control Group B

There was no significant increase in the employees' level of information security awareness: z = -5.31, p = 0.00, with a large effect size (r = 0.71) as seen the descriptive statistics (Table 7.7) and Wilcoxon signed-rank test (Table 7.8). Participants' pre-test and post-test scores are presented in

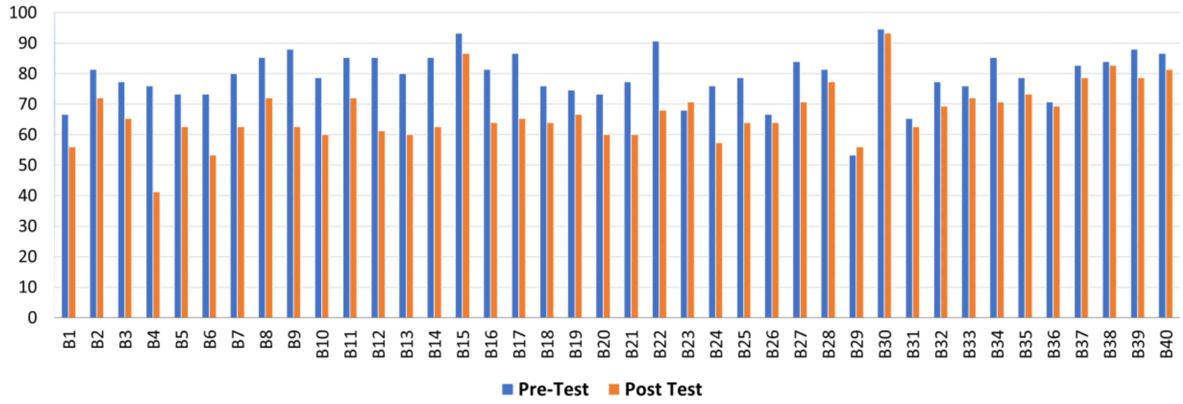


Figure 7.5 Control Group B before and after

Table 7.7 Descriptive statistics: Group B

Group B	N	Mean	Std. Deviation	Minimum	Maximum
Pre-test	40	79.1	8.2	53.3	94.6
Post-test	40	67.2	9.6	41.3	93.3

Table 7.8 Wilcoxon signed ranks test: Group B

	Ranks	N	Z-value
Pre-test – Post-test	Negative Ranks	38	**-5.35**
	Positive Ranks	2	**P-value**
	Ties	0	**0.00**
	Total	40	

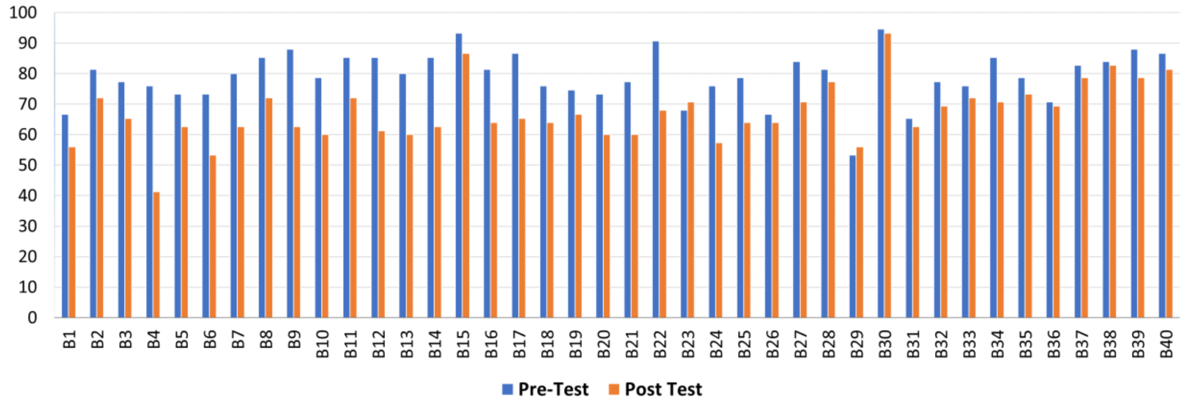


Figure 7.5 Control Group B

7.6.1.2 Comparison Between and Within Groups

There were no statistically significant differences in pre-test scores for security knowledge. The mean rank was 39.76 in Group A, while Group B was 40.24, illustrating no significant difference between control and intervention.

The intervention group significantly improved their knowledge (mean rank = 57.23) after the intervention. The control group demonstrated no significant differences between pre-test and post-test scores in security knowledge (mean rank = 23.2), as seen in Table 7.9. Unexpectedly, the control group result in the post-test was lower than the pre-test, most likely due to the fact that they did not know the answers and therefore did not spend much time answering the questions. The results were z = -6.59, p = 0.00, with a large effect size (r = 0.56). The mean for both can be seen in Figure 7.6.

The decrease in group B caused the participants not to care about their score the second time around. After noting that the average time taken to complete the pre-questionnaire was 10–12 minutes, we noticed that the post-questionnaire took 4–6 minutes. The STOW was able to improve engagement.

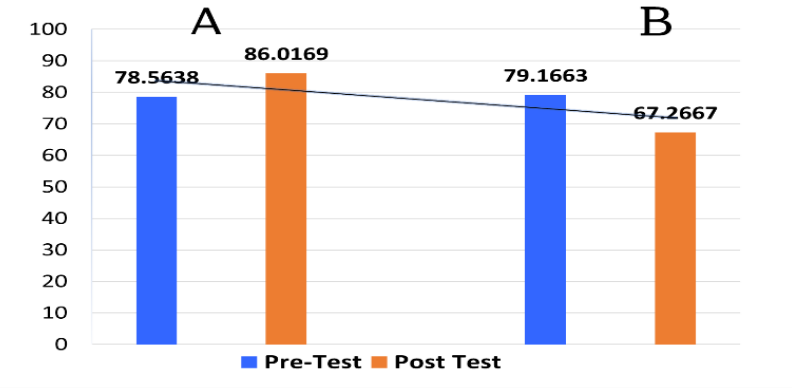


Figure 7.6 Mean of A and B

**mean is the average score*

Table 7.9 Mann–Whitney test - Ranks

	Group	N	Mean Rank	Sum of Ranks
Pre-Test	Intervention A	39	39.76	1550.5
	Control B	40	40.24	1609.5
Post Test	Intervention A	39	57.23	2232
	Control B	40	23.2	928

7.6.2 Qualitative Results

7.6.2.1 Pre-Assessment Test

Prior to the game, we evaluated each player's level of information security knowledge. As shown in Figure 7.9, the players' awareness levels were a good 21%, an average 16%, and a poor 3%. We also counted how many times employees shared their information before using the STOW system. As shown in Figure 7.7, the employees were 2% daily, 6% weekly, 16% monthly, and 76% never.

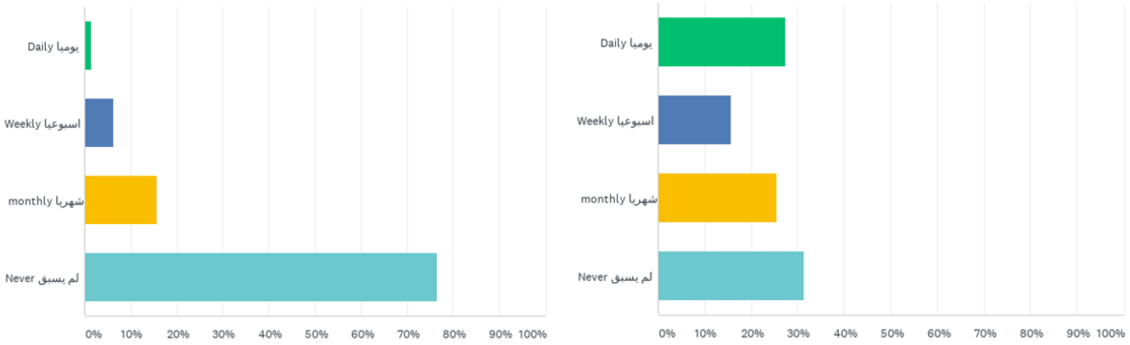


Figure 7.7 Group A: Frequency of employees sharing knowledge

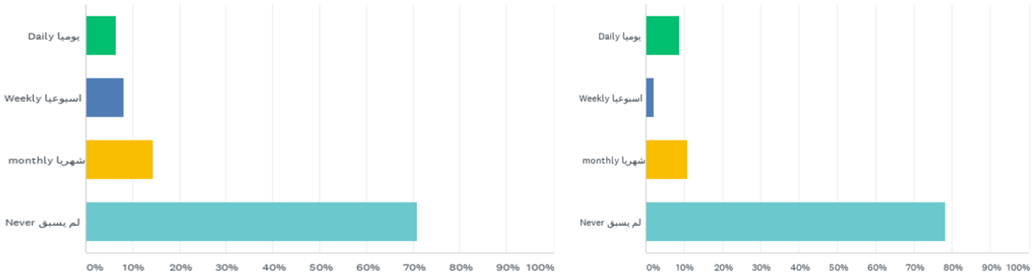


Figure 7.8 Group B: Frequency of employees sharing knowledge

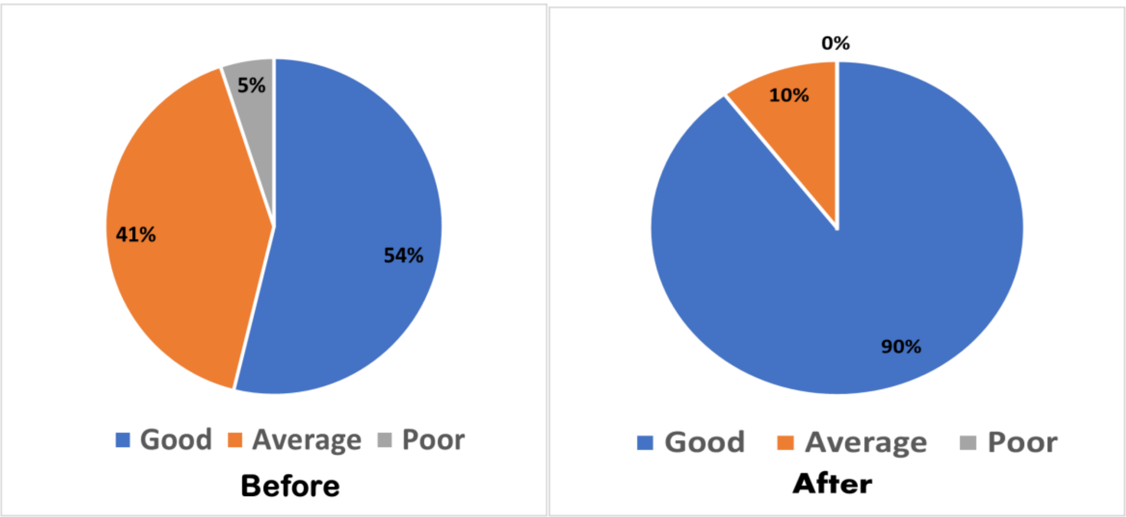


Figure 7.9 Player awareness levels

7.6.2.2 During the Games

Many players were registered on the STOW SYS as the record was confirmed from the file that tracked the players during the game. Forty players completed the steps of the games until they have completed all rounds of the games. One of the main goals of the STOW was to encourage employees to interact with one another during the game. Consequently, 39 out of 40 employees interacted with STOW and shared their knowledge with others. They evaluated 372 answers in order to evaluate the knowledge added by the employees and to obtain the correct answer, as seen in Table 7.10.

Table 7.10 STOW's panel control

Players registered	Players completed game	Player Interaction	Answer evaluated
52	40	39	372

Best players based on contributions and evaluated answers: To track players and award them tags based on their expertise, the STOW offered them numerous tags, such as "Expert User", based on their performance on the pre-assessment test. Furthermore, employee evaluation was used to find the best replies. Finally, based on the tags, the best three players were identified and validated by the IT department, who supplied the best response (Table 7.11).

