The Web Engineering Security (WES) Methodology

William Bradley Glisson

Submitted for the Degree of Doctor of Philosophy
University of Glasgow
Department of Computing Science

April 2008

Abstract

The World Wide Web has had a significant impact on basic operational economical components in global information rich civilizations. This impact is forcing organizations to provide justification for security from a business case perspective and to focus on security from a web application development environment perspective. This increased focus on security was the basis of a business case discussion and led to the acquisition of empirical evidence gathered from a high level Web survey and more detailed industry surveys to analyse security in the Web application development environment. Along with this information, a collection of evidence from relevant literature was also gathered. Individual aspects of the data gathered in the previously mentioned activities contributed to the proposal of the Essential Elements (EE) and the Security Criteria for Web Application Development (SCWAD).

The Essential Elements present the idea that there are essential, basic organizational elements that need to be identified, defined and addressed before examining security aspects of a Web Engineering Development process. The Security Criteria for Web Application Development identifies criteria that need to be addressed by a secure Web Engineering process. Both the EE and SCWAD are presented in detail along with relevant justification of these two elements to Web Engineering.

SCWAD is utilized as a framework to evaluate the security of a representative selection of recognized software engineering processes used in Web Engineering application development. The software engineering processes appraised by SCWAD include: the Waterfall Model, the Unified Software Development Process (USD), Dynamic Systems Development Method (DSDM) and eXtreme Programming (XP). SCWAD is also used to assess existing security methodologies which are comprised of the Orion Strategy; Survivable / Viable IS approaches; Comprehensive Lightweight Application Security Process (CLASP) and Microsoft’s Trust Worthy Computing Security Development Lifecycle.

The synthesis of information provided by both the EE and SCWAD were used to develop the Web Engineering Security (WES) methodology. WES is a proactive, flexible, process neutral security methodology with customizable components that is based on empirical evidence and used to explicitly integrate security throughout an organization’s chosen application development process.

In order to evaluate the practical application of the EE, SCWAD and the WES methodology, two case studies were conducted during the course of this research. The first case study describes the application of both the EE and SCWAD to the Hunterian Museum and Art Gallery’s Online Photo Library (HOPL) Internet application project. The second case study presents the commercial implementation of the WES methodology within a Global Fortune 500 financial service sector organization. The assessment of the WES methodology within the organization consisted of an initial survey establishing current security practices, a follow-up survey after changes were implemented and an overall analysis of the security conditions assigned to projects throughout the life of the case study.

Table of Contents

List of Tables

List of Figures

Acknowledgements

There are a number of people I would like to thank for their various contributions. Without their help and encouragement this dissertation would not have been possible. I am indebted to many colleagues and friends for their participation in its development. I would like to extend a specific thank you to the following individuals.

First and foremost I would like to thank my parents Dr. Lawrence Milton Glisson and Mrs. Shirley Glisson for their patience, understanding, friendship, love, support and encouragement to follow my dreams wherever they may take me.

Professor Ray Welland for his immeasurable contribution through the gift of common-sense, knowledge, direction, focus and the plethora of paper and dissertation critiques throughout the course of this project. I am truly thankful for his mentoring.

Dr. Andrew McDonald, for being my “Un-Official Second Supervisor”, for his insightful contribution through his candid enlightenment on the both the Ph.D. process and the dissertation subject matter. I am thankful for his confidence in my abilities and his mentoring.

I would like to thank a very wonderful sister, Margaret Elizabeth Glisson Sollod, also known as Meg, for her support, her belief in my abilities and encouragement to always follow my heart.

I would also like to recognize a number of individuals who assisted me during my research providing priceless support and feedback. Their names appear in no particular order: Dr. Richard Cooper, Dr. Leif Azzopardi, Dr. Iain Darroch, Jim Devine, and John Wilson.

In addition to the individuals who assisted in my research, I would like to thank the individuals from the organizations who participated in the surveys and case studies presented in the dissertation.

Slàinte mhath

Declaration

I declare that this thesis has been composed by myself, that the dissertation presented embodies the results of my own work and that it does not include work forming part of a thesis presented for a degree in this or any other University.

The author’s original work presented in this dissertation has contributed to a number of publications [56, 75-82] that have been co-authored with Jim Devine, Dr. Andrew McDonald, Dr. L. Milton Glisson and my supervisor Professor Ray Welland.

Date: ___________________ Signature: ___________________________________

1 Introduction

The World Wide Web (WWW) has been predominantly responsible for instigating radical paradigm transformations in today's global information rich civilizations. Many societies have basic operational economical components such as health care, government agencies, and financial services that depend on Web enabled systems in order to support daily commercial activities. E-commerce has achieved global acceptance as a valid channel for conducting business. Researchers estimate revenue results from e-commerce activities in 2005 will be in the trillions of dollars [113]. The money spent on e-commerce applications to support this new revenue stream is in the billions. The criticality of the Web can also be demonstrated via organizational budgeting practices. The percentage of an organization's total information technology budget that is designated to e-business initiatives has increased from 17.5 % in 2001, to 19.3% in 2002, to 20.3 % in 2003 [122]. E-business continues to grow in significance in today's business environment. The economic, legal and societal interest in the growth of e-business has created a demand for a more secure Web enabled business environment. Despite the critical role that security plays in the potential growth of e-commerce, reports are repeatedly produced by CSI/FBI [83-85], Deloitte [47, 49, 50] and PricewaterhouseCoopers [157, 158] illuminating the fact that security breaches continue to cost organizations millions of dollars yearly.

Over the past several years, security has become a focal point of interest in the industry. This is evident through the statements announcing major security initiatives and their commitment to security from large corporations like Microsoft [121], Oracle [29, 165], and IBM [101, 102]. This is also supported by industrial investment in Information Technology (IT) security. The latest Deloitte survey revealed that ninety-five percent of their respondents experienced an increase in their IT security budgets [50]. PricewaterhouseCoopers takes this a step further by stating that the portion of the IT budget spent on information security has increased significantly [158].

This upward trend directly affects the Web Engineering community. Web Engineering is:

> "the application of systematic, disciplined and quantifiable approaches to development, operation, and maintenance of Web-based applications" [53, 55].

It is important to recognize that 'Vanilla - Off the Shelf' Web Engineering methodologies do not inherently make any direct references to security, consequently today's Web applications face increased susceptibility to major security problems.

There have been increasing academic and commercial discussions highlighting the need for security integration into the software development life cycle. This battle cry, echoed by many in the industry, generally fails to detail how this integration can be effectively achieved. The market is producing economic support for an idea, as quoted by Steven R. Rakitin, that W. Edwards Deming put forth several years ago stating that "The quality of a product is directly related to the quality of the process used to create it" [160]. One of the major differences between Web application development and conventional software development is a greater emphasis on security [55]. Hence, the increase in costs associated with security issues should raise concerns over the way security is addressed in the Web application development process. Application development for the World Wide Web has specific security needs that are broader and more complex than those normally experienced in traditional software development processes. The following sections in this chapter cover the thesis statement, a dissertation overview and the research contribution that this dissertation presents.

1.1 Thesis Statement

Organizations need to strengthen security in their web application development processes to address security threats that are increasingly impacting e-commerce activities leading to potential financial losses and to meet escalating global legislative requirements. The thesis proposition is that developing a process impartial security methodology applicable to different Web Engineering development processes will help organizations strengthen security in their Web application development process. To achieve this, security should be built into the Web application development process up-front by explicitly integrating a process neutral security approach, which is specifically applicable to Web application development, throughout the organization's Web development process.

At the time of writing, nobody has designed a security process based on criteria that are specifically applicable to a Web Engineering development process. Therefore, a flexible process neutral security methodology with customizable components, complementing the organization’s chosen application development process is necessary for the development of this research. The utility of the new methodology will be determined through commercial case studies requiring close collaboration with industry to test the methodology in the ‘real world’.

This thesis attempts to answer the following research questions regarding the above hypothesis:

1. Is it possible to define a set of criteria that a Web Engineering Security process must fulfil?
2. Can a new development process be defined to meet the criteria for a Web Engineering Security process?
3. Can it be argued that the introduction of this new process strengthens security within Web Engineering application development processes?
4. Is it possible to demonstrate that this new Web Engineering Security Process can be successfully used in industry?

1.2 Dissertation Overview

The objective of this research was to define the criteria that a secure Web Engineering process needs to address, to develop and to evaluate a process specifically for Web Engineering Security. A chapter breakdown is provided detailing the various areas of research conducted to achieve this objective.

Chapter two details the methodology that was used in the construction of this dissertation.

Chapter three examines the evolution of security methodology research. It also sets the scope for the dissertation in terms of the definition of security and focuses the scope of the discussion on Web Engineering.

Chapter four provides the business justification in terms of economic incentive and legislative incentive for conducting research into a Web engineering security methodology.

Chapter five analyzes Web application development from a security perspective. This analysis starts with a discussion of the results of a Web survey that attempts to determine how security is realistically perceived and implemented in industry during Web application development. The results analysis, of the Web survey, identifies five elements that organizations appear to fail to address.

The chapter also presents the results from a survey conducted in a Global Fortune 500 financial organization that endeavoured to examine security from the overall application development perspective and from the perspective of security within the process. An analysis of the results of the Global Fortune 500 financial organization survey derives six Security Criteria for Web Application Development (SCWAD) that can be used to assess the security of an existing Web engineering process and also to guide Security Improvement Initiatives in Web Engineering.

Chapter six evaluates existing application development processes and security processes employed in Web engineering using the Security Criteria for Web Application Development (SCWAD).

Chapter seven describes the Web Engineering Security (WES) methodology in detail. The description covers both the principles behind the methodology and the actual process. This includes a brief discussion on the WES process stakeholders, deliverables and goals along with an analysis of the advantages and disadvantages of the methodology.

Chapter eight reviews existing security methodologies that have been proposed by both industry and academia. The chapter highlights the differences between the existing solutions and the WES methodology.

Chapter nine examines the life cycle compatibility of the Web Engineering Security (WES) methodology with traditional and agile Web engineering application development methodologies.

Chapter ten describes a practical case study application of the Security Criteria for Web Application Development (SCWAD). The practical application of SCWAD was part of a case study, in which the author participated, with the Hunterian Museum and Art Gallery at the University of Glasgow from February of 2005 to January of 2006.

Chapter eleven describes the first commercial implementation of WES in a Global Fortune 500 financial organization. The implementation was part of an internship on which the author worked from July of 2005 until September of 2006. The internship consisted of several stages that included an initial survey / process analysis design stage, a recommendation stage, an implementation and data gathering stage, a data analysis stage and a write up stage. The first two stages and the implementation aspect of the third stage were conducted from July, 2005 to October, 2005. The data gathering portion of the third stage was carried out from November, 2005 until the end of the project in August of 2006. The data analysis stage and write up stage ensued from that point. Chapter eleven also presents the results of a second survey conducted with the individuals who participated in the implementation of the various aspects of the WES.

Chapter twelve presents the conclusions to the research questions detailed in the introduction and discusses further work. The following sections include the Appendices, Abbreviations, Glossary, References and Index.

1.3 Research Contribution

This research presented in the dissertation presents several contributions to the body of knowledge that include:

Web Engineering Security Essential Elements (EE)
Web Engineering Security Essential Elements are elements that need to be acknowledged and resolved before examining a Web Engineering process from a security perspective. These elements can be used to help guide Security Improvement Initiatives in Web Engineering. The Web Engineering Essential Elements are presented in chapter five and published in a paper titled *Web Engineering Security: Essential Elements* in *The Second International Conference on Availability, Reliability and Security (ARES) Conference 2007* [81] and in a technical report published by Glisson and Welland [82].

Secure Web Engineering Process Recognition of Legislation
A high-level review of United States and United Kingdom legislation that impacts the World Wide Web is included in this document. This body of research establishes the increasing need to acknowledge legislative compatibility in secure Web application development methodologies. This research is presented in chapter four and published in a paper titled *Secure Web Application Development and Global Regulation* in *The Second International Conference on Availability, Reliability and Security (ARES) 2007* [76].

The Security Criteria for Web Application Development (SCWAD)
The Security Criteria for Web Application Development (SCWAD) can be used to assess the security of an existing Web engineering process. SCWAD can also be used to guide future Security Improvement Initiatives in Web Engineering. The criteria are presented in chapter five and published in a paper titled *Web Engineering Security: A Practitioner's Perspective* in the *International Conference on Web Engineering (ICWE) 2006* [77] and in a technical report published by Glisson and Welland [79].

The Web Engineering Security (WES) Methodology

The WES process is the first security methodology for Web Engineering that is specifically designed to address the Web Engineering Essential Elements and the Security Criteria for Web Application Development (SCWAD). The WES methodology is presented in chapter seven and published in a paper titled *Web Development Evolution: The Assimilation of Web Engineering Security* in the *3rd Latin American Web Congress 2005* [78] and in a technical report published by Glisson and Welland [80]. The WES methodology also specifically acknowledges the legislative obligations that are mounting in Web application development as discussed above.

Hunterian Museum and Art Gallery (Hunterian) Case Study

The Hunterian case study demonstrates the practical application of the Essential Elements and the Security Criteria for Web Application Development (SCWAD) during the construction of the Hunterian Online Photo Library (HOPL) Internet application. The results gained from this analysis can help organizations establish the environmental context and analyze a development process facilitating informed secure managerial decisions. The results of this research are presented in chapter ten and discussed in a paper titled *Picture this: developing a museum online photo library* in the *International Conference on Hypermedia and Interactivity in Museums (ICHIM) 2007* [56].

Industrial Case Study

The industrial case study presents, in chapter eleven, the commercial research that was conducted in a Global Fortune 500 financial service sector organization. The study presents the results gained from conducting research in a business environment through the application of a section of the WES methodology, the hurdles that were experienced and the results.

Future Work

The dissertation concludes, in chapter twelve, with a discussion of possible future research in the area of Web Engineering Security. Future areas identified during the course of this research include legislative issues, development issues and in-depth practical investigation into specific aspects of industry development practices.

2 Research Methodology

This chapter focuses on the research methodology utilized in this dissertation. Several approaches to research were utilized in the construction of this dissertation. These approaches included literature reviews, surveys, and case studies. Section 2.1 discusses case studies, section 2.2 examines the literature review and the surveys. Section 2.3 discusses the combined perspective while section 2.4 summarizes the chapter.

2.1 Case Study

Initial research in 2004 revealed a paper by Zelkowitz and Wallace [218] that put forth a taxonomy, for software engineering experimentation, that comprises twelve different experimental approaches. The twelve experimental approaches described in the taxonomy are categorized into one of three broad categories: observational methods collect data as a project develops; historical methods collect data from projects that have been completed and controlled methods provide for multiple instances of an observation for statistical validity of the results. Out of the twelve approaches that were described, three were used in the construction of this research and they are summarized in Table 1.

It should be noted that Zelkowitz and Wallace do not accurately account for a situation where the Experimental Approach utilized is a case study and the Category is a 'Real', live business environment. Zelkowitz and Wallace simply classify the category for the case study as observational without accurate recognition that a change has been injected into the environment. The closest that they get to acknowledging this issue is noted when they discuss a weak experimental approach that they define as "Assertion" [218]. Zelkowitz and Wallace classify this as observational and define it as a situation where the developers are "both experimenters and subjects of (the) study" [218]. They do qualify this situation with the following statement.

> "However, if the developer is using a new technology on some larger industrial project, we classify it as a case study, since the developer of the technology does not have the same degree of control over experimental conditions" [218].

Table 1 - Experimental Approaches Reproduced from Zelkowitz and Wallace (1998).

Experimental Approach	**Category**	**Description**	**Weaknesses**	**Strengths**
Lessons Learned	Historical	Examine qualitative data from completed projects	No quantitative data; cannot constrain factors	Determine trends; Inexpensive
Case Study	Observational	Monitor project in depth	Poor controls for later replication	Can constrain one factor at low cost
Literature Search	Historical	Examine previously published studies	Selection bias; treatments differ	Large available database; Inexpensive

However, more recent research published in 2006 by Oates [140] presents a more detailed idea of a conceptual framework that is derived and justified by a literature review. This conceptual framework attempts to provide a structure for research topics that addresses ideas like:

- Different factors that contribute to the research topic
- Any relevant theories on the research topic
- The research methodology comprised of the research strategy and the data generation methods
- Data analysis approach, i.e., qualitative or quantitative analysis [140].

Oates expands the idea of a strategy as the "overall approach to answering your research question" [140]. She goes on to define six strategies that include: survey, experiment, design and creation, action research, ethnography and case study [140]. The two strategies that were utilized in this research are surveys and case study. Oates defines these research strategies in Table 2 – Research Strategy:

Table 2 - Research Strategy

Research Strategy	Definition
Survey	Focuses on obtaining the same kinds of data from a large group of people, in a standardized and systematic way.
Case Study	Focuses on one instance of the 'thing' that is to be investigated. The aim is to obtain a rich and detailed insight into the 'life' of that case and its complex relationships and processes.

Oates defines data generation as the "means by which you produce empirical data" [140] and she defines the following four methods in which to achieve this goal: interview, observation, questionnaire and documents. All four data generation methods, as defined by Oates, were used in the course of this research and are defined in Table 3 – Data Generation Methods. The research presented in this dissertation uses two different data generation methods which Oates defines as "Method Triangulation" [140]. The research in this dissertation also uses more than two research strategies which Oates defines as "Strategy Triangulation" [140]. The multiple strategies that were implemented along with the multiple methods used in data generation, in this overall research approach, attempts to corroborate or highlight differences in findings and enhance research validity.

Oates cites Yin's [215] definition of a case study as "an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident"[140]. Oates goes on to define the three types of case studies; exploratory, descriptive and explanatory. The case studies that were conducted as part of this dissertation utilized the exploratory and the descriptive approaches. The Hunterian case study is a descriptive case study in that it provides a detailed account of the project and a detailed analysis of the project through the use of the Essential Elements (EE) and the Security Criteria for Web Application Development (SCWAD). The Fortune 500

Industry case study uses the results of the initial survey to define the WES methodology. The WES methodology is then implemented in the organization and the data is gathered through one-on-one semi structured interview, observation of the governing committee and collection of relevant documents. Both case studies conducted as part of this dissertation can be classified as longitudinal studies due to the fact that they were conducted over long periods of time. The Hunterian case study lasted from February of 2005 to January of 2006. The Fortune 500 Financial case study lasted from July of 2005 to August of 2006.

Table 3 - Data Generation Methods

Data Generation Method	Definition
Interview	A particular kind of conversation between people where, at least at the beginning of the interview if not all the way through, the researcher controls both the agenda and the proceedings and will ask most of the questions.
Observation	Watching and paying attention to what people actually do, rather than what they report they do.
Questionnaire	A pre-defined set of questions assembled in a pre-determined order. Respondents are asked to answer the questions, often via multiple choice options thus providing the researcher with data that can be analysed.
Documents	Documents that already exist prior to the research and documents that are made solely for the purposes of the research task.

The selection of both case studies can be explained from two perspectives which include typical instance and convenience. The Hunterian is a small organization that has limited resources, i.e., time money, expertise, etc., to devote to internet development which is a typical issue for small organizations. The Fortune 500 financial industry case study is representative of other organizations, in that financial category, from the perspective of size, bureaucracy, project resource constraints, and interest in security. From a convenience perspective, both organizations agreed to give the author access to the respective organizations. The opportunity to work with both organizations also coincided with the author's research time lines. The idea behind the Hunterian case study was to test the application of the theory behind the EE and SCWAD. The idea behind the fortune 500 case study was to gather data that would contribute to the construction of a methodology and test it in a real-world environment.

Another prospective of a case study process is provided by Yin [215] and summarized by Host et al. as:

1. Case study design: objectives are defined and the case study is planned.
2. Preparation for data collection: procedures and protocols for data collection are defined.
3. Collecting evidence: execution with data collection on the studied case.

4. Analysis of collected data
5. Reporting [95]

The Hunterian case study attempts to answer two questions. The first question is ‘Can it be demonstrated that parts of the WES methodology, i.e., the Essential Elements (EE) and the Security Criteria for Web Application Development (SCWAD), can be successfully applied in a business environment?’ The second question is ‘How?’ The Fortune 500 Industry case study attempts to answer two similar questions. The first question is ‘Can it be demonstrated that WES can be successfully implemented in industry?’ The second question is ‘How?’

In the Hunterian case study, the author interacted with the development team and attended several meetings. However, it should be noted that the author only advised and observed the development team. The author did not directly implement suggested changes into development. The objectives of the study were to show how EE and SCWAD could be used by an organization. The data collection for the Hunterian case study was collected via meetings with the Hunterian staff. The analysis of the information from the interaction took place through the application of this information against both the EE and SCWAD. The results are reported in chapter ten.

In the industry case study, the first stage is where the initial negotiation with the financial organization took place to determine their perceived problem and relevant activities were researched in the market. Observations and the initial survey were also conducted at this time to acquire a more in-depth understanding of the problem. Once these issues had been agreed upon, the project moved to its second stage. The second stage outlines specific organizational actions designed to relieve or improve the problems that were agreed upon in the first stage. This is where several recommendations were made to the organization. A collaborative negotiation between the researcher and the organization ensued resulting in a decision detailing which recommendations were acceptable for implementation.

The third stage implements the agreed upon changes into the organization. The author implemented the changes into the financial organization’s production environment making it a direct intervention case study. The effects of the implemented changes were observed for a period of time. At the end of that time period, the financial case study used data collected from a survey and security condition data as sources of information to evaluate the effectiveness of the changes. This evaluation took place in the fourth stage and the results are reported in the last stage.

2.2 Literature Reviews and Surveys

Relevant literature was examined from a variety of sources which included industry papers, the International Conference on Web Engineering, the Journal of Web Engineering, IEEE, ACM conferences, ACM journal publications and relevant books. Relevant literature is discussed throughout the dissertation where appropriate. The literature revealed that the overall topic of security is a popular area of research and that there is a lot of technical research in specific areas of security. However, the analysis of this information revealed that at the time of this writing nobody had designed a security process based on criteria that are specifically applicable to a Web Engineering development process. This information was the major driver behind the surveys.

2.2.1 Web Survey

The Web survey endeavoured to determine practitioner opinions [161] and acquire practical information regarding their experience with security and development methodologies. In order to acquire information, a Web survey was hosted at the University of Glasgow during June and July of 2005. In an attempt to ensure that the Web survey was "effective" [115] which means mitigating researcher bias, the instrument was validated [114, 115] in an attempt to ensure that the instrument is appropriately understood and that it is cost-effective for the participants. The Web survey was validated by two different individuals in the financial industry. The first individual is a Technical Lead for a major financial institution in the United States and the second individual is a Security Specialist for a financial institution in the United Kingdom. These individuals were used to check for question comprehension and to evaluate instrument reliability and viability. They did this by taking the survey and providing feedback. This was conducted twice due to suggested changes. These changes included simplifying questions and adding options to closed questions. The survey was designed to encourage participation so that the majority of the questions had specific answers utilizing, as much as possible, a closed question survey design [116]. The Web survey targeted computing industry professionals via an e-mail request sent by the Glasgow chapter of the British Computing Society and communications with colleagues. This aligns with the purpose and relevance of the study while supporting the selection of the individuals who validated the survey.

The sample size was relatively small, (fifty-three initial respondents) and a high number of respondents did not complete all of the sections (eighteen), reducing the value of any statistical data that could be derived from the survey results. The product of the survey was determined from the analysis of query results. The idea behind the analysis of the results was to attempt to identity trends, anomalies, and patterns.

2.2.2 Industry Surveys

A small survey was conducted at the beginning of the Hunterian Case study to learn more about the project and the Hunterian development environment. The Hunterian survey questions are available in Appendix XII. The initial industry survey conducted in the Fortune 500 Organization endeavoured to attain a more in-depth understanding of security from the overall application development perspective and from the perspective of security within the process. The second survey attempted to ascertain the impact of the changes implemented into the development process. In an attempt to mitigate researcher bias, the initial Fortune 500 industry survey and the follow up survey were both validated by two different individuals in the financial industry. One individual was an architect and one individual was a security expert. It should be noted that this validation for both surveys was only conducted once due to participant time constraints. Again, questions were simplified through the course of the conversation.

The survey style for both industry surveys and the Hunterian survey is best described as semi-structured interviews [140]. In that there was a list of questions that were asked in the same manner. In other words, there were a set number of survey questions that were read to each participant. However, if the participant wanted to talk about related issues, at any level of detail, during the course of answering questions, this line of thought was allowed to go to completion. The idea was to get the participant to speak honestly and openly about the questions. However, when the participants completed voicing their thoughts and answered the question that had been put forth they were directed to the next question. The question format for both of these surveys were open ended questions [116].

The participants, for both industry surveys, were read a statement at the being of the interview thanking them for participating, explaining the reason for the research and reassuring respondent anonymity. The interviews were conducted in conference rooms or coffee shops depending on participant time constraints and preference. The responses to the individual questions were initially recorded by hand. It should be noted that voice recording the interviews was considered but dismissed due to cultural resistance to the idea. The hand written results for both of the surveys were digitally recorded as soon after the interview as reasonably possible, typically within an hour. The results were recorded in a large spread sheet that was then examined by hand to identify trends, patterns, and anomalies.

2.3 Combined Perspective

The application of the individual data generation activities that were employed during the construction of this research, in conjunction with the appropriate experimental activity and research strategies presents a more accurate picture of the overall research methodology and is available in Table 4. The research methods and experimental approaches implemented during this work can be summarized as follow:

Lessons Learned. Two groups of surveys were conducted during the summer of 2005 contributing to the understanding of the role security plays in the ‘real world’.

- Web Survey. As discussed earlier in this chapter, the Web survey conducted during the summer of 2005 attempts to determine how security is realistically perceived and implemented in industry during application development. The survey questions are available in Appendix I and the answers are available in Appendix II.

  The approach taken with the Web survey was a qualitative approach rather than a quantitative approach. Due to the fact that the survey was capturing current / past information, as noted earlier in this chapter, Zelkowitz and Wallace categorized this approach as a historical “Lessons Learned” approach to software engineering experimentation [218]. The idea with the Web survey was to attempt to identify trends. As Oates noted, the benefit to the survey approach is that it presents the opportunity to acquire a lot of data at a reasonably low cost [140]. One of the drawbacks is that it provides a picture at a particular point in time[140]. Another drawback is that surveys are good at showing associations, but not good at establishing cause and effect [140]. There is also a lack of control, in Web surveys, over the validity of the respondents and their answers.

- Global Fortune 500 Financial Organization Surveys (GFFFOSs). Two GFFFOSs were conducted by the author during the course of the case study. The initial survey was conducted at the beginning of the case study, in July of 2005, and attempted to determine the state of security within the organization's development process. A second GFFFOSs was conducted, in May of 2006, following up on the security changes that were implemented in the organization. The survey questions are available in Appendices III and VI. The answers for the respective surveys are available in Appendices IV and VII.

  Both of the surveys conducted in the financial organization adopted Zelkowitz and Wallace's [218] Lessons Learned approach, from the historical category that "examines qualitative data from completed projects" [218]. This took the form of a series of structured interviews using a qualitative one-on-one interview technique for gathering the opinions and experience of others during Web application development. This approach has the advantages of enabling the determination of trends and is inexpensive [218]. However, it does not allow for the production of quantitative data and constraining factors [218]. A historical approach was selected to help the author understand how security challenges and issues had been perceived during recent projects within the company.

Case Study. The author's personal experience in Web development for a Fortune 500 Financial Organization based in the US pre-commencement of Ph.D. research 1999 – 2004 contributed to the foundational ideas behind the research. Two case studies were conducted during the three years devoted to the Ph.D. research. One case study was conducted with the Hunterian Museum and Art Gallery at the University of Glasgow and another with a Global Fortune 500 financial organization.

Literature Search. Literature reviews were conducted to acquire supporting evidence establishing the business case for the research, to examine Web Engineering development processes and for the criteria that were established during the research. Reviews were also conducted for the application of the criteria established during the research and the analysis of the Web Engineering Security (WES) methodology against established Web engineering development methodologies. Ideally, the foundation for these evaluations would include a combination of empirical evidence and first hand detailed reports of the processes being used in the working world. However, an empirical study has not been attempted due to constraints that include willing participants, time, and consistent experimental conditions. These fundamental evaluation constraints apply to chapters six, eight and nine.

2.4 Summary

The qualitative research provided in this dissertation consists of a review of the literature, a Web survey, a case study with the Hunterian museum, and two surveys that were conducted as part of a case study in a Global Fortune 500 financial organization. The industry case study can be summarized as follows:

- A problem was diagnosed in conjunction with the organization and used to determine the objectives of the case study.
- Potential solutions were examined and debated that would attempt to solve the organization's issues.
- The changes were implemented within the organization based upon an agreed course of action and data was collected.
- The data was evaluated and the results reported.

An overall picture of the methodologies implemented during the course of this research is available in Table 4 – Applied Research.

Table 4 - Applied Research

Data Generation Method	**Experiment Activity**	**Strategy**
Interview	Initial GFFFO Survey GFFFO Follow-up Modified Process Survey Hunterian Case Study	Case Study
Observation	GFFFO Process Observation Hunterian Case Study	Case Study
Questionnaire	Web Survey	Survey
Documents	GFFFO Case Study Hunterian Case Study	Case Study

* GFFFO – Global Fortune 500 Financial Organization

3 Security in Web Engineering

This chapter examines security methodology evolution in section 3.1. Section 3.2 provides a working definition of security for the dissertation. Section 3.3 focuses on the aspects of Web application development that make it unique. Section 3.4 provides a functional understanding of Web engineering security and section 3.5 summarizes the chapter.

3.1 Security Methodology Evolution

In order to appreciate the current state of the security methodology research, it is necessary to acknowledge previous research in the field of information security design methods. Baskerville's analysis separated numerous system methods into three generations [13]. The first generation consisted of check list and risk analysis. This stage focused on actual physical systems specifications. The second generation engineering methods focused on complex customization through the use of engineering concepts and mechanistic procedures that relied heavily on functional requirements. Baskerville cites Waters in his explanation of mechanistic engineering methods; stating that mechanistic engineering methods

> "focus on the production of mechanical specification of input, storage, and output formats, along with details of procedures needed to transform input or storage into outputs" [13].

Baskerville goes on to indicate that common tools implemented with these methodologies include system and program flow charts, record layouts and print charts. Baskerville notes that the waterfall methodology [164] is an example of a mechanistic engineering application development approach. The second generation security development methods are summed up by Baskerville as top-down engineering, rapid prototyping system and logical flow chart methods. This summary would include solutions like Fisher's approach, Parkers' security diagram and the U.K. Government's Central Computing and Telecommunications Agency's (CCTA) Risk Analysis Management Method (CRAMM)[13]. The third generation of security methods are model driven. Baskerville sited Structured Systems Analysis and Design Methods (SSADM) and the Logical Controls Design method as examples of third generation security models. Even though Baskerville's analysis of the security design methods did not directly examine the applicability of the security methodologies to the Web development, he did make an important point that is applicable to Web Engineering application development. Baskerville's analysis did suggest that

> "systems methods will neither be trustworthy nor successful unless the general research regarding systems methodology incorporates security analysis design as an explicit objective" [13].

Siponen updates and expands on Baskerville's analysis of information security development approaches declaring that there are five information system security generational classifications [171]. Siponen arrives at his conclusion after an examination of the contributing research disciplines and an evaluation of seventeen modern information system security methodologies. Security is a highly diverse research subject that has been an area of interest for a variety of disciplines. Siponen identifies four research communities as contributors to information security research including Management Information Systems (MIS), computer science, software engineering and mathematics. According to Siponen's research, MIS accounts for the social and the organizational aspects of a problem. Computer science has a 'positivist' [93, 171] orientation, which is understood to be the application of scientific methods, to solving computing problems. Software engineering has both a positivist and an interpretive approach while mathematics takes a quantitative approach to solve problems. An interpretive approach, in this context, is read to mean that the researcher is attempting to understand the data and the results generally within the social context and the context of the information system [117, 171]. The reality is that research from any of the contributing disciplines can be classified as interpretive or positivist depending on the specifics of the research. The evaluation of seventeen modern information systems contributed to the creation of the two additional security methodology generations.

Siponen's first three generations correspond with Baskerville's generational classifications. Siponen explains that the first and second generations include: checklist, management criteria and maturity criteria [173]. Checklist attempts to solve security problems through the identification and implementation of countermeasures via a list [173]. An example of a checklist is the Security Audit and Field Evaluation (SAFE) for Computer Facilities and Information Systems [172]. According to Siponen, the idea of standards evolved from checklist into recommendations that the organization should implement. Siponen explains that by meeting specific standards and / or achieving certifications, organizations are able to display a level of management and trustworthiness to business partners and customers [173]. Some well known standards in use today include the International Organization for Standardization and the International Electrotechnical Commission standard (ISO/IEC) 17799 / 27002 [36, 104, 173], the Systems Security Engineering - Capability Maturity Model (SSE-CCM) [183] and the Common Criteria (CC) [35].

ISO/IEC 17799 / 27002 attempts to provide fairly comprehensive information security management recommendations in regards to initiating, implementing and maintaining systems that are concerned with information security [36]. ISO/IEC 17799 consists of several sections that contain information on everything from security policies, to asset management, to human resource security, to business continuity management [36]. ISO/IEC 17799 does define information security in terms of confidentiality, integrity, and availability [36]. It should be noted that there is an ISO 9000 category of standards that includes software development in its remit. The standard tries to address a broader scope that this dissertation covers by examining aspects of the following areas: Project initiation and planning; Functional requirements; System design specifications; Build and document; Acceptance; Transition to production; Operations and maintenance support; and Revision and system replacement [90].

SSE-CCM presents a document intensive best practices highly structured model solution designed to support statistical process control to all forms of software engineering [183]. The SSE-CCM version of the life cycle includes concept, development, production, utilization, support and retirement stages [183]. This all-inclusive approach is composed of twenty-two processes. The first eleven process areas focus on security and the last eleven focus on "project and organizational activities" [183]. The process areas that focus on security provide a high level initiative telling organizations what to address. For example, under Coordinate Security, they indicate that

> "all members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions" [183].

This statement focuses on the team, not the methodology being used. While there is minimal concept commonality, in general, the scope of SSE-CMM is much broader than the dissertation scope. The CC attempts to fuse an assortment of international standards into a set of evaluation criteria to be utilized against information technology products [163].

Siponen defined the third generation as consisting of structural and object-oriented security methods, information modelling methods, and stepwise security methods. He also indicates that the third generation is focusing on modelling information system security requirements. Third generation security models would include approaches like the Spiral Approach, the Logical Approach, and Data Flow Diagrams (DFD) and Entity Relationship (ER) modelling. According to Siponen, the fourth generation builds on the third generation by addressing the social and socio-technical aspects of the methods. The term socio-technical was originally coined by Bostrom and Heinen in a paper where they were examining Management Information Systems (MIS) project failures [28]. They described an organization work system as being comprised of two components: the social and the technical. Bostrom and Heine went on to explain that the technical aspects focused on the task, the processes and the technology. While the social side of the system is focused on people attributes, relationships, reward systems and authority structures. Basically, the social component is concerned with the management aspect of the business. Bostrom and Heinen defined the socio-technical perspective as an intermediate position between the two extremes [28]. Siponen give the Survivable IS approach as an example of a fourth generation methodology.

The fifth generation, of security methodologies, that Siponen discusses [171] is really the next generation of methodologies. This implies that the fifth generation security methodologies do not currently exist, a point which he also articulates in a later article [173]. Siponen describes four criteria that the fifth generation security methodologies should strive to achieve. These criteria are as follows:

- Use of social ideas and techniques ensuring congruent design and user expectations
- Integration with all types of software development methodologies
- Painless adaptability of security methods with practitioners
- Provide empirical evidence of their usefulness [173].

Siponen's points, regarding the fifth generation, bring us to the heart of the security problem. There have been few industrial attempts to comprehensively address user focused aspects; methodology integration; practitioner malleability and employment of Web engineering security throughout the Web-based application development process via the establishment of a comprehensive security methodology.

Regardless of where one stands on security methodologies, the initial problem with tackling security is the terminology. Terminology in various environments has the potential to have multiple meanings. As Anderson indicated, reality is a complex environment in the real world [6]. Hence, what the terms security and vulnerability mean to one organization, such as a large financial institution, may or may not have the same relevance to another business, such as a newsagent or a small legal firm. Logically, different organizations will require "some combination of user authentication, transaction integrity and accountability, fault-tolerance, message secrecy and covertness" [6]. So what is the definition of security?

3.2 Security Definition

For the purpose of this dissertation, we will define a Web enabled secure system in terms of well established security concepts which consist of confidentiality, integrity and availability [90]. The system should protect confidentiality by limiting access to the appropriate individuals [153]. This would involve user identification, authentication and authorization. The integrity of the system should be maintained by only allowing modifications to be conducted by the appropriate individuals and within established guidelines [153]. The availability of the system is defined by providing access to the appropriate parties at designated times [153]. It should be noted that there are two additional categories that are commonly included when discussing security and they are 'non-repudiation' and 'accountability'. Non-repudiation is the capability to prevent, in this case, a software user, a system, or an application from denying actions they have performed. Accountability is the recording of the software user's actions. Since "accountability includes authenticity and non-repudiation" [119] and authenticity is the "property that allows the ability to validate the claimed identity of a system entity" [119], i.e., the authentication aspect, we will consider these topics to be subtopics of confidentiality that are utilized to help ensure integrity.

Vulnerabilities will be defined using The Organization for Internet Safety (OIS) definition. It has been said that "security is about preventing adverse consequences from the intentional and unwarranted actions of others" [168]. OIS publishes Guidelines for Security Vulnerabilities Reporting and Response. In this document, security vulnerability is defined as

> "a flaw within a software system that can cause it to work contrary to its documented design and could be exploited to cause the system to violate its documented security policy" [142].

It should be noted that this statement makes the assumption that a documented security policy exist. The reality of the OIS vulnerability definition is that any flaws in the system design or application coding can potentially lead to security vulnerabilities.

The need to improve security in the Web application development is reinforced by testimony from Robert F. Decay, Director, Information Security Issues indicating that patch management is critical in mitigating cyber vulnerabilities [45]. According to the same report, the number of security vulnerabilities reported is increasing and attacks are becoming automated [45]. Software security encompasses more than encryption and password maintenance. The ability to defend against software attacks, in the long run, will need to come from "more rigorous software engineering practices, better tools and technologies" [45].

Using these broad definitions to understand security supports the idea that security means more than implementing encryption, Secure Socket Layer (SSL), firewalls and creating and maintaining secure networks [58, 64]. It is also more than the use of digital certificates, the different technologies used for authentication and authorization or intrusion detection systems [58, 64]. In-depth discussions on these topics and research into their improvement are occurring on a daily basis. However, a system's security is not determined solely by the technology that is implemented. Web security is determined by a number of factors that include legal issues, social issues, technical issues, and Web engineering practices. The synergic factor highlighted in this research is the necessary integration of a broad security solution into Web engineering methodologies. This expansive perspective on the scope of security was reinforced by Eugene Spafford, a security expert and professor at Purdue University when he stated in an interview that "security is a total-picture issue, not a set of spot problems to patch" [126].

3.3 Dissertation Scope

A method may be defined as "a procedure, technique" [59] or "way of doing something" [9, 59, 212]. In this specific discussion, it is a way of integrating Web engineering security into Web Engineering application development methodologies. Accepting this concept limits this dissertation to matters pertaining specifically to Web engineering security methodologies. This excludes the technical details of security implementations. The scope of this dissertation is further limited to new Web-based applications developed for business needs. Web enabled software systems defined as human safety critical or national infrastructure critical systems are, therefore, out of scope. The focus on Web Engineering application development naturally leads to a discussion about what makes it different from traditional software engineering application development.

3.4 Web Engineering

As discussed in the introduction, Web Engineering is "the application of systematic, disciplined and quantifiable approaches to development, operation, and maintenance of Web-based applications" [53, 55]. Research indicates that there are several criteria that differentiate Web Engineering from traditional software engineering. McDonald's empirical software engineering research identifies seven criteria that

Web engineering processes need to address [129]. These characteristics are as follows:

1. Short development life-cycle times (generally less that six months);
2. Different business models;
3. Multidisciplinary development teams;
4. Small development teams working in parallel on similar tasks;
5. Analysis and Evaluation;
6. Requirements and Testing;
7. Maintenance [129].

The different business models acknowledge the interactions among the business model, the software model, the domain model and the creative design model by discussing the impact of the various models on each other. The multidisciplinary development team means that there are stakeholders from different areas of the business that are a part of the application development team. The Web engineering process needs to support small development teams working in parallel on the same project. The analysis and evaluation aspect refers to the need of the development team to truly understand the overall problem they are attempting to solve. This includes a sound understanding of the business problem, the expected end-user usage and the expected deliverables in order to optimize system functionality. McDonald also stresses the need for requirements engineering and a testing phase during Web application development projects. He also acknowledges the need to address maintenance.

A separate survey by Baskerville [14] identifies six common practices for high-speed Internet software development as follows:

1. Parallel Development and Frequent Releases
2. Tools and Reusable Components
3. Production Prototyping
4. Customer Implantation
5. Multi-tiered Architecture
6. Tailored Methodology [14].

Baskerville's [14] research arrived at the six common practices by identifying common problems faced by the organizations involved in the case study. Parallel development and frequent releases are used to address compressing time-to-market demands. It is interesting to note that Baskerville did not assign a time frame to frequent releases. In contrast, as discussed above, McDonald did assign a general indication of the time frame for frequent releases. Tools and reusable components came about in response to insufficient programmer productivity. Production prototyping tries to address ambiguous requirements, while customer implantation is used to address the need for fluid requirements. Baskerville acknowledges the security dangers of prototyping when he states that "critical requirements like security, scalability, and robustness are hard to appraise through prototyping" [14]. A lack of design time and experience is countered by a multi-tiered architecture and an emphasis on acquiring the right experience. A tailored methodology attempts to handle a changing environment.

There are similarities in the findings of the two studies by McDonald and Baskerville et al. Both identify short development cycles and parallel development. It could also be argued that tools and reusable components realistically play a part in the short development cycles, maintenance and testing of Web applications. It should be noted that McDonald's research focused specifically on process while the Baskerville survey identified common practices for high-speed Internet development. It is interesting to note that Baskerville's survey noted tailored methodologies as a common practice. The willingness of businesses to modify their methodologies is perceived as a benefit to methodology research that modifies and / or expands existing methodologies.

While the research objectives for these studies may be slightly different and the results provided include deviations in the overall information produced, the research recognizes that Web Engineering has different attributes than traditional software development. These differences support research into how to address development issues in Web Engineering. These divergences also support research into supporting the characteristics of Web-based application development projects while effectively integrating security into those methodologies. The integrated security methodology needs to be compatible with the same Web engineering characteristics.

3.5 Web Engineering Security

The need for information security has been noted and attributed to several factors ranging from the enormous interconnection of assorted and distributed systems, the existence and availability of sensitive information, computer crime anonymity, the lack of geographic boundaries and forensic evidence [109]. The lack of security in development methods has been noted in the literature [13]. Baskerville noted that third generation information systems development methodologies lacked security considerations[13]. This problem still exists today. The lack of security methodologies that are compatible with existing application development methodologies has also been noted. Siponen's analysis only found three approaches that could be smoothly integrated in information systems development methodologies [171]. According to Siponen [171] these methodologies are Baskervill's logical approach [15], Booysen and Eloff's spiral approach [27] and McDermott and Fox's abuse case methodology [128]. These methodologies are discussed in more depth in Chapter 8. It has also been noted that Agile methodologies "have few features specifically addressing security risk" [170].

Security is inherently not a part of 'Vanilla - Off the Shelf' Web engineering development processes and this inherent lack of security encourages environments that are susceptible to exploitation via potential breaches [81]. Web Engineering methodologies do not make any direct references to security, consequently today's web applications face major security problems [78]. Therefore, my definition of Web Engineering Security modifies Deshpande's explanation of Web Engineering [53, 55] as follows:

Web Engineering Security is the systematic, disciplined and quantifiable amalgamation of security with a Web-based application development process.

A specific Web engineering security methodology provides a road map for developers and management to follow during a Web-based application development project. A methodology attempts to provide guidance for all of the various aspects of security during the individual stages of the application development process. In order to allow organizations and individuals to preserve and capitalize on existing Web application development capabilities, and possible market advantages, a process neutral approach was explored. The phrase '*a process neutral approach*' has been chosen to convey the idea that the design of the security methodology endeavours to seamlessly integrate with a variety of existing Web application development methodologies.

A process neutral approach to the implementation of security is based on the fact that organizations use a variety of methodologies during their Web application development projects [79, 82]. This variety ranges from the traditional Waterfall approach, or some variant thereof, through to agile approaches in order to support Web application development. A process neutral approach provides an organization with the opportunity to support its existing Web application development methodology regardless of the style of the methodology. It also complies with Siponen's recommendation that new methodologies should strive to integrate with all types of software development methodologies

The process neutral approach provides a roadmap for organizations that are using a more traditional methodology for Web application development from a deliverable perspective. The number of deliverables that an organization will require depends on the culture of the organization, the methodology that the culture is comfortable with implementing and, to a large extent, the regulatory impact on the business. Businesses that are more conservative in nature and under a large amount of regulation, such as a large financial institution, are going to require deliverables at every stage of the development process. On the other hand, smaller businesses are more inclined to be agile in nature and require fewer deliverables during each stage of the development process. A process neutral approach allows a methodology greater flexibility to support agile methodologies. The Agile community's manifesto states that:

> "We are uncovering better ways of developing software by doing it and helping others do it. We value:
>
> - Individuals and interactions over processes and tools.
> - Working software over comprehensive documentation.
> - Customer collaboration over contract negotiation.
> - Responding to change over following a plan.
>
> That is, while there is value in the items on the right, we value the items on the left more" [4, 71].

In order to support the agile community's manifesto, a new security methodology needs to be flexible enough to integrate with existing Web application development methodologies in order to meet the needs of specific organizations. At the same time it needs to encourage interaction among project members. This increased interaction among all of the individuals involved in the project, over security issues, raises the overall security visibility of the Web application while supporting software deliverables. The security methodology needs to encourage customer input into the security aspect of the Web application. The flexibility of the methodology provides the implementing organization the freedom to decide on the amount of documentation that is appropriate for the Web application being developed and the culture of the organization. The overall flexibility of the methodology allows the implementing organization the capability to decide the rigidity of the methodology. Pursuing a process neutral approach attempts to support the ideals of the agile manifesto along with providing the flexibility to integrate into traditional application development methodologies.

The author's personal experiences indicate that the direct contributions of individuals involved in Web development projects provide the fundamental ingredients for a project's ultimate success or failure. This is especially true in the security arena. The methodology should support the individuals involved in the development process by providing guidance so that the end product is a secure Web application, while meeting the needs of the customer / business. This necessity for versatility supports research into a process neutral approach in order to allow appropriate customization while meeting the needs of the individual stakeholder groups.

3.6 Summary

This chapter examined the evolution of security methodologies and identified criteria that new methodologies, also referred to as fifth generation methodologies, need to endeavour to satisfy. These criteria include the use of social ideas and techniques ensuring congruent design and user expectations, security methodology integration with all types of software development methodologies, painless adaptability of security methods with practitioners and empirical evidence of the methodologies ineffectiveness or effectiveness. Along with the acknowledgement of the fifth generation criteria, a working definition of security is provided for this dissertation based on the concepts of confidentiality, integrity and availability. The chapter also addressed the concept of a method which limited the scope of the dissertation discussion to matters pertaining specifically to Web engineering security methodologies excluding the technical details of security implementations.

After defining the scope of the security methodology discussion, existing research into some of the characteristics that make Web Engineering projects different from traditional software development projects is acknowledged. The process characteristics identified by the research included short development life-cycle times; different business models; multidisciplinary development teams; small development teams working in parallel on similar tasks; analysis and evaluation; requirements and testing; and maintenance.

A working definition of Web Engineering Security is established that states: Web Engineering Security is the systematic, disciplined and quantifiable amalgamation of security with a Web-based application development process. The chapter concludes with a discussion acknowledging the need for a process neutral approach to the security methodology solution. This chapter established the academic area of research that is being investigated. The next chapter investigates the incentive for industrial research in the area of secure application development.

4 Business Case for Researching Web Engineering Security

Some of the most precious commodities in today's business environment include data, information and knowledge. Management of the data asset is becoming increasingly challenging as the global community progressively utilizes the World Wide Web to conduct business. It has been said that "one man's data can be another man's knowledge, and vice versa, depending on context" [180]. Once data is collected, through a Web enabled application, then the challenge morphs into information and knowledge management as businesses take advantage of Internets, intranets, and extranets. As Ralph Basham, the Director of the Secret Service put it, "Information is the world's new currency; information has value" [87]. This point was reinforced by Thomas A. Stewart when he wrote in The Wealth of Knowledge "Knowledge is what we buy, sell, and do" [180].

> "Knowledge management involves capturing, classifying, evaluating, retrieving and sharing all of a company's information assets in a way that provides context for effective decisions and actions" [68].

As strategic alliances and partnerships develop, it will become increasingly necessary for a company's information and knowledge to be available to all parties in the appropriate forms, at the appropriate place and time [68]. The main conduit for this transfer of knowledge, information and data is the Web. A major management issue that has become increasingly visible in today's Web market place is the security of an organization's data, information, and knowledge assets. Section 4.1 discusses the economic incentive. Section 4.2 examines the US Legislative Incentive and section 4.3, the US Legislation with International impact. Section 4.4 talks about the UK Legislative Issues, section 4.5, the International Legal Forum and section 4.6 summarizes the chapter.

4.1 Economic Incentive

Security failures can cost companies staggering amounts of money and have become a global epidemic that affects everyone in the world of e-business. There are several factors that contribute to an organization's security cost. The cost associated with application development is one of those factors. An article published in Secure Business Quarterly titled "*Tangible ROI through Secure Software Engineering*" (Fourth Quarter of 2001) states that

> "one dollar required to resolve an issue during the design phase grows into 60 to 100 dollars to resolve the same issue after the application has shipped" [94].

They also indicate that the return on investment (ROI) can be as high as 21 percent when examined during the design phase [94]. Even if the security flaw is not caught until the test phase, Gartner estimates that the cost to fix a "security vulnerability during testing to be less than 2 percent of the cost of removing it from a production system" [151].

Even though there has been a decline over the last couple of years in the average loss per respondent to the CSI/FBI Computer Crime and Security Survey, it should be noted estimated losses from Internet security breaches in the US are still in the millions of dollars [83-85]. An interesting point to note in the 2006 CSI/FBI Computer Crime and Security Survey, that supports the idea that a business' reputation is important, is that the

> "number of respondents willing to report their losses this year was less than half the number of the previous year" [85].

The PricewaterhouseCoopers (PWC) indicates that large companies appear to be handling the cost of the disruptions better than small companies [158]. However, they still estimate that the average cost, for a large United Kingdom company's most serious security breach is still between £65,000 and £130,000 and smaller businesses between £8,000 to £17,000 [158]. PWC also stated that:

> "The median number of incidents suffered is roughly eight a year. This has increased from two years ago. The cost associated with security incidents has also risen" [158].

PWC goes on to indicate that "the biggest single impact of security breaches continues to be business disruptions" [158] via attacks on web-sites and /or internet gateways. This corresponds with a previous CSI/FBI survey which indicated that there are problems with Web site defacement, misuse of public Web applications, unauthorized access, insider net abuse, denial of service attacks and viruses [83]. This information clearly demonstrates that there are individuals actively looking for software vulnerabilities on the Web. According to Deloitte & Touche's *2004 Global Security Survey,* the number of systems being compromised in the financial sector is on the rise and attacks are on the increase [47, 48]. The 2006 Global Security Survey elaborates on this point by stating that internet threats are on the rise and that the attacks are becoming more sophisticated [50]. Now, either more companies are being more forthcoming with information, or more systems are being compromised, or possibly both. However, given the statement by the CSI/FBI survey that the number of respondents willing to report losses is less than half of the previous year, it is likely that more systems are being compromised.

The truth of the matter is that we really do not know the exact number of systems that are being compromised. Most companies do not want this information made public for a variety of reasons. For example, they do not want to admit, from a reputation standpoint, that their systems have been compromised; they do not want to endure the expense necessary to rectify the problem; they do not know how to fix the problem or, even worse, they are not even aware that their systems have been compromised.

These issues can be summarized in terms of potential economical cost. Since bad news sells in today's press environment, companies do not want to sustain damage to their reputations or lose public good-will which could translate into soft cost. Soft cost, also referred to in the accounting profession as indirect cost, in this instance, refers to costs that are hard to quantify economically [202]. In opposition, hard cost, also referred to in the accounting profession as direct cost, refers to cost that are easily quantifiable [202]. There is some research that provides validity to company fears in terms of hard cost i.e., stock price. Telang and Wattal's research indicates that a software vendor loses, on average, approximately 0.6% of their stock price per vulnerability announcement [184]. Granted, there appears to be a lot of contributing factors in their calculation of the estimated stock hit per vulnerability announcement. Those factors included whether the vulnerability announcement comes from the vendor or the press, if there is a patch currently available, the type of breach, and the extent of market competition [184]. The point is not to argue the economic validity of their findings but to note that there appears to be a potential connection between security announcements and company profitability. It is only when a company's security issues start to seriously interrupt business or application functionality or evidence of an attack appears that they may admit to having a problem. Another possible reason for not wanting to admit to security breaches on the Internet is to minimize the chance of copy cat attacks on their systems until the issue has been resolved.

4.2 US Legislative Incentive

The purpose of this section along with section 4.3, 4.4 and 4.5 is to acknowledge the legal pressures that are mounting through the introduction of legislation throughout the world in response to computer crimes and acknowledge the importance of a stable Internet and World Wide Web. Internet and World Wide Web legislation still has many problems to address that include the common definitions on computer crimes, international relations, sovereignty and jurisdiction [210]. To win the war on Internet and World Wide Web crime, legislation must not only be enacted but enforced as well. Enforcement of legislation in computer crimes is very difficult due to an array of factors that include anonymity, global reach through multiple jurisdictions, and the retention and preservation of evidence [120]. Additional factors include resources, technical knowledge, and the speed at which technology develops on the Web, coupled with the need to counteract emerging problems [131].

As the World Wide Web continues to become an integral part of everyday life, the demands for secure Web applications in the business world will continue to grow. This societal pressure is being felt in the corporate environment through legislation that exists in the US on both the Federal and the State levels. Since there are fifty states, covering the impact of all individual state legislation is beyond the scope of this dissertation. However, the existence of the legislation needs to be acknowledged. An example of state legislation is the Minnesota Security Breach Disclosure Act. This Act requires businesses to contact individuals when their personal data has been released to unauthorized parties due to a security breach [186]. Federal level executive orders / legislation that have affected the computer industry include the following:

- Electronic Communications Privacy Act - provided some of the foundations for investigating computer crimes [138].
- Federal Information Security Act (FISA) of 2002 - "requires each agency to inventory its major computer systems, to identify and provide appropriate

security protections, and to develop, document, and implement an agency-wide information security program" [138].

- Executive order - National Strategy to Secure Cyberspace - makes recommendations to network operators [138].
- Homeland Security Act of 2002 - provides authority to the Secretary of Homeland Security to develop Information systems to encourage the storage, analysis and exchange of information [138].
- Homeland Security Presidential Directive No. 7 (HSPD-7) - stresses the improvement of protecting US critical infrastructure [138].
- Cyber Security Research and Development Act - authorized the National Science Foundation to award funding for computer security related activities [138].
- Check Clearing for the 21st Century Act - enables banks to process checks electronically and provide substitute checks to customers [200].

As discussed in the Web Development Evolution: The Business Perspective on Security [75], societal pressure has encouraged the development of U.S. legislation. This legislation includes the following acts which are explained below:

- The Economic Espionage Act of 1996 (EEA)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Graham-Leach-Bliley Act of 1999
- The Sarbanes-Oxley Act which was passed into law in July of 2002 [216]
- The Fair and Accurate Credit Transaction Act of 2003 (FACTA)
- The Family Rights and Privacy Act (FERPA)
- Identity Theft Penalty Enhancement Act of 2004.

The EEA was the first law that explicitly makes the theft of commercial trade secrets a federal crime [52, 75, 91]. The Act defined information in very broad terms which includes storage of information in intangible forms like that of a document on a computer [52, 75]. The EEA was liberal in how it defined "the phrase 'obtaining information' which includes merely reading it" [52, 75]. Possible penalties for violating the EEA range from fines, to imprisonment, to forfeiture of any property used to commit or facilitate the crime [34, 75, 91].

HIPAA is concerned with disclosure and transmission of healthcare information [159]. The Graham-Leach-Bliley Act focuses on how financial organizations use and distribute a customer's personal information [39, 75]. The Sarbanes-Oxley (SOX) Act was designed to help restore confidence in publicly traded financial companies, due to accounting debacles like the one experienced at Enron, by making the chief executive officers and chief financial officers personally responsible for validating financial information [75, 98]. However, the wording in the law has a broader reach than just the financial industry. The law (Sarbanes-Oxley) states that company CEOs and CFOs establish and maintain proper "internal controls" [75, 98, 216]. This means that by signing off on the validity of the data within the system they are also signing off on its security [75, 98]. It is important to note that this is only applicable in situations where the data can have a material impact on the organization's financial results [216]. The impact of the SOX legislation is the application of immense additional pressure for organizations to provide secure applications, in those scenarios, increasing the overall visibility of security in these organizations.