Table 7.11 Best STOW players during the game

Best Player	Assessment test	Measurement	Reward
A17	93.33%	Expert	Expert User, 3 Best Answers and Second-best player
A1	96%	Expert	Expert User, 1 Best Answer and First best player
A31	90.66%	Expert	Expert User, 1 Best Answer and Third best player

Lower players before and after the game: The experiment focused on lower-level players both before and after the game, with the findings reported by four employees who had improved their game knowledge. The first employee, B8, scored 48% in the pre-assessment, which was poor. After he used the STOW, completed all of the scenarios, and interacted with others to evaluate the best answers, he improved his score to 64% in the post-assessment, which is average. Employee B24 scored 58%, which was also low, but he improved to 68% after following all of the game instructions. The third user scored 66%, which is considered poor after scoring 85% in the first one. This user completed all of the scenarios but did not select the best answer because experts had recommended some of them. During the game, he also interacted with many other players. The last user, B29, scored 68% in the pre-assessment. After the interaction with the STOW, he completed all of the scenarios, but he also did not select the best answer because experts had recommended some of them. He also interacted with many other players during the game, and he improved to 85%, as shown in Table 7.12.

Table 7.12 Lower scoring players before and after the game

Lower Player	Before	During	After
B8	48%	All scenarios completed and best answers evaluated	64%
B24	58%	All scenarios completed but best answers not evaluated	68%
B33	66%	All scenarios completed but best answer not chosen as experts recommended some answers. Interacted with other players during the game	85%
B29	68%	All scenarios completed, best answers evaluated, and user interacted with other players during the game	89%

7.6.2.3 Post-Assessment Test

After the game, each player’s level of information security knowledge was evaluated. As shown in Figure 7.9, players’ awareness levels were good at 90% rather than 54%, an average 10% instead of 41%, and a poor 0% instead of 5%. Additionally, there was an increase in the frequency with which employees shared knowledge following the implementation of STOW. Following the game, we found that employees increased their daily sharing by 28% rather than 2%, their weekly sharing by 15% rather than 6%, their monthly sharing by 35% rather than 16%, and never sharing reduced to 31% from 76%. In contrast, as seen in Figure 7.8, the control group did not improve.

7.7 Discussion and Implications

The main experimental contribution of our study lies in extending TMS and SDT theory beyond the delivery of ISA training [113], which tends to create an ‘objectivist’ view of the collaborative model [27]. We discuss the overall findings, which include both qualitative and quantitative sections, as well as the implications for the results.

7.7.1 Qualitative Section Overall Findings

This section shows the impact of the results on improving cybersecurity awareness training to help interpret the findings and understand how to incorporate them into the field of study. The research question was to determine the impact of the SKS model, which includes intrinsic motivation and KS. To answer this question, we conducted an empirical investigation consisting of two theories into the SKS model. Some authors have speculated that the connection between motivation and KS at work is an important issue, but the data on the topic are contradictory [186, 187]. However, a number of issues were identified, including the fact that the use of KS interventions can improve KS and that meeting employees' self-determination requirements facilitate that sharing [188, 189]. According to Choi et al. [36], despite attempts, no earlier empirical research has explicitly examined the impact of information technology in the development of TMS. This study set out with the aim of assessing the importance of SKS at work. The study examined empirical research to add the impact of SKS in the real world to the literature [36].

To interpret the statement, we divided the TMS and SDT dimensions into three sources. Each source, together with supporting quotations from participants, is included in the following sub-sections, as are the application's observations. The three sources are: interaction and facilitating learning, self-efficacy and encouraging others, and the impact of enjoyment on learning [162]. The following section discusses the consequences of these findings.

7.7.1.1 Interaction and Facilitating Learning

Interaction and facilitating learning are essential factors required to develop an understanding of interaction among employees and understanding what needs must be met in the system [62, 162]. The study included interaction within the app to satisfy the relatedness of the SKS model [62]. As mentioned in the literature review, relatedness is the need for connection, i.e., a person's wish for support and feelings of connection with others around them [96]. This is a type of intrinsic motivation which encourages humans to change their behaviour by being self-motivated [96]. It connects employees via the app. Furthermore, the study satisfies the facilitated coordination requirements in our model, which was included in the app. As previously stated in the review of the literature, coordination describes the efficiency of the team in terms of knowledge processing while working together [83, 72].

The majority of the previous studies investigated a specific strategy for increasing employees' security knowledge based on an individual theory [162, 123, 66, 127]. In particular, the individual approach considers a person in isolation [62]. However, according to our findings, coordination and relatedness can make a difference in changing employees' attention and interaction during training. These results match those observed in earlier studies using the SKS model that established a relationship between those factors [62, 162]. Empirical research has also confirmed such a link [62]. Participant A15 indicated that:

> *"The knowledge repository aids in the resolution of recurring problems and allows us to get solutions from sources other than IT. It also keeps us together during COVID-19".*

This statement conveys the significance of those factors in managing knowledge and connecting employees via the app, especially when working from home during the COVID-19 pandemic. Additionally, the app's recording revealed the actions that occurred during the game, as seen in Table 7.10, in which the employees interacted with one another in order to answer all the scenarios. This finding is consistent with Tortorella et al. (2021). The results demonstrate the critical nature of organisational learning practices via TMS and individual behaviour when individuals are not in their usual work environment, for instance during a pandemic [190].

7.7.1.2 Self-Efficacy and Encouraging Others

Self-efficacy is an important factor in instilling trust in employees as well as validating their knowledge during KS [191]. Credibility, specialisation at the organisational level, and individual competence were the elements adopted to achieve the self-efficacy factor in our app. As stated in the existing literature, Credibility is the way in which individual team members perceive the reliability of the knowledge held by the other members of the team. Specialisation is the term used to describe the degree of differentiation of the knowledge held by team members [83, 72]. Moreover, **competence** is the need for a sense of competence, which is when a person desires self-efficacy, which shows the ability of the person to do something. Competence is one of the intrinsic motivations that can cause changes in the behaviour of humans.

To date, only a few studies on the effect of TMS on motivation have been conducted [62, 192, 187]. The SKS model adopted competence as an intrinsic motivation in order to demonstrate the ability of employees through the elements of our intervention [85]. This study produced results which corroborate the findings of a great deal of the previous work on competence related to an individual's sense of self-efficacy. When feelings of competence are experienced during a particular action as a result of evaluation and feedback, intrinsic motivation increases [103, 85]. Positive performance feedback has been demonstrated to increase intrinsic motivation in previous research. Furthermore, recent evidence confirms that user feedback and evaluation can positively influence behavioural intentions to engage in secure behaviours [103, 170]. Moreover, the result of reinforcing a person's competence in terms of computer-based activities was a rise in their confidence in their aptitude in this area [171]. Credibility and specialisation define the extent to which team members trust that the relevant task expertise of another team member is correct and accurate [78].

The current study's findings support our theoretical model, which was implemented in the STOW [62]. STOW created a feature that converted the challenge scenarios' elements into points and badges. Additionally, a leader board was created, which was crucial in building confidence in employees regarding their ability to choose the correct answer during the game [103, 85]. Likewise, the best answer tag was the means used to evaluate employees during the game [103, 170]. Our findings report that employees' confidence improves when they have a sense of self-efficacy. As a result, we strive to maximise SKS within our organisations. The majority of participants expressed confidence in their ability to find the correct answer based on STOW.

> *"The electronic system facilitated communication with colleagues and was available at all times. We can know the validity of the data through evaluation and through badges granted to experts".* (A15)

> *"Providing collaborative training and sharing data through the mobile program, which facilitates the exchange and preservation of knowledge, and a friendly knowledge assessment system capable of raising credibility with correct information".* (A13)

7.7.1.3 The Impact of Enjoyment on Learning

As a new finding in the study was the impact of intrinsic motivation through autonomy. According to the existing literature, autonomy is defined as a person's desire to self-organise his or her own actions in order to feel like they have control over what they do. The game, as stated in the previous study, was a type of intrinsic motivation [88]. The game gave employees complete control over their actions. Because of their enjoyment of the game, the majority of employees completed their tasks, as shown in Table 7.10. Most previous studies, according to Alzahrani and Johnson, have overlooked intrinsic motivational elements, which refer to doing something purely for the sake of intrinsic interest or enjoyment [193, 194]. Moreover, some participants shared their experiences with the STOW:

> *"It saved a lot of time, and I had a fun time".* (A18)

> *"It gave a highly reliable collaborative and electronic training system that allowed easy communication in a safe environment and had flexible time to complete the scenarios".* (A14)

Finally, as Alkaldi et al. confirmed, enjoyment plays a vital role in persuading employees to change their behaviour [87]. Additionally, Alzahrani et al. demonstrated that a satisfactory SDT is effective at encouraging such compliance in organisations [102]. Furthermore, our findings confirmed the positive effect of autonomy, such as changing security training to gamification that includes features mentioned in the previous sections to implement the SKS model [162]. According to Rigby and Ryan (2011), if a game is designed using meaningful stories, avatars, and teammates, a shared goal is introduced, and this leads to perceptions of relevance. Feelings of social relatedness were induced [109, 127]. An important aspect of gamification is that players are provided with specific feedback that serves to induce feelings of competence in their performance. There is thus an expectation that leader boards, badges, and performance charts will induce these feelings of competence in our users [127]. Consequently, these features enable employees to develop social bonds, allowing them to cooperate in person. Designing appropriate competition dynamics will help persuade employees to be engaged in their assignments [109, 127]

7.7.2 Quantitative Section Overall Findings

The results show that the STOW improved employee security knowledge among participants (as measured by a post-assessment exam) in comparison to who did not receive the training. In addition, the intervention participants showed various other significant differences from the control group after training, including attitude changes relating to both positive and negative outcomes. As a result, slots 1-4 have been confirmed. Additionally, employees who completed the STOW game demonstrated significantly higher self-efficacy perceptions than those who did not receive the training. Finally, the results revealed that employees who received STOW training perceived and interacted with the game in a more positive light than employees who did not interact with the game.

The intervention group worked through a number of scenarios and debriefings that included a range of different types of learning methods, including active learning, cooperative learning, and expert evaluation. Deliberate practise and feedback have been found to enhance trust and validate knowledge [170].

Overall, our study revealed that the intervention group participants, who received training, had superior knowledge in assessing and responding to security incidents compared to the control group. Moreover, due to the lack of studies confirming the association, the study eliminated autonomy and relatedness. However, a limited study conducted in a security context confirmed that autonomy positively affects human behaviour changes. According to recently published policy compliance research, satisfying SDT successfully encourages such compliance in organisations [102, 88]. Alkaldi et al. (2019) confirmed the critical effect of applying autonomy to security tool adoption decisions [87]. The new findings explored the positive relationship between autonomy as intrinsic motivation and relatedness, which previous research did not investigate.

Thus, the STOW has mitigated the challenges of SKS, such as the competence and credibility needed to build trust, which was one of the main challenges. Moreover, the reluctance and coordination helped the functioning of the SKS to maximise and facilitate the KS in organisations.

7.8 Chapter Contribution

Empirical experiment involving security knowledge sharing app: The experiment evaluates the effect of using the app in the real world to enhance training and improve employees' security awareness in organisations. The experiment contributes to the knowledge by examining how the app can identify how SKS can be enhanced, and also how the app can be used to encourage employees to improve and share their knowledge.

Autonomy as intrinsic motivation and relatedness: This study extends the knowledge on how to deliver security training by exploring the positive effects of the inclusion of autonomy as intrinsic motivation and relatedness in training (STOW). Both encouraged the employees to complete the training without any external influence, which led to enhancing the employees' security knowledge.

7.9 Summary

This chapter described an intervention in information security training for an organisation in Saudi Arabia. The purpose of the experiment was to look at how app adoption may enhance employee security awareness and training. It investigated how the app could improve SKS, as well as how it could be used and encouraged to help employees learn more.

The study has identified that the participating organisation implemented STOW for use by 39 employees – Group A – who received the intervention, as well as 40 employees as a control group, namely Group B. Each group was located in a different geographical area to ensure that they did not affect each other during the experiment. Employees completed a pre-survey (Information Security Assessment). They completed the game in the app over a two-week period, which included some knowledge about how users may increase their awareness as well as scenarios concerning email use and password management. They also received a post-questionnaire (Information Security Assessment) to assess the STOW and employee security knowledge.

The findings from the experiment indicate that the intervention group, which received training, had superior knowledge of assessing and responding to security incidents compared to the control group, and their ISA was increased. Along with obtaining additional data, new findings explored the positive relationship between autonomy as intrinsic motivation and relatedness, which has not been investigated before.

To ascertain employees' actual behaviours, we asked the IT department whether there had been any security incidents in the preceding three months among the employees who received the training. According to the IT report, there were no incidents to report.

The study results reveal those various underlying causes of the improvement following the STOW were tracked before, during, and after the game, proving the effect of the SKS model on changing how security training is delivered.