FACTA falls under the broad category of privacy and data protection [176]. FACTA specifically targets the accuracy of consumer financial information in an attempt to address identity theft and consumer fraud [38, 161, 196]. This could potentially impact any business system that captures and manipulates a consumer's financial information during the course of normal business activities.

FERPA protects the privacy of student records [197] and The Identity Theft Penalty Enhancement Act introduces stricter penalties for identity theft [141]. The legislative story continues to evolve. A ninety-one page bill was introduced in the Senate by Senator Patrick Leahy and Senator Arlen Specter [127]. The proposal is an aggressive "regulation-oriented" bill containing "an avalanche of new rules for corporate data security and stiff penalties for information burglars" [127]. The motivation for the legislation is the result of a series of high profile security problems [127].

4.3 US Legislation with International Impact

It should be noted that the SOX Act has an international impact.

> "It is significant to note that – in contrast to the traditional accommodation provided under the Securities Exchange Commission (SEC) and national exchange rules for listed non-U.S. companies – the requirements of the Act apply to all foreign private issuers:
>
> that have securities, including American Depositary Receipts ("ADRs"), registered under section 12 of the Securities Exchange Act of 1934;
>
> that are required to file reports under section 13(a) or 15(d) of the Securities Exchange Act (including all European companies filing Form 20-F); or
>
> that have filed a registration statement that has not yet become effective (under the Securities Act of 1933) and that have not been withdrawn"[125].

This translates into the Act being applicable to a large portion of the non-US companies that are registered with the SEC. Other acts that have an international impact include:

- Electronic Signatures Act - grants electronic contracts the same weight as paper contracts [198].
- The Computer Fraud Act of 1984 - dealt with computer violations to government computers [217].
- The National Information Infrastructure Protection Act of 1996 amended the Computer Fraud Act of 1986 [195] - expanded the legal reach to include non-government computers making unauthorized access to computers, not in the same state, a federal crime [217].

- The USA Patriot Act of 2001 - greatly expands the US government's capabilities to legally intercept a multitude of communications including communications relating to computer fraud and abuse [155].
- The US Safe Harbor Act - an agreement that allows US companies conducting business in the EU to conform to EU data protection laws [179].

4.4 UK Legal Issues

The US is not the only country that is concerned with cyber crime. Several countries have created legislation to address issues that have developed through the expansion of the net. Some of the legislation for forty-four different countries is listed in a report by Stein Schjolberg [167]. The United Kingdom laws that have impacted technology include the following:

- The Theft Act 1968 - applicable to fraud [32]
- The Forgery and Counterfeiting Act 1981 [32]
- The Criminal Damage Act 1977 - applicable to physical damage of computers [32]
- The Protection of Children Act 1978 - applicable to child pornography [32]
- The Telecommunications Act 1984 [32, 136]
- The Public Order Act 1986 - applicable to racist materials [32]
- The Criminal Justice Act 1988 [32]
- The Malicious Communications Act 1988 [188]
- The Copyright, Designs and Patents Act 1988 [32]
- The Computer Misuse Act 1990 [32]
- The Criminal Justice and Public Order Act 1994 [32]
- The Data Protection Act 1998 [32]
- Regulation of Investigatory Powers Act(RIP) 2000 [192]
- Electronic Communications Act 2000 [191]
- The Telecommunications Regulations 2000 [193]
- The Electronic Signatures Regulations 2002 [194].

All of the Acts listed above have influenced the application legality of Information Communication Technology. Four commonly examined laws when discussing computer crimes, the World Wide Web and the internet are:

- The Telecommunications Act 1984 [32, 136]
- The Computer Misuse Act 1990 [136]
- The Data Protection Act 1998 [136]
- Regulation of Investigatory Powers Act (RIP) 2000 [136].

The Telecommunications Act makes it a criminal act to transmit obscene materials via a telecommunications network or to deceive a licensed telecommunications service. The Act defines a telecommunication network broadly enough to include Internet traffic [136]. In August of 1990, the Computer Misuse Act became law in the United Kingdom. The Act is concerned with three specific offences that include:

- Unauthorised access to computer material
- Unauthorised access with intent to commit or facilitate commission of further offences
- Unauthorised modification of computer material [136, 189].

As with any Act there are always possibilities for amendments. An amendment has been proposed to The Computer Misuse Act of 1990 that would clearly criminalise interference with computer systems via denial of service attacks and significantly lengthen the maximum imprisonment terms for offences for unauthorized access and unauthorized modification [16].

The Data Protection Act specifically addresses offences concerned with unauthorised procurement or processing of data [136]. An interesting point in the Data Protection Act is that where a proven offence has taken place, the wording referencing the liability within corporate bodies in section sixty-one states that

> "any person who was purporting to act in any such capacity, he as well as the body corporate shall be guilty of that offence and be liable to be proceeded against and punished accordingly" [190].

Understanding this information in conjunction with the SOX legislation, discussed earlier in the chapter, indicates that there may be an increasing trend towards personal liability in computer related legislation.

The Regulation of Investigatory Powers Act (RIP) 2000 deals with two major points: the interception of data and the relinquishing of encryption keys. This means that the UK government can compel Internet Service Providers (ISP) to copy its traffic and divert this information to a government location for analysis. It also means that individuals holding encryption keys can be subject to prosecution for non-disclosure and for notifying any one that they have been served with a disclosure notice [88, 136, 192].

4.5 International Legal Forum

The importance of the Internet and the World Wide Web is voiced in the US report The National Strategy to Secure Cyberspace via the statement that, in regards to the nation's critical infrastructure, "Cyberspace is their nervous system — the control system of our country" and that "the healthy functioning of cyberspace is essential to our economy and our national security" [201]. International support for this perspective is visible through efforts attempting to address computer crime which include agreements by the G8 nations [118], the Mutual Legal Assistance Treaties (MILAT) [199], the European Union border controls (Interpol) and United Nations (UN) recommendations [37, 90].

A major event on the international level occurred in November of 2001 when twenty-two European countries along with Japan, Canada, South Africa and the US signed the Cyber-crime treaty [153] also referenced as the Convention on Cyber-crime. The treaty is unique in that it is "the first international treaty on crimes committed via the

Internet and other computer networks" [40]. The Cybercrime treaty was put into force in July of 2004 (which required five ratifications including a minimum of three member countries). The treaty attempted to address a range of activities that includes computer-related fraud, copyright violations, network security breaches and child pornography [40]. The overall impact of the treaty is that it endeavours to address:

> "issues of substantive and procedural criminal law, which member states are obliged to take measures to implement in national law, as well as issues of international co-operation" [209].

4.6 Summary

The environment can be described through the business foundational concepts of supply and demand. As pressure continues to escalate, i.e., demand increases in reference to application security through legislation and dissatisfied customers, not following a Web application development methodology that specifically addresses security is a potentially expensive and dangerous strategy for any business. Previous research has indicated that it is cost effective to address security flaws during development. In theory, the implementation of a Web engineering security methodology should translate into a higher Return on Investment (ROI) for the company and help improve application and application feature time-to-market through constant and consistent security testing during application development. The implementation of security during the development process should positively impact application maintenance as well as helping to improve the overall profit for the organization, in effect, increasing the supply of more secure applications.

Security, from a business perspective, has become a critical issue in today's Web enabled society. The question is not whether an attack will happen to an organization's Web site, but when, and how will it be handled? The best approach to security, from a Web application development point of view, is to address security issues upfront in the design of the Web application, mitigating both soft and hard costs. The decision that an organization has to address is how much risk is it willing to accept and at what financial cost. The policies, procedures, standards, processes, and technical controls that are developed and implemented will define the system via the terms that were discussed in chapter three, i.e., confidentiality, integrity and availability. How the policies, procedures, standards, processes, and technical controls define security results from an analysis of the organizations' business objectives, business assessment on the necessity of security and financial capabilities. This collaborative approach defines the overall security of the system within an organization. The next chapter examines how security is realistically perceived and implemented in industry during Web application development.

5 Web Application Development Security Analysis

Chapter three established the broad deficiency, in current research and practice, regarding security during the Web Engineering Development process. The business case established the industrial viability for attempting to address organizational security needs during the Web application development process. The next logical step was to determine practitioner opinions [162] and acquire practical information regarding their experience with security and development methodologies. This was approached from a general industry perspective and a specific business perspective.

This chapter focuses on understanding security in the Web engineering development process. Section 5.1 examines the results of a Web survey. Section 5.2 presents an analysis of the Web survey data. Section 5.3 examines the results of a survey conducted in a Global Fortune 500 financial organization. Section 5.4 presents the analysis of the financial organization's survey results and section 5.5 summarises the chapter.

5.1 Web Survey Results

In order to acquire information, a Web survey was hosted at the University of Glasgow during June and July of 2005. The Web survey was validated by two different individuals in the financial industry. The first individual is a Technical Lead for a major financial institution in the United States and the second individual is a Security Specialist for a financial institution in the United Kingdom.

The survey was designed to encourage participation so that the majority of the questions had a specific answer. The sample size was relatively small, (fifty-three initial respondents) and a high number of respondents did not complete all of the sections (eighteen), reducing the value of any statistical data that could be derived from the survey results.

The majority of the respondents were acquired through e-mail requests. The e-mail requests were initiated through the British Computing Society in Glasgow. These requests helped to target professionals in the industry. The balance of the respondents was acquired via communication with colleagues. The small sample size helped support the initial qualitative approach to the implementation of the survey instrument. The purpose of the survey was not to argue the validity of the sample size, the presentation / design [42, 89, 152], or the incomplete survey responses [41, 89]. In academia, there has also been a great deal of debate over the demographic groups that have access to the Internet, also know as the "digital divide" [92]. The effort behind the survey focused on the questions, not the presentation, demographic groups or plausible reasons for respondent abandonment.

This survey endeavoured to determine the responder's opinion [162] and acquire practical information regarding his or her experience with security and development methodologies. The Web provided the vehicle with the broadest industrial coverage, with the least cost and risk to organizations, while providing information on trends in the industry. Other approaches such as gathering log data will not indicate where security is in the development process and interviews are very time consuming and costly to all parties.

5.1.1 Demographics

The initial questions were used to determine the interviewee's current role in the development process and to determine the overall size of the organization. The titles indicated that the interviewees were experienced IT professionals. Out of the initial fifty-three valid respondents who participated in the Web survey, forty-one of the respondents were from the United Kingdom. The balance of the respondents consisted of seven from Jordan, one from France, one from Japan, and three from the United States. Fifty-three respondents participated in the survey; however, only thirty-seven respondents completed the survey. The options for the size of the respondent's organization and their responses are detailed in Table 5 - Organization Size.

Table 5 - Organization Size

Categories	Size	Responses
1	0 – 500	28
2	500 – 1,000	4
3	1,000 - 5,000	9
4	5,000 - 10,000	3
5	10,000 - 50,000	5
6	50,000 - 100,000	2
7	100,000 or More	2

Although the specific industry was not captured in the survey, the result in the first category supports the idea that a lot of Web development companies are small companies. Even though the majority of the respondents worked in small businesses, there is a reasonable spread of the respondents over the balance of the categories.

5.1.2 Results

As expected, the number of respondents decreased as the survey progressed from Internet, to intranet to extranet questions. Out of the total number of respondents, fifty-one indicated that they had an Internet; thirty-two indicated that they had an intranet and twelve indicated that they had an extranet.

It should be noted that most of the respondents represent small businesses. The majority of the respondent's organizations have Internet sites. The break down of the type of application development process implemented by the various organizations is shown in Table 6 – Application Development Process.

Development Processes

The traditional systems development process appears to remain very prevalent in industry Web development. The responses that included some form of the traditional development process appeared in five out of the thirteen responses for Internet development and eight out of the thirteen for intranet development and four out of six responses for extranet development. Oddly enough, none of the respondents indicated that they use both agile and traditional processes depending on the nature of the project. This suggests that the organizations involved in the survey implement a single development methodology to address all their needs during application development. This result supports previous application development research findings where specific organizations have taken a “one size fits all approach” [129].

Table 6 - Application Development Process

	1	2	3	4	5	Total Number of Respondents
Internet	2	3	2	0	6	13
Intranet	1	6	2	0	4	13
Extranet	0	2	2	0	2	6

Table 6 - Key

1– Agile Development Process (Extreme Programming, DSDM)
2– Traditional Systems Development Processes (Water Fall Approach, Spiral Model)
3– A process that is a combination of Traditional and Agile Development Processes
4– Use both Agile and Traditional process depending on the nature of the project.
5– In-House

An interesting point is that the data did not totally reflect expectations where the methodology and the size of the company were considered in the Internet development process. The expectation was that the small companies would be using agile approaches and large companies would be using some form of a traditional approach. There was a ‘category-six’ company using an agile approach, two companies in category one using a traditional approach and one using an in-house approach. As the survey progressed to the intranet development questions, the number of companies using a traditional systems approach doubles to six companies. Two of these companies were in ‘category one’, three were in ‘category five’ and one was in ‘category seven’. There were no agile answers to the extranet development question. As expected, there were no companies in ‘category one’ that responded to having an extranet. The category classification is available in Table 5 and the overall application development process information is available in Table 6.

It is encouraging that seventeen of the respondents indicated that they had a defined application Internet development process; however, nineteen out of thirty-six respondents indicated that they did not. At this point in the survey, the idea was to determine the existence of a defined process within an organization and not the specifics of the process. One issue that did surface through analysis is the question of a defined vs. implicit development process. An alternative set of questions would have been to ask if participants had an implicit development process and to have expanded on exactly what that entailed.

It is worth noting that there were more positive answers to the question asking about the existence of a defined application development process for intranet and extranet applications. The same question, posed about the Internet, yielded more negative responses. It should be noted that out of the six respondents who have a defined extranet application development process, five of the respondents have all three forms of application development processes defined. The trend indicates that organizations with a defined extranet process are more likely to have defined processes for Internets and intranets. The high-level application development process results are summarized in Table 7 – Defined Application Development Process.

Table 7 - Defined Application Development Process

Question	YES	NO	DNK*	Respondents
Internet	14	19	3	36
Intranet	13	11	3	27
Extranet	6	4	1	11

*DNK: Do Not Know

Security Processes

There were thirty-five responses to a question about the organization having a defined application development Internet security process. Out of the thirty-five responses, seventeen indicated that they have an Internet application development security process, while fourteen indicated that they did not and four indicated that they "Do Not Know".

The expectation was that there would have been more responses that had a defined Internet application development process than a defined Internet security process. Another expectation would have been for the respondents who answered positively to the defined application development process question to be the same as the respondents in the defined application development security process question.

In other words, the organizations that have an application development process would have been expected to have a security development process. A detailed examination reveals that there were seven responders who confirmed having a defined security development process but who also did not indicate positively that they had a defined application development process. This result, however, was neither logical nor expected from the survey.

The organizational demographics for the seven respondents who had a security process and did not have a defined development process indicates that these respondents are from relatively small organizations. The data are summarized in Table 8 – Security Process & No Defined Application Development Process.

Table 8 - Security Process & No Defined Application Development Process

Size	Count
0-500	5
1,000 – 5,000	1
5,000 – 10,000	1

The results of the organizational demographics of the ten respondents that had both a defined application development process and an Internet security process were as expected. The results were spread out across the respondent categories. This information is summarized in Table 9 – Security Process & a Defined Application Development Process.

Table 9 - Security Process & a Defined Application Development Process

Size	Count
0-500	3
500 – 1,000	2
1,000 – 5,000	2
5,000 – 10,000	0
10,000 – 50,000	1
50,000 – 100,000	2
100,000 or More	0

The survey did indicate that security is being substantially recognized 'During the initial design phase' for Internet, intranet, and extranet development. This is an excellent indicator that security is starting to be included at the beginning of the development process. To what depth security is being addressed in the design phase is still open to debate.

The survey then attempted to determine the phases that were included in the security process, whether there is an individual responsible for ensuring that the security process is followed and if there is any job related impact for not following the security process. The specifics that the survey revealed, in reference to the organizations that claimed to have defined application development security processes, are summarized in Table 10 – Security Process Information.

Table 10 - Security Process Information

Phases	Internet	Intranet	Extranet
Total Respondents	**17**	**13**	**5**
Risk Analysis	12	6	3
Security Requirements	14	9	5
Security Design	13	9	5
Controlled Implementation	14	7	5
Testing	12	5	4
Feedback	9	6	5
Employees Follow Security Process	14	9	5
Individual Responsible for Insuring Security Process is followed	15	9	5
Job Impact for not following the Security Process	4	5	3

The table reveals that the weakest phase is the feedback phase. Most of the organizations that responded indicated there was an individual on the team who is responsible for ensuring that the intranet security process is followed, but there was a drop in positive responses to the question inquiring about a job related impact for not following the intranet security process. It is also worth noting that twenty-three of the respondents felt that their organizations considered security to be "Very Important" in its Internet, intranet, and extranet applications. However, the number of "Very Important" responses fell to sixteen when asked how important security was within the development process.

Organizations appear to be contributing to the security education of their employees. Thirty seven respondents indicated that they take some actions to educate employees about computer security. The survey did not attempt to define this information to determine the type of security education that was being distributed in organizations. The education numbers compared with the perception of importance indicates that there still appears to be a gap between understanding security and integrating security into the development process. This observation is also supported by the fact that out of a potential thirty-five respondents that completed the survey only seventeen had an Internet security process.

Only nineteen (one more than half of the respondents) gave a positive answer to the question of the organization having a disaster recovery plan that includes the applications in the security design requirements. Only ten of the nineteen responses indicated that the organization had tested the disaster recovery plan through execution.

5.2 Web Engineering Security Missing Elements

Viega stated the issues well in the statement "the problem is, building secure software is not easy" [205]. The survey captured relevant data regarding how security is realistically perceived and implemented in industry during Web application development. In doing so, the survey attempted to gain an understanding of the current role security plays in the Web application development process in industry. Since the survey specifically targeted Web Application development the information derived from the results is targeted in the same area. That is not to say that the information may or may not be relevant in other areas of application development, but that the research conducted specifically inquired about Web application development processes.

The analysis of the survey data reveals several elements that organizations appear to be failing to address. These identified elements need to be stressed when considering a Security Improvement Approach (SIA) for Web development projects. An SIA for the purposes of this dissertation is defined as the high level theoretical approach to making security improvements. The detailed analysis of the information presented in this dissertation is reported in the Web Survey Technical Report [82]. The five Essential Elements identified in this survey and discussed in the following subsections of this chapter are as follows:

1. Web Application Development Methodology
2. Web Security Development Process Definition
3. End-Users Feed Back
4. Implement & Test Disaster Recovery Plans
5. Job Related Impact

5.2.1 Web Application Development Methodology

Before security can be addressed in an organization's Web application development process, there needs to be an application development methodology in use within the organization. This methodology can be either implicit or explicit, though it is recommended that the development process be explicit. An explicit development methodology helps encourage understanding among existing employees and can be used to help foster new employee training. The point supported by the survey is that there needs to be a Web application development methodology within the organization, regardless of approach. A Web development methodology also helps to provide structure to the complex, agile, time sensitive development environment. The survey responses indicated that there is the possibility that environments exist that claim to have a security process and no application development process.

This result initiates several queries. The natural questions include: was the survey too strict in asking for a defined documented process; are there organizations that do not have an implicit or explicit development environment; and are there potential discrepancies on the definition of security among the participating parties? These concerns are valid observations to note and warrant a discussion in their own right. Regardless of the outcome of those discussions, security cannot be implemented into a development environment that does not exist. Hence, the identification of the Web application development process (even if it is implicit) is a critical starting point when trying to integrate security into a development environment.

5.2.2 Web Security Development Process Definition

The discrepancy in the responses around the questions concerning a defined application development process and a defined application development Internet security process indicates that there is possibly some confusion over the definition of an Internet security process in the industry. In general, most of the respondents indicated that the phases of the security development process were present. This indication naturally leads one to suspect that the respondents could have simply added a security checklist to a small piece of a traditional process and called it a security development process.

In order to cut down on possible confusion and to ensure that everyone is communicating properly, organizations should define:

- What security means to the business
- What it means to a Web application
- What it means in the development process
- What a Web Engineering Security development process entails.

Defining this information naturally supports the Web engineering criteria for a usability focused design. For the purposes of this discussion, security should be defined in terms of Confidentiality, Integrity and Availability also know as the CIA [153]. Security, in terms of a Web application, means that the information resources are suitably protected in terms of the CIA and, it should also consider, the level of protection desired based on acceptable risk and appropriate end-user requirements. Security in the development process means integrating appropriate security measures into the existing development process in order to produce a more secure end-product. A Web Engineering Security process should clearly define all aspects of security in the development process. It should specifically capture security requirements, integrate these requirements into code development, and test to ensure that they were successfully addressed. Clearly defining the Web security development process will encourage clearer communication among employees and help with future employee training.

5.2.3 End-User Feedback

The survey noted that there was a lack of end-user feedback in the Internet, intranet and extranet development processes. If a development process does not attempt to acquire feedback from the end-users, this could signal potentially large problems with the development process alignment with the needs of the business. Strong support for end-user participation in Web Application development has been previously indicated in a journal article by McDonald and Welland [130].

This lack of feedback potentially has a direct impact on the potential effectiveness of a security solution. Actual end-users, not surrogate end-users, need to be used in the testing of the application. End-users will perform operations, submit data, and interpret instructions in ways that the development team, the business team or the technical staff within an organization could easily overlook. This is also true from a security perspective.

End-users should be observed and consulted for information on the effectiveness of the implemented security solution. Observing employees has the potential to reveal security issues and application problems that could be manipulated into contributing to a security breach.

It could be argued that employees are not always forthcoming with information, especially if the lack of security or the potential security vulnerability either does not directly affect their duties or actually helps them to accomplish their assigned task. This indicates that “users often deliberately disable or ignore security to get their work done” [12]. The opposite could also be argued in that employees may not be aware that they are creating security problems through a lack of knowledge, general education and training. Therefore, a multiple stream approach consisting of end-user involvement in testing, end-user observation, and end-user consultation is recommended when working with end-users.

The concept of involving end-users in the security aspect of the application development process is not a new concept. Saltzer and Schroeder categorized “Psychological Acceptability” as one of eight

> “useful principles that can guide the design and contribute to an implementation without security flaws” [166].

Saltzer’s and Schroeder’s viewpoint was from the perspective of minimizing mistakes through the human interface design which is a valid point, but it does not specifically address end-user involvement in testing or observation of the end-user during testing. Existing research [12, 166] coupled with the results of the survey discussed in this paper strengthens the case for an organization to seek end-user feedback from a security perspective.

5.2.4 Implement & Test Disaster Recovery Plans

Nineteen of the thirty-seven respondents indicated that they have a disaster recovery plan that includes the individual applications. When asked if the organization had tested the disaster recovery plan by execution within the past twelve months the number fell to ten. Testing the disaster recovery plan implies that the plan is relatively up-to-date and is functional as of the last execution. The survey was really saying that there were ten out of a potential thirty-seven organizations that have an up-to-date, tested and functional disaster recovery plan. This information concurs with an AT&T "survey of more than 1,200 businesses conducted from January to August, 2005; (where) nearly 40 percent stated that business continuity planning was not a priority" [11]. A Business Continuity Plan (BCP) addresses an organization's capability to respond to events that disrupt critical business systems [90]. This comprehensive approach to disruptions would include a disaster recovery plan.

Security is really a risk management game in today's society [205]. In today's Web enabled environment disruptions are measured in minutes, not hours [103]. When it comes to risk, organizations have to make hard decisions on exactly how much risk they are willing to accept and exactly how much money they are willing to spend to achieve the agreed upon level of security [75]. This would comprise the inclusion of a Web Security process that interfaces with a disaster recovery plan in the application development life cycle.

The logical progression, once the risk and cost decisions have been made, is to address the need for a disaster recovery plan. There are a multitude of reasons for developing and implementing a disaster recovery plan. These reasons not only include the obvious technical attacks on an organization's Web site, as reported by The Open Web Application Security Project (OWASP) [185], but also natural disasters and terrorist attacks. These possibilities have been blatantly exhibited over the past year or so and include: The Asian Tsunami; Hurricane Katrina; Madrid Bombings [33]; Terrorist bombing in London; and The Hemel Hempstead Oil Depot Fire [108].

These events stress the need for organizations to have and test a disaster recovery plan. If the organization does not have a disaster recovery plan, then it is difficult to develop a cost effective secure design solution for a Web application.

5.2.5 Job Related Impact

The survey revealed that the majority of the organizations did not have a job related impact for not following the security development process. There needs to be a job related impact associated with security process compliancy. Employees need to understand that there are consequences for not following organizational processes. This becomes even more important when considering security.

One solution would be to provide positive and negative reinforcement. The idea is to reward individuals that adhere to the security process. An example would be to provide monetary rewards to programmers based on the amount of secure code they produce, not the total amount of code that they generate. On the other side of this issue, there needs to be repercussions for individuals who do not follow the organization's security development process. Another idea that has surfaced is to tie security to the employees yearly evaluation [214].

Web Application development takes place in a fast paced environment where business reputations, market shares, financial opportunities and losses are at risk daily. This increased performance pressure supports the business need for increased job related impact measures in secure Web application development. It also supports the need to conduct more in-depth industry surveys in order to gain a better understanding of security practices and the role of security in large organizations.

5.3 Fortune 500 Industry Survey Results

In addition to the Web survey discussed in the previous sections, a more in-depth survey was conducted during July and August of 2005, at a Global Fortune 500 financial organization, which focussed on security. The survey involved a variety of individuals engaged in the overall systems development process. The goals behind the survey were to determine the areas where security practices were being successfully applied and to gain an accurate understanding of the role that security plays in a large organization's application development process.

The survey examines security from the overall application development perspective and from the perspective of security within the process. This survey was conducted in the same organization as the research for the Agile Web Engineering (AWE) process and the new results from the application development component of the survey support previous findings [129]. In-depth survey details are available in a technical report [79] and in Appendices III and IV.

5.3.1 Interviewee Demographics

Within the organization, sixteen interviews were conducted. This survey sample consisted of various employees representing a variety of roles with a diversity of work experiences within the technical side of the organization. The initial questions were used to establish the interviewee's current role in the organization; his/her number of years of experience and a brief idea of the individual's history. These questions revealed that the interviewees are experienced IT professionals who have a variety of technology backgrounds; and, in general, several years of experience. The average number of years of experience among the sixteen respondents was just under fourteen years. To comprehend the security challenges, the application development process was examined first in order to understand the environment. Then the security implications of the environment were scrutinized.

5.3.2 Application Development Process

The Web application development findings that are of particular interest to Web engineering security research are as follows:

- At a high level the organization used a customized plan driven document centric waterfall approach for all application development including Web applications.

- After going through a formal design approval process there was no verification that the design implemented in production is the design that was originally approved.
- It is questionable as to whether the development process was always followed.
- Realistically, the organization was operating two different approaches to application development at different levels within the organization. The high level approach was a customized version of the plan driven waterfall approach. The low level approach consisted of a number of ad-hoc processes contrived by the individual coding teams.
- Interviewee answers indicated that the current application development process is not effective when considering time-to-market issues, rapid application development needs and the introduction of new technology, resulting in a lack of efficiency.
- The general indication from the interviewee answers was that projects exceed estimated budgets and time frames on a fairly regular basis.

5.3.3 Security within the Process

Interviewees were asked about where security is involved in the development process. The results of that inquiry are summarized in Table 11. This revealed a lack of consideration for security in the business analysis stage of the development life cycle. It also indicates that there were deficiencies in the Evaluation, Deployment, and Maintenance and Evolution stages. The variety of answers that were received when asking employees where security was involved in the development life cycle demonstrates the lack of consistent security application throughout the development process. It also suggests a lack of employee understanding of the role security plays in the application development process. When asked specifically about a security process, the majority of the respondents indicated that there was no documented process. However, when asked if someone was responsible for security within the organization, six out of the eleven positive respondents named a variation of the risk team. This is an indicator that security is viewed as someone else's problem within the organization.

Table 11 - Security Involvement

STAGE	YES	NO	OTHER
Business Analysis	4	9	3
Requirements	10	1	5
Design	13	0	3
Implementation	9	4	3
Testing	9	3	4
Evaluation	5	5	6
Deployment	9	4	3
Maintenance and Evolution	6	5	5

*Other is any answer that was not a YES or a NO

The company does have a documented security process in the Project Risk team. The interviewee responses reveal that the knowledge of the document is restricted to specific groups. Of the five 'yes' answers to the existence of a security development process, it was unanimous among those five respondents that the security development process applies to all types of application development, including Web development projects.

The problems that were discussed concerning the current security process included a lack of emphasis on the employee, a lack of utilization of that process, a lack of security involvement after the design has been signed off, and a lack of security awareness and stakeholder buy-in to security. The point of break down appears to be the length of time around the entire development process. The business has the power to circumvent the process to keep projects on track from a time line and budget perspective.