The next chapter presents the study conclusions and recommendations for future work.

Chapter Eight: Conclusions and Future Work

This chapter discusses the research contributions and achievements of the SKS that has been created. Additionally, the chapter summarises the study's overall findings and examines the final research outcomes. The chapter concludes with a discussion of the research limitations, recommendations, and future research directions.

8.1 Answering the Research Questions

8.1.1 Research Sub-question 1

The answer to the first sub-question, "What are the challenges of SKS to improve security awareness?", can be derived from the exploratory study of SKS challenges in the organisations presented in Chapter 4. The study identifies the challenges that prevent SKS within an organisation. The study identified a number of factors that limit knowledge exchange within organisations. To gain a better understanding of these aspects, a qualitative method was used, with semi-structured interviews conducted in Saudi and British organisations located in various geographical regions. Interviewing is the most effective strategy for eliciting thorough insights that enable the most accurate analysis of information transfer in real settings. The data gathered enabled the development of practical solutions. These findings should make an essential contribution to the field of cooperative training. Organisations must consider practical and theoretical solutions that help ease these barriers to obtain the advantage of SKS in the workplace and learn from mistakes.

8.1.2 Research Sub-question 2

The answer to the second sub-question, "How can information security knowledge be facilitated through the understanding of a transactive memory system (TMS)?", can be derived from Chapter 5. The study examined the scale reliability and relationships between the TMS and other constructs at an organisational level. This is a new finding in the security context. The IT department can develop the ISA based on the TMS as an organisational theory that can be applied in security training, and in particular, in ISA training. Additionally, the thesis suggested a model that considers the aspects that contribute to an organisation's SKS. The model evolved from the study's findings and contained two theories: one at the organisational level and the other at the individual level. TMS theory discusses how organisational knowledge is stored and shared at the organisational level, while SDT promotes individual sharing.

8.1.3 Research Sub-question 3

The answer to the third sub-question, “Can security knowledge sharing be modelled using TMS and sharing encouraged by satisfying the self-determination needs of employees?”, can be derived from Chapters 5 and 6. The experiment evaluates the effect of using the app in the real world to enhance training and improve employees’ security awareness in organisations. The experiment contributed to the knowledge by examining how the app can identify how SKS can be enhanced, and also how the app can be facilitated and encouraged among employees to improve their knowledge. Moreover, the dissertation led to the design of a system and implementation based on the findings from the first and second experiments to mitigate the challenges identified in the literature review. Then we developed and tested the app via Android Studio and CSS.

8.1.4 Main Research Question

The answer to the main research question, “How can knowledge sharing improve security awareness in organisations?”, can be derived from Chapters 6 and 7. The thesis provides practical implications for system designers and developers who seek to improve employee security awareness within organisations via a collaborative model. Moreover, the study encourages employees to engage in prosocial behaviour through educational security games.

This study extends the knowledge on how to deliver security training by exploring the positive effects of including autonomy as intrinsic motivation and relatedness into training (STOW). Both encouraged the employees to complete the training without any external influence, which led to enhancing the employees’ security knowledge.

The findings from the experiment indicate that the intervention group, which received training, had superior knowledge of assessing and responding to security incidents compared to the control group, and their ISA was increased. Along with obtaining additional data, new findings explored the positive relationship between autonomy as intrinsic motivation and relatedness, which has not been investigated before.

To ascertain employees' actual behaviours, we asked the IT department whether there had been any security incidents in the preceding three months among the employees who received the training. According to the IT report, there had been no such incidents.

The study results revealed those various underlying causes of the improvement following the STOW were tracked before, during, and after the game, proving the effect of the SKS model on changing how security training is delivered.

In summary, based on these findings, it can be said that ignoring the difficulties inherent in social engineering training and ISA programmes may end in the loss of the organisation's information. Security training that is provided effectively is considered the first line of protection against security attacks. The IT department must consider the effective delivery of ISA. If an employee is not up to date with the current security risk fraud methods, attackers may obtain access to the organisation's information systems via an open door. The STOW's objective is to offer an interactive and user-friendly method to enhance employees' knowledge of cybersecurity. The system utilises several strategies to ensure that employees acquire necessary knowledge at the appropriate time: a set of interactive scenarios that need the adoption of cybersecurity threats to address one or more actual security concerns. This strategy ensures that employees are kept up-to-date with potential risks and damage due to security incidents. IT practitioners must consider the findings to create interactive training capable of changing employee behaviour. According to Frank and Ament (2021), information security expertise sharing adds value to organisations by assisting employees in resolving problems or defending themselves against cyberattacks. They strongly encouraged organisations to gather such stories since incident experience may lead to successful learning. Narratives about other human perspectives on information security may act as a motivator to avoid making the same errors again. Organisations may offer a platform for their workers to share their learning experiences [100].

8.2 Research Limitations and Future Work

Regarding the limitations of this study and recommendations for future work, research might be expanded and enhanced by considering the following points:

- There were difficulties obtaining authority and permission from the organisations to perform this investigation due to the sensitive nature of the information. We signed a contract with Fortune 100 to obtain approval to begin implementing the framework. All of these procedures took considerable time.

- The intervention's data were collected from a single organisation, which may introduce sample-specific biases. As a result, caution should be used when extrapolating results to other organisations.

- IT practitioners must change their organisational culture to foster an attitude toward information security rules that views them as a necessary evil rather than a hindrance to workers performing their jobs. The training plan should be changed to consider individual and organisational factors to deliver practical training to the employees.

- There might be a bias in the responses to the interview and questionnaires. We faced difficulties when we collected the data because employees were not accustomed to participating in research studies. For example, many participants did not read the instructions to understand the aim of the study, despite the short instructions and an attempt to give an oral brief to clarify the objectives. Thus, we excluded a significant amount of data due to bias.

- It was not possible to cover all fields of information security training during the empirical research because it requires more time than was available. The thesis covered the most common human errors in the organisation: social engineering phishing and password management.

- In all the qualitative and quantitative studies, the sample was not limited to a single sector. The primary industries that this study identified as more dynamic include information technology and software and management consulting. Other industries, on the other hand, were not eliminated, potentially diluting the sample. While the study revealed no significant differences in information sharing and interaction across sectors, the research findings and suggestions may be more relevant to the more innovative IT and software and management consulting industries.

- Information security has become an organised process as more and more companies recognise its importance. One of the most difficult aspects of managing an information system is implementing appropriate security measures. Various studies have shown the critical importance of protecting valuable information, and one critical element that must be addressed is information security awareness. ISA is about ensuring that all employees of the information security function understand their role and are aware of the rules and regulations they must follow.

- According to the findings of the literature study, there is a significant need for and value in addressing ISA and its multidisciplinary aspects. While security awareness is a critical proactive step for protecting personal and organisational information technology through effective security procedures, much work remains to reach an adequate degree of knowledge among general employees. Both of the studies conducted in Chapters 4 and 7 suggested that they lacked sufficient awareness. The study addressed the training’s limitations and established a method capable of avoiding prior failures. Employees were also urged to change their behaviour through appropriate information security awareness-raising initiatives.

- The majority of ISA training is developed using the traditional method, which does not accurately reflect reality in organisations. The evidence of this is that the employees attended training, but they could not defend themselves when they encountered a security breach. This thesis utilised a unique technique based on real-world scenarios to educate employees about security risks. Any subsequent study must take these findings into account and construct the ISA based on real-world settings. IT practitioners must consider the findings to create interactive training capable of changing employee behaviour.

- This study was concerned with the fundamentals of TMS for different teams, where team members benefit from the successful utilisation and coordination of various expertise. The findings have provided insights into why expertise variety may stimulate TMS [79]. Thus, the findings shed light on why expertise variety has the potential to both boost and harm TMS. The SKS model has deduced this issue using a combination of motivation and collaboration theory. For instance, employees can find expertise (specialisation) through feedback and evaluation via the STOW system (competence). Future work may consider these findings to adapt e-learning among employees or students.

Recent studies show that conventional social engineering and information security training approaches often lack actual exposure for employees [6, 124]. These techniques do not expose employees to real-world situations in the way that contemporary training methods do. Employees are educated about the assault via traditional methods, but they may fail to identify it when confronted with the actual attack. These conventional techniques alone are insufficient to foster a culture of safety among employees [6, 124].

Additionally, expanding the cycle of the SKS model to incorporate additional iterations of awareness sessions and a greater number of assessment tests may be a future extension of this study. Due to the fact that awareness gains in SKS are time and location dependent, extended studies will examine the importance of the two dynamic factors (TMS and SDT) in the SKS model, which may be expanded upon in future studies.

8.3 Closing Remarks

Based on the thesis findings, ignoring the difficulties inherent in social engineering training and ISA programmes may end in victimisation. Security training that is provided effectively is considered the first line of protection against security attacks. The IT department must consider the effective delivery of ISA. If an employee is not updated on the current security risk fraud methods, attackers may obtain access to the organisation's information systems via an open door. The STOW's objective is to offer an interactive and user-friendly approach to enhance employees' cybersecurity knowledge. The system utilises several strategies to ensure that employees acquire necessary expertise at the appropriate time: a set of interactive scenarios that need the adoption of cybersecurity threats to address one or more actual security concerns. This strategy ensures that employees are kept up to date with potential risks and damage due to security incidents.

This thesis proposed a SKS model that aims to improve how employees are made aware of information security risks. The empirical study shows that it can help enhance security knowledge and deliver training by adopting the cooperation model.

Bibliography

1. Nieles, M., K. Dempsey, and V. Pillitteri. *An introduction to information security*. 2017.
2. He, Y. *Generic security templates for information system security arguments: Mapping security arguments within healthcare systems*. Doctoral thesis, 2014, University of Glasgow.
3. Wright, L. Rethinking people, risk, and security. In *People, Risk, and Security*. 2017, Springer. pp. 7-24.
4. Ulrich, P., V. Frank, and R. Buettner. *One single click is enough – An empirical study on human threats in family firm cybersecurity*. 54th Hawaii International Conference on System Sciences, 5–8 January 2021.
5. Karjalainen, M., M. Siponen, and S. Sarker. Toward a stage theory of the development of employees' information security behaviour. *Computers and Security*, 2020. 93: p.101782.
6. Aldawood, H. and G.J. Skinner. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, 2019. 11(3): p. 73.
7. Ahmed, G., G. Ragsdell, and W. Olphert. Knowledge sharing and information security: A paradox? In *European Conference on Knowledge Management*. 2014. Academic Conferences International Limited.
8. Becerra-Fernandez, I. and R. Sabherwal. *Knowledge management: Systems and processes*. 2014: Routledge.
9. Mermoud, A., M.M. Keupp, K. Huguenin, M. Palmié, and D.P. David. Incentives for human agents to share security information: A model and an empirical test. *In 17th Workshop on the Economics of Information Security (WEIS)*, Innsbruck, Austria. 2018.
10. Dang-Pham, D. and M. Nkhoma. Effects of team collaboration on sharing information security advice: Insights from network analysis. *Information Resources Management Journal (IRMJ)*, 2017. 30(3): pp. 58-72.
11. Dang-Pham, D., S. Pittayachawan, and V. Bruno. Why do employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, 2017. 67: pp. 196-206.
12. Politis, J.D. The connection between trust and knowledge management: What are its implications for team performance? *Journal of Knowledge Management*, 2003. 7(5): pp. 55-66.
13. Dixon, N.M. *Common knowledge: How companies thrive by sharing what they know.* 2000: Harvard Business School Press.
14. Siponen, M. A conceptual foundation for organizational information security awareness. *Information Management and Computer Security,* 2000. 8(1).
15. Abawajy, J. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 2014. 33(3): pp. 237-248.
16. Bauer, S. and E. Bernroider. From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *Data Base for Advances in Information Systems*, 2017. 48(3): pp. 44-68.
17. D'Arcy, J., A. Hovav, and D. Galletta. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 2009. 20(1): pp. 79-98.

18. Vance, A. and M.T. Siponen. IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, 2012. 24(1): pp. 21-41.

19. Killmeyer, J. *Information security architecture: An integrated approach to security in the organization.* 2006: CRC Press.

20. Puhakainen, P. and M. Siponen. Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 2010: pp. 757-778.

21. Bada, M., A.M. Sasse, and J.R. Nurse. *Cyber security awareness campaigns: Why do they fail to change behaviour?* arXiv preprint arXiv:1901.02672, 2019.

22. Haeussinger, F. and J. Krantz. Understanding the antecedents of information security awareness: An empirical study. In *19th Americas Conference on Information Systems*, 2013. pp. 3762-3770.

23. Khando, K., S. Gao, S.M. Islam, and A.J.C. Salman. Enhancing employees' information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 2021. 106: p. 102267.

24. Mejias, R.J. An integrative model of information security awareness for assessing information systems security risk. In *45th Hawaii International Conference on System Sciences*. 2012. IEEE.

25. Albrechtsen, E. and J. Hovden. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 2010. 29(4): pp. 432-445.

26. Bauer, S. and E.W. Bernroider. From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems,* 2017. 48(3): pp. 44-68.

27. Safa, N.S., C. Maple, T. Watson, and S. Furnell. Information security collaboration formation in organisations. *IET Information and Security*, 2017. 12(3): pp. 238-245.

28. Tsohou, A., M. Karyda, S. Kokolakis, and E.J. Kiountouzis. Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, 2015. 24(1): pp. 38-58.

29. Vance, A., M. Siponen, and S. Pahnila. Motivating IS security compliance: insights from habit and protection motivation theory. *Information and Management*, 2012. 49(3-4): pp. 190-198.

30. Mejias, R.J. and P.A. Balthazard. A model of information security awareness for assessing information security risk for emerging technologies. *Journal of Information Privacy and Security,* 2014. 10(4): pp. 160-185.

31. Choi, S., J.T. Martins, and I. Bernik. Information security: Listening to the perspective of organisational insiders. *Journal of Information Science*, 2018. 44(6): pp. 752-767.

32. Ki-Aries, D. and S. Faily. Persona-centred information security awareness. *Computers & Security,* 2017. 70: pp. 663-674.

33. Furnell, S., R. Esmael, W. Yang, and N. Li. Enhancing security behaviour by supporting the user. *Computers & Security,* 2018. 75: pp. 1-9.

34. Thomson, M.E. and R.J. von Solms. Information security awareness: educating your users effectively. *Information Management and Computer Security,* 1998. 6: pp. 167-173.

35. He, Y. and C. Johnson. Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization. *Informatics for Health and Social Care*, 2017. 42(4): pp. 393-408.

36. Choi, S.Y., H. Lee, and Y.J. Yoo. The impact of information technology and transactive memory systems on knowledge sharing, application, and team performance: A field study. *MIS Quarterly*, 2010: pp. 855-870.

37. Davison, R.M., C.X. Ou, and M.G. Martinsons. Information technology to support informal knowledge sharing. *Information Systems Journal,* 2013. 23(1): p. 89-109.

38. Chen, Y.-H., T.-P. Lin, and D.C. Yen. How to facilitate inter-organizational knowledge sharing: The impact of trust. *Information and Management,* 2014. 51(5): pp. 568-578.

39. Safa, N.S., C. Maple, T. Watson, and S.J. Furnell. Information security collaboration formation in organisations. *IET Information and Security,* 2018. 12(3): pp. 238-245.

40. Chen, S.-S., Y.-W. Chuang, and P.-Y. Chen. Behavioral intention formation in knowledge sharing: Examining the roles of KMS quality, KMS self-efficacy, and organizational climate. *Knowledge-Based Systems*, 2012. 31: pp. 106-118.

41. Lin, T.-C., S. Wu, and C.-T. Lu. Exploring the affect factors of knowledge sharing behavior: The relations model theory perspective. *Expert Systems with Applications,* 2012. 39(1): pp. 751-764.

42. Tamjidyamcholo, A., M.S.B. Baba, N.L.M. Shuib, and V. Rohani. Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security,* 2014. 43: pp. 19-34.

43. Feledi, D., S. Fenz, and L. Lechner. Toward web-based information security knowledge sharing. *Information Security Technical Report*, 2013. 17(4): pp. 199-209.

44. Feledi, D. and S. Fenz. Challenges of web-based information security knowledge sharing. In *Seventh International Conference on Availability, Reliability and Security*, 2012. pp. 514-521.

45. Fenz, S. and A. Ekelhart. Formalizing information security knowledge. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security,* 2009. ACM.

46. Flores, W.R., E. Antonsen, and M. Ekstedt. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 2014. 43: pp. 90-110.

47. Gal-Or, E. and A. Ghose. The economic incentives for sharing security information. *Information Systems Research*, 2005. 16(2): pp. 186-208.

48. Bartnes, M., N.B. Moe, and P.E. Heegaard. The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, 2016. 61: pp. 32-45.

49. Stanton, J.M., K.R. Stam, P. Mastrangelo, and J. Jolton. Analysis of end user security behaviors. *Computers & Security*, 2005. 24(2): pp. 124-133.

50. Zhang, T., Knowledge expiration in security awareness training. *Annual ADFSL Conference on Digital Forensics, Security and Law*, 2018.

51. Junger, M., L. Montoya, and F.-J. Overink. Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior,* 2017. 66: pp. 75-87.

52. Gcaza, N. and R. von Solms. Cybersecurity culture: An ill-defined problem. In *IFIP World Conference on Information Security Education. 20*17. Springer.

53. Kim, S.S. and Y.J. Kim. The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management*, 2017. 21(4): pp. 986-1010.

54. Safa, N.S., R. von Solms, and S. Furnell. Information security policy compliance model in organizations. *Computers & Security*, 2016. 56: pp. 70-82.

55. Rocha Flores, W., E. Antonsen, and M. Ekstedt. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 2014. 43: pp. 90-110.

56. Hawryszkiewycz, I. and M.H. Binsawad. Classifying knowledge-sharing barriers by organisational structure in order to find ways to remove these barriers. In *Eighth International Conference on Knowledge and Systems Engineering (KSE)*, 2016. IEEE.

57. Hassan, N.H., Z. Ismail, and N. Maarop. A conceptual model for knowledge sharing towards information security culture in healthcare organization. In *International Conference on Research and Innovation in Information Systems (ICRIIS)*, 2013. IEEE.

58. Hassan, N.H., Z. Ismail, and N. Maarop. Understanding relationship between security culture and knowledge management. *Lecture Notes in Business Information Processing,* 2014. 185: pp. 7-38.

59. Herzog, A., N. Shahmehri, and C. Duma. An ontology of information security. *International Journal of Information Security and Privacy,* 2007. 1(4): pp. 1-23.

60. Ibragimova, B., S.D. Ryan, J.C. Windsor, and V.R. Prybutok. Understanding the antecedents of knowledge sharing: An organizational justice perspective. *Informing Science*, 2012. 15.

61. Im, G.P. and R. Baskerville. A longitudinal study of information system threat categories: The enduring problem of human error. *ACM SIGMIS Database*, 2005. 36(4): pp. 68-79.

62. Alahmari, S., K. Renaud, and I. Omoronyia. A model for describing and maximising Security Knowledge Sharing to enhance security awareness. In *European, Mediterranean, and Middle Eastern Conference on Information Systems*, 2019. Springer.

63. Johnson, G., K. Scholes, and R. Whittington. *Exploring corporate strategy: Text & cases*. 2009: Pearson Education.

64. Liu, D., Y. Ji, and V. Mookerjee. Knowledge sharing and investment decisions in information security. *Decision Support Systems*, 2011. 52(1): pp. 95-107.

65. Nonaka, I. A dynamic theory of organizational knowledge creation. *Organization Science,* 1994. 5(1): pp. 14-37.

66. Safa, N.S. and R. von Solms. An information security knowledge sharing model in organizations. *Computers in Human Behavior*, 2016. 57: pp. 442-451.

67. Persadha, P.D., A. Waskita, M. Fadhila, A. Kamal, and S. Yazid. How inter-organizational knowledge sharing drives national cyber security awareness? A case study in Indonesia. In *18th International Conference on Advanced Communication Technology (ICACT)*, 2016. IEEE.

68. Tsai, W.J. Social structure of “coopetition” within a multiunit organization: Coordination, competition, and intraorganizational knowledge sharing. *Organizational Science*, 2002. 13(2): pp. 179-190.

69. Newell, S. and R. Galliers. Facilitating–or inhibiting–knowing in practice. *European Journal of Information Systems*, 2006. 15(5): pp. 441-445.

70. Simeonova, B.J. *Knowledge sharing and knowledge interaction processes within Bulgarian firms*. Doctoral thesis, 2014. University of London.

71. Wegner, D.M. Transactive memory: A contemporary analysis of the group mind. In *Theories of group behavior*. 1987, Springer. pp. 185-208.

72. Lewis, K. and B. Herndon. Transactive memory systems: Current issues and future research directions. *Organization Science*, 2011. 22(5): pp. 1254-1265.

73. Jackson, P. and J. Klobas. The organization as a transactive memory system. In *Becoming virtual*. 2008, Springer. pp. 111-133.

74. Lehner, F. and R. Maier. How can organizational memory theories contribute to organizational memory systems? *Information Systems Frontiers*, 2000. 2(3): pp. 277-298.

75. Liao, J., N.L. Jimmieson, A.T. O'Brien, and S.L. Restubog. Developing transactive memory systems: Theoretical contributions from a social identity perspective. *Group and organization Management,* 2012. 37(2): pp. 204-240.

76. Liang, D.W., R. Moreland, and L. Argote. Group versus individual training and group performance: The mediating role of transactive memory. *Personality and Social Psychology Bulletin,* 1995. 21(4): pp. 384-393.

77. Argote, L., S. Lee, and J. Park. Organizational learning processes and outcomes: Major findings and future research directions. *Management Science*, 2020.

78. Lewis, K.J. Measuring transactive memory systems in the field: Scale development and validation. *Journal of Applied Psychology,* 2003. 88(4): pp. 587-604.

79. Cronin, M.A. and L. Weingart. Representational gaps, information processing, and conflict in functionally diverse teams. *Academy of Management Review,* 2007. 32(3): pp. 761-773.

80. Ali, A., H. Wang, and A. Khan. Mechanism to enhance team creative performance through social media: A transactive memory system approach. *Computers in Human Behavior*, 2019. 91: pp. 115-126.

81. Rico, R., M. Sánchez-Manzanares, F. Gil, and C. Gibson. Team implicit coordination processes: A team knowledge–based approach. *Academy of Management Review*, 2008. 33(1): pp. 163-184.

82. Zhong, X., Q. Huang, R.M. Davison, X. Yang, and H. Chen. Empowering teams through social network ties. *International Journal of Information Management*, 2012. 32(3): pp. 209-220.

83. Kotlarsky, J., B. van den Hooff, and L. Houtman. Are we on the same page? Knowledge boundaries and transactive memory system development in cross-functional teams. *Communication Research,* 2015. 42(3): pp. 319-344.

84. Wang, Y., Q. Huang, R.M. Davison, and F. Yang. Effect of transactive memory systems on team performance mediated by knowledge transfer. *International Journal of Information Management,* 2018. 41: pp. 65-79.

85. Ryan, R.M. and E. Deci. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist,* 2000. 55(1): pp. 68-78.

86. Perkins, S.J. and S. Jones. *Reward management: Alternatives, consequences and contexts*. 2020: Kogan Page Publishers.

87. Alkaldi, N. and K. Renaud. Encouraging password manager adoption by meeting adopter self-determination needs. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*. 2019.

88. Alzahrani, A., C. Johnson, and S. Altamimi. Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation. in *4th International Conference on Information Management (ICIM)*. 2018. IEEE.

89. Ambrose, M.L. and C. Kulik. Old friends, new faces: Motivation research in the 1990s. *Journal of Management,* 1999. 25(3): pp. 231-292.

90. Wang, W.-T. and Y.-P. Hou. Motivations of employees' knowledge sharing behaviors: A self-determination perspective. *Information and Organization*, 2015. 25(1): pp. 1-26.

91. Deci, E.L. and R. Ryan. *Intrinsic motivation*. 2010: John Wiley & Sons.

92. DeCharms, R.. Personal causation training in the schools 1. *Journal of Applied Social Psychology,* 1972. 2(2): pp. 95-113.

93. Arachchilage, N. Serious games for cyber security education. *Computers and Society,* 2016.

94. Gunton, L.-A. Exploring the role of UK public sector managers in rewarding their employees: a self-determination theory perspective. Doctoral thesis, 2018. University of Northumbria at Newcastle (United Kingdom).

95. Ryan, R.M. and E. Deci. Overview of self-determination theory: An organismic dialectical perspective. In *Handbook of self-determination research*, 2002: University of Rochester Press.