One of the thoughts behind the lack of a known security process within the organization seems to be around the fact that the individuals involved in security do not record the process. They just do what needs to be done. These people are viewed as a resource and are accessed as needed during the development process. However, there is some confusion over when and where the Project Risk team actually gets involved in the process. This is taken to the point that security is viewed as the architect's problem.

5.3.4 Security Determination

When asked how applications are deemed secure within the organization, the answers ranged from requirements, to policies, to security standards, to processes, to testing, audits and reviews. Requirements refer to the business and the application requirements. The policies and standards are set by the Project Risk team and industry standards are used to help ensure security within the organization. The process refers to the creation of the Design Architecture Document (DAD) and submitting it to the Design Architecture Committee (DAC). The testing from the organizational perspective refers to internal penetration testing and third party testing. Testing from the development perspective is subjective and tailored around the needs of the application based on the functional and non-functional requirements. The general rule is that high risk applications require more testing and, potentially, third party testing.

The answers indicate that the test used on specific applications depends on the needs of the individual application. Outwardly facing applications (i.e. Web Applications) are more rigorously tested than inwardly facing applications. Some issues related to in-house testing did surface through conversation generated via the survey. Some of the respondents indicated that time losses occurred between testing windows. If the start time for a specific test is missed, the respondents indicated that it could be as long as two weeks before another testing opportunity could be seized. When it comes to testing, audits and reviews, as far as the criteria applying to all applications, the general consensus was that it depends on the environment, the amount of risk presented and the application 'facing' that determines the security criteria that would be applied.

The survey confirmed that conflicts arise between the stakeholders and the individuals responsible for security. Fourteen of the respondents indicated that conflicts arise between the two groups. The types of conflicts range from financial and time constraints, to conflicts over security solutions. The disagreement over the security solution appears to have its roots in the perception of the level of risk that an application presents to the organization. A higher level of risk would necessitate a stronger security solution. This disagreement about perceived risk could logically take place between the business unit and the application developers. An interesting point that did surface is that certain business units also have their own individuals specifically assigned to evaluate the risk a new application presented. When there are conflicts on the analysis of a project's potential risk, this work environment has the potential to exaggerate disagreements between the technology area and the business unit.

The survey revealed that contractors are used heavily in the organization. The majority of the respondents indicated that contractors are held to the same application development methodology as employees. If they use a different process, then the process is examined and approved by the organization. The majority of the respondents indicated that contractors are also held to the same security requirements as employees. However, reading between the lines in conversations, the organization does not consistently test contractor constructed applications. Hence, there is the possibility that there are discrepancies in application testing. How effectively this is monitored and addressed appears to be up to the discretion of the project manager.

5.3.5 Practical Security

When the interviewees were asked their opinions on the emphasis security plays within the organization, some individuals thought that the emphasis on security was strong, due to outside factors such as legislation, while others felt that the emphasis was weak. A couple of individuals felt that the emphasis had improved over recent months, while others felt that the security focus was still mis-aligned. Some individuals felt that security played a large role in the organization while others felt that the emphasis was small and that security was effectively seen as an inhibitor rather than an enabler in the development process.

An attempt was made to determine if the elements of the existing in-house security process were always followed. The result was that seven out of the sixteen respondents indicated that it was not always followed. There was one 'sometimes' answer and the rest indicated that it was always followed. The interesting point was that there were only five respondents indicating that a process exists but there were eight individual solid 'yes' answers and one 'sometimes' answer that indicated that the elements of the in-house security development process were always followed. This indicates that there was at least an implicit security development process, or interviewees felt that it was politically correct to say that it is always followed even if it is perceived not to exist or is not understood! The reasons for not following the development process range from time pressures, to bureaucracy, to lack of awareness, to a lack of security involvement in certain aspects of the process. Other reasons that were mentioned include a complete lack of a process and where the application sits, i.e., does the application face the Internet or is it internal.

Eleven of the individuals who were surveyed felt that security should play a larger role in the organization's development environment. Four of the individuals surveyed felt that the current role security plays in the development environment was accurate and one felt that there were cases where it should play a smaller role. The individuals who felt that the role should be larger based their opinion on several different reasons. The reasons that seem to recur throughout the answers to this question are focused around the business. They indicate that the financial world is a relatively small world and protection of the reputation is critical. They also indicate that, in the current environment, security can be de-scoped due to numerous reasons. Integrating security into the development process up front would cut development overhead and increase security awareness within the organization potentially helping to alleviate some of these issues. Various views on the accuracy of the current security role included a good balance between security and the development environment; that the current role meets project needs; a need to extend security throughout the development life cycle and a need to engage the Risk Team as early as possible.

Eight out of the sixteen individuals surveyed felt that there is no job related impact for not following the development security process. Two of the respondents indicated that they did not know if there was an impact and six of the respondents felt that there was a job related impact.

5.3.6 Perceived Threats

An attempt was made to determine major threats to the organization during application development. There were a variety of answers that ranged from "ignorance, naivety, and incompetence of the people implementing the technical solutions", to coding issues, to coder issues, to general management issues. One of the respondents questioned the skill level of the individuals who were creating and implementing the design and the security model of the proposed solution. This was echoed via other interviewee responses. The coding issues that were discussed seemed to focus on the production of bad code. This could be caused by completing code rapidly, bad coding practices, not understanding requirements, or malicious activity on behalf of a developer.

The issues around the coder seemed to focus on the dangers associated with contractor reliance. Reliance on an outside contractor creates vulnerability from a coding practice perspective and from a skill set perspective. If you do not have the skills in-house to support the product and the contractor leaves, then the organization has to scramble to replace that individual at the risk of a high cost. This also brings up another issue that surfaced in this line of questioning, and that is, single developer reliance and high contractor reliance. This indicates that the organization does not do a good job of sharing development knowledge.

The managerial issues seemed to focus on unreasonable time scales and poor project management from a time and budget perspective. The unreasonable time scales imply a lack of understanding of the project requirements on the part of the manager. The poor project management of time scales and budgets is inevitably going to put pressure on the coding teams to produce a product within shortened time scales.

The previously mentioned management, coder and contractor issues support the idea that security needs to address the people issue, indicating that there needs to be a way to establish trust with individual employees and maintain trust with those employees. The process needs to be examined from an end-to-end-perspective to be sure that it delivers the desired results. These results need to be examined from a product, a security and both an effectiveness and efficiency perspective. The results of the survey support the idea that there are fundamental security problems with the methodologies being used in Web application development.

Education is an important area of the security process. Security education should not only include raising awareness of the different types of technical attacks and social engineering attacks [78, 135], but it should also include information about the current environment. Employees should know with whom they should discuss security, how it fits into their everyday work environment (i.e. their development process), and the potential impact security has on the Web application solution that they are proposing or introducing into the organization.

When the interviewees were asked about the issues they thought were being met and the ones they thought were not being met, a variety of answers were received. The answers ranged from the coding issues being addressed within the company, to a good implementation of separation of duty, to a lack of completely re-testing applications when updates are implemented, to out-of-synch testing and production environments, to a lack of specific security skills.

When asked about areas that require more or less emphasis, some of the recurring themes included business requirements, education, and testing. When the interviewees were asked about the major security risk that they perceived during application development, the range of answers included these common themes; seven mentioned code/design/testing /requirements, three mentioned people and behavior, two mentioned policy circumvention and enforcement, and two mentioned viruses. There were a variety of answers to the question inquiring which of these issues are being met by the existing process, which ranged from none to all. A few individuals did indicate that separation of duty, code reviews and testing is sufficient within the organization. There were several respondents who indicated that issues were not being satisfied by the existing process. Other answers ranged from a lack of documentation, to internal and external coding issues, to a lack of security in the design architecture.

The survey confirmed that conflicts arise between application developers and the individuals who are responsible for security. Thus, security from time-to-time is perceived as the culprit when Web application development projects do not hit pre-determined goals. This supports the thought process behind implementing security from the beginning of the project and sustaining it throughout the life of the project. Integration of security early in the development process helps move security from a perceived application development blocker to that of an application development enabler role.

The survey attempted to capture relevant data regarding security practices and gain an accurate understanding of the role that security plays in a specific organization's application development process. The next section examines the captured data from the perspective of identifying security criteria that are applicable to Security Improvement Approaches.

5.4 Security Criteria for Web Application Development

Industry surveys have established the global problem and the organizational survey has established the local problem in developing secure Web applications. Together, they support the need to establish a Security Improvement Approach (SIA) that can be applied to different Web engineering development processes. In order to accomplish this goal, a set of criteria needs to be established that is specific to Web engineering processes.

Exler makes an excellent point in that "the best protection" during application development "comes from a bullet-proof, practical, rigorous, and scalable process that includes security" [65]. The questions then becomes what does an organization use as a guide to achieve the best protection and how does an organization effectively critique a Web application development process? The answers to these questions are derived from the Fortune 500 financial survey discussed in the previous section and relevant literature. The Security Criteria for Web Application Development (SCWAD) identifies six security criteria within methodologies:

1. Active organizational support for security in the Web development process
2. Proper Security Controls in the development environment
3. Security Visibility throughout all areas of the development process
4. Delivery of a cohesive system, integrating business requirements, software and security
5. Prompt, Rigorous Security Testing and Evaluation
6. Trust and Accountability

5.4.1 Active Organizational Support

Active organizational support for security in the Web development process is critical. Without the support of management, there is little hope for effective integration of security within the development process. Managerial support for security needs to be both proactive and reactive. Management needs to be proactive by supporting employees, hence, giving them the necessary tools to be successful in their endeavors. Likewise, management needs to be reactive by stating and enforcing job repercussions if employees do not follow security practices within the development process or the development process in general upon which the security process depends. This lack of enforcement is noticeable in the organizational survey through the number of respondents who indicated that there was not a job related impact associated with not following the development process. This also means that the development process and any existing security measures need to apply to all employees including contractors and permanent employees. Again, this issue is questionable in the organizational survey.

Active organizational support includes encouragement of security communication among employees. The process itself should encourage communication among employees. The increased communication should translate into a better working understanding of the role security plays in the development process and the organization. This better understanding should increase the overall level of security in the development process. A key component of security is education. Employees need to be formally educated on the role security plays in the development process and in the organization, i.e., all stakeholders need to understand all of the security requirements along with the role security plays in the development process.

5.4.2 Proper Security Controls

The organization has to have proper security controls. The term proper security controls is a very broad term that encompasses policies, knowledge, technology, and processes. These controls help to provide structure to the development environment.

5.4.2.1 Policies/Standards/Procedures

Policies, standards and procedures are utilized to assist in providing a cohesive organizational infrastructure.

> "The goal of an information security policy is to maintain the integrity, confidentiality and availability of information resources" [91].

The policy indicates "what" is to be done while the standards and procedures indicate "how" it is to be accomplished [90]. The detail to which these controls are developed and implemented will depend on cultural and business DNA of an individual organization. The organizational survey revealed that development and security policies have been created and are maintained in the company. However, if the development process is not always adhered to, then it stands to reason that the policies are not always enforced. If a project goes through under the wire, there is no guarantee that the risk team has been properly briefed on the project details.

5.4.2.2 Knowledge

Organizations need to encourage knowledge transfer among employees and provide for proper training. Such training is necessary with respect to comments regarding incompetence which were covered in section 5.3.6 *Perceived Threat*, issues with coding, issues with the coders themselves, and managerial issues, all of which impact security issues in Web Development.

As discussed in chapter three, section two, the Organization for Internet Safety (OIS) publishes Guidelines for Security Vulnerabilities Reporting and Response in which they define a security vulnerability as

> "a flaw within a software system that can cause it to work contrary to its documented design and could be exploited to cause the system to violate its documented security policy" [78, 142].

This translates into the fact that any flaws in the system design or application coding can potentially lead to security vulnerabilities [78]. This problem is emphasized due to the availability and accessibility of Web applications. Common Web development security problems include un-validated parameters, cross-site scripting, buffer overflows, command injection flaws, error-handling problems, insecure use of cryptography, and broken access controls [20, 78, 134]. Designers and developers should be educated on common development flaws, best coding practices and the implementation of practical development solutions. Coupling the OIS definition with the results of the survey supports the idea that security can not be left to the acquisition of the functional and non-functional security requirements. It also supports the idea that security is more than a technical issue; it is a people, a process and an educational issue that must be addressed in its entirety.

As mentioned earlier in this chapter security should cover a variety of topics. These topics include technical attacks, social engineering attacks and information pertaining to the impact of security against the daily operational Web application development activities within the organization.

5.4.2.3 Technology

Technological controls can be as granular as implementing proper authentication in order to preserve confidentiality, integrity and availability through policy enforcement. Technological controls can also include the use of source control applications, the use of standardized application development software and up-to-date code libraries. Software can be used to analyze code to reduce the number of security vulnerabilities. Technology can also be utilized during application development by using project management software and monitoring programs such as network intrusion detection and host based intrusion detection systems.

5.4.2.4 Process

A Gartner report refers to the process as

> "The newest and least-mature lens added to the resources of the information security officer" [72].

Gartner goes on to say that

> "focus(ing) on process maturity can improve the quality of work and the efficiency with which it is accomplished (and that) the ability to translate efficiency into cost savings makes process maturity an easily justified investment" [72].

The process that an organization decides to implement is another form of control. This process can be in the form of a development process and a specific security process. It should be noted that there needs to be an application development process established either explicitly or implicitly within the organization. Without a development process there is serious potential for chaos. The results of the project then depend on the skill levels of the individuals involved.

The survey revealed three problems within the organization. The first problem is that the process is not used on all projects or is not followed properly for all projects. The second issue is that, realistically, the organization is operating two different approaches to application development at different levels within the organization.

The risk with the issues is that security is implemented at the high level approach and ignored at the lower levels. This situation can mask security problems and make them more complicated to resolve. The third problem, the split process environment, naturally encourages a lack of consistency in the coding, documentation and delivery abilities between different development areas within the organization.

5.4.3 Security Visibility

The third criterion is that security is visible throughout all areas of the development process. The organization’s application development findings indicate that there is a problem with visibility due to the fact that, after a design has been formally approved, there is no verification that the implemented design matches the approved design. It also indicated that there is a much deeper security issue within the organization. The fact that the organization is operating two different development methodologies at different levels within the organization violates the visibility criteria. Security could potentially be implemented at the higher level and never filter down to the lower level. The security aspect of the organizational survey revealed that there are deficiencies in the areas of Business Analysis, Evaluation, Deployment, and Maintenance and Evolution.

Security should be visible in all steps of the development process if it is to be implemented with any success. This implies that the development process needs to be security focused. The term security focused translates into the use of effective and efficient designs, good coding practices, addressing security issues such as authentication and authorization issues, having specific security testing criteria, and acquiring feedback from the end-user that is security specific. This means that the process encourages secure practices such as: acquiring specific security requirements, infrastructure re-use, re-usable components, coding standards, coding practices, end-to-end data security, secure designs, and takes into account security policies, procedures and standards.

Security solutions should also be confirmed with the end-user. Does the solution meet the needs of the end-user? If not, is the end-user circumventing the security measure? The survey indicates that there is a deficiency in the acquisition of end-user feedback. This end-user feedback deficiency is supported by other work in the same organization [130].

5.4.4 Delivery of a Cohesive System

The goal of any development process should be to deliver a cohesive system, integrating business requirements / needs, software and security. This means that the security requirements of the business need to be identified as early as possible in the development process so that they can be incorporated into the design and the construction in order to produce secure software. The survey indicates that this does not happen within the organization. Security is lacking in the business analysis stage.

The incorporation of security into the development process should be as seamless as possible. The security that is implemented should meet the needs of the organization so that it adds value to the end product and to the overall business process. The application development area of the survey indicates that this criterion is not being met. The development process is not effective when considering time to market, rapid application deployment needs, introduction of new technology, and efficiency. Since security is not explicitly stated in the analysis phase of the process, the organization does not truly know if the business needs are being satisfied. To make matters worse, the survey revealed that budgets and time frames are often exceeded.

A metric system should also be developed that helps the organization determine the success of the development process security initiative. This should include issues ranging from general security education, to training, to monitoring and tracking all development bugs. This will help the organization determine if it is actually delivering a cohesive system that integrates the business, the software and the security perspectives.

5.4.5 Prompt, Rigorous Security Testing and Evaluation

The development process should include rigorous end-user relevance testing and evaluation. The idea of collecting information from end-users is not a new idea in the testing world. Rakitin advocates primarily a post-implementation solution when he indicates that

> "data collected on the types of problems reported by customers (an example of a product metric) can be used to change the software validation test suite to be more representative of actual customer use of the product" [160].

Testing is critical to the success of many applications. This is especially true of applications that live on the World Wide Web. The criticality of testing Web applications is due to the unlimited exposure provided by the Internet. This extreme exposure reinforces the idea that software testing should be conducted from different perspectives such as structure-driven, requirements-driven, statistics-driven and risk-driven testing [74]. Testing should be conducted from a design and programming perspective using both automated tools [74, 86] and manual scripts. Testing should also consist of activities that include: code reviews [86], and black and white box testing [160]. Likewise, testing should also take into consideration as much as is realistically achievable and financially viable by the organization. The risk presented by the application coupled with financial capabilities could warrant additional testing in the areas of penetration testing [153] and end-user evaluation testing. End-user testing translates into the process being accountable for the security requirements, the environment and the practicality of the solution from the end-user's perspective. Another sound testing practice is to bring in external testers [153] to validate application security, when the risk is deemed appropriate for such an action.

The survey revealed, in the Security Determination section, that the process is not efficient in creating a situation where certain types of testing can occur on demand. Rigorous testing is a necessity in Web application development; however, the idea of possibly losing two weeks based on strict testing windows directly contradicts the Web application development need for short development life cycles. In a perfect world, testing should take place throughout the development life cycle; hence, utilizing short focused development cycles. However, this issue is dependent on the development life cycle the organization decides to implement as well as the cultural environment.

5.4.6 Trust and Accountability

The development process should encourage the development and maintainability of trust and accountability within the organization. Trust can be defined as "Firm reliance on the integrity, ability, or character of a person or thing" [60]. It is the foundation for a good relationship because it realistically adds value to the communication that takes place in the relationship [110]. Kaplan's reference to Gerick's explanation of trust is that

> "trust is not transitive, distributive, associative, or symmetric except in certain instances that are very narrowly defined" [110].

This information is of key importance to understanding the overall concept of trust. Establishing trust is the heart of security for without trust you can not rely on the information that is presented. A major component in gaining trust is to manage risk and then to implement appropriate controls, educate employees and monitor effectiveness [110]. A tried and true approach to identifying risk is a risk assessment initiative. Trust should be identified in the risk assessment and mitigated in the design to establish and maintain trust. Since nothing is truly risk free, the goal is to mitigate the risk so that it is at an acceptable level. Therefore, the development process has to take risk into consideration. This is typically done via a risk analysis. The earlier this is completed in the development process the better.

Accountability is critical to the enforcement of security. Individuals have to be successfully identified and authenticated in order to be held accountable for their actions through the use of logs and the effective implementation of access methodologies. The effective establishment of trust and realistic implementation of accountability controls should be visible within the organization's security policy, the application's design, coding practices, coding standards, application testing, and project feedback, as a project progresses through the application development life cycle.

5.5 Summary

The results from the Web survey have identified five Essential Elements that can be used in a Security Improvement Approach (SIA) and, optimally, should be examined prior to conducting a Security Improvement Initiative (SII) within an organization. The five Essential Elements identified in this survey are as follows:

1. Web Application Development Methodology
2. Web Security Development Process Definition
3. End-User's Feed Back
4. Implement & Test Disaster Recovery Plans
5. Job Related Impact

The basic idea is that there appears to be fundamental issues with industrial Web application development that need to be addressed. The survey indicates that the elements listed above appear to be problem areas and warrant additional research. This does not mean that the list is exhaustive or conclusive or that these elements are mandatory for an organization to function. However, their presence will potentially improve the results of the SII and/or provide a less resistant path to identified areas that need improvement. This information can also be utilized to help critique security identifying potential problem areas in a SII that is currently being executed. Once the foundational issues for conducting a SIA have been established, the next step examined where security practices have been effectively applied in a large organization.

The Global Fortune 500 financial organization demonstrates a lack of security integration in the application development process. This lack of integration is supported through deficient security discussion in the beginning of the development process, a lack of encouragement for re-usable components, a lack of follow-up after design approval, and a lack of employee understanding of the role security plays in the application development process. The results also indicate that there is a gap between the application development process and the implementation of security from an end-to-end perspective. Therefore, it is vital to develop a security process that addresses security issues throughout the entire process. Empirical evidence from the organizational survey coupled with relevant literature supports the identification of six Security Criteria for Web Application Development (SCWAD):

1. Active organizational support for security in the Web development process
2. Proper Security Controls in the development environment
3. Security visibility throughout all areas of the development process
4. Delivery of a cohesive system, integrating business requirements, software and security
5. Prompt, rigorous testing and evaluation
6. Trust and Accountability

SCWAD provides an avenue for assessing existing Web Engineering processes and a guide to future Security Improvement Approaches and Initiatives. The next chapter examines SCWAD in conjunction with Web Engineering processes and security processes.

6 Security Criteria for Web Application Development (SCWAD) Analysis

The objective of this chapter is to evaluate existing application development processes and security processes used in Web engineering via the Security Criteria for Web Application Development (SCWAD). Therefore, this chapter is based on a critical literature review that examines popular Web engineering processes and security processes assessing their compatibility with the SCWAD.

The point of this chapter is not to provide an exhaustive evaluation or to argue the validity of either Web engineering development processes or security methodologies. The purpose of this analysis is to examine popular Web application development processes and security processes from the SCWAD perspective. The analysis at this stage of the dissertation will also assist with future process discussion throughout the remainder of the dissertation. The Web engineering processes that were chosen include both agile and traditional software engineering processes. The reason for this is twofold. First, it demonstrates that the criteria are applicable to both traditional and agile engineering approaches. Secondly, and more importantly, the Web survey discussed in chapter five indicates that both approaches to Web engineering are used in industry.

SCWAD identifies six criteria which were discussed in detail in chapter five. The rating of the various methodologies is examined from the perspective of:

- None – no direct reference was determined from the materials
- Weak – minimal indication of applicability
- Partial – indicates that there was some evidence of applicability
- Strong - clear support for the criteria.

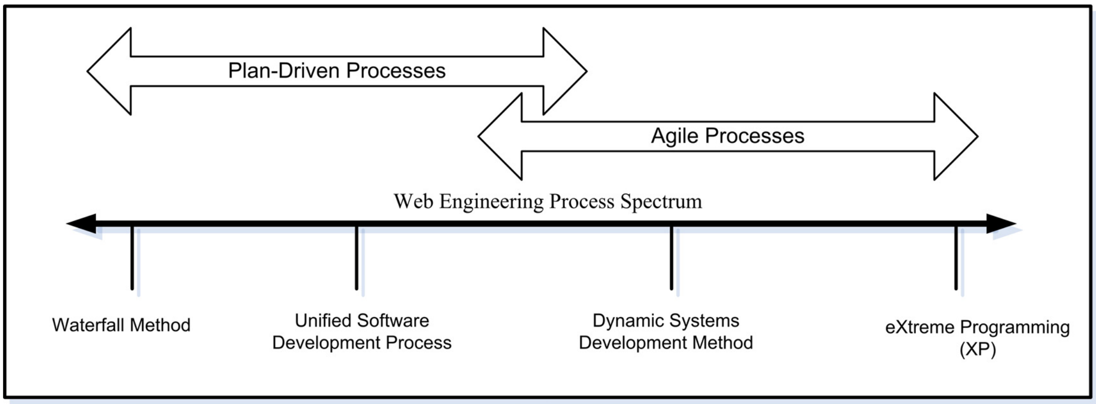
The criteria are summarized in Table 12 - Security Criteria for Web Application Development (SCWAD).

Table 12 - Security Criteria for Web Application Development (SCWAD)

No.	**Security Criteria for Web Application Development (SCWAD)**
1	Active organizational support for security in the Web development process
2	Proper Security Controls in the development environment
3	Security visibility throughout all areas of the development process
4	Delivery of a cohesive system, integrating business requirements, software & security
5	Prompt, rigorous security testing and evaluation
6	Trust and Accountability

There are several methodologies that can be used in Web application development. These include both traditional plan driven approaches and agile approaches. Figure 1 – Process Positions on the Web Engineering Process Spectrum presents the spectrum of Web engineering application development methodologies that are discussed in this chapter. The methodologies were chosen for discussion in this chapter for two reasons. The first reason is that they provide a good representation of methodologies across the broad spectrum. The second reason is that they are reasonably popular in industry. The chapter briefly describes the individual processes displayed in Figure 1 - Process Positions on the Web Engineering Process Spectrum along with ranking them according to SCWAD. Section 6.1 examines plan driven processes. Section 6.2 inspects agile process. Section 6.3 looks at security methodologies and section 6.4 provides a summary of the chapter.

Figure 1 - Process Positions on the Web Engineering Process Spectrum


Plan-Driven Processes
Agile Processes
Web Engineering Process Spectrum
Waterfall Method
Unified Software Development Process
Dynamic Systems Development Method
eXtreme Programming (XP)

6.1 Plan-Driven Processes

The Waterfall approach and the Unified Software Development (USD) process represent traditional approaches, also known as plan-driven approaches, to software development. Plan-driven approaches follow a series of fairly rigid steps in order to progress through the development life cycle.

6.1.1 Waterfall Model

The waterfall method is the classic traditional software engineering methodology. The waterfall model is attributed to Royce [164]; however, it should be noted that Royce's waterfall model was a refinement of Benington's Stagewise model [19] which was discussed in 1956 [24]. The refinements consisted of the addition of feed back loops between stages and the initial introduction of the idea of prototyping through the emphasis on "build it twice" [19, 24].

The basic waterfall process according to Royce included the following stages: systems requirements, software requirements, analysis, program design, coding, testing and operations [164]. Since its inception, the waterfall methodology has been condensed into five stages. The information regarding the individual stages of the waterfall method, which is displayed in Table 13 - Waterfall Method, has been taken directly from the Sommerville's Software Engineering text book eighth edition [175].

Security is not specifically discussed in any of the original documentation. There is, however, reference in the original documentation and subsequent discussions of the waterfall method about specifications and requirements [164, 207]. If security was talked about at all, the requirements stage and system specification are traditionally where security would have been discussed. Subsequent phases make direct reference to verification and validation of either the specifications and/or the requirements [207]. In a perfect world, if security had been specifically documented in the requirements, then it should have trickled-down to the other stages of the life cycle. However, since this has not specifically been documented as an area that needs to be addressed in the requirements stage there can be no assumption that this issue is being addressed. It has also been noted that the identification of sub-phases may have taken place; however, since "there is no general agreement on what the sub-phases are" [174] and they are not a part of the original methodology, this topic is not pursued.

Table 13 - Waterfall Method

1	Requirements Definition	The system's services, constraints and goals are established by consultation with system users. They are then defined in detail and serve as a system specification
2	System and Software Design	The system design process portions the requirements to either hardware or software systems. It establishes an overall system architecture. Software design involves identifying and describing the fundamental software system abstractions and their relationships.
3	Implementation and Unit Testing	During this stage the software design is realised as a set of programs or program units. Unit testing involves verifying that each unit meets its specifications
4	Integration and System Testing	The individual program units or programs are integrated and tested as a complete system to ensure that the software requirements have been met. After testing, the software system is delivered to the customer.
5	Operation and Maintenance	The system is installed and put into practical use. Maintenance involves correcting errors which were not discovered in earlier stages of the life cycle, improving the implementation of system units and enhancing the systems services as new requirements are discovered.

*Source: Sommerville's Software Engineering, Seventh edition [175]

The waterfall method does not support the first criteria 'active organizational support for security in the Web development process'. The methodology does not make any reference to the policies, standards and procedures to which the application needs to comply. Nor does it discuss employee knowledge or technological controls. The very nature of the discussion acknowledges the process as a control on the subconscious level. The control discussed in Royce's original article is heavily concentrated on documentation. Royce does talk about controlling the testing phase and specifically controlling input values while acknowledging the need to control certain aspects of the development process. However, there is no discussion of the process as an overall control of the development process.

While the methodology does attempt to identify specific requirements and specifications along with compliance, the methodology does not make direct reference to security. At best, security is presumed to be a part of the requirements and the specifications. This translates into security, at best, being a superficial issue in the waterfall methodology.

It could be argued that it is presumed that the security requirements are being captured in the requirements stage. Progression of the requirements through the process is supported by the fact that the System and Software Design, of the waterfall methodology, allocates requirements to the software design to be used in the development of the architecture. The Implementation and Unit Testing stage, of the waterfall methodology, involves verification with specifications. The Integration and System Testing stage makes direct reference to meeting the requirements. However, since security is not specifically called out in the development process the rating is 'None' for the third criteria.