96. Roca, J.C. and M.J. Gagné. Understanding e-learning continuance intention in the workplace: A self-determination theory perspective. *Computers in Human Behaviour*, 2008. 24(4): pp. 1585-1604.

97. Baard, P.P., E.L. Deci, and R.M. Ryan. Intrinsic need satisfaction: A motivational basis of performance and well-being in two work settings. *Journal of Applied Social Psychology,* 2004. 34(10): pp. 2045-2068.

98. Deci, E.L., H. Eghrari, B.C. Patrick, and D. Leone. Facilitating internalization: The self-determination theory perspective. *Journal of Personality,* 1994. 62(1): pp. 119-142.

99. Flores, W.R., H. Holm, G. Svensson, and G.J. Ericsson. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management and Computer Security,* 2014. 22(4)

100. Frank, M. and C. Ament. How motivation shapes the sharing of information security incident experience. In *Proceedings of the 54th Hawaii International Conference on System Sciences*. 2021.

101. Cone, B.D., C.E. Irvine, M.F. Thompson, and T. Nguyen. A video game for cyber security training and awareness. *Computers & Security,* 2007. 26(1): pp. 63-72.

102. Alzahrani, A. and C. Johnson. Autonomy motivators, serious games, and intention toward ISP compliance. *International Journal of Serious Games*, 2019. 6(4): pp. 67-85.

103. Dixon, M., N.A. Gamagedara Arachchilage, and J. Nicholson. Engaging users with educational games: The case of phishing. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems,* 2019.

104. Arachchilage, N.A.G. and S. Love. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behaviour*, 2014. 38: pp. 304-312.

105. Aladawy, D., K. Beckers, and S. Pape. PERSUADED: Fighting social engineering attacks with a serious game. In *International Conference on Trust and Privacy in Digital Business*, 2018. Springer.

106. Hart, S., A. Margheri, F. Paci, and V. Sassone. Riskio: A serious game for cyber security awareness and education. *Computers & Security,* 2020. 95: p. 101827.

107. Huotari, K. and J. Hamari. A definition for gamification: Anchoring gamification in the service marketing literature. *Electronic Markets,* 2017. 27(1): pp. 21-31.

108. Koivisto, J. and J. Hamari. The rise of motivational information systems: A review of gamification research. *International Journal of Information Management*, 2019. 45: pp. 191-210.

109. Rigby, S. and R.M. Ryan. Glued to games: How video games draw us in and hold us spellbound. 2011: Praeger.

110. Francisco-Aparicio, A., F.L. Gutiérrez-Vela, J.L. Isla-Montes, and J.L.G. Sanchez. Gamification: Analysis and application. In *New trends in interaction, virtual reality and modeling*. 2013: Springer. pp. 113-126.

111. Xi, N. and J. Hamari. Does gamification satisfy needs? A study on the relationship between gamification features and intrinsic need satisfaction. *International Journal of Information Management*, 2019. 46: pp. 210-221.

112. Hamari, J., J. Koivisto, and H. Sarsa. Does gamification work? A literature review of empirical studies on gamification. In *47th Hawaii International Conference on System Sciences.* 2014. IEEE.

113. Abawajy, J.J.B. User preference of cyber security awareness delivery methods. *Behaviour and Information Technology*, 2014. 33(3): pp. 237-248.

114. Ghazvini, A. and Z. Shukur. A serious game for healthcare industry: Information security awareness training program for Hospital Universiti Kebangsaan, Malaysia. *International Journal of Advanced Computer Science and Applications*, 2018. 9(9): pp. 236-245.

115. Lindberg, D. Gamified systems for security awareness: A literature analysis. In *3rd International Conference on Information Systems, Security and Privacy*, 2016.

116. Gjertsen, E.G.B., E.A. Gjære, M. Bartnes, and W.R. Flores. Gamification of Information Security Awareness and Training. In *3rd International Conference on Information Systems, Security and Privacy*, 2017.

117. Alotaibi, F., S. Furnell, I. Stengel, and M. Papadaki. Design and evaluation of mobile games for enhancing cyber security awareness. In *12th International Conference for Internet Technology and Secured Transactions*, 2017.

118. Gagné, M. A model of knowledge-sharing motivation. *Human Resource Management*, 2009. 48(4): pp. 571-589.

119. Wickramasinghe, V. and R.J.V. Widyaratne. Effects of interpersonal trust, team leader support, rewards, and knowledge sharing mechanisms on knowledge sharing in project teams. Vine, 2012. 42(2): pp. 214-236.

120. Cabrera, E.F. and A. Cabrera, Fostering knowledge sharing through people management practices. The international journal of human resource management, 2005. 16(5): p. 720-735.

121. Lebek, B., J. Uffen, M. Neumann, B. Hohler, and M.H.J.M.R.R. Breitner, Information security awareness and behavior: a theory-based literature review. 2014.

122. Bulgurcu, B., H. Cavusoglu, and I. Benbasat. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 2010. 34(3): pp. 523-548.

123. Safa, N.S., C. Maple, T. Watson, and R. von Solms. Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*, 2018. 40: p. 247-257.

124. Olusegun, O.J. and N. Ithnin. People are the answer to security: Establishing a Sustainable Information Security Awareness Training (ISAT) program in organization. *arXiv*, 2013.

125. Yuan, Y.C., J. Fulk, and P. Monge. Access to information in connective and communal transactive memory systems. *Communication Research*, 2007. 34(2): pp. 131-155.

126. Sharif, K.H. and S.Y. Ameen. A review of security awareness approaches with special emphasis on gamification. In *International Conference on Advanced Science and Engineering (ICOASE)*, 2020. IEEE.

127. Sailer, M., J.U. Hense, S.K. Mayr, and H. Mandl. How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction. *Computers in Human Behavior,* 2017. 69: pp. 371-380.

128. Collins, H. *Creative research: The theory and practice of research for the creative industries*. 2018: AVA Publishing.

129. Jonker, J. and B. Pennink. *The essence of research methodology: A concise guide for master and PhD students in management science*. 2010: Springer Science & Business Media.

130. Rajasekar, S. and V. Philominathan. Research methodology. *arXiv*.

131. Kaplan, B. and D.J. Duchon. Combining qualitative and quantitative methods in information systems research: A case study. *MIS Quarterly,* 1988: pp. 571-586.

132. Goertzen, M. Introduction to quantitative research and data. *Library Technology Reports*, 2017. 53(4): pp. 12-18.

133. Mangan, J., C. Lalwani, and B. Gardner. Combining quantitative and qualitative methodologies in logistics research. *International Journal of Physical Distribution & Logistics Management,* 2004. 34(7).

134. Rasinger, S.M. *Quantitative research in linguistics: An introduction*. 2013: A&C Black.

135. Marczyk, G., D. DeMatteo, and D. Festinger. *Essentials of research design and methodology*. 2005: John Wiley & Sons, Inc.

136. Moriarty, J., Qualitative methods overview. *NIHR School for Social Care Research*, 2011.

137. Arrow, K.J. *The limits of organization*. 1974: WW Norton & Company.

138. Magaldi, D. and M. Berler, Semi-structured interviews. *Encyclopedia of Personality and Individual Differences*, 2020: pp. 4825-4830.

139. Fylan, F., Semi-structured interviewing. *A Handbook of Research Methods for Clinical and Health Psychology*, 2005. 5(2): pp. 65-78.

140. Polit, D.F. and C.T. Beck. *Essentials of nursing research: Appraising evidence for nursing practice*. 2009: Lippincott Williams & Wilkins.

141. Kallio, H., A.M. Pietilä, M. Johnson, and M. Kangasniemi. Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, 2016. 72(12): pp. 2954-2965.

142. Ke, F.J. A qualitative meta-analysis of computer games as learning tools. *Handbook of Research on Effective Electronic Gaming in Education,* 2011: pp. 1619-1665.

143. Battou, A., O. Baz, and D. Mammass. Learning design approaches for designing virtual learning environments. *Communications on Applied Electronics*, 2016. 5(9): p. 31-37.

144. Tripp, D. Action research: A methodological introduction. *Educação e Pesquisa*, 2005. 31(3): pp. 443-466.

145. Kazdin, A.E., Methodology: What it is and why it is so important. In *Methodological issues & strategies in clinical research*, 2003: APA. pp. 5-22.

146. Mays, N. and C. Pope. *Quality in qualitative health research*. 2006: Blackwell.

147. Kruger, H.A. and W. Kearney. A prototype for assessing information security awareness. *Computers & Security*, 2006. 25(4): p. 289-296.

148. Burnard, P. A method of analysing interview transcripts in qualitative research. *Nurse Education Today*, 1991. 11(6): pp. 461-466.

149. Bryman, A. Quantitative and qualitative research: Further reflections on their integration. In *Mixing methods: Qualitative and quantitative research*. 2017, Routledge. pp. 57-78.

150. Al Ahmari, S., K. Renaud, and I. Omoronyia. A systematic review of information Security Knowledge-Sharing research. In Proceedings of the *12th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018)*. 2018. Lulu.com.

151. Kvale, S. *Interviews: An introduction to qualitive research interviewing*. 1994: Sage.

152. Okumus, F. A framework to implement strategies in organizations. *Management Decision*, 2003. 41(9): pp. 871-882.

153. Burnard, P.J. A method of analysing interview transcripts in qualitative research. *Nurse Education Today*, 1991. 11(6): pp. 461-466.

154. Joffe, H. Thematic analysis. *Qualitative Research Methods in Mental Health and Psychotherapy*, 2012. pp. 209-253.

155. Hsieh, H.-F. and S.E. Shannon. Three approaches to qualitative content analysis. *Qualitative Health Research*, 2005. 15(9): pp. 1277-1288.

156. Braun, V. and V. Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 2006. 3(2): pp. 77-101.

157. Gagné, M. A model of knowledge-sharing motivation. *Human Resource Management*, 2009. 48(4): pp. 571-589.

158. Wickramasinghe, V. and R. Widyaratne. Effects of interpersonal trust, team leader support, rewards, and knowledge sharing mechanisms on knowledge sharing in project teams. *Vine*, 2012. 42(2): pp. 214-236.

159. Tamjidyamcholo, A., M.S.B. Baba, H. Tamjid, and R. Gholipour. Information security–Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education*, 2013. 68: pp. 223-232.

160. Vakilinia, I., D.K. Tosh, and S. Sengupta. Privacy-preserving cybersecurity information exchange mechanism. In *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*. 2017. IEEE.

161. Islam, M.Z., S.M. Jasimuddin, and I. Hasan. Organizational culture, structure, technology infrastructure and knowledge sharing: Empirical evidence from MNCs based in Malaysia. *Vine*, 2015. 45(1): pp. 67-88.

162. Alahmari, S., K. Renaud, and I. Omoronyia. Implement a model for describing and maximising Security Knowledge Sharing. In *15th International Conference for Internet Technology and Secured Transactions (ICITST)*. 2020. IEEE.

163. Hair Jr, J.F., G.T.M. Hult, C. Ringle, and M. Sarstedt. *A primer on partial least squares structural equation modeling (PLS-SEM)*. 2016: SAGE Publications.

164. Hollingshead, A.B. and D. Brandon. Potential benefits of communication in transactive memory systems. *Human Communication Research*, 2003. 29(4): pp. 607-615.

165. Ryan, R.M., J. Kuhl, and E. Deci. Nature and autonomy: An organizational view of social and neurobiological aspects of self-regulation in behavior and development. *Development and Psychopathology*, 1997. 9(4): pp. 701-728.

166. Arachchilage, N.A.G., S. Love, and K.J. Beznosov. Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, 2016. 60: pp. 185-197.

167. Huang, H.-C., T. Cheng, W.-F. Huang, and C.-I. Teng. Impact of online gamers' personality traits on interdependence, network convergence, and continuance intention: Perspective of social exchange theory. *International Journal of Information Management*, 2018. 38(1): pp. 232-242.

168. Teng, C.-I. Impact of avatar identification on online gamer loyalty: Perspectives of social identity and social capital theories. *International Journal of Information Management*, 2017. 37(6): pp. 601-610.

169. Zin, N.A.M. and W.S. Yue. History educational games design. In *2009 International Conference on Electrical Engineering and Informatics*. 2009. IEEE.

170. Zhang, T., W.Y.C. Wang, and A. Techatassanasoontorn. User's feedback contribution to enhance professional online community: A motivational process. *Vine*, 2019. 49(3).

171. Menard, P., G.J. Bott, and R. Crossler. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, 2017. 34(4): pp. 1203-1230.

172. Butz, N.T. and R.H. Stupnisky. Improving student relatedness through an online discussion intervention: The application of self-determination theory in synchronous hybrid programs. *Computers & Education*, 2017. 114: pp. 117-138.

173. Garrison, D.R. *E-learning in the 21st century: A framework for research and practice.* 2011: Taylor & Francis.

174. Davis, A.L. Using instructional design principles to develop effective information literacy instruction: The ADDIE model. *College and Research Libraries News*, 2013. 74(4): pp. 205-207.

175. Amalfitano, D., A.R. Fasolino, and P. Tramontana. A GUI crawling-based technique for android mobile application testing. In *IEEE 4th International Conference on Software Testing, Verification and Validation Workshops*. 2011. IEEE.

176. Gefen, D. and D. Straub. A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, 2005. 16(1): pp. 91-109.

177. Ahmed, M., H.R. Kambam, Y. Liu, and M.N. Uddin. Impact of human factors in cloud data breach. In *International Conference on Intelligent and Interactive Systems and Applications*. 2019. Springer.

178. Hadlington, L. The "human factor" in cybersecurity: Exploring the accidental insider. In *Research Anthology on Artificial Intelligence Applications in Security*. 2021: IGI Global. pp. 1960-1977.

179. Kruger, H.A. and W.D. Kearney. A prototype for assessing information security awareness. *Computers & Security*, 2006. 25(4): pp. 289-296.

180. Tabachnick, B.G., L.S. Fidell, and J.B. Ullman. *Using multivariate statistics. Vol. 5.* 2007: Pearson.

181. Diggle, P.J., J. Mateu, and H.E. Clough. A comparison between parametric and non-parametric approaches to the analysis of replicated spatial point patterns. *Advances in Applied Probability*, 2000: pp. 331-343.

182. Kitchen, C. Nonparametric vs parametric tests of location in biomedical research. *American Journal of Ophthalmology*, 2009. 147(4): pp. 571-572.

183. Luengo, J., S. García, and F. Herrera. A study on the use of statistical tests for experimentation with neural networks: Analysis of parametric test conditions and non-parametric tests. *Expert Systems with Applications*, 2009. 36(4): pp. 7798-7808.

184. Gibbons, J.D. and S. Chakraborti. *Nonparametric statistical inference.* 2020: CRC Press.

185. Dinneen, L. and B. Blakesley. Algorithm AS 62: A generator for the sampling distribution of the Mann-Whitney U statistic. *Journal of the Royal Statistical Society*, 1973. 22(2): pp. 269-273.

186. Heilmann, S.G., S.E. Bartczak, S.E. Hobbs, and S. Leach. Assessing influences on perceived training transfer: If I only knew then what I need to know now. *Journal of Business and Educational Leadership*, 2013. 4(1): pp. 34-48.

187. Sáiz-Pardo, M., M.C.H. Domínguez, and L. Molina. Transactive memory systems mediation role in the relationship between motivation and internal knowledge transfers in a military environment. *Journal of Knowledge Management*, 2021 (pre-print).

188. Govaerts, N., E. Kyndt, and F. Dochy. The influence of specific supervisor support types on transfer of training: Examining the mediating effect of training retention. *Vocations and Learning*, 2018. 11(2): pp. 265-288.

189. Govaerts, N., E. Kyndt, S. Vreye, and F. Dochy. A supervisors' perspective on their role in transfer of training. *Human Resource Development Quarterly*, 2017. 28(4): pp. 515-552.

190. Tortorella, G., G. Narayanamurthy, and J. Staines. COVID-19 implications on the relationship between organizational learning and performance. *Knowledge Management Research & Practice*, 2021: pp. 1-14.

191. Hsu, M.-H., T.L. Ju, C.-H. Yen, and C.-M. Chang. Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *International Journal of Human-Computer Studies,* 2007. 65(2): pp. 153-169.

192. David, E.M., L.U. Johnson, C.-Y. Meng, and T. Lopez. Stronger together: Conditional indirect effect of servant leadership on Transactive Memory Systems. *Organizational Science*, 2020: p. 1548051820969137.

193. Alzahrani, A. and C. Johnson. Autonomy motivators, serious games, and intention toward ISP compliance. *International Journal of Serious Games*, 2019. 6(4): pp. 67-85.

194. Son, J.-Y. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *International Journal of Information Management,* 2011. 48(7): pp. 296-302.

195. Kim, S. and H. Lee. The impact of organizational context and information technology on employee knowledge-sharing capabilities. *Public Administration Review*, 2006. 66(3): pp. 370-385.

196. Ali, A., H. Wang, and A.N. Khan. Mechanism to enhance team creative performance through social media: A transactive memory system approach. *Computers in Human Behavior,* 2019. 91: pp. 115-126.

197. Choi, S.Y., H. Lee, and Y. Yoo. The impact of information technology and transactive memory systems on knowledge sharing, application, and team performance: A field study. *MIS Quarterly,* 2010: pp. 855-870.

198. Wang, Y., Q. Huang, R.M. Davison, and F. Yang. Effect of transactive memory systems on team performance mediated by knowledge transfer. *International Journal of Information Management*, 2018. 41: pp. 65-79.

199. Tidwell, C.L. *Testing the impact of training with simulated scenarios for information security awareness on virtual community of practice members*. 2011.

Appendices

Appendix A

Appendix B: Exploratory Interviews

The Question	Reason for the Question
Do you trust your colleagues enough to ask their advice? In other words, are their colleagues who have knowledge that you would ask them to share with you? -If yes, will ask: when was the last time you asked them a question and was about a security problem? If no, will ask: what is it that prevents you from asking them? -What do you think the motivations are that encourage you to believe that your colleagues can give you advice? For example, Skills, Education, Experience and the Position. How do you think organisations can foster knowledge sharing when it comes to security knowledge?	Trust: It is an important factor to be measured which affects SISK [66] [159], [58], [11].
When did you start working at NBU? Did you have any prior experience before you came to work at NBU? If yes, how much security experience did you have? Did you undertake any training to improve your security skills after you got your degree? If yes, what kind of training?	Experience: These questions are designed to determine how much experience the employees have.
What is your highest educational level? What is your major?	Education: Educational level has a high impact on SISK in the workplace [66].
Do you think the style of the job (The position) could impact your ability to give you more power to encourage the employees to share their security knowledge?	The style of the job: [66]
Do you want to participate in guiding your colleagues at work (security guidance)? If yes, will ask: What are the motivations which encourage you to share security advice? If no, will ask: What are the barriers that	To explore a new factor that is not included in our study. This is essential due to different situations, culture, geography. In some cases, users have neglected the instructions which they must follow.

prevent you from sharing security advice? - Did you use the local system of Security Knowledge Sharing to share your problem or solutions for any occurrences at your workplace? If yes: What was the problem? If no: Why did you not use the system? (If they did not have any problems, then this is not applicable).	
- Do you think about Security Knowledge Sharing system is contribute to employees and the University to mitigate the Information Security risk? - How appropriate are the processes of the system with aim of it? Do you think it needs improvement? If Yes? Give me an example? - Is the system easy to use? If No, why?	Usability: To measure the System Usability and to have feedback if the system was built based on the User Experience Design or based on the required of the organisation to mitigate the risk of the information security [67] [43] [195].
Does the organisation distribute any 'post-incident' information to the employees? If YES, is there a formal process for that? If No, why not? Did you get any benefits from the previous security incidents? If YES, what it was? If NO, do you think if you get any trouble related to the security, you will find it from the 'post-incident'?	Security incident: To measure responsible for the security incidents from the responsibility of the stakeholder and employees.

Appendix C

Appendix D1

Appendix D2: Questionnaire questions

Your views on Information Security Knowledge Sharing

A questionnaire to explore the influence behind Knowledge Sharing in relation to Information Security

Section 1: About you

Please tell us a bit about yourself

1. **Gender***

   □ Male □ Female

2. **Age**: _____________ years*

3. **What is the highest level of education completed by you to date?** *

   □ School leavers/ standard grade/GCSE □ Highers/ A levels □ Higher education HND/HNC/NVQs □ Bachelors degree

   □ Masters degree □ PhD □ N/A

Section 2: Your opinions on Security Knowledge Sharing

Please tick the number that closely reflects the extent to which you agree or disagree with the following statements, where 1=strongly disagree, 2=disagree, 3=neutral, 4=agree and 5=strongly agree

	1	2	3	4	5
4. Our team members have specialized knowledge of some aspects of Information security	□	□	□	□	□
5. I have knowledge about an aspect of the Information Security that no other team member has.	□	□	□	□	□
6. Different team members are responsible for expertise in different areas.	□	□	□	□	□
7. The specialized knowledge of several different team members was needed to protect our information at the university.	□	□	□	□	□
8. I know which team members have expertise in specific areas.	□	□	□	□	□
9. I was comfortable accepting procedural suggestions from other team members.	□	□	□	□	□
10. I trusted that other members' knowledge about Information Security was credible.	□	□	□	□	□

11. I was confident relying on the information that other team members brought to the discussion.	□	□	□	□	□
12. When other members gave information, I wanted to double-check it for myself.	□	□	□	□	□
13. I did not have much faith in other members' "expertise."	□	□	□	□	□
14. I trusted the anonymity members' knowledge about Information Security based on the review from other colleagues.	□	□	□	□	□
15. Our team worked together in a well-coordinated fashion	□	□	□	□	□
16. Our employees had very few misunderstandings about what to do.	□	□	□	□	□
17. Our employees needed to backtrack and start over a lot. (reversed)	□	□	□	□	□
18. We accomplished the task smoothly and efficiently.	□	□	□	□	□
19. There was much confusion about how we would accomplish the task. (reversed)	□	□	□	□	□
20. Provide App will enhance the team worked together in a well-coordinated fashion.	□	□	□	□	□
21. Repository Knowledge helps employees to encode, storing, and retrieving information.	□	□	□	□	□
22. Our employees are provided with IT support for collaborative work regardless of time and place.	□	□	□	□	□
23. Our employees are provided with IT support for communicating among team members.	□	□	□	□	□
24. Our team is provided with IT support for searching and accessing necessary information.	□	□	□	□	□
25. Our employees are provided with IT support for systematic storing.	□	□	□	□	□
26. Our employees are provided with an update of the common incident in the workplace that causes by employees from the Security Dept.	□	□	□	□	□
27.	□	□	□	□	□

Thank you for your time.

Note:

All these questionnaires have validated in the previous study [196-198].

The second question of the research questions:
How can Knowledge Information security be described by Transactive Memory system (TMS)?
The question is to confirm the relationship between the Challenges of Security Knowledge and TMS.