Couple this information with the original comments by Royce stating that it is

> "important to involve the customer in a formal way so that he has committed himself at earlier points before final delivery (and that) to give the contractor free rein between requirement definition and operation is inviting trouble" [164].

This information warrants acknowledgement; however, security is not seen as a specific issue that needs to be addressed. A 'None' rating is assigned to the 'prompt and rigorous testing and evaluation' criteria. The waterfall methodology does not presents specific evidence to support the idea of proper controls in the development environment, or the delivery of a cohesive system that supports integrating business requirements, software and specifically security; nor does the methodology discuss trust and accountability. Therefore, the Waterfall method does not explicitly support any of the criteria listed in Table 12 – Security Criteria for Web Application Development.

6.1.2 The Unified Software Development Process (USD)

The inception of the USD process can be traced as far back as 1967 in the Ericsson Corporation [105]. It has undergone many modifications since that time. The current USD process actually consists of a matrix of phases and workflows. The phases of the process include inception, elaboration, construction, and transition. The workflows take place, to varying degrees, within each of the phases. The workflows consist of requirements, analysis, design, implementation and test. The USD process is use-case driven, architecture-centric, iterative and incremental [105]. It should be noted that risk is mentioned as the driver for the iterative approach that the USD process promotes. However, when discussing the iterative and incremental process, it is from a project risk perspective, not a security risk perspective. All of these points are good points for a development process. However, the process does not specifically address security. Hence, the USD process does not explicitly support the SCWAD listed in Table 12.

6.1.3 Plan-Driven Development Summary

There are other plan-driven development processes in existence that contain similar basic elements such as a requirements gathering stage, a development stage, a testing phase and an implementation phase. The two that were discussed above are arguably two of the more popular traditional development processes used in industry. When explicitly compared with SCWAD, both of these processes demonstrate the inherent lack of security within basic plan-driven application development processes.

6.2 Agile Methodologies

Agile approaches have been broadly characterized as incremental, straight forward, cooperative and adaptive [2]. A review and analysis of agile software methodologies by VTT Technical Research Center of Finland examined several different agile methodologies through five different lenses [1]. It is interesting to note that security was not a separate lens or considered as an aspect of one of the examined lenses.

6.2.1 Dynamic Systems Development Method (DSDM)

The first version of DSDM was published in the mid nineties. DSDM has been described as a frame work of controls for Rapid Application Development (RAD). According to Stapleton, DSDM is based on the following nine principles:

1. Active user involvement
2. DSDM teams must be empowered to make decisions
3. The focus is on frequent delivery of products
4. Fitness for business purpose is the essential criterion for acceptance of deliverables
5. Iterative and incremental development is necessary to converge on an accurate business solution
6. All changes during development are reversible
7. Requirements are base lined at a high level
8. Testing is integrated throughout the lifecycle
9. A collaboration and cooperative approach between all stakeholders is essential [177].

None of the nine principles discussed above explicitly state the need to address security from the perspective of SCWAD. Stapleton goes on to define the five stages of DSDM as follows:

1. Feasibility study
2. Business study
3. Functional model iteration
4. Systems design and build iteration
5. Implementation [177].

Even though the five original stages support individual ideas that are prominent in the SCWAD, they are not discussed from a security perspective. DSDM supports improved communication in organizations. In this case, DSDM describes it as

> "speeding up the development process through shortening the communication lines between all parties involved" [177].

However, there is nothing to indicate that the communications are about security related matters. DSDM supports active involvement of the end-user throughout the development process. Again, this is great. However, users are not explicitly being asked to provide input on the security of the system, the effectiveness, or to test the implemented security solution?

A DSDM.org white paper [63] does describe the implementation of the DSDM process in an organization slightly differently. They describe it as follows:

1. Pre-Project
2. Feasibility Study
3. Business Study
4. Identify Suitable Projects
5. Deliver DSDM Project
6. Post Project DSDM Promotion
7. Critical Success Factors [63].

The difference between the implementation approach and the actual methodology is really the level of execution. The implementation points discussed above are from a higher level of functioning than the actual methodology. The phases that exist, in some form, in the previous discussion of DSDM, include phases two, three and five. The new phases include phases one, four, six and seven. It should be noted at this point that a later release of the DSDM methodology does add in the pre-project and post project phases [178]. The general idea behind the points mentioned above could be argued to take place in any development process. According to the white paper, the ‘Pre-Project’ phase identifies a specific problem that DSDM can address. The ‘Identify Suitable Projects’ phase selects a project, highlights the main project risk and details the working environment. The ‘Post Project’ phase reviews the project, examines any applicable matrix, promotes the project’s successes, communicates this information out to the public, and starts looking for another project. The ‘Critical Success Factors’ phase is what is commonly referred to as a lessons learned phase. This phase looks at everything from the solution’s business fit, to measurable benefits of the solutions, to team satisfaction, to management expectations.

DSDM is very pro-business; however, it does not explicitly recognize security integration with the business needs in either approach discussed above. Thus, DSDM shows no explicit support for SCWAD criteria listed in Table 12.

6.2.2 eXtreme Programming (XP)

The XP life-cycle has six phases as described in Beck’s first book [17]. The individual cycles include: exploration, planning interactions to first release, productionising, maintenance and death. The Extreme programming Web site presents a slightly different picture of the extreme programming project which is displayed in Figure 2 - eXtreme Programming Project. They have a release planning stage, an iteration stage, an acceptance stage and a small release stage. The iteration stage is refined to include iteration planning, development and the latest version stages which are shown in Figure 3 - Iteration Refinement.

Several individual XP tasks were analysed via SCWAD criteria. It should be noted that at no point does Beck make direct reference to a security solution while discussing the individual tasks. In fact, Beck states that

> “A system isn’t certifiably secure unless it has been built with a set of security principles in mind and has been audited by a security expert”[18].

Beck goes on to state that XP is compatible with security but that the security practices would have to be incorporated into the team's daily activities. The inherent security compatibility of XP could be suggested to support the first criteria 'Active organizational support for security in the Web development process' through the implementation of pair programming. Two people coding amounts to on-the-spot code reviews. However, security was not explicitly stated. Another XP activity that shows inherent support for one of the criteria is testing. The fifth criteria states that there are 'Prompt, rigorous testing and evaluation'; testing is a major activity in XP. XP promotes short development cycles along with early, frequent and automated testing of code.

It should be noted that Beck does mention trust but from a social perspective. He explains that the customers need to trust the software; developers need to trust progress reports and developers need to trust each other. He does not explicitly call out trust from a security perspective. One could argue that if you trust the software and security was a requirement of the system, then trust from a security perspective has been established on an implicit level. However, for security to be truly integrated into a development life cycle, security needs to be explicitly stated. The results of the analysis indicate that XP does not show explicit support for the criteria listed in Table 12.

Figure 2 - eXtreme Programming Project

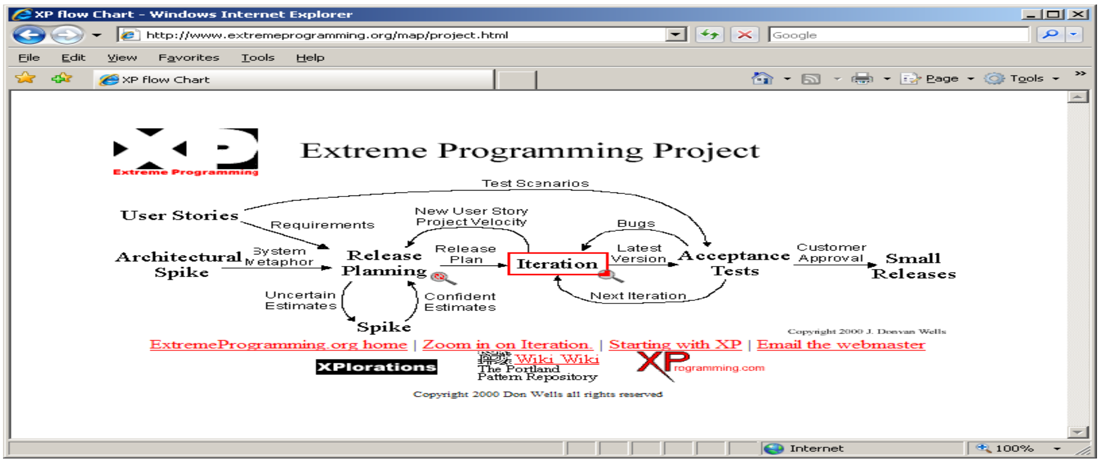
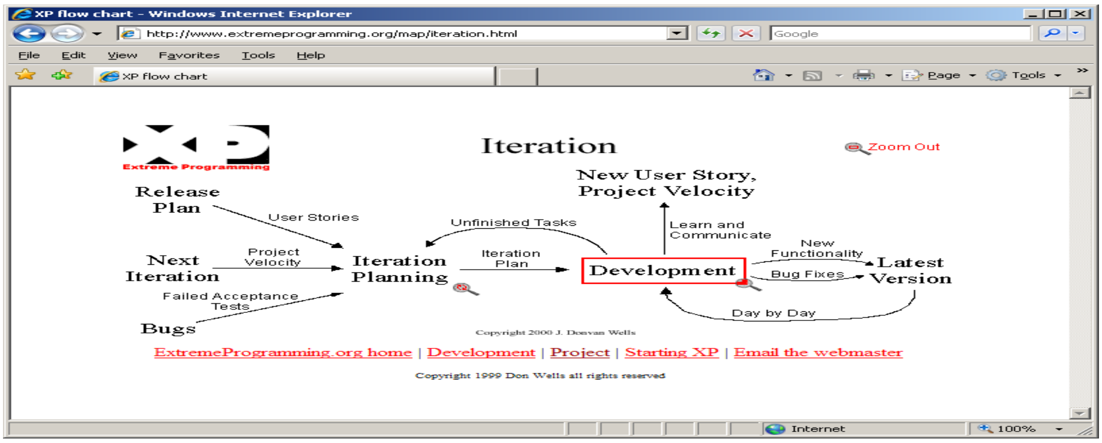


Figure 3 - Iteration Refinement


XP flow chart - Windows Internet Explorer
http://www.extremeprogramming.org/map/iteration.html
Google
File Edit View Favorites Tools Help
XP flow chart
Page Tools
Extreme Programming
Iteration
Zoom Out
New User Story, Project Velocity
Release Plan
User Stories
Unfinished Tasks
Learn and Communicate
Next Iteration
Project Velocity
Iteration Planning
Iteration Plan
Development
New Functionality
Latest Version
Bug Fixes
Failed Acceptance Tests
Bugs
Day by Day
Copyright 2000 J. Donvan Wells
ExtremeProgramming.org home | Development | Project | Starting XP | Email the webmaster
Copyright 1999 Don Wells all rights reserved
Internet
100%

6.2.3 Agile Development Summary

Again, there are many other agile development processes in existence that share common attributes such as short development cycles, parallel development, heavy user involvement and development stages. The two that were discussed above are arguably two of the more popular agile development processes used in industry. When explicitly compared with SCWAD both of these agile processes demonstrate an inherent lack of security within basic agile application development processes.

6.3 Security Methodologies

Security methodology research has been reasonably well covered by Dhillon and Backhouse [57], Siponen [171] and Baskerville[13]. Dhillon and Backhouse categorized Information System security research into four categories which consisted of functionalist, interpretive, radical humanist and radical structuralist. Baskerville analyses early security solutions and Siponen developed a generational classification scheme. Industrial attempts have also been conducted in this area along with specific academic initiatives into agile development.

According to Dhillon and Backhouse, they use a framework derived by Burrell and Morgan to categorise information systems security research. They state that the functionalist paradigm is based on the natural sciences. The interpretive is based on social situations and the actions of the individuals within those situations. The radical humanist focuses on "harnessing the competence of people" [57] rather than technology and rational models. The radical structuralist believes that the organization is composed of the business, social and computer environments and that these environments are driven by conflicting interest. Discordance among these groups is resolved through compromise and negotiation.

Siponen indicates that the contributors to this field of security research consist of four communities which include: computer security, MIS/IS security, database security and cryptology [171]. The two categories that contributed to the areas where WES is focused include MIS/IS security and computer security. As discussed in Chapter three, Siponen expanded on Baskerville's security methodology analysis creating a generational classification system. The first three generational approaches focus on specific activities such as check list, standards, and structured step wise methods. According to Siponen, the fourth generation focuses on the social and the socio-technical facets of the third generations. Siponen mentions the James's soft approach [106] and Karyda's, et. al., Viable Information System (VIS) approach in this category [111].

6.3.1 Orion Strategy

A more detailed examination of James's soft approach, also know as the Orion Strategy [106], reveals that it is really more adept at providing information security than security during application development. This point is demonstrated in a paper published by Armstrong [8]. The phases associated with the Orion strategy focus on information security and associated activities. These activities, really, should be conducted before a specific application goes through the development process. The eight phases associated with the Orion strategy are as follows:

1. Acknowledgement of Possible Security Vulnerabilities
2. Analyse Current Security Situations
3. Analyse Systems of Information Security
4. Model Ideal Information and Security Situations
5. Compare Ideal security with Current Security
6. Identify and Analyse Measures to Fill Gaps
7. Establish and Implement Security Plan
8. Monitor and control Activity [106].

The first stage of the strategy calls for vulnerability recognition by an empowered senior manager who can take actions to resolve matters. The second stage investigates the organization's current security situation. This analysis involves staff briefings, security reviews, security awareness seminars and a big picture compilation. The third stage examines the systems of information and the security of the information through system identification, a high level systems analysis, the creation of security profiles for core systems and a detail risk analysis. The fourth stage creates a model of the ideal information security situation based on the information from the previous stage. The fifth stage compares the ideal security model with reality. The idea is to use the comparison of the system to identify security gaps in the organization, not an individual application that is under construction. The sixth stage identifies and analyses possible solutions to the gaps identified in the fifth stage. The seventh stage calls for a decision from senior management on the preferred solutions along with preferred solution implementation. The last stage calls for monitoring and controlling actions when necessary. This would entail the establishment of system goals and measurable performance criteria. All of the stages of the Orion strategy are more attuned with solving security problems post system construction not prior system construction. Thus, these activities are better suited for a high-level information security initiative. Even though the applicability of this strategy to the development process is considered possible, but not probable, it can still be examined, from a high-level perspective, under the light of SCWAD.

When the Orion strategy is compared with SCWAD, there is 'Strong' support for the first criteria. SCWAD's first criterion focuses on encouragement for security communication among employees. The Orion strategy encourages this in the analysis of the current security situation stage through the staff briefings and security awareness seminars. The issue is also revisited in the final stage through training and education.

The second criteria can be subdivided into four important points which include: Policies/Standards/Procedures, Knowledge, Technology and Process. The strategy does not discuss the policies, standards or procedures within the organization or the impact of these items on information security. The strategy does encourage knowledge transfer through training and education but not at the design or coding levels of the construction of an application. Technology is examined as part of the solution to identified problems but not from an application development perspective. Simply following the Orion strategy which is a process for improving information security helps with the criteria but again the development process is not discussed in conjunction with the Orion strategy. The strategy shows ‘Weak’ support for the second criteria at best.

The Orion strategy does not discuss the actual development process or the integration of the strategy into a development process; however, the phases of the Orion strategy could be loosely associated with application development stages. Thus, the rating for the third element is ‘Weak’. The fourth criterion focuses on the delivery of a cohesive system. The Orion strategy claims to attempt to do this but it is vague about the capturing of the business security requirements. There appears to be an assumption that the compatibility of the security recommendation offered in stage seven will be evaluated by senior management and they will make the appropriate decision. This inference is supported by a couple of observations. The first is a statement made when discussing user participation indicating

> “technical experts may be knowledgeable in their own field of speciality, however, they cannot be expected to know the business operations of the organisation to the same depth or as widely as a body of employees will” [106].

The second observation is that the business requirements are not explicitly stated when discussing the phases of the strategy. Nor does the strategy discuss software development during any of the phases. These observations lead to a ‘Weak’ compliance with the fourth SCWAD criteria.

The Orion strategy does not specifically discuss testing and evaluation of the implemented security solution. In the monitor and control stage they do put forth the idea that measurement criteria needs to be established to determine effectiveness but this is after the solution has been implemented. Therefore, the rating for the fifth criteria is ‘Weak’. The strategy does indicate that a risk analysis is conducted in the stages that examine the current system and the ideal system. However, the strategy does not indicate that the risk analysis is used to determine or establish trust and accountability of the security system. The rating for the sixth criteria is ‘None’. The results are summarized in Table 14.

Table 14 - Orion Strategy / SCWAD Analysis

No.	Security Criteria for Web Application Development (SCWAD)	Results
1	Active organizational support for security in the Web development process	Strong
2	Proper Security Controls in the development environment	Weak
3	Security visibility throughout all areas of the development process	Weak
4	Delivery of a cohesive system, integrating business requirements, software & security	Weak
5	Prompt, rigorous security testing and evaluation	Weak
6	Trust and Accountability	None

6.3.2 Survivable / Viable IS Approach

Karyda, et. al., propose a Viable Information System (VIS) process that takes its roots from Stafford Beer’s Viable System Model (VSM) [111]. The thought is to broaden the idea of survivability of the individual system to the survivability of the system in relation to the organization. The viable information system consists of three main phases: diagnosis, re-design, and transformation. The main idea behind a VIS is to "maintain its existence, by managing risk" [111].

The diagnosis phase is where VSM is implemented. The risk analysis is conducted in conjunction with the VSM. They do expand the idea of the diagnosis stage by putting forth the idea that the parameters for this stage should include performance, risk and cost. They also propose a process modelling technique in the paper which they claim is based on a popular business process re-engineering technique.

According to the paper, the re-design phase may include the following steps:

1. Design processes that implement the missing, underdeveloped or flawed VSM functions.
2. Add processes that serve as attenuators or amplifiers.
3. Add controls and mechanisms to mitigate risk for the processes with a high risk factor
4. Re-evaluate [111].

The first step in the re-design is trying to address any issues that are deficient functions identified in the VSM and the risk analysis. This could include the introduction of a process that is designed to amplify potential problems. The third specifically identifies high risk processes and tries to address these issues. The last step evaluates the changes to see if they actually achieved their goals. Once this has been completed, then the changes are implemented in the transformation stage.

At this point it is appropriate to elaborate on Beer's VSM. Beer was a well published researcher in the various areas of research, but he was probably most famous for his contributions to cybernetics. The core architecture behind VSM is composed of the following five tasks:

1. Doing things (within an organization)
2. Coordinating (within the organization)
3. Optimizing (operative corporate management)
4. Observing and drawing conclusions (strategic corporate management)
5. Deciding on and keeping track of values and ensuring identity [44].

The viable system model identifies five sets of rules that were developed by Beer that coincide with the core architectural components listed above. These include:

1. The operational elements that produce the system and interact with the external environment
2. The co-ordination functions that ensure that the operational elements work harmoniously
3. The control activities, which maintain and allocate recourses to the operational elements
4. The intelligence functions that consider the system as a whole its strategic opportunities, threats and future direction.
5. The identity function, which identifies self-awareness in the system [44]

The Viable Information System (VIS) process does not perform well when it is compared with the Security Criteria for Web Application Development (SCWAD). VIS process acknowledges the importance of security incorporation into the organization's management. However, it does not elaborate on what this means to the development process. This means that the result for the first criteria is 'Weak'. VIS utilizes a risk analysis in its process. It does not elaborate on the risk analysis from a security perspective. For this reason, the rating for proper controls is 'Weak'. It also does not specifically state how the risk analysis will be used in terms of trust and accountability. Since there is no discussion of trust and accountability, the rating for the last criteria is 'None'. Also, there is no discussion from a specific security testing perspective which indicates that the rating for the testing criteria is 'None'. The other criteria that it could be argued that the process faintly addresses is the fourth criteria 'Delivery of a cohesive system, integrating business requirements, software & security'. This criterion is faintly addressed through the use of the VSM model which originally had a business orientation. The original orientation of the VSM coupled with the fact that the VIS process is designed to address security warrants at least a 'Weak' result. The results are summarized in Table 15.

Table 15- Viable Information System / SCWAD Analysis

No.	Security Criteria for Web Application Development (SCWAD)	Results
1	Active organizational support for security in the Web development process	Weak
2	Proper Security Controls in the development environment	Weak
3	Security visibility throughout all areas of the development process	Weak
4	Delivery of a cohesive system, integrating business requirements, software & security	Weak
5	Prompt, rigorous security testing and evaluation	None
6	Trust and Accountability	None

6.3.3 Comprehensive Lightweight Application Security Process

The commercial organization, Secure Software, recognizes the importance of implementing security in the software development life cycle [169]. Secure Software has attempted to address this problem with the introduction of the Comprehensive Lightweight Application Security Process (CLASP) as a stand alone process and a plug-in to the Rational Unified Process (RUP) [203]. CLASP provides a list of thirty possible activities that can be included in the development process [203]. However, an application security development methodology needs to encompass not only specific design and development activities but also needs to address overall project risk, cultural, environmental, testing, implementation and end-user feed back issues.

Viega has published an article [204] titled "*Building Security Requirements with CLASP*" that examines a critical area in establishing appropriate security. However, the article focuses on requirements and does not go into the aspects of these requirements and their cohesiveness with organizational compatibility or foundation issues that need to be acknowledge and addressed before the security requirements are captured.

CLASP, realistically, utilizes the integration of several types of lists, activities and supporting technology such as security analysis software and databases and even an application development process. The core CLASP activities and analysis of them is available in Appendix X. The result is that the core CLASP activities do not show specific support for the active organizational support criteria. The core activities show 'Partial' support for the second criteria 'Proper Controls in the development environment'. Security visibility is a 'Partial' rating as well. This is due to the fact that the core activities lack references to the business analysis aspect of software development projects and to following up with the end-user specifically on the subject of security. The rating for the fourth criteria is 'Partial' as well. The core activities place a lot of emphasis on the software and security but they lack references to the business requirements. In the area of 'Prompt rigorous testing and evaluation' the CLASP methodology receives a 'Strong' rating. The core activities indicate that detailed misuse cases should be constructed. However, there is no indication that these misuse cases will be used in the establishment of trust or accountability. It certainly would not hurt to have them, but it could be argued that this exercise is being conducted for testing purposes. Therefore, the rating for the final criteria is 'None'. The results are summarized in Table 16.

Table 16 - CLASP / SCWAD Analysis

No.	Security Criteria for Web Application Development (SCWAD)	Results
1	Active organizational support for security in the Web development process	None
2	Proper Security Controls in the development environment	Partial
3	Security visibility throughout all areas of the development process	Partial
4	Delivery of a cohesive system, integrating business requirements, software & security	Partial
5	Prompt, rigorous security testing and evaluation	Strong
6	Trust and Accountability	None

6.3.4 Trustworthy Computing Security Development Lifecycle

Microsoft has attempted to address the security shortcomings presented by the waterfall approach and the spiral approach through their Security Development Lifecycle (SDL) solution. Microsoft's SDL is based on the concept of trustworthy computing. Microsoft's Trustworthy Computing program was originally introduced in a white paper in 2002 [132]. The latest version of the white paper defines the overall goals from the user's point of view as:

1. Security
2. Privacy
3. Reliability
4. Business Integrity [133].

The overall scope of the trustworthy computing initiative is broader than simply analysing the software development process. The document acknowledges that security challenges are prevalent throughout the hardware, the software and the service components of the computing industry. The Trustworthy Computing concept was expanded in a conference paper to extend specifically to the development lifecycle which was published in the Computer Security Applications Conference in 2004 titled "*The Trustworthy Computing Security Development Lifecycle*" [123]. As of March 2005, an updated version of the document is available via Microsoft's Web site [124]. It is important to note that the SDL proposed by Microsoft makes no claims to be applicable to Web application development. In fact, it is more applicable to general application development than application designed to function on the

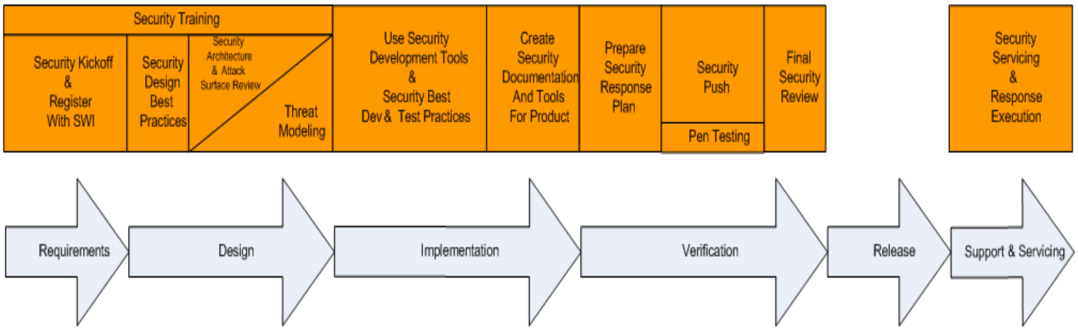
World Wide Web. However, the SDL does put forth some interesting points that warrant acknowledgement and discussion.

The SDL process appears to be a waterfall approach, based on the stages that are discussed in the methodology. However, they go on to state that it is actually a spiral process due to the fact that "requirements and design are often revisited during implementation" [123]. The SDL methodology maps into the following stages: requirements, design, implementation, verification, release, and support and servicing. Specific aspects of security are inserted into the various stages of the development process. The SDL stages are shown in Figure 4 – Microsoft's Security Development Lifecycle.

However, an examination of the original spiral model and Microsoft's SDL reveals that Microsoft takes a broad interpretation of the term spiral methodology. The spiral model was originally demonstrated using the waterfall model [24]. The spiral model presents a situation where

> "each cycle involves a progression through the same sequence of steps, for each portion of the product and for each of its levels of elaboration, from an overall concept-of-operation document down to the coding of each individual program" [24].

Figure 4 - Microsoft's Security Development Lifecycle


Security Training
Security Kickoff & Register With SWI
Security Design Best Practices
Security Architecture & Attack Surface Review
Threat Modeling
Use Security Development Tools & Security Best Dev & Test Practices
Create Security Documentation And Tools For Product
Prepare Security Response Plan
Security Push
Pen Testing
Final Security Review
Security Servicing & Response Execution
Requirements
Design
Implementation
Verification
Release
Support & Servicing

Closer examination of the spiral model indicates that this means going through an iterative process that consists of four distinct phases that includes:

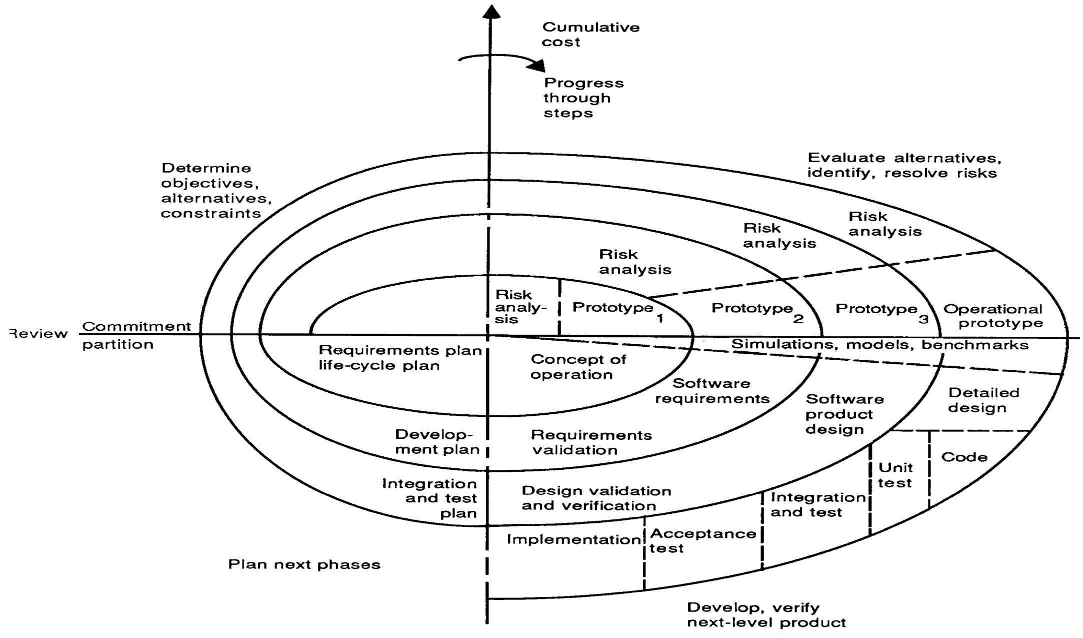
- Evaluate alternatives, identify resolve risk
- Determine objectives, alternatives, constraints
- Develop, verify next-level product
- Plan next phase

It is not until the last iteration of the 'development objectives, alternative, constraints' phase that the waterfall method is clearly used in Boehm's example of the spiral model. Based on this information, any methodology could be implemented into the last iteration of the 'development objectives, alternative, constraints' phase in the spiral methodology. The use of any methodology would need to conform to the iterative process of the four phases and include the prototyping and the identification of project risk as identified in Figure 5.

For the purpose of this discussion, I will assume that the waterfall methodology is used in the last iteration of the ‘develop, verify next-level product’ phase. The spiral model does place a greater emphasis on risk analysis, software analysis and requirements validation than the waterfall methodology through the iterative nature of the methodology.

Figure 4 indicates that Microsoft has modified a waterfall process to include security in the various stages. Microsoft’s SDL is then applicable to the final iteration of the ‘develop, verify next-level product’ phase in the spiral methodology. While the original version started off with a risk analysis, a prototype, a concept of operation and a requirements plan, the stages are expanded in later iterations of the spiral methodology. Microsoft’s spiral makes no mention of the other three phases or the prototyping which is noted in the original methodology. It also does not discuss the individual iterations and exactly what they entail.

Figure 5 - Spiral Method



*Source: Barry W. Boehm - Spiral Model[25]

SCWAD’s evaluation of Microsoft’s SDL is summarized in Table 17. SDL shows ‘Strong’ support for the first criteria. Microsoft believes that executive support for the security initiative is critical along with education and awareness. They also nominate point people to be responsible for security. The four parts of the second criteria include: Policies/Standards/Procedures, Knowledge, Technology and Process. As stated previously, Microsoft is a firm believer in security education and awareness which contributes to the knowledge portion of the second criteria. The SDL only discusses policy from the perspective of implementing the SDL in Microsoft. In the formalization of the SDL process Microsoft established a “Policy for implementing mandatory application of the SDL” [124]. This is the only aspect of policy that is discussed. There is no discussion of other policies that have a potential impact on applications that are developed in the organization. Microsoft does support the use of standards from a requirement, a coding and a testing perspective. Lipner, et. al. March 2005 document posted on Microsoft’s Web site lacks specific discussion on the use of procedures [124]. Microsoft does discuss educating developers in terms of special technologies [124] and technology that they have added to their development environment, i.e., Visual Studio 2005 [96]. The SDL is a process which they recommend and contributes to the second criteria. Therefore, the rating for the second criteria is ‘Partial’.

In addressing the third criteria, the only stage that the SDL does not show support for is the business analysis stage. This is the point at which the business unit surfaces the initial project idea. The rating for the third criteria is ‘Partial’. The methodology does not discuss interactions with the business units or the production of a cohesive system that meets the business requirements, the software requirements and the security requirements. The SDL does support on-going testing by the development team, a focused security push that includes user beta testing and code reviews, and a final security review. The final security review is an independent review of the software from within the organization. The rating for the fifth criteria is ‘Strong’.

The last criterion addresses trust and accountability. Microsoft’s SDL does a good job of discussing trust. They examine trust from the levels in a computer and from a threat modelling perspective. The threat modelling provides an avenue for addressing the risk that an application presents to the organization. Lipner, et. al. [124] mentions accountability along with metric as a major facet of building secure software but does not provide any elaboration on the idea. Therefore, the rating for the last criteria is ‘Partial’.

Table 17 - Microsoft SDL / SCWAD Analysis

No.	Security Criteria for Web Application Development (SCWAD)	Results
1	Active organizational support for security in the Web development process	Strong
2	Proper Security Controls in the development environment	Partial
3	Security visibility throughout all areas of the development process	Partial
4	Delivery of a cohesive system, integrating business requirements, software & security	None
5	Prompt, rigorous security testing and evaluation	Strong
6	Trust and Accountability	Partial

6.3.5 Agile Method Security

It should be noted that there have been specific attempts to add security to the agile application development processes by Ge [73] and Beznosov [23]. These endeavours acknowledge and validate the inherent lack of security within the ‘vanilla-off the shelf’ methodologies used for Web application development.

An analysis of Ge’s et al. [73] attempts to address security within the agile development process is to primarily review and update the security policy and to add a risk assessment into an agile development process. There is no discussion of active organizational support for security. The solution makes two direct references to security and they include a security policy decision and a security risk analysis. Both of these address two aspects of the criteria for proper controls in the development process. Since the proposed solution is trying to add security into a development process, this contributes to the process aspect of the proper controls criteria. These contributions warrant a ‘Partial’ rating for this criterion.

The paper touches on requirements analysis, use case analysis, content design and implementation but from a Feature-Driven Development (FDD) methodology perspective not specifically a security perspective. They indicate that there is a link between the development requirements and keeping the security policy up to date. They do indicate that security risk analysis is “an iterative, incremental, ongoing process” [73] and that the results of the risk analysis “may modify the content design” [73]. This implies that there is at least a weak level of intent for security visibility throughout all areas of the development process.

The business model is addressed through use cases and functional design content modelling in the FDD. They do allude to the fact that security needs to be built into the development process early in the life cycle. However, there is no discussion of whether this meets the needs of the business or any metric to see if the goal has been achieved. This warrants a ‘Weak’ rating for the criteria of ‘Delivery of a cohesive system, integrating business requirements, software & Security’. There is no specific discussion of security testing or accountability. The results are summarized in Table 18 – Ge et al. /SCWAD Analysis.

Table 18 - Ge et al. / SCWAD Analysis

No.	Security Criteria for Web Application Development (SCWAD)	Results
1	Active organizational support for security in the Web development process	None
2	Proper Security Controls in the development environment	Partial
3	Security visibility throughout all areas of the development process	Weak
4	Delivery of a cohesive system, integrating business requirements, software & security	Weak
5	Prompt, rigorous security testing and evaluation	None
6	Trust and Accountability	None

Beznosov discusses Extreme Security Engineering [23] which delves into a discussion about XP practices and how to achieve good enough security. The paper does not put forth a solid methodology that can be easily identified and transferred to other agile processes. In doing so, there is no discussion about active organizational support in the paper. The rating for the first criteria is ‘None’.

The discussion around small releases does mention the need for a well organized development environment that includes testing, scripts and duplicate resources but does not make a direct reference to security specific uses for these points. The rating for the second criteria is ‘None’. This indicates that XP is compatible with controls from a security perspective but this point is not elaborated on in the paper. The very nature of tailoring the security approach to the individual stages of a development methodology leads to a ‘Strong’ rating for the security visibility criteria. The paper does discuss user involvement in the XP process, the business stories from a security point of view and mentioned continuous integration from a security perspective. This warrants at least a ‘Partial’ rating for the fourth criteria. The paper does discuss ‘Strong’ support for testing from a security perspective. There was no discussion of trust and accountability, leading to a ‘None’ rating for the last criteria. The results are summarized in Table 19 – Extreme Security Engineering / SCWAD Analysis.

Table 19 - Extreme Security Engineering / SCWAD Analysis

No.	Security Criteria for Web Application Development (SCWAD)	Results
1	Active organizational support for security in the Web development process	None
2	Proper Security Controls in the development environment	None
3	Security visibility throughout all areas of the development process	Strong
4	Delivery of a cohesive system, integrating business requirements, software & security	Partial
5	Prompt, rigorous security testing and evaluation	Strong
6	Trust and Accountability	None

6.4 Summary

As the US Department of Homeland Security has stated "there is nothing inherently 'security-enhancing' about most development methodologies"[51]. The Waterfall methodology, the Unified Software Development Process (USD), Dynamic Systems Development Method (DSDM), and eXtreme Programming (XP) are all used to illustrate the fact that 'Vanilla - Off the Shelf' application development processes that can be used for Web engineering do not inherently include security from the SCWAD perspective. An examination of existing security methodologies demonstrates the deficiencies in the areas highlighted by SCWAD. A Summary of the security methodologies SCWAD analysis is available in Table 20 – Overall Security SCWAD Analysis. This analysis also provides a baseline for further work in Web engineering methodologies. The next chapter examines the Web Engineering Security (WES) methodology in detail.

Table 20 - Overall Security SCWAD Analysis

No.	Orion	VIS	CLASP	Microsoft	GE	ESE
1	Strong	Weak	None	Strong	None	None
2	Weak	Weak	Partial	Partial	Partial	None
3	Weak	Weak	Partial	Partial	Weak	Strong
4	Weak	Weak	Partial	None	Weak	Partial
5	Weak	None	Strong	Strong	None	Strong
6	None	None	None	Partial	None	None

7 Web Engineering Security (WES) Methodology

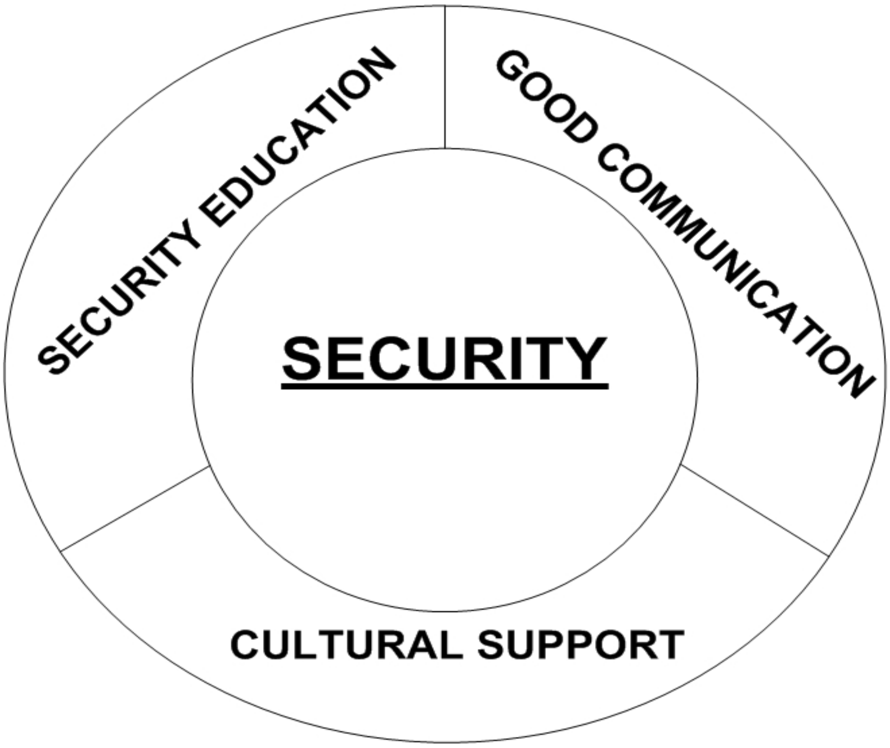
This chapter provides an overview of the Web Engineering Security (WES) methodology. WES is a proactive, process neutral, security specific methodology that is based on the empirical evidence used to identify the Essential Elements and the Security Criteria for Web Application Development (SCWAD) as discussed in chapter five. Section 7.1 presents the WES principles. Section 7.2 describes the WES process in detail. Section 7.3 briefly discusses the stakeholders involved in the WES process. Section 7.4 covers WES process deliverables. Section 7.5 presents the goals of the WES methodology. Section 7.6 presents the advantages and disadvantages of the WES methodology and section 7.7 provides a chapter summary.

7.1 WES Foundation Principles

The Web Engineering Security (WES) methodology was designed to complement Web software development through customer communications, short development cycles, and practical security solutions to business problems [4]. WES attempts to achieve this by stressing core principles while providing a general outline with customizable sub-components.

The core principles behind the development of WES include good communication, security education, and cultural support. These principles are interdependent and need to work in concert in order to achieve and maximise the desired effect from a security perspective. This concept is illustrated in Figure 6 - Principles.

Figure 6 - Principles



7.1.1 Security Education

As discussed in 3.2 and in 5.4.2, the Organization for Internet Safety (OIS) publishes Guidelines for Security Vulnerabilities Reporting and Response [78, 142]. These guidelines highlight the fact that any flaws in the system design or application coding can potentially lead to security vulnerabilities [78]. Meaning that security education should cover an array of issues including knowledge transfer, coding practices, technical attacks, social engineering attacks, security processes, every day activities and potential impact analysis methods.

This problem is emphasized due to the availability and accessibility of Web applications. As mentioned in chapter 5.4.2, common Web development security problems include un-validated parameters, cross-site scripting, buffer overflows, command injection flaws, error-handling problems, insecure use of cryptography, and broken access controls [20, 78, 134]. Hence, designers and developers should be educated on common development flaws, best coding practices and the implementation of practical development solutions. Security should not be left to the acquisition of the functional and non-functional security requirements. Security is more than a technical issue; it is a people, a process and an educational issue that must be addressed in its entirety. Organizations need to encourage knowledge transfer among employees and provide for proper training.

Education is an important area of the security process. Security education should not only include raising awareness of the different types of technical attacks and social engineering attacks [78, 135], but it should also include information about the current environment. Employees should know with whom they should discuss security, how it fits into their everyday work environment (i.e. their development process), and the potential impact security has on the Web application solution that they are implementing.

7.1.2 Good Communication

Good communication is a critical component of the methodology, as it is needed to assure solution cohesiveness within the development team and with the organization. Good communication helps to provide the foundation for security visibility throughout the entire application development methodology. Hence, good communication should encourage security visibility through the development process, an auditable process, a clear understanding of the defined metrics, the delivery of a cohesive system, and the dissemination of the importance of the integration of development and security methodologies.

In order to achieve these goals, there needs to be good stakeholder communication. This includes good communication between management and the development team, among members of the development team and between the development team members and the end-users. The communication between management and the development team is needed due to the fact that management is responsible for setting the policies, standards and procedures to which the development team must adhere.

7.1.2.1 Development Team Communication

Communication has to be encouraged and fostered in the technical side of the organization. The organization’s management, in concert with the architects, need to provide a security vision for the future. This can be communicated, in the present, through the creation of current and future standards. An excellent example of this is the development of software standards to be used for the design process. If an organization is currently on Windows XP, that standard should be published along with the expected standard for the future, such as the next version of Windows and when that standard is to become effective. Communication of this information through standards has a direct effect on the organization’s coding teams. They now know the appropriate time frames, based on the published standard, so that they can code from a compatibility perspective. This idea can be expanded to include testing environments, compatibility with specific security software such as host intrusion detections systems (HIDS) and network intrusion detection systems (NIDS). The point is that this directional support needs to be driven by upper management and provided for by the relevant parties. This support and integration with communication is a critical component for the purpose of driving future security initiatives in an organization. The marketing and dissemination of this information is necessary to effectively implement this initiative. If your employees do not know about the tools that are available, they will not use them. It is also true that if the tools and/or methods are not effective in completing the job, are too complicated to use effectively, or are just not user friendly, then employees are likely to avoid using them.

If the tools or the methods are not productive for various reasons then the individual members of the development team should suggest alternative tools or methods to be evaluated. A channel for communicating feedback to management for both positive and negative communication needs to be established in the organization. If this channel is not established, then developers will inevitably use their own tools to complete the job. Their decisions realistically could range from using off-the-shelf solutions to open source software. Off-the-shelf software could put the organization in jeopardy from a legal perspective. If the software in question has been sold for personal use and is being used in a commercial environment then there are legal implications. Open source software could introduce potential security breaches into the organization. The interaction between management and the developers helps to introduce and sustain flexibility in the Web application process. More importantly, it gives the development team a sense of ownership in reference to the methods and the tools that are used in the development process. Along with this interaction, all of the tools and the methodologies that are used in the development process need to be reviewed frequently. This review helps to ensure that the tools and the methodologies are achieving the desired goals.

Developers should also be encouraged to share technical knowledge with each other. This distribution of information encourages debate on technical solutions and distributes application knowledge through the group. This distribution of knowledge helps keep a balance in the group, thereby reducing dependency on individual employees.

7.1.2.2 End-User Communication

Communication with the end-user is needed to acquire the appropriate application requirements. Security solutions also should be confirmed with the end-user. Does the solution meet the needs of the end-user? If not, is the end-user circumventing the security measure? The security that is implemented should meet the needs of the organization so that it adds value to the end product and to the overall business process. Essential Elements that contribute to good communication include a clearly defined application development methodology and a clearly defined Web security development process. The security process should explicitly include the end-user.

This communication has a direct impact on the potential effectiveness of a security solution. Actual end-users, not surrogate end-users, need to be used in the testing of the application [81]. End-users will perform operations, submit data, and interpret instructions in ways that the development team, the business team or the technical staff within an organization could reasonably not consider! This is also true from a security perspective.

End-users should be observed and consulted for information on the effectiveness of the implemented security solution. Observing employees has the potential for revealing security issues and application problems that could be manipulated into contributing to a security breach [81].

It could be argued that employees are not always forthcoming with information, especially if the lack of security or the potential security vulnerability either does not directly affect their duties or actually helps them to accomplish their assigned tasks. Therefore, a multiple stream approach consisting of end-user involvement in testing, end-user observation and end-user consultation is recommended when working with end-users [81].

7.1.3 Cultural Support

Cultural support should drive the efforts in security and education along with the efforts in good communication. Cultural support for security should embrace confidentiality, integrity and availability throughout the management structure. Active organizational support for security in the Web development process is critical. Without the support of management, there is no hope for effective integration of security within the development process. Managerial support for security needs to be both proactive and reactive. Management needs to be proactive by supporting employees, hence, giving them the necessary tools and developing the necessary policies so that employees can be successful in their endeavours. This would include proper controls for the development environment such as software versioning controls, providing up-to-date code libraries, setting the policies for testing code and for establishing trust and accountability within and outwith the organization. Likewise, management needs to be reactive by stating and enforcing job repercussions if employees do not follow security practices within the development process or the development process in general upon which the security process depends.

7.1.4 Security Synergy

The environment that is most conducive for fostering security in the Web application development environment is the intersection of all three principles. The intersection of security education and practising good communication should help build confidence in the overall security of the organization, the general security knowledge of the employees and encourage compliance with organizational policies. The distribution of security information and how that impacts the daily activities of employees helps to provide practical solutions to security issues. This approach helps to propagate the concept that security needs to be viewed in the application development process as "everybody's problem" [86]. Integrating security responsibilities and security education into the development process increases employee confidence in addressing security issues and sends the signal to the development group that security is an important issue that has to be addressed.

A key component of security is education. Employees need to be formally educated on the role security plays in the development process and in the organization, i.e., all stakeholders need to understand all of the security requirements along with the role security plays in the development process. The support for this education should originate from management!

Cultural support for good communication helps to provide the necessary tools to get the job done and demonstrates that the organization supports the security movement within the company. Active organizational support includes encouragement of security communication among employees. Increased communication should translate into a better working understanding of the role security plays in the development process and the organization. This better understanding should increase the overall level of security in the development process.

The incorporation of security into the development process should be as seamless as possible. As discussed in greater detail in 5.4, this seamless integration of security into the development process should support the goals of meeting the Security Criteria for Web Application Development (SCWAD):

1. Active organizational support for security in the Web development process
2. Proper Controls in the development environment
3. Security visibility throughout all areas of the development process
4. Delivery of a cohesive system, integrating business requirements, software and security
5. Prompt, rigorous testing and evaluation
6. Trust and Accountability

7.2 WES Process Life Cycle

The Web Engineering Security (WES) methodology, as shown in Figure 7 - WES Methodology, starts with a Project Development Risk Assessment.

This Project Development Risk Assessment is the initial phase and it examines the security risk associated with the implementation of a project. The Application

Security Requirements phase examines the requirements from the customer perspective within the frame work of organizational compatibility. Security Design / Coding examine the architecture, the solution design and the coding practices that are implemented to solve the issue. A Controlled Environment Implementation scrutinizes the application's interactions with the entire environment before specific aspects of the application are examined.

Testing is critical to the success of many applications. This hypothesis holds true in the area of security as well. Testing not only includes the examination of code but incident management and disaster recovery. Implementation of the application in a production environment should only take place after it has successfully completed testing. End-user evaluation is used to establish the success of the application's security features and for security maintenance.

The WES methodology implicitly supports the concept of separation of duty between everything that happens before testing and everything that happens after testing. This is demonstrated through the colour of the line, the line style and the directional arrows displayed in Figure 7 - Wes Methodology. The ideal situation is that the developers and the testers who work on the project are not the same individuals who implement the project into production. Depending on the size of the organization, this may not be possible. Regardless, once code has been moved from the test environment to the production environment it should not be allowed to return to testing without going through another iteration of the process.

After the application has been implemented into the production environment, end-users should be consulted in an attempt to determine the usability of the security solution, suitability of the security solution and to help identify any security issues that need to be resolved. Once this information has been attained then the process should start the next iteration of the WES development process. Ideally, the iterations in the process should be concise. Succinct iterations encourage smaller frequent code releases which, by nature, mean that less code is introduced into a system at a single point in time. Injecting a smaller quantity of code into an existing system, in theory, denotes that smaller chunks of code are being tested at a single point in time. This potentially allows testers to focus in detail on smaller amounts of code and hopefully improve security test results.

7.2.1 Project Development Risk Assessment

The purpose of the risk assessment is to identify any risk associated with the development of the proposed application functionality. An excellent definition of risk is

> "…risk is a measure of the loss of what you consider valuable, the impact of losing it, the threats to those assets, and how often those threats could be successful" [187].

This would include examining appropriate data protection legislation that might apply to your organization's application. There are several tools and suggested practices available in the market for conducting risk analysis. These tools include

Cobra [31], the Facilitated Risk Analysis Process (FRAP) [146] and the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [5]. The National Institute of Standards and Technology (NIST) has recommendations for conducting company wide risk analysis on their Web site [147]. OCTAVE is an in-depth organization wide risk analysis approach developed at Carnegie Mellon [5].

If an organization wide risk analysis is conducted periodically, then the information in the analysis can be used as a starting point for the application risk analysis. The reverse is also true. Information from the individual application analysis can be used as an initial guide to organizational analysis. The risk assessment piece of the methodology can be customized to work in conjunction with an organization's existing risk analysis processes. The basic idea is to:

- Detail critical functions,
- Determine the necessary service levels in doing so, identify possible threats and outline their motivating factors,
- Estimate the probability of an attack,
- Estimate the probability of a successful attack,
- Outline the cost of providing protection [64, 153, 154].

The answers generated from researching the statements above should help answer the following questions proposed by Ozier:

1. "What could happen? (What is the threat?)
2. How bad could it be? (What is the impact or consequence?)
3. How often might it happen? (What is the frequency?)
4. How certain are the answers to the first three questions? (What is the degree of confidence?) The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no 'risk', per se" [144].

Application threats can cover a wide range of possibilities including: human errors in coding, user errors, external attack, fraudulent individuals, technical sabotage, acts of God, and disgruntled employees; all of which should be accounted for in the risk assessment [64]. Once the risk assessment has taken place, the specific application security requirements need to be determined through in-depth conversations with the end-users and evaluation of organizational compatibility. Organizational compatibility determines how well security requirements fit into the frame work of an organization. The general areas that make up this category include security policy compatibility, corporate culture compatibility and technical compatibility.

By conducting a **Project Development Risk Assessment**, the business and the information technology group can analyze each stage of the development by identifying the associated risks. This would include determining the states of the application and how they can be used or misused as the case may be. This step provides an opportunity for the organization's development team to understand the application from a risk point of view and helps to generate appropriate questions to address the application security requirements phase. Depending on the size of the organization and the market requirements, both the governmental and commercial perspectives, the risk analysis can be used to help identify known risks, point out new risks and ensure that these risks are acceptable. Depending on the needs of the organization, this can be either a very formal process or a very informal process. If it is a formal process, then the advantage for management is that it presents a clear understanding of the risks before a substantial investment is made in the development of the Web application. The disadvantage of a highly formalized process is that it can slow down the development process. In reality, there will be a lot of cross-over communication between the Project Development Risk Assessment stage and the Application Security Requirements stage. Informal processes tend to be faster but introduce more risk through a potential lack of environmental and risk understanding. The deliverables that could possibly be generated at this stage include a formal project risk analysis document and a risk analysis document used to gather end-user requirements, and a document detailing high-level issues for design and testing.

7.2.2 Application Security Requirements

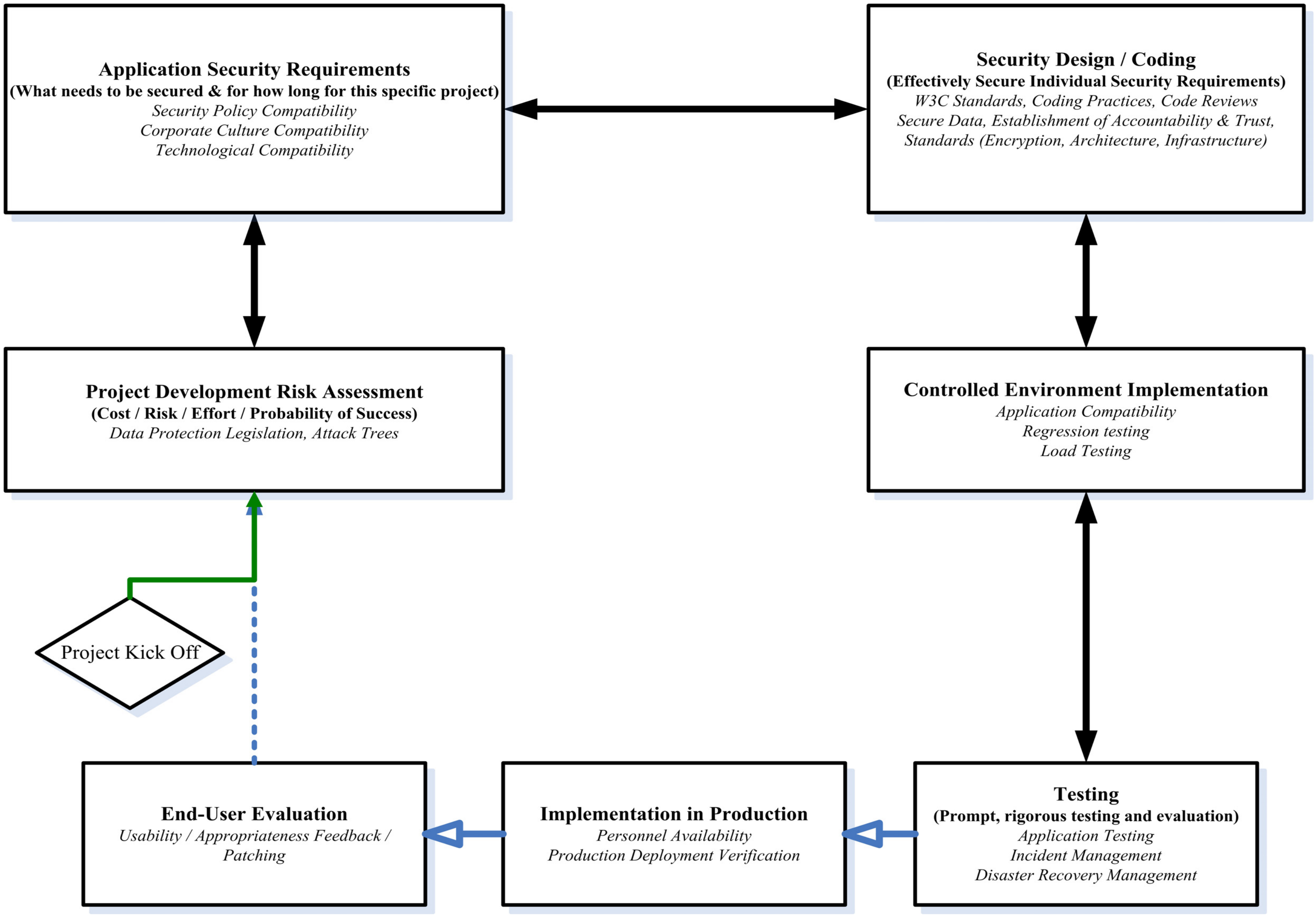
Specific application security requirements have to be acquired from the end-users. The project risk analysis should be used to help gather the security requirements by generating a series of questions and responses that filter the desires of the end-users into a list of detailed needs. The **Application Security Requirements** phase allows the development team to make a specific effort to acquire the security requirements through effective communication with the end-users. Hence, the stakeholders involved in this stage would probably include the business unit and the technical staff. They should coordinate these requirements with the organization's security compatibility constraints. The security compatibility constraints encompass several important issues that include security policies, standards, baselines, procedures, guidelines, the corporate culture and existing technology. For the purposes of this dissertation, the terms listed in Table 21 -Terms have been taken directly from *The Security Policy life Cycle: Functions and Responsibilities* by Patrick D. Howard [97]. Once these requirements have been captured, they should be examined against the organization's security policy, the corporate culture, and technical compatibility.

Table 21 - Terms

Policy:	A broad statement of principle that presents management's position for a defined control area.
Standards:	Rules that specify a particular course of action or response to a given situation.
Baseline:	A platform-specific security rule that is accepted across the industry as providing the most effective approach to a specific security implementation.
Procedures:	Define specifically how policies, standards, baselines and guidelines will be implemented in a given situation. Procedures support policies, standards and baselines.
Guidelines:	A general statement used to recommend or suggest an approach to implementation of policies, standards, and baselines.