Appendix E

Appendix F: Questionnaire (Information Security Assessment)

Your views on Information Security Knowledge Sharing

A questionnaire to explore the influence behind Knowledge Sharing in relation to Information Security

Section 1: About you

Please tell us a bit about yourself

1. **Gender***

   □ Male   □ Female

2. **Age**: _____________ years*

3. **What is the highest level of education completed by you to date? ***

   □ School leavers/ standard grade/GCSE   □ Highers/ A levels   □ Higher education HND/HNC/NVQs   □ Bachelors degree

   □ Masters degree   □ PhD   □ N/A

Section 2: Your opinions on Information Security Awareness:

Answer each of the following questions by selecting the letter of the answer that you think is correct. Select only one answer for each question. Use the drop-down box to the right of each question to select your answer (a, b, c, d, or e)

4. Anti-virus software should be installed on all computers.

a) True (5)

b) False (1)

c) Depends if the computer is connected to the Internet (4)

d) Depends on who uses the computer (2)

e) Anti-virus software is not necessary if the computer has a firewall (3)

5.Users should change their password to a password protected site every ____?

a) day (2)

b) week (4)

c) month (5)

d) 6 months (3)

e) year (1)

6. A strong password is a password that contains which of the following?

a) letters (1)

) Letters and numbers (3)

c) letters and non-numeric characters (4)

d) letters, numbers, and non-numeric characters (5)

e) upper case and lower-case letters (2)

7. When sharing a file with someone else over the Internet, which one of the following procedures should you follow?

a) Make sure that you know the person on the receiving end. (5)

b) Make sure that you encrypt the information before sharing. (4)

c) Never send confidential information over the Internet. (2)

d) Don’t upload the information to a shared site. (1)

e) Make sure that you review the data before sharing. (3)

8. When opening an email message attachment, you should always do this before opening the attachment?

a) Make sure that you know the person that sent the email (4)

b) Make sure that the attachment is not an executable file (3)

c) Open the attachment if it is from an email address within your organisation (2)

d) Only open if you have scanned it for viruses (5)

e) Never open email attachments (1)

9. What is the best way to protect your computer, files and data from being infected by a computer virus?

a) Keep anti-virus software up to date. (5)

b) Don’t have a connection to the Internet. (1)

c) Don’t download files or open files from any web site. (3)

d) Have a firewall installed between your computer and the Internet. (4)

e) Keep a backup of all critical software programs. (2)

10. What is computer phishing?

a) The process of looking for confidential data on a remote computer system. (3)

b) The process of seeking to gain access to another computer system. (4)

c) The fraudulent process of attempting to acquire sensitive information. (5)

d) The process of passing along a computer virus from one web site to another web site. (2) e) The fraudulent process of trying to steal computer configuration codes. (1)

11. Confidential data that is no longer needed or used should be?

a) Destroyed when no longer needed or out of date. (4)

b) Backed up and stored for later use. (2)

c) Stored on a system that is used for archiving purposes. (3)

d) Printed out and then destroyed on the computer system. (1)

e) Deleted and permanently erased from all computer systems (5)

12. Which one of the following, in your opinion, is the biggest risk of data sharing on the Internet?

a) Sharing confidential data on a secure site. (3)

b) Sharing non-confidential data on a community site. (1)

c) Hackers knowledge of the existence of the community site. (4)

d) Sharing confidential data on a community site. (5)

e) Sharing executable files on a secure site. (2)

13. If a member of the information technology group at your organisation calls and asks for confidential data you should do which one of the following?

a) Ask them to provide proof of their identity. (4)

b) Provide them with the information they requested in writing. (2)

c) Provide them with the information they requested verbally. (1)

d) Don’t give them the confidential data, they shouldn’t be asking. (5)

e) Ask to speak to their supervisor to verify the necessity of this information. (3)

14. It is not necessary to have a password on your mobile devices like a PDA (e.g. Palm Pilot), cell phone, laptop, etc. since you should always keep these devices in your position or locked away?

a) True. (1)

b) False. (5)

c) True, as long as they are kept secure. (3)

d) False, since it is impossible to always keep these devices in your position or locked up.(4)

e) False, because passwords just make it more difficult to use the devices. (2)

15. What should you do if you notice someone that you don't know using a co-workers computer?

a) It is probably just a new person from the IT department, just ignore them. (1)

b) Question them and ask why they are there. (5)

c) Call the police. (3)

d) Get another employee and then approach this person. (4)

e) Send an email to the IT department to see if they have an employee working on your co-workers computer. (2)

16. If you discover that a computer security breach has occurred you should?

a) Immediately notify your information technology department. (5)

b) Shut down your computer so that it is not vulnerable to the breach. (4)

c) Call the FBI or other law enforcement agency to report the breach. (1)

d) Notify the president of your organisation so that they can take appropriate action. (2)

e) Run a virus scan on your computer to see if you have been infected with a virus. (3)

17. A "strong" password to a shared site should be ___ characters in length.

a) 6 (1)

b) 8 (2)

c) 10 (3)

d) 12 (4)

e) 14 (5)

18. To prevent unauthorized access to data on your computer or portable device, you should utilize a password and what other computer security practice?

a) Set up a VPN connection on your device. (2)

b) Make sure that you have a spam filter on the device. (1)

c) Utilize the firewall features of the device. (3)

d) Encrypt the data on the device. (5)

e) Make sure that antivirus software is installed on the device. (4)

Section 3: Knowledge Sharing measurements (Qualitative Data)

19. How many times do you share your information security knowledge with your coworker?

a. Daily
b. Weekly
c. Monthly
d. Never

Add a comment:

20. The specialized knowledge of several different team members was needed to protect our information in
the organisation

a. True
b. False

Add a comment.

21. Provide App (to share security knowledge) will facilitate and encourage team worked together in a well-coordinated fashion.

a. True
b. False (Why?)

Add a comment.

22. Repository Knowledge helps employees to encode, storing, and retrieving information.

a. True
b. False

Add a comment.

22. The organisation encourages me to share solutions to work-related problems

a. True
b. False

Add a comment.

23. Senior management demonstrates commitment and action with respect to KM policy, guidelines, and
Activities

a. True
b. False

Add a comment.

24. The organisation award incentives and mechanisms put in place to encourage knowledge-sharing

a. True

b. False

Add a comment.

Note:

All questionnaires were validated in the previous study.

Questions from 4 to 18: The Impact of Training with Simulated Scenarios For Information Security Awareness [196-198].

Appendix G

Scenarios: during the security game

Jerry is a new employee at your school and is concerned about his students' privacy issues and records. He has asked you to respond to concerns about information compromises at other colleges and universities. He wants to share information with his colleagues but is concerned about the safety of this "shared" information. What would you tell him, in your opinion, is the biggest risk of data sharing on the Internet? S

a) haring confidential data on a secure site. (4)

b) Sharing non-confidential data on a community site. (1)

c) Hackers' knowledge of the existence of the community site. (3)

d) Sharing confidential data on a community site. (5)

e) Sharing executable files on a secure site. (2)

Chris has been using the same password for the last 5 months. His password is the word "scuba diver" because he is really into scuba diving, and his password is easy to remember. What type of password is Chris using?

a) A weak password (5)

b) A medium password (4)

c) A strong password (2)

d) A difficult password (3)

e) A hack-proof password (1)

Karen has recently joined a Virtual Community of Practice for a project she is working on at her company. The company has sites located throughout the US, KSA and England. Recently, a new member of the community located in England, Mark, has been requesting documents that are increasingly confidential in nature. Karen is not comfortable with Mark's latest requests for information. What should she do?

a) Double-check the identity of the person making the requests. (4)

b) Encrypt the information before sharing it with Mark using the company's encryption tool (3)

c) 5c) Don't provide the requested information to Mark. (5)

d) Check with the administrator of the virtual community to make sure that the site is secure. (2)

e) Ask Mark for more information on why he needs this data. (1)

You are working from home during the coronavirus pandemic; you receive an email from the systems administrator of the V-CoP asking for your Employee ID and your drivers' license number for verification purposes. You notice the return address seems to be from your company. What should you do?

a) Do not respond to the email – this is probably a phishing attempt. (5)

b) Call the system administrator and see if he/she needs that information. (4)

c) Send them your employee ID but not your drivers' license number. (1)

d) Ask the systems administrator for more information by responding to the email (2)

e) Respond to the email stating that you will not provide the information. (3)

Dr Inah has a desktop computer and a laptop that he uses at work. The laptop he takes home and uses on his home network, and he also uses it at conferences and at public sites where he can get wireless access. A local coffee shop has recently told customers to be wary of using their wireless network since some customers have complained about having their computers infected with viruses and hacked by computer hackers. What should Dr Inah do to protect his laptop?

a) Make sure his anti-virus software is always up to date. (3)

b) He should not connect to the Internet from the coffee shop. (5)

c) He shouldn't download files or open files from the web. (2)

d) Make sure that he has a firewall installed on his laptop. (4)

e) Make sure that he has a backup of all critical software programs. (1)

Dr Ahmed, the head of the Chemistry Department at AA University, received an email from the information technology department. The email stated that all employees of Central University needed to provide their user account information (login and password) along with other information such as email address, home address information, etc. They claim this is part of the project to make sure that data is kept secure. How should Dr. Ahmed respond to this request? The email seems to be from an address within the organization.

a) Respond to the request since it is from an email address from within the University. (1)

b) Respond to the request, but don't provide his password. (2)

c) Just ignore the email. (4)

d) Contact the information services department to see if they sent the email. (5)

e) Reply to the email and ask the person to provide proof of their identity. (3)

Blair has been sending a lot of personal emails from work. He is not using his work email system but logs on to Yahoo.com and uses his Yahoo email account. Blair is not happy at his job and has been sending negative emails about his boss and the company's management. Blair doesn't think he has anything to worry about since he is not using his work email, so it is his property. Is Blair correct?

a) Yes, it is his account, so there is no problem (3)

b) Yes, because his employer does not have a legal right to look at messages coming to and from his Yahoo account. (2)

c) No. Even though Blair is using his private email account, the messages are being sent on the company’s network. (5)

d) No, email is never private anywhere. (4)

e) Yes, email is always private. (1)

Employees of CC future system do contract work for the Department of Defense and a few other government agencies. Dr Ali, head of research, maintains copies of all data he is collecting for one of the projects on human performance. What method of backup should he follow so that his data is not at risk of being lost?

a) Back up everything on his computer, data and programs. (2)

b) Back up only the data that he uses on a regular basis. (4)

c) Back up data from his My Documents folder only. (1)

d) Back up all data on his computer at least once, and then changed data as needed. (5)

e) Back up all of his data once per quarter (every 3 months). (3)

The IT help desk has called you because they are performing a trace of all data packets that come in and out of the corporate network. The employee, Aileen, has asked for your user account name and password that you are currently using so that she can map the packets that are coming from and going to your computer system. What should you tell Aileen?

a. Give her the information since she states she is from the IT department. (1)

b. Verify that there really is a Joanne that works for the IT department first. (3)

c. Ask Aileen a couple of questions that only an employee of the company should know. (2)

b) d) Don’t give Aileen the information since she should already have that information. (5)

a. Tell her that you will call her back after you clear this with your supervisor. (4)

Saad has been emailing information to colleagues at the RUH Research Center in Jeddah, KSA, for the past two years. He is a research chemist at AA and has been collecting data on experiments he is running in collaboration with RUH. Yesterday, he received an email

from a new employee he doesn't know at AA who attached a file that has a new protocol that he is supposed to follow. How should he handle this email?

a) Make sure that he knows the person that sent the email (5)

b) Make sure that the attachment is not an executable file (4)

c) Open the attachment if it is from an email address within the organization (1)

d) Only open the file if he has scanned it for viruses (3)

e) Never open email attachments (2)

Hail State College loans laptop computers to faculty and staff on sabbatical or who need to work away from campus or at home. Dr Tim is doing some work for the Department of Defense and needs a laptop while visiting the Pentagon in Washington, DC. He is a bit concerned about using the laptops from the college as many different college employees share them. He has heard of some faculty picking up viruses from these shared computers. What would be the most effective way to protect his data while using the laptop?

a) Make sure the anti-virus software is up to date. (5)

b) He should not connect to the Internet while using the laptop. (2)

c) He should not download files or open files from any website. (3)

d) He should make sure that the laptop has a firewall installed on the computer. (4)

e) He should make a backup of all critical software programs on the laptop. (1)

EE State created a web portal community for faculty to share best teaching and student learning strategies. Allen, an active participant of the community, has used the site to get lots of good instructional ideas for his classes. Yesterday, he received a phone call from an IT support staff asking for his username and password because they need to do maintenance on the site. How should Allen respond to this request?

a) Do not respond to the call – this is probably a phishing attempt. (5)

b) Call the system administrator and see if he/she needs that information. (4)

c) Send his user name, but not his password. (1)

d) He should ask for more information before responding. (2)

e) He should respond to the call by stating that he will not provide the information. (3)

Gail is a member of the English Community of Practice shared online site at her college. Part of the site requires a username and password to gain access. Gail has only changed her password once since joining 2 years ago. Her current password is "3@CHauCeR3". What type of password is she using?

a) A weak password (2)

b) A medium password (4)

c) An easy password (3)

d) A strong password (5)

e) A hack-proof password (1)

You have been working on some important research for your next major conference in biotechnology. You have been saving some of the data to a USB drive and some to your hard drive. What would be the most effective method to follow so that your data is backed up properly?

a) Back up everything, data and programs (4).

b) Back up only the data that you use on a regular basis (3).

c) Back up data from the My Documents folder only. (2)

d) Back up all data at least once and then changed data regularly. (5)

e) Back up all data once per year. (1)

Which ONE of the following passwords would you consider to be the strongest?

a) 1New@PassworD (5)

b) 23Smith45 (2)

c) 9@fghl7 (4)

d) 1newpassword23 (1)

e) PassWorD23 (3)