Howard, P.D., The Security Policy life Cycle: Functions and Responsibilities[97]

Figure 7 - WES Methodology



Application Security Requirements
(What needs to be secured & for how long for this specific project)
Security Policy Compatibility
Corporate Culture Compatibility
Technological Compatibility
Security Design / Coding
(Effectively Secure Individual Security Requirements)
W3C Standards, Coding Practices, Code Reviews
Secure Data, Establishment of Accountability & Trust,
Standards (Encryption, Architecture, Infrastructure)
Project Development Risk Assessment
(Cost / Risk / Effort / Probability of Success)
Data Protection Legislation, Attack Trees
Controlled Environment Implementation
Application Compatibility
Regression testing
Load Testing
Project Kick Off
End-User Evaluation
Usability / Appropriateness Feedback /
Patching
Implementation in Production
Personnel Availability
Production Deployment Verification
Testing
(Prompt, rigorous testing and evaluation)
Application Testing
Incident Management
Disaster Recovery Management

7.2.2.1 Security Policy

Policies, standards, baselines, procedures, and guidelines can assist in large organizations to provide cohesiveness within the organization.

> "The goal of an information security policy is to maintain the integrity, confidentiality and availability of information resources" [91].

In smaller organizations, where it is not mandatory through regulation, they can be implicit to the organization. The policy provides the "what" and the standards, baselines, procedures and guidelines provide the "how" [90]. They can work in concert to support the organization from a security perspective. The security policy encompasses all business interactions providing overall guidance to protecting resources [156]. This includes acceptable computing practices, all interactions with the network, Internet, messaging, and business specific applications or services [64]. Companies may need to meet security policy standards requirements like the ones put out by the International Standards Organization (ISO) [104]. In the context of Web development, the main area of concentration, with regards to the security policy, would be application compatibility within the corporation. However, all areas would need to be addressed to ensure overall compatibility. The security policy should be a living document and updated as new architectures and applications are developed [182]. If a security policy does not exist at project inception, then the organization may need to investigate the validity of creating the appropriate document.

7.2.2.2 Legal Compliancy

It is important to recognize that a company's policies, standards, baselines, procedures and guidelines should be compliant with relevant legal obligations. Cyber-crime is a reality that cannot be ignored in today's global business environment. The ramifications from a financial perspective and a legal perspective are potentially enormous. Web application security needs to be incorporated into the entire development methodology. This includes upfront acknowledgement of the potential legal implications involved with the development and deployment of the Web applications. Effective security resolutions need to acknowledge the legal ramifications that the application introduces to the company and the attendant risks need to be mitigated to the organization's satisfaction. For this reason, a check list of relevant legislation has been compiled from the legislative information discussed in chapter four. The current list of legislation is available in Appendix V. The purpose behind the check list is not to introduce a debate over the legislative or the legal enforcement challenges that computer crime presents. Nor is it to discuss the effectiveness of the current legislation or potential conflicts between legislation enacted in different countries.

The point is to acknowledge the increasing global legislation that is developing due to the growing impact of the World Wide Web on everyday life, on business economical environments and national importance. The legislative list provides a snap shot in time of current relevant legislation. Due to the dynamic nature of legislation, it is understood that the list will continue to change over time as the Web integrates into global environment. Economies continue to integrate with the Web to produce and/or provide goods and services. Societies continue to increase dependence on the Web to help provide basic operational economical components. This increasing dependency introduces potential national security risks. Therefore, societies are demanding a more secure World Wide Web which leads to the continued creation of new and refinement of existing security legislation. This security legislative growth potentially has world wide ripple effects on the global economy.

7.2.2.3 Corporate Culture

Corporate culture needs to take everything into account, ranging from employee security awareness programs, to employee education on social engineering attacks (discussed below), to recognition of organizational norms. Corporations need to educate the application end-user employees and their development staff in terms of security. They also need to remind employees periodically about security policies, standards, baselines, procedures, and guidelines. One approach to this is to make the issue important to the employee by integrating it into their annual evaluation [214]. This will not solve all of an organization's security problems; however, it does provide an avenue for encouraging good security practices [214].

Corporate culture needs to be examined from several different perspectives that include managerial acceptance of the importance of security, the threat of social engineering, employee perception of security and security habits, and technological acceptance of cultural norms. Managerial acceptance and habits, from a cultural stand point, are critical to the success of security within an organization. Large organizations, looking to strengthen security in their corporate cultures, need to have the highest possible ranking champion promoting the change. In small organizations, the change should be introduced by the owner. If management takes security seriously and encourages a secure environment through their actions, then the odds of this having a positive trickle down effect to employees within the organization are good.

7.2.2.4 Technology Compatibility

Existing technology needs to be examined from two view points; a compatibility point of view and a value added point of view. When an application is being proposed, the solution needs to be compatible with the existing infrastructure in the organization. Does the technical expertise exist in the organization to write the application in the proposed language? Does the hardware infrastructure support the new applications? Is the existing code repository compatible with the development of the new application? There are both hard and soft costs associated with these types of questions that need to be taken into consideration when considering any new application development.

Technology needs to be examined from a value added point of view. Whether or not you subscribe to the individual aspects of the "value configuration(s)" [3] which include the value chain, the value shop and the value network, one of the goals of the organization is to provide added value regardless of the product or service that is being offered [3]. Technology is a major contributor to this goal in today's market place. Hence, when examining the validity in developing a new application, the organization should be asking how this will help them add value to their organization.

In general, the area of technological compatibility has to do with an organization's existing applications, software compatibility, legacy systems and the acquisition of new software and technology [26]. When considering the technical compatibility of a system, it is necessary to consider the existing employee skill set within the company. To implement a technical solution, does the necessary skill set exist within the company, can it be acquired easily through employee training or will it require the company to acquire the necessary skills though outsourcing? To answer these questions, an in-depth analysis will need to be conducted and compared with the solutions requirements. Technological compatibility, from a security standpoint, needs to examine the application to see if it is compatible with existing security solutions already in production. An example would be a new application that is not compatible with the company's existing single sign-on solution. If a solution requires new technologies, the organization should rate the security capabilities of the new technologies and determine if they meet the company's security standards out of the box. If they do not, can they be brought up to speed and at what cost?

This does not mean that these are the only areas that can contribute to this category or that they all have to be present within this section to ensure compatibility. There are environments that may choose not to implement a security policy or to investigate corporate culture due to the size of the company. For instance, a large financial institution will probably have all three categories (security policy compatibility, corporate culture compatibility and technical compatibility) documented to some extent. However, a small family run business, like a local restaurant, probably will not have a security policy and the culture in that business will be implicit. However, more than likely, they will have technical compatibility issues that they will need to address.

7.2.2.5 Security and the Human Element

Technical solutions alone will not provide protection against the human element. They will not provide protection against an end-user who reveals his/her passwords, users who circumvent security to complete a specific task, or insider attacks [64]. When it comes to information security "the human factor is truly security's weakest link" [135]. This fact has spawned an area of warfare in the business world known as social engineering.

Social engineering attacks take place when an outsider or insider observes an organization, gathers information and makes necessary business contacts under the premise of a legitimate purpose in order to gather information [135]. This information is then used to acquire more information until the intruder has acquired something of value [135]. The same tactics can be used by a current employee to gain unauthorized privileges. Company employees need to be educated on the existence of social engineering attacks and how to identify and prevent these attacks from occurring [135].

The perception of security, and its importance to the business, needs to be effectively communicated at an employee level. If the employees do not place a great deal of importance on security and they regularly post passwords on screens or in accessible areas, trade passwords with colleagues, or grant system access to outside vendors, then they are creating a security risk for the company.

Technological acceptance of corporate norms is when a solution has been implemented in the environment, becomes accepted and then becomes expected. If an organization has implemented a single sign-on solution for several of the existing applications then it would be reasonable for employees to expect new applications to take advantage of this technology. The justification for complying with this expectation or going against the grain needs to be examined and justified to the employees. Otherwise, employees could start to circumvent security when it suits their needs.

7.2.3 Security Design / Coding

Once the application security requirements have been determined, the next issue that needs to be addressed is security design. The design of the application needs to consider the overall architecture, the application design, and good design principles.

This information then allows the technical architect, in the **Security Design / Coding** phase, to pick the most appropriate technical controls from a design, risk and cost perspective. Once the high level design decisions have been made, then the coding takes place. The programmers should take into consideration coding standards, good coding practices, code reviews and appropriate security measures. Encouraging programmers to adhere to coding standards and to pursue good coding practices will increase the code readability which will inherently improve software maintenance. This improvement should be felt in both enhancement maintenance and patch maintenance. It has been estimated that maintenance accounts for an average of 60% of an application's software expense [74]. In reality, "better software engineering development leads to more maintenance, not less" [74]. If an application meets the needs of a particular market, then the application will be enhanced through the addition of new features and improved functionality. It should be noted that this is considered new development in a lot of organizations. Patch maintenance is another area that is critical to defending against cyber vulnerabilities [45]. Any improvement in an organization's software maintenance capabilities translates into long term savings.

Code reviews ensure that the code is doing what it is suppose to do, decrease errors in the code and ensure that more than one person understands the application. The implementation of the type of code review is up to the individual organization. Code reviews can encompass everything from pair programming, to design reviews, to manual reviews of code after it has been written. It is up to the organization to decide the best avenue for implementation so that the organization is not dependent on a single employee for modifications and support for a specific application. Applying appropriate security measures will help ensure data security and security consistency throughout the application.

The architecture needs to fit into the existing organizational environment. There are several issues that need to be addressed within the realm of architecture. Some of those issues are:

- Application layers [66]
- Application maintainability [86]
- Information compatibility from a data transfer standpoint
- How strongly typed the language needs to be, [123]
- Approach to privileges i.e. role based or inheritance
- The approach to default privileges from the application and the user's standpoint [153]
- Security in-depth - use passwords and another mechanism, such as an encrypted key of some sort, for determining object access [153].

The design of the application needs to address:

- The language that will be used [123]
- Ease of use – the easier security solutions are to use, the less likely that they will be circumvented [153]
- Authorization techniques
- The use of encryption algorithms
- The establishment of trust
- The establishment of accountability.

It should be noted that the establishment of trust should link back to the project risk assessment. The amount of trust that is designed into an application is directly related to the amount of risk that an organization is willing to tolerate and the total cost that they are willing to absorb. Accountability, through the implementation of appropriate mechanisms, is an essential ingredient to security.

The design needs to examine the code from common attack standpoints and implement the appropriate controls to ensure secure data. A professional code management system should be used by the development team to ensure accountability, within the team, and provide a means of roll back [70].

Once the design has been chosen, the solution is coded. During coding, the developer should be cognizant of the World Wide Web Consortium (W3C) coding standards and pursue secure coding practices [208]. One idea that a designer should keep in mind, when designing a secure solution, is to balance the need for a secure application with the need for a particular functionality.

Another idea that a designer should strive to attain is the creation of simple design solutions that solve specific problems and fit into the applications global architecture.

The design will depend on the level of security the customer is willing to accept from a risk and/or cost standpoint.

7.2.4 Controlled Environment Implementation

Depending on the needs of the organization, the **Controlled Environment Implementation** can be as complex as implementing it into an environment that mirrors the production environment or it can be as simple as running the application on a desktop [78]. In this case, both the desktop application installation and the server mirroring environment can be used to test the security controls. The point here is to release the code in a secure environment that simulates the production environment for compatibility testing before the application is made available to the general public. The goal of the environment is to minimize surprises. Basically, this phase allows the developers to test the application's compatibility with the operating system and interfacing programs before application testing and a production release.

The controlled environment implementation should also take into consideration application compatibility, load testing and regression testing. The new application has to be compatible with the native operating system and with the other pre-existing applications. Compatibility also needs to be verified with applications on the same server and applications that live off site (internal to the organization or external to the organization) where data is being exchanged.

7.2.5 Security Testing

Testing takes place from both the developer and the end-user perspective. Developers should be running their own battery of tests when the code is conceived. Again, it should be stressed that the methodology is designed to work in conjunction with existing organizational tools and processes. If the organization already has an investment in automated testing tools, they should be used in this stage to augment the testing process.

Actual end-users should be incorporated into the testing campaign whenever possible. The end-users should be writing test scripts and actively interfacing with the application to ensure that the program is performing accordingly. End-users participation in the security testing of the Web application holds the process and the solution accountable from a practicality perspective.

The National Institute of Standards and Technology (NIST) estimates that "93% of reported vulnerabilities are software vulnerabilities" [143]. The Organization for Internet Safety (OIS) publishes Guidelines for Security Vulnerabilities Reporting and Response. In this document, they define a security vulnerability as

> "a flaw within a software system that can cause it to work contrary to its documented design and could be exploited to cause the system to violate its documented security policy" [78, 142].

Hence, any flaws in the system design or application coding can potentially lead to security vulnerabilities [78]. The Open Web Application Security Project (OWASP) provides an excellent listing of the top ten vulnerabilities in Web Applications. The top ten vulnerabilities, listed below in Table 22, are taken directly from the OWASP report.

Table 22 - Top Vulnerabilities in Web Applications

Unvalidated Input	Information from Web requests is not validated before being used by a Web application. Attackers can use these flaws to attack backend components through a Web application.
Broken Access Control	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.
Broken Authentication and Session Management	Account credentials and session tokens are not properly protected. Attackers who can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
Cross Site Scripting (XSS) Flaws	The Web application can be used as a mechanism to transport an attack to an end-user's browser. A successful attack can disclose the end-user's session token, attack the local machine, or spoof content to fool the user.
Buffer Overflows	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and Web application server components.
Injection Flaws	Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the Web application.
Improper Error Handling	Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the Web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.
Insecure Storage	Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.
Denial of Service	Attackers can consume Web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.
Insecure Configuration Management	Having a strong server configuration standard is critical to a secure Web application. These servers have many configuration options that affect security and are not secure out of the box.

The Open Web Application Security Project (OWASP). [185]

This list complements information discussed in the previous articles the "Top Web application security problems identified" and "The Bugs Stop Here" which were published in 2003 [20, 134]. Only after testing has been completed and the vulnerabilities removed to the satisfaction of the organization should the application be moved into production.

Developers need to examine their code independently and the program as a complete entity in order to determine possible misuse from a functional standpoint. That is, programs should do precisely what they are designed to accomplish.

> "Vulnerabilities can stem from the rapidly evolving use of software, in which programs meant for a limited purpose are applied in ways not anticipated by their developers" [213].

Thus, can a program be manipulated in a manner that might create problems and can this be stopped or mitigated? A primary example is an e-mail server that is used to propagate a virus or used in a denial of service attack.

Testing is critical to the success of many applications. Testing should cover application testing, incident management and disaster recovery plans. Application testing includes validation errors, program behaviour testing, and code analysis. This will involve implementing appropriate programs to test static and runtime code, penetration, and application scanning. Automation, where possible, of the testing process will help provide stability. Testing should also involve executing scripts from both the developer and the end-users to test the application. An important part of the testing phase should be to decide appropriate action plans for incidences. When there is an issue, what are the procedures that need to be implemented to resolve the situation? This should also include amending the disaster recovery plan where appropriate. If the organization does not have a disaster recovery plan, then, they should investigate the creation of a plan**.** The disaster recovery plan on the organizational level should be a living document. The disaster recovery plan for the application should be flexible enough to allow for the addition of a new functionality. Once the plan either has been created or amended then it should be tested. Testing is where everything should come together in the development process. Hence, testing should:

- Contain a requirements check against the application to ensure that they have been satisfied and that any risks that were identified in the risk analysis have been sufficiently mitigated.
- Be as prompt as is reasonably possible so that an organization is competitive in the Web application development market
- Involve actual end-users, not surrogate end-users
- Be as comprehensive as possible. This will be determined based on the amount of risk the application presents to the organization's reputation and the organization's core business.
- Tailored for security.
- Take advantage of an organization's existing testing infrastructure.
- Should include external testing to verify application security where the risk warrants the expense.

- Implement a matrix to measure the success of the testing and effectively track bugs.

7.2.6 Implementation into Production

After testing has been completed, then and only then is the application prepared for **Implementation into Production**. The introduction of the application into the production environment needs to be completed with the involvement of the appropriate security personnel. The appropriate personnel need to be present to ensure that the application has been deployed properly into the production environment. If possible, this allows for immediate issues resolution at the time of implementation. If issues are discovered after the application has been implemented into production, then the application must go through the process again and be re-implemented into production.

7.2.7 End-User Feed Back

End-User Evaluation is critical from the standpoint of security. Whenever it is possible, actual end-users should be used in the security evaluation of a Web application. End-users are the ultimate variable in the execution of an application. If end-users are circumventing the application's security in order to make their lives easier or perform their jobs in a timely manner, then these issues need to be investigated and resolved [78].

An efficient and effective response to application security breaches is mandatory to Web based business survival. If the application has been compromised due to a flaw in the design or the code, then the security issue needs to be addressed, realistically, as rapidly as possible. If the application is not secure, businesses run the possibility that the application will be abused, corporate credibility lost, and financial consequences incurred.

End-User Evaluation involves both communicating with the user to determine the success of the application's security and security maintenance. This can range from informal communication, to surveys, to structured interviews with the end-user. Security has to find a balance between usability and providing a secure environment.

Security maintenance has to do with discovering vulnerabilities after a production release. As new technologies emerge from the view point of development and maintenance, new vulnerabilities will be created and uncovered and these issues will have to be addressed to maintain application security [123, 153]. Patches will need to be tested to ensure that they resolve the newly discovered issue and to ensure that they do not create new security vulnerabilities in the application.

7.3 WES Stakeholders

The stakeholders who are involved in a specific project obviously depend on several criteria ranging from resources, to project visibility, to project risk, to funding. A large organization is more likely to have the resources available to assign different people from different areas to the project. A small company, on the other hand, may have employees conducting multiple job functions.

Project visibility is a factor when considering the amount of resources that will be assigned to a specific project. If an organization has a project that is considered to be a high profile project, then the project affects many people within and/or out-with the organization and will probably receive more attention than a low profile project.

The risk associated with the profile is another matter. If the application has a high profile and a high risk to the core business function of the organization then it stands to reason that most organizations would assign more resources to the project. An example of this is a Web site that conducts financial transactions for a banking institution. On the other hand, if a project has a high profile and a low risk, such as an intranet phone book application, then fewer resources are probably going to be assigned to the project.

As always, funding is an issue with all projects. If the funding is not available, regardless of the size of the organization, then resources will simply not be assigned to the project. If funding is available but at a smaller amount than initially requested then corners are cut in order to reduce expenditures. Easy targets for reducing expenditures include security testing, ongoing end-user input and feedback, and developer security education and training but this is potentially a dangerous strategy.

General stakeholder who would be expected to be involved in the development process would include the project sponsor, project manager, business analysts, architect, programmer, tester, risk and security personnel, release personnel, and the end-user.

7.4 WES Deliverables

After the process has been customized to satisfy the needs of a specific business, it can then be documented so that it can be replicated for future projects. Depending on the needs of the organization, this can also serve as an audit trail. The amount of documentation implemented will depend on the needs of the particular organization. A financial institution, due to regulations, will probably have to provide detailed documentation of their processes. In contrast, a small local business will probably document only the bare necessities in order to conduct business.

The deliverables that are required during each stage of the Web Engineering Security development process depends on two issues. The first issue that has to be recognized is the culture of the organizations, which is directly related to the industry to which the organization belongs. If the organization is in a highly regulated industry, such as banking or insurance, then there will be a greater emphasis on the individual deliverables that are required at each stage of the process. However, the converse is also true; if the organization is not in a highly regulated business then there will be fewer deliverables that are required during the various stages of the process.

The second issue that has to be acknowledged is the application development methodology that the organization is implementing to create Web software. This usually will be linked, as well, to the culture and the industry to which the business belongs. An organization that uses a waterfall approach will be more inclined to generate documentation and specific deliverables between the various stages. However, an organization that is implementing an agile approach to application development will, by nature, produce fewer deliverables between the various stages. Understanding the previously mentioned issues, the decision as to whether to create deliverables and to what extent the deliverables are created is left to the organization to determine.

7.5 WES Goals

WES tries to achieve several goals. These goals include upfront integration of security, security comprehensiveness, structured security implementation and industrial practicality.

7.5.1 Upfront Integration of Security

The WES methodology strives to integrate security from the beginning of the application development process. This is why security discussions are initiated during the business analysis stage of the development process. This up-front integration should help the organization reap benefits ranging from faster application development, to positive effects on budgets and time frames by proposing realistic security solutions at the onset of the project. The idea is to move security from the typical view point of an inhibitor to that of an enabler in the eyes of the end-user.

Granted, this move is, to some extent, dependent on the security team that is involved in assisting in the implementation of the WES methodology. They need to not only be defining what is possible in the current organization but be providing an architectural strategy for the future and providing realistic alternatives to business needs rather than stating that something is not possible, full stop.

7.5.2 Security Comprehensiveness

The WES methodology hopes to address the questions of “How do I build application security into the fabric of my company?” [46]. The solution is to approach the problem from the idea of presenting a proactive comprehensive approach to the security development process. The security methodology should be compatible with the existing application deployment process capitalizing on current core competencies while providing a road map for improving security during the application development process.

7.5.3 Structured Security Implementation

The WES methodology provides an overall structure that allows organizations to customize the level of security to its individual needs and implement security into their application development process. This structure can then be hardened to provide an organization with the desired level of continuity, reusability and audit-ability for future development projects.

7.5.4 Industrial Practicality

The general categories in the WES methodology are not set in stone but are strongly recommended. The items within the categories will need to be tailored and, where necessary, expanded to meet the specific needs of the individual organization and their current policies and procedures. The methodology is designed to complement an organization's current methodology, while providing guidance to the development process from a security perspective.

The idea behind the WES methodology is to provide a roadmap for Web application development that will help guide organizations to a more secure system. The goal is to proactively help developers create applications that are secure by design. Following the WES methodology means that the development process has taken into account risk analysis, application security requirements, various organizational policies, organization architecture, code design and coding practices, proper testing procedures and end-user feedback.

WES provides the individuals involved in the Web development process with a practical method by which to address security. There are several solutions in existence that tell you "what" to do to improve general security within an organization and some within the organization's development process. There are currently a multitude of technical solutions that offer possible solutions to very specific questions which basically answer "how" to solve specific security problems. The technical contribution is growing rapidly daily.

Previous to the WES methodology, nobody has designed a security process based on criteria that are specifically tailored to address the needs of a Web Engineering development process. The general solutions that have been proposed in the past tend to lack accurate details that address the practical issue of "where" actions should be performed in the software development process. WES provides the Web Engineering community with a practical methodology to solve the inherent security deficiencies present within generic Web development life cycles.

7.6 WES Analysis

A real world understanding of application security indicates that it is a multifaceted issue in an increasingly complex environment. This becomes especially apparent when examining Web facing applications. The need to address security in application development has increased over the past several years. However, one of the major challenges facing organizations in today's Web enabled environment is balancing technological needs with the business needs of the organization. Another potential challenge for organizations is structuring the overall development process so that there is not a general frustration within the organization in terms of overall process efficiency. A lack of process efficiency potentially hinders aggressive Web development from a business perspective. A lack of security integration and understanding of the application development process creates an environment that is conducive to fostering security deficiencies.

WES is a proactive approach that is designed to operate at a high level of abstraction. There are advantages and disadvantages to a high level abstract solution. The advantage that a high-level of abstraction provides is inclusiveness to the overall process. A high-level process is naturally conducive to security issues, business issues, software development issues, and organizational issues being more inclusive. If these issues are narrowed through too much detail then there is the possibility that the details will be biased in some way or that they will simply have missed an important issue. The disadvantage of an abstract approach to a security methodology is that the implementation of the process is demanding from an individual knowledge perspective.

WES is constructed from empirical research that consisted of two surveys and relevant literature. Meaning that the WES methodology is based in reality, in that, the goal of the WES methodology is to strengthen security in Web development applications.

7.7 Summary

This chapter describes the Web Engineering Security (WES) methodology covering both the principles behind the methodology and specific process details. The security education, good communication and cultural support principles provide the foundation for the WES methodology. Creating an environment that is conducive to initially fostering and continually encouraging security in an organization’s application development environment.

Security is an ever elusive target in today’s application development environment. No application is ever going to be one hundred percent secure due to things like human error, advances in technology and hardware associated vulnerabilities. The idea behind the WES process is to strengthen security in a Web application development environment by implementing a security process that integrates seamlessly into an organization’s development process capitalizing on existing synergies. This seamless integration places the responsibility for defining the process stakeholders and the process deliverables with individual organizations implementing the WES process. The chapter covered the goals of the WES methodology along with an analysis of the advantages and disadvantages of the methodology.

WES was engineered to address security specifically for Web Application development processes. This does not mean that WES is not applicable to application development in other fields. It only means that WES has been designed to address specific characteristics associated with Web engineering.

8 Security Methodology Evaluation

The objective of chapter eight is to review existing security methodologies that have been proposed by both industry and academia comparing their solutions with WES. The idea is to identify the differences between the existing solutions and the WES methodology. As discussed in chapter two, this is accomplished via a critical review of the literature.

Section 8.1 examines a generational security methodology classification along with specific methodologies that have been deemed as compatible with application development processes. Section 8.2 examines the Comprehensive Lightweight Application Security Process also known as CLASP. Section 8.3 inspects Microsoft's Trustworthy Computing Security Development Lifecycle. Section 8.4 covers a range of additional attempts to solve application development security problems and section 8.5 provides a summary of the chapter.

8.1 Generational Security Methodology Analysis

As discussed in chapter four, industry surveys recognize the importance of security in reference to the World Wide Web [21, 49, 84]. This recognition has prompted several organizations and some academicians to recognize and investigate the importance of security in the development life cycle. As discussed in chapter three, this has resulted in work being produced in a variety of fields that includes Software Engineering, Management Information Systems (MIS), Computing Science, and mathematics. In academia, Siponen and Baskerville have attempted to analyze information security development methodologies, thereby, producing a generational security methodology analysis.

The latest analysis produced by Siponen builds off of work originally conducted by Baskerville. The end result, as discussed in chapter three, is the development of a generational framework consisting of five generations for the security methodology evolution. The WES methodology attempts to satisfy the criteria for the fifth generation of information systems methods. Siponen broadly defines the fifth generation criteria as social ideas and techniques that are in agreement with designer and user expectations, integration with a variety of development methodologies, practitioner adaptability and empirically examined evidence of usefulness.

Siponen and Baskerville classified the first two generations basically as containing checklist, management criteria and maturity criteria. While these items have their place in helping to examine and rectify potential security issues, they do not provide methodical, holistic solutions specifically applicable to secure Web application development.

Out of the other generations, it should be noted that Siponen identified, in his analysis, only three methodologies that could be "smoothly integrated into Information Systems

(IS) development methods" [171]. Since this is a major criterion for WES these articles are the focus of the discussion. The three methodologies classified as third generation solutions include:

- Baskerville's logical control approach
- Booysen and Eloff's spiral approach
- McDermott and Fox's abuse case solution.

Siponen did go on to hypothesize that it might be possible to integrate four other approaches with varying degrees of modification to various parts of the methods. These methods were identified as:

- Pernul's security constraint modelling
- Pernul and Quirchmayr's data and security semantics
- Pernul's, et. al., DFD and ER modelling
- Karya, et. al., survivable IS.

Baskerville's logical control approach [15] focuses specifically on the design aspect of the methodology. Baskerville identifies five areas in which controls need to be examined when designing a system, whether the system is computerized or not. These areas include the system user, system designer, human entity, the client and the owner. All of which are valid points to consider. However, Baskerville does not go into detail on how these controlled approaches specifically fit into a development methodology, much less the integration of these controls into a Web application development methodology. The WES methodology considers controls when acquiring the application's security requirements and the analysis that takes place when examining organizational compatibility. This is done prior to the security design stage so that the requirements help the designer in the construction of the application. Baskerville's approach does not specifically identify the same controls as WES and he specifically puts them in the design stage.

Baskerville does make two very important points in the summary of the paper that concurs with the WES methodology. He states that "management cannot be expected to blindly finance controls, nor can the knowledge worker be expected to completely accept controls" [15]. This statement alludes to the fact that the final decision to the implementation of controls in an application is ultimately a business decision and that the knowledge worker (which also could be referred to as an end-user) input is important.

A couple of key points on which Booysen and Eloff's [27] Automated Secure Systems Development Methodology (ASSDM) and WES concur are the integration of security with application development together with the involvement of end-user in the development process. Booysen and Eloff mention that the end-user should be involved during the development process. WES takes this further and indicates that they should be involved in the requirements stage, the testing stage and at the end to provide feed back. Granted, Booysen and Eloff do not take end-user involvement to this degree, but they do at least acknowledge involvement during the development process. ASSDM also concurs with the a major idea behind the WES methodology that

> "a key notion underlying the creation of a security development methodology is to include security activities as part of system development" [27].