Your school wants you to participate in a new community of practice that connects teachers with interested students to help "mentor" them through their college experience. A new student named Gloria has been assigned to you. You have never met Gloria, but she seems very excited about college and learning as much as she possibly can. Recently, Gloria has asked you for personal information - where you live, names of your kids, type of car you drive, etc. You don't feel comfortable sharing this information, even though you believe Gloria is harmless. How should you handle Gloria's requests?

a) Make sure that you really know the person on the receiving end. (3)

b) First, ask Gloria to provide personal information to you. (1)

c) Don't provide Gloria with this information. (5)

d) Ask Gloria why she wants this information? (4)

e) As long as the information is not too personal, feel free to share. (2)

Dr Fleming has been working remotely over the past 3 months as part of her fieldwork in marine biology. She regularly goes to the local library to use their wireless access. However, she is concerned that she might pick up a virus since the library does not require secured access to their wireless network (anyone can use it). What would be her best method of protecting her computer from getting a virus?

a) Keep her anti-virus software up to date. (5)

b) Don’t use the connection to the Internet. (2)

c) Don’t download files or open files from any website. (3)

d) Have a firewall installed on her computer. (4)

e) Keep a backup of all critical software programs. (1)

Dr Holmes is looking for information on biochemical reactions in insects. He has found many sites with the appropriate information, but one, in particular, seems to have exactly what he wants. However, to access the site, he must provide personal information that

doesn't seem to be warranted for what he needs. He thinks this may be a phishing site. What would make him believe the site is a phishing site?

a) The site is looking for confidential data on a remote computer system. (4)

b) The site is seeking to gain access to another computer system. (3)

c) The site is trying, fraudulently, to attempt to acquire sensitive information. (5)

d) The site is trying to pass along a computer virus from one website to another website. (2) e) The site is fraudulently trying to steal computer configuration codes. (1)

Jerry is a new employee at your school and is concerned about his students' privacy issues and records. He has asked you to respond to concerns about information compromises at other colleges and universities. He wants to share information with his colleagues but is concerned about the safety of this "shared" information. What would you tell him, in your opinion, is the biggest risk of data sharing on the Internet?

a) Sharing confidential data on a secure site. (4)

b) Sharing non-confidential data on a community site. (1)

c) Hackers knowledge of the existence of the community site. (3)

d) Sharing confidential data on a community site. (5)

e) Sharing executable files on a secure site. (2)

Dr Thomas from the chemistry department has received an email from someone in the college. He doesn't know this person, but the email states that the attachment is important information regarding the school's retirement plan. The email also says that there is time-sensitive information in the attachment that must be replied to by 5 pm today. How should Dr Thomas respond to this email, or what should he do before he opens the attachment?

a) Make sure that you know the person that sent the email (4)

b) Make sure that the attachment is not an executable file (3)

c) Open the attachment if it is from an email address within your organization (2)

d) Only open if you have scanned it for viruses (5)

e) Never open email attachments (1)

Your manager is extremely busy, so she requests you to get specific reports from the HR Server using her user ID and password. So, what are your options?

a) Since it is your employer, it's OK to do so and then request that she reset the password.
b) Ignore the request in the hopes that she would forget about it.
c) Decline the request and remind your manager that it is against organization policy.
d) Passwords and user IDs must not be shared. Report the matter to management if you are being pressed any further.

The mouse on your computer screen begins to move around and click on items on your desktop on its own. So, what exactly do you do?

Call your co-workers over so they can see.

Disconnect your computer from the network.

Unplug your mouse.

Tell your supervisor.

Turn your computer off.

Run anti-virus.

All of the above.

Answer #8:

B & D.

سيناريو 1: محمد يستخدم نفس كلمة المرور خلال الأشهر الخمسة الماضية. وقد اختار كلمة مرور تحتوي على كلمات من (swimmingpool) هوايتة في الغوص وسهلة التذكر. ما نوع كلمة المرور التي يستخدمها محمد؟ كلمة المرور

أ. كلمة مرور ضعيفة

◉

ب. كلمة مرور متوسطة

○

ج. كلمة مرور قوية

○

كلمة مرور صعبة

○

هـ. كلمة مرور تحمي من الاختراق

سيناريو 2: خلال جائحة فيروس كورونا؛ تلقيت رسالة بريد إلكتروني من مسؤول الأنظمة في تقنية المعلومات يطلب منك الرقم الوظيفي وبيانات شخصية لغرض التحقق من هويتك. لاحظت أن عنوان البريد الالكتروني من جهة عملك. ماذا عليك ان تفعل؟

○

أ) تجاهل البريد الإلكتروني - ربما تكون هذه محاولة تصيد

○

اتصل بمسؤول النظام واستفسر إذا كانوا بحاجة إلى هذه المعلومات

○

ج) أرسل لهم رقم الموظف الخاص بك ولكن بدون اي معلومات إضافية

○

هـ) الرد على الرسالة الإلكترونية التي تفيد أنك لن تقدم المعلومات

سيناريو 3: تلقى الدكتور أحمد رئيس قسم الكيمياء بالجامعة بريدًا إلكترونيًا من قسم تقنية المعلومات. ذكر البريد الإلكتروني أن جميع موظفي الجامعة بحاجة إلى تقديم معلومات عن حساب المستخدم (رمزالدخول وكلمة المرور) وعنوان البريد الالكتروني. حسب افادتهم بأن المعلومات المطلوبة لتحديث البيانات. كيف يجب أن يستجيب الدكتور أحمد لهذا الطلب؟ مع العلم ان البريد الإلكتروني من عنوان داخل الجامعة

○

أ) الرد على الطلب لأنه من عنوان بريد إلكتروني من داخل الجامعة

○

ب) الرد على الطلب، ولكن يجب أن لا يفصح عن كلمة المرور

○

ج) فقط تجاهل البريد الإلكتروني

○

د) الاتصال بقسم تقنية المعلومات لمعرفة ما إذا كانوا قد أرسلوا البريد الإلكتروني

○

هـ) الرد على البريد الإلكتروني وطلب الموظف تقديم إثبات هويته

سيناريو 4: اتصل بك مكتب مدير تقنية المعلومات محمد، وطلب معلومات الكمبيوتر وحساب المستخدم وبرر الطلب بأنهم يقومون بفحص حزم البيانات التي تدخل وتخرج من الشبكة. ماذا يجب أن ترد على طلب محمد؟

○

أ) قدم المعلومات لأنه من مكتب مدير تكنولوجيا المعلومات

○

ب) تحقق من هوية المتصل وأنه يعمل في تكنولوجيا المعلومات أولاً

○

ج) يجيب أن لا تقدم أي معلومات لمحمد لان المعلومات المطلوبة من المفترض أن تكون معروفه لدى موظفي تقنية المعلومات

○

د) أخبره أنك ستعاود الاتصال به لاحقا ثم تأكد من مشرفك ماذا يجب ان تفعل

سيناريو 5: سعد يعمل مع مركز ابحاث الكيمياء في شركة رابغ منذ عامين. وقد جمع سعد الكثير من البيانات الهامة بالتعاون مع شركة الرياض الكيميائية. استقبل سعد رسالة بريد الالكتروني من زميل بالشركة لايعرفه يطلب منه فتح ملف مرفق يحتوي على بروتوكول جديد يفترض أن يتبعه في عمله. ماذا يجب على سعد ان يفعل؟

○

أ) تأكد من هوية الشخص الذي أرسل البريد الإلكتروني

○

ب) تأكد من أن المرفق ليس ملفًا قابلاً للتنفيذ

○

ج) يفتح الملف المرفق إذا كان من عنوان بريد إلكتروني داخل المنظمة

○

د) يمكن له فتح الملف إذا قام بفحصه ببرنامج مكافحة الفيروسات

○

هـ) يجب عليه عدم فتح مرفقات البريد الإلكتروني مطلقًا

سيناريو 6: أنشأت مدرسة الاقصى بوابة إلكترونية لأعضاء هيئة التدريس لمشاركة أفضل الممارسات في استراتيجيات التدريس وتعليم الطلاب. خالد، المشارك النشط في بوابة إلكترونية، استخدم الموقع للحصول على الكثير من الأفكار التعليمية الجيدة لصفوفه. بالأمس، تلقى مكالمة هاتفية من موظفي تقنية المعلومات لأنهم بحاجة إلى صيانة الموقع. كيف يجب أن يستجيب خالد لهذا الطلب؟

○

أ) تجاهل الطلب - ربما تكون هذه محاولة تصيد

○

ب) اتصل بمسؤول النظام وتحقق مما إذا كان يحتاج حقًا إلى هذه المعلومات

○

ج) إرسال اسم المستخدم بدون كلمة المرور

○

د) أن يطلب المزيد من المعلومات قبل تقديم المعلومات

سيناريو 7: محمد طلب نصيحة عن اقوى كلمات المرور، أي من كلمات المرور التالية تعتبرها الأقوى؟

○

A) 1New@PassworD

○

B) 23Smith45

○

C) 9@fghl7

○

D) 1newpassword23

سيناريو 8: عبد الله يبحث عن معلومات عن الأنظمة الإدارية والقوانين. وقد وجد موقع يحتوي على المعلومات المناسبة التي يريدها. الدخول للموقع ، يُطلب منه تقديم معلومات شخصية. عبد الله يعتقد أن هذا الموقع لتصيد المعلومات الشخصية بغرض استغلالها. ما الذي يجعل عبد الله يعتقد أنه موقع تصيد؟

○

أ) لان الموقع يبحث عن بيانات شخصية على نظام كمبيوتر بعيد

○

ب) لان الموقع يسعى للوصول إلى نظام كمبيوتر آخر

○

ج) يحاول الموقع ، عن طريق الاحتيال ، محاولة الحصول على معلومات شخصية

○

د) يحاول الموقع تمرير فيروس كمبيوتر من موقع ويب إلى موقع ويب آخر

سيناريو 9: مديرك مشغول وطلب منك تسجيل الدخول إلى نظام الموظفين باستخدام اسم المستخدم وكلمة المرور الخاصة به لطباعة بعض التقارير. ماذا عليك ان تفعل؟

○

أ) لأنه رئيسي، لذا لا بأس بذلك ثم اطلب منه تغيير كلمة المرور

○

ب) اتجاهل الطلب وآمل أن ينسى

○

ج) رفض الطلب وتذكير مديرك بأنه يخالف سياسة المؤسسة

○

د) اوافق بدون تردد لأنه مديري والمسؤول الأول

سيناريو 10: بعد دخولك موقع على الانترنت والتسجيل فيه، لاحظت الفأرة بدأت بالتحرك من تلقاء نفسها والنقر على الايقونات الموجودة على سطح المكتب. ماذا عليك أن تعمل؟

●

أ) افصل جهاز الكمبيوتر الخاص بك عن الشبكة ثم تواصل مع تقنية المعلومات

○

ب) افصل الماوس من الكمبيوتر

○

ج) تواصل مع تقنية المعلومات

○

د) تشغيل مكافحة الفيروسات

Note: All Scenarios were validated in the previous study:

Scenarios from 1 to 21: [199], and 22 to 23: [18].

Appendix H

University of Glasgow

College of Science & Engineering

School of Computing Science

Statement of Originality

Name: *Saad Abdullah S Alahmari*

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.

The copyright of this thesis rests with the author. No quotation from it is permitted without full acknowledgement.

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 review 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. **Saad Alahmari,** Karen Renaud, & Inah Omoronyia, (2018, September). "A Systematic Review of Information Security Knowledge-Sharing Research." In 12 International Symposium on Human Aspects of Information Security & Assurance, HAISA 2018, Dundee, United Kingdom (pp. 101-110).

2. **Saad Alahmari,** Karen Renaud, & Inah Omoronyia. (2019, December) "A model for describing and maximising security knowledge sharing to enhance security awareness," in European, Mediterranean, and Middle Eastern Conference on Information Systems. Springer, 2019, pp. 376–390.

3. **Saad Alahmari,** Karen Renaud, & Inah Omoronyia. (2020, December), "Implement a Model for Describing and Maximising Security Knowledge Sharing". In 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 1-4). IEEE.

4. **Saad Alahmari**., 2019. "Enhancing Knowledge Sharing in Information Security by Transactive Memory System." SICSA DemoFest. Edinburgh, United Kingdom.

The author (**Saad Alahmari**) 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.

Karen Renaud: Methodology, Review & Supervision.

Inah Omoronyia: Conceptualisation, Review & Supervision.

Signature:

Date: 19/07/2021.

Appendix I