This indicates that both the security activities and the development activities should take place concurrently. Booysen and Eloff's [27] approach adds security into Boehm's spiral approach [24] that was discussed in chapter six. The ASSDM is achieved by integrating the following tasks into Boehm's spiral approach:

- Determine the sensitivity level of the application
- Define the goal state of the application system
- Conduct a security risk analysis
- Create a security model and object classification
- Conduct an Information flow analysis

Determining the sensitivity level of the application involves examining the data from the perspective of the source and the value of the data. This exercise would involve the application of security models like the Bell-Lapadula model [91]. Booysen and Eloff's define the goal state of the application system as "a breach between the current state and the expected state of the application" [27]. The goal state is defined in the same terms in which WES defines security which is integrity, availability and confidentiality.

Conducting a security risk analysis is pursued from the view point of reaching the goal state of the application based on the organization's available resources. At this point, the authors acknowledge access control lists and security policies. WES concurs with the acknowledgement of the security policies and access control, which is supported in its organizational compatibility discussion examined in chapter seven. However, Booysen and Eloff do not acknowledge cultural compatibility, making it a point on which the solutions differ.

Security models are created through the use of entity relationship diagrams and data flow diagrams. Object classifications are based on sensitivity levels, the objects are then modelled on a dataflow diagram to determine data flows. This information is then put into a matrix and examined from a source and destination perspective to determine if the data flows are valid.

There are several differences between Booysen and Eloff's solution and the WES methodology that should be acknowledged. Their approach concentrates on the user requirements and the design stages of the application development process. On the other hand, the WES process examines security throughout the development process. Their approach focuses specifically on the spiral approach. The paper does not discuss the applicability of the solution to other application development processes nor does it make specific reference to Web application development. It should also be noted that ASSDM relies on prototyping to validate security requirements. Prototyping plays a major part in Boehm's iterative process. WES relies on the testing of the actual product rather than a prototype. The WES process strives to present a process neutral approach that is specifically designed for Web application development. The paper presents a hypothetical scenario to which the security approach is applied. They do not present any evidence that the approach has actually been implemented in industry or any industrial indication as to the success of the solution.

McDermott and Fox [128] present abuse cases as a solution to analyzing security requirements. McDermott and Fox define an abuse case to be a specification that completely describes the interaction between an actor and the systems resulting in harm to the actors, the system or a system stakeholder. They indicate that abuse cases can be helpful during the requirements, design, and testing phases of a security engineering process" [128]. While abuse cases can be helpful during these stages, it is not recommended that they be used to provide the sole source for requirements analysis, design specs or testing specs. They even admit that they "intentionally make abuse case models ambiguous and incomplete and do not worry about their soundness. Abuse case models do not replace any other part of a sound security engineering process" [128]. It should also be noted that abuse cases do not provide assistance with organizational compatibility, environment compatibility or user feedback.

All of the models proposed by Pernul are classified as third generation security solutions. Pernul's [148] paper on security constraint modelling along with Pernul and Quirchmayr's [149] paper on data and security semantics focuses on aspects of security that are directly relevant to databases. The first paper focuses on conceptual modelling and design of multilevel secure databases [148]. The later paper acknowledges that its main contribution is to the logical design of MLS database [149]. Pernul, et. al., present a DFD and ER modelling technique that is based on security semantics (security classifications) to be used in "a design environment for multilevel secure database applications" [150]. All of these articles focus on database security, an important issue in security, but only one aspect of security that needs to be addressed in Web application development methodologies.

Solutions are still being explored and developed today that are based on modelling techniques. Byers and Shahmehri [30] recently published an idea that they are calling a Software Process Improvement (SPI). They claim that the process can be conducted at all stages of the development process; however, the practicality of this is debatable for Web application development projects. This debate is due to the Web engineering characteristics and common Internet development practices discussed in chapter three. The process contains three stages which include vulnerability modelling, vulnerability cause mitigation and process components definition.

The end goal of the SPI process appears to be the same as the WES process. The goal is to reduce vulnerabilities. WES does not specifically put a number to this goal for a couple of reasons. First, the security challenges are going to be unique to individual companies. These companies will have strengths and weaknesses in different areas affecting the influence of WES. Secondly, it is realistically very difficult in industry to determine the overall affect a security process has on an organization. Security is invisible when it is working correctly. The only time it is noticed is when it fails and/or there is a breach of some sort to the system. WES takes the stand that it wants to strengthen security in an organization. If WES increases the overall Web application security in an organization by decreasing the number of security breaches that an organization experiences in its Web applications or simply increases security awareness through acknowledging and addressing security issues, in the Web application development process, then it has been a success.

There are several differences in the two approaches to solving the security problems in application development. The first difference is the fact that SPI is not specifically designed for Web application development. The second difference is that SPI is a model based solution. The idea behind the process is that vulnerabilities should be modelled using what Byers calls a vulnerability-cause graph. As discussed in this paper and another paper by Ardi, et. al., [7], this is simply a model of the vulnerabilities and their causes. The next step is to attempt to mitigate the risk through the construction of what they are calling a security activity graph. They claim that this is used to fully document activities in the software life cycle. According to the article, this includes complete information on implementation and success verification. The article also talks about the future creation of a vulnerability analysis database and the collecting of information into this database. The article also claimed to be working with three organizations in industry but, to date, has not implemented anything in industry. They also claimed that one of the three organizations uses an agile application development approach. The compatibility of their solutions with agile methodologies is debatable, based on the amount of documentation that they desire with the vulnerability-cause graph, the security activity-cause graph and the vulnerability database. Heavy documentation goes against the agile manifesto's idea of 'Working software over comprehensive documentation' [4].

Building upon Siponen's classification scheme where he defined "the third generation approaches (as) focus(ing) on different means of modelling organizations ISS requirements" [171], the view was taken that model driven approaches embraced a narrowly defined security application scope. Modelling security problems is only one way to identify and solve problems. It does not present a comprehensive solution to security in the Web application development process, nor does it attempt to build upon existing synergies within an organization.

The survivable IS approach is classified by Siponen as a fourth generation approach which he defined as

> "add(ing) the social and socio-technical design aspects to the third generation approaches" [171].

Karyda, et. al.'s, [111] survivable IS approach, which Siponen classifies as a fourth generation approach, does not provide information on exactly how the three main phases, which consist of diagnosis, re-design, and transformation, fit into an application development methodology. These phases also do not address all of the issues addressed by the WES methodology like organizational compatibility, environment compatibility, testing, and end-user feedback. The fourth generation suffers from the same issues as the third generation. Fourth generation solutions have a slightly broader scope than the third generation security solutions but they still embrace a narrowly defined security application scope.

The previously proposed solutions enforce the idea that application development security is a broad area of study in which there is an abundant number of research solutions that have been proposed. However, none of the previously discussed solutions specifically targeted Web application development. All of the previously discussed solutions, except for one (Byers and Shahmehri [30]), specifically targeted individual aspects of security improvement vs. trying to provide a comprehensive methodology.

8.2 Comprehensive Lightweight Application Security Process (CLASP)

The Comprehensive Lightweight Application Security Process (CLASP) provides a list of thirty possible activities that can be included in the development process [203]. However, an application security development methodology needs to encompass not only specific design and development activities but also needs to address overall project risk, cultural, environmental, testing, implementation and end-user feed back issues.

In the areas of design, coding and testing, companies can, where appropriate, use additional tools at their disposal like CLASP, automated testing tools, and in-house application testing procedures to enhance the security process. The purpose of the WES security methodology is to provide cohesion and flexibility to an organization's security process. WES stresses that once the designing, coding, testing and the process of implementation have been completed, then end-user feedback is mandatory. CLASP does not stress end-user feed back.

CLASP presents a lot of really good practices that can be implemented into the development environment. However, there are several differences between WES and CLASP. WES was designed around two sets of criteria that were discussed in chapter five. The Security Criteria for Web Application Development (SCWAD) is used to analyse CLASP in chapter six. The result is the identification of several areas where CLASP and WES differ to varying degrees.

Two significant differences include the promotion of security throughout the development life cycle and the establishment of trust and accountability. There are also two founding principles that WES established that are not mentioned in the thirty core activities of CLASP. These include good communication and cultural support as discussed in 7.1.2 and 7.1.3. Without either one of these principles, adding security into a development process will be very difficult or is unlikely to be effective.

CLASP is a set of process pieces that appear to be designed around best industry practices. CLASP claims to be process agnostic but there is a tight association with the Rational Unified Process (RUP). RUP is basically IBM's commercial version of the Unified Software Development (USD) process. WES is a process neutral methodology that is specifically designed to be used for applications that are being created for use on the World Wide Web.

8.3 Trustworthy Computing Security Development Lifecycle

Microsoft has also attempted to address security issues through their Security Development Lifecycle (SDL) which is discussed in "Trustworthy Computing Security Development Lifecycle" [123]. Microsoft states that the "SDL is process-agnostic as far as how you go about developing software" [96]; however, there are several issues with this statement. As Figure 4 in chapter 6 displays, the SDL is clearly laid out to follow a traditional waterfall / spiral approach. Fundamental components of the Web engineering development environment have been outlined to include multidisciplinary involvement [54]; a complex, agile, time sensitive development environment [129]; a diverse end-user population[139] and a usability focused design [139]. Which brings up an important issue, Microsoft's SDL methodology was designed for traditional software development. The SDL was not designed for use on Web applications. Another issue to note is the fact that it has only been used in the Microsoft environment.

The documentation makes reference to acknowledging security requirements through the need "to comply with industry standards and by certification processes such as the Common Criteria" [124]. This directly goes against the concept of a complex, agile, time sensitive development environment. The Common Criteria is a document and a labour intensive certification process that is not conducive to short development cycles. The SDL process does not address multidisciplinary involvement, a diverse end-user population or a usability focused design in its documentation.

The Microsoft Security Development Lifecycle (SDL) solution concurs with WES in that it stresses the importance of designing security into the application from the beginning and places value on following guidelines and coding standards. However, there are differences in the methodologies. Their approach lumps coding and testing into an implementation phase. WES places more of an emphasis on these activities and places them in separate categories. Microsoft's solution has a security advisor assigned within the requirements stage. Its solution references specific documentation in the design stage; a built-in verification stage which encompasses a specific security push and, within the release, they have a final security review. Clearly, these stages and requirements are more suited toward large corporations that have separate security individuals who can be assigned to projects and support a large security push during application development. Large corporations are usually much more inclined to support documentation as referenced in the design and release stages. These same security professionals are required to sign off on the project in the release phase [124]. Another major difference in the Microsoft solution is the support and servicing phase. The support and servicing phase is viewed as a fix-it stage where vulnerabilities are analyzed and where warranted patches are released [123]. Granted, this is an important area to address but they make no reference to determining the effectiveness of the security from the customer's point of view. The customer's perception and acceptance of an application's security is an equally important security issue. Microsoft's SDL paper [123] introduces four principles which are 'secure by design', 'secure by default', 'secure in deployment', and 'communications'.

Secure by design states that "the software should be architected, designed and implemented so as to protect itself and the information it processes, and to resist attacks"[123].

This is a narrow view of security within the development process. WES supports the idea that security is visible through-out the development process. This goal is supported via the principles of WES which includes good communication, security education and cultural support.

Secure by default states that the "software's default state should promote security"[123]. In the WES methodology, this is stated by applying appropriate security principles and good coding practices to the architecture design, coding and testing phases of the application development methodology.

Secure in deployment talks about the "tools and guidance that help end users and/or administrators use it securely" [123]. WES agrees that providing the right tools to developers and administrators is necessary to provide a secure environment, but WES takes the idea further, as discussed in section 7.1.3, by viewing the issue as a cultural support topic.

Communication states that "software developers should be prepared for the discovery of product vulnerabilities and should communicate openly and responsibly with end users and/or administrators to help them take protective action (such as patching or deploying workarounds)" [123].

WES concurs that communication is an extremely important issue in the development process. However, WES breaks communication into two very important categories. There needs to be effective communication among the development team members. This includes communication on issues like software standards, testing environments, security software compatibility, etc. There also needs to be effective communication between the development team and the end-users. This is not only to establish the need for patches but simply to determine if the security solution that was implemented meets the needs of the end-user and is technically effective.

Another point worth acknowledging when examining the differences between the two methodologies is the topic of compatibility. Microsoft's SDL does not discuss organizational compatibility from a security policy, cultural or a technical perspective. The WES methodology does address these issues and even goes a step further by acknowledging legislation that potentially impacts Web application development.

8.4 Additional Attempts to Address Application Development Security

Relevant security articles, white papers and books exist on an array of topics that focus on improving specific aspects of security. The security information in this area ranges from general security advice, to security requirements [204], to security risk [211], to the use of patterns, to books published on security. However, these attempts do not comprehensively address Web engineering security during the application development process through the establishment of a security methodology.

Viega and McGraw's book on "Building Secure Software" [205] provides a good introduction to security. The book takes a general approach to tackling the topic of secure software in a networked world. The book makes two important statements. The first is that "there is no such thing as 100% security" [205] but they do support writing "secure-enough" [205] programs. The second is that "malicious hackers don't create security holes; they simply exploit them" [205]. They go on to say that

> "Security holes and vulnerabilities – the real root cause of the problem – are the result of bad software design and implementation" [205].

The book discusses managing software security. It examines various security technologies that are important to understand and it provides advice on security's best practices and principals. In the software security section, Viega and McGraw do discuss software engineering. In that section they make very valid points in that the development time for Internet applications is compressed compared to traditional development. This has an adverse effect on gathering requirements, design and testing in the development life cycle. They talk about security goals that include prevention of attacks, traceability and auditing, monitoring, privacy and confidentiality, multilevel security, anonymity, authentication, and integrity.

They look at prevention from the eyes of repeat attacks. Once information on vulnerabilities has been discovered on the Internet, it can be propagated through scripts so that anyone can execute the attack. Traceability and auditing are considered from the viewpoint of forensics and monitoring is viewed along the same line of thought through applications, like intrusion detection systems. Privacy and confidentiality can be viewed from both the users and the businesses perspectives. As they note, by nature, software is not really designed to protect these topics. Software is designed to complete a function by running on a machine. Hence, the machine is a natural vulnerability to the software. Multilevel security is analysed through the concept of classifications and anonymity is discussed from the view point of design and the capturing of data within programs. Authentication of application is stressed from both the system side and the end-user side. Systems should know with whom they are dealing and end-users should not blindly trust universal resource locators (URLs). Integrity is stressed in that data should not be modified during transport.

The authors do touch on the topic of security integration into the development life cycle. They stress the integration of risk analysis and security requirements into the life cycle. For discussion purposes, they used a spiral software development model but they clearly state that they “don’t care which processes you apply” [205]. They continue with the statement that “the main thing is to work explicitly to manage software risk, especially from a security perspective” [205]. They also consider “sound software engineering a prerequisite to sound software security” [205].

Viega and McGraw provide a lot of their information in the context of a networked world. A lot of their advice is good general advice for Intranets or Internets. They do stress risk management in the software development life cycles, but they do not address the idea of a security methodology, much less a security methodology that is applicable specifically to Web Engineering.

Wang’s article discusses software quality and inspects risk at various levels in the application along with the effects on quality factors [211]. The article makes the point that

> “software security needs to be considered from the very beginning of the development cycle” [211].

It goes on to say that

> “the majority of the security compromises can be attributed to one or more weaknesses within integral components that make up the software” [211].

The article discusses specific software quality factors, presented by McCall, which consisted of correctness, reliability, efficiency, integrity, and usability [211]. The article then proceeds to break down software risk into three categories which included the application layer, the platform layer and the network layer. Along with this information they present a study that examines the specific technology approaches like secure tokens, packet filters, and the use of Public Key Infrastructure (PKI) and their effectiveness against security threats and risk.

This article provides interesting and relevant information on specific aspects of security. However, the paper does not tackle organizational foundation issues that need to be addressed before security can be implemented successfully, effectively and continually. The article makes reference to the need for security throughout the development cycle but does not address all of the aspects of the development life cycle.

Another proposed solution has been to apply security patterns through the use of a secure software lifecycle as discussed in “A methodology for secure software design” [67]. The proposed pattern solution agrees with the WES methodology in that security needs to be ingrained in the application from the beginning and throughout the entire application life cycle [67]. The idea behind the pattern is to capitalize on proven design solutions. There are a couple of assumptions with this philosophy. First, there is the assumption that the individual applying the security pattern understands the pattern solution and, secondly, that they will apply the solution in the correct manner. The logical postulation gains complexity when the security pattern requires customization in order to be applicable to the current environment. Patterns do not address all of the areas engaged by WES such as the risk analysis and the organizational compatibility. Patterns could be used in conjunction with WES in the design and coding area of the methodology. However, patterns alone do not provide a comprehensive solution to Web application security.

There are several differences between Fernandez’s [67] methodology and WES. The paper proposes that security verification and testing take place between the four proposed stages. It ties itself directly to the use of the Unified Modelling Language (UML) and object oriented languages. It also makes no direct reference to the critical need for communication with the end-user / customer for requirements and end-user feed back.

Ellis and Speed propose a process for developing a security project in their book [64]. While they do support risk analysis and feedback in the security project, there are several differences between their approach and the WES methodology. Their solution treats the security aspect of a project as a project in itself. Security needs to be viewed as a critical component of the development process, not a stand alone project. Their process contains a stage for reviewing the business where extensive knowledge of the business is required. This would include an in-depth understanding of the business’ markets. The process also contains an “Understanding the Technology” [64] stage where a comprehensive knowledge of technical solutions and technology that is currently in use by the business is expected. Their solution also calls for an implementation and feed back stage that is executed with a pilot of the application. After possibly several iterations of the pilot, then the application progresses to final roll-out. Their feedback appears to be in reference to training and end-user support, not necessarily determining the effectiveness of the security from the end-user perspective. The scope of the process proposed by Ellis and Speed is larger than the scope of the WES methodology.

A recent attempt by Cross recognizes the importance of considering security from the start and throughout the development process [43]. Instead of providing a methodology for the implementation of security into the development process, Cross provides good high level advice for developers. The initial advice starts off with the statement “as soon as you get the initial requirements” [43]. WES advocates involving security during the business analysis discussion prior to the requirements gathering stage. The advice given at this point focuses on developer meetings, establishment of project goals, brain storming on security, an estimation of the project work effort and a go / no-go decision based on the output form the previous points. The balance of Cross's advice deals with code reviews; setting publishing standards for developers; the use of version control systems; establishing testing schedules and the institution of a release process.

8.5 Summary

Literature is replete with articles and books that describe implementing general security improvements; however, they have the same issues. They make excellent points about the need to improve code from specific perspectives. They provide generic information that is not specific to Web Engineering and they fail to address underlying organizational issues that affect the ability of an organization to efficiently and effectively implement security into the development process.

There have also been attempts in industry to solve security issues in application development processes. Industry solutions range from process plug-ins, to modified system development life cycles, to the application of security patterns. However, they do not attempt to solve the broad security problem during Web Application development. Some of these attempts include efforts by Secure Software and Microsoft. While these industrial attempts present good information, they fail to address all of the issues that have been recognized by WES. These areas include addressing security during all of the stages described in the WES methodology, SCWAD and the EE. The next chapter focuses on the integration of WES into various Web application development life cycles.

9 Life Cycle Compatibility

This chapter examines the compatibility of the Web Engineering Security (WES) methodology with traditional and agile Web engineering application development methodologies. Each of the methodologies discussed in this chapter was introduced and discussed briefly in chapter six. A critical assessment of traditional and agile life cycle compatibility with the WES methodology is presented using descriptions from available literature.

The point of this chapter is not to provide an exhaustive evaluation or to argue the validity of the plan-driven or agile approaches to Web development. The chapter examines the approaches based on the information that both are currently used in industry to develop Web applications. Section 9.1 examines the waterfall methodology, section 9.2 covers the Unified Software Development (USD) Process, section 9.3 examines the Dynamic Systems Development (DSDM) Methodology, section 9.4 takes a look at extreme programming, section 9.5 inspects agile methodologies in general and section 9.6 summarizes the chapter.

9.1 Waterfall Model

The waterfall model is arguably the best known of the traditional methodologies. The WES model can be moulded so that it complements both the original and the revised versions of the waterfall methodology. Table 23 illustrates how the WES methodology could be integrated into the original version of the waterfall methodology. The project development risk assessment could be conducted while the systems requirements are being gathered. Then, while the software requirements are being gathered, acquire the security requirements at the same time. There are aspects of the security design / coding stage that are applicable to the analysis, program design and coding stages of the original waterfall model. The organization would need to choose the specific aspects from the security design / coding stage and apply them to the appropriate stages of the original waterfall model. An example would be the architect reviewing the project development risk analysis and the security requirements during the analysis.

Table 24, on the other hand, shows how WES can be integrated into the Sommerville version [175] of the waterfall model. Note, two stages of the WES methodology are being addressed during a single stage of the waterfall process where the need warrants. Regardless of how these are integrated into the methodology or to what depth an organization decides to take the WES stages, they can be integrated.

Table 23 - Basic Waterfall Method and WES Compatibility

Original Waterfall Model*	WES Process
Systems Requirements	Project Development Risk Assessment
Software Requirements	Application Security Requirements
Analysis	Security Design / Coding
Program Design	Security Design / Coding
Coding	Security Design / Coding Controlled Environment Implementation
Testing and Operations	Testing Implementation in Production End-User Evaluation

* Royce [164]

Table 24 - Sommerville Waterfall Method and WES Compatibility

Sommerville Waterfall Model *	WES Process
Requirements Definition	Project Development Risk Assessment Application Security Requirements
System and Software Design	Security Design / Coding
Implementation and Unit Testing	Security Design / Coding Controlled Environment Implementation
Integration and System Testing	Testing
Operation and Maintenance	Implementation in Production End-User Evaluation

* Sommerville [175]

9.2 The Unified Software Development Process (USD)

The phases of the process include inception, elaboration, construction, and transition and the workflows consist of requirements, analysis, design, implementation and testing [105]. The compatibility of WES with the individual phases of the USD process is displayed in Table 25.

Table 25 - USD Phase and WES Compatibility

USD Process Phases *	WES Process
Inception	Project Development Risk Assessment
Elaboration	Application Security Requirements
Construction	Security Design / Coding Controlled Environment Implementation Testing
Transition	Implementation in Production End-User Evaluation

* USD Process [105]

However, Table 25 only displays half of the picture. WES can be integrated into both the workflows and the phases of the Unified System Development (USD) process. The work flows in the USD process are really the main activities in the development process. The five USD workflows are as follows: requirements, analysis, design, implementation and test. There is, realistically, going to be some cross over between the phases of the USD methodology. Pragmatically, there could be cross over between the individual work flows due to the fact that activities in the business environment do not always stop and start on a specific schedule. During the requirements workflow and the inception phase, a project development risk analysis should to take place, prior to acquiring the security requirements, which will probably start in the inception phase as well and migrate into the elaboration phase. The analysis workflow then needs to go back and pick up the risk analysis and compare the results against the security requirements to ensure that all of the issues are being identified and acknowledged.

Once this has been achieved, the process moves into the design workflow which has activities in the elaboration phase and the construction phase where security design and coding issues are resolved. The security design and the coding issues will need to be compliant with the security requirements. Once this particular piece of the application has been developed, it will need to be implemented into a controlled environment. Once the application is compatible with the environment, the next workflow is security testing. The testers will probably identify errors in the application and request modifications from the coders. The testers should, according to WES, go back and compare the application with the security requirements and the risk analysis to ensure that the design is correct and the risks have been appropriately mitigated. After testing has been completed, then the application should progress into production and feedback from the end-user should be acquired. As Jacobson, et. al. stated

> "you integrate, test, and run each iteration a little (and) between each step, you take, you get feedback that permits you to adjust your focus for the next step" [105].

WES complements this approach nicely. Table 26 provides a more realistic perspective on the integration of the WES methodology with the USD process. The cross sections that are in bold and have a large font indicate the main activities for that phase / workflow. The cross sections that are not in bold and contain a smaller font represent work that has already been completed. The idea is that the main activities should be able to access previously generated data if desired. The Project development risk analysis fits well into the USD iterative process. As noted in chapter six, the iterative concept in the USD process is risk driven. Hence, adding risk from the security perspective should integrate well with the existing risk emphasis from a project point of view.

The people perspective of the WES process is also compatible with the USD process. Both processes believe that people are crucial to the development process life cycle. The difference is that WES not only believes the process should work well for the individuals implementing it but it should also strive to minimize breaches through guidance.

Table 26 - USD Process and WES Compatibility

		Phases		
Core Workflows	Inception	Elaboration	Construction	Transition
Requirements	**Project Development Risk Assessment**	**Application Security Requirements**		
Analysis	Project Development Risk Assessment	**Application Security Requirements**		
Design	Project Development Risk Assessment	Application Security Requirements	**Security Design / Coding**	
Implementation	Project Development Risk Assessment	Application Security Requirements	**Security Design / Coding**	**Controlled Environment Implementation**
Test	Project Development Risk Assessment	Application Security Requirements	Security Design / Coding **Testing**	**Testing** **Implementation in Production** **End-User Evaluation**

9.3 Dynamic Systems Development Method (DSDM)

As outlined in chapter six, Stapleton [177] defines the five main phases of DSDM along with "two non-development phases" [178] which are as follows:

0. Pre-Project
5. Feasibility Study
6. Business Study
7. Functional Model Iteration
8. Systems Design and Build Iteration
9. Implementation
10. Post-Project [177, 178]

The pre-project stage is the first non-development phase and is described as a phase that "ensures that only the right projects are started and that they are set up correctly" [178]. Realistically, this translates into a focus on funding and general business continuity. At this point, it would not hurt to have a security officer with whom to discuss ideas. However, it is not mandatory from a WES implementation perspective. WES maps very well into the five main phases of the DSDM process. The first main stage is the feasibility study. Some of the considerations that the business needs to address include the definition of the problem that the business is trying to solve; can the business problem be solved with technical solutions and, if so, "is the impact on the current business process acceptable?" [177]. Organizations should also be asking the question, what is the security risk that the proposed application introduces to the organization? The specific security question compliments the business impact question very well.

The business study's primary activity "is to get a good understanding of the business perspective to be automated and (its) information needs" [177]. This is where detailed security requirements should be captured by the development team. WES does not mandate how this task is to be resolved. It can be accomplished through one-on-one interviews, group discussions, or as Stapleton recommends for a DSDM project, through a series of facilitated workshops. The end goal is to capture the application's security requirements. How this is accomplished is up to the cultural comfort of the executing organizations. As described by Stapleton, the functional model iteration activities are:

1. Identify what you are doing in the cycle
2. Agree how you are going to go about it
3. Do it
4. Check that you did it right [177].

Including security in each of these activities does not create any conflicts. Stapleton goes on to state that testing takes place as components are produced.

> "As developers produce a software component, it is tested by them-selves (for technical aspects) and the users in the team (for functional suitability). In this way, all forms of testing, including acceptance testing, are carried out incrementally throughout a project" [177].

All forms of testing should include security testing as described by WES in chapter seven. One of the products of the functional model is a risk analysis of future development. Conducting a risk analysis on future development would probably help to identify areas that may need additional research and investigation from a security requirements perspective and help to propel future conversation in the area of security.

The design and build iteration stage is where the major construction, testing and general tuning of the application takes place. It should be noted that DSDM does not consider testing a separate activity. The method states that testing "is thinly spread throughout the development process" [177]. This being the case, hopefully, there should be a controlled environment, for testing purposes, available to the development staff and any testers. The implementation stage is where the transition from the development environment to the operational environment takes place. This activity includes end-user education and training. DSDM also believes that "Active user involvement is imperative"[62]; a point on which WES concurs.

The last stage is the post-project stage which is the second non-development phase mentioned at the start of this section. The goal of this section is to "assess the success of the solution in achieving the intended benefits" [178] which Stapleton notes generally does not consider the lessons learned throughout the life of the project since these should have been covered incrementally as the project progressed. It is reasonable to presume that there could be input / influence from the end-user evaluation stage in the WES methodology at this point in the DSDM. Pragmatically, it is recommended that end-user evaluation information be gathered incrementally at the end of the implementation stage in the DSDM.

The consortium does mention an e-DSDM lifecycle which "follows the same process as a DSDM project with the exception of a Vision Phase. The Vision phase precedes a set of e-DSDM projects. Its aim is to set the e-business strategy for an e-business programme" [62]. Again there is no mention of security in this vision phase.

Table 27 provides an overview of the integration of the WES methodology with the five main stages of DSDM. There is a small bit of repetition between the functional model iteration systems design and build iteration due to the nature of the methodology. The extent of the replication that is experienced is dependent upon the organization executing the methodology. If the organization simply chooses to model the system without construction of the prototype then there will obviously be less repetition.

Table 27 - DSDM / WES Compatibility

DSDM	WES
Feasibility study	Project Development Risk Assessment
Business Study	Application Security Requirements
Functional Model Iteration	Security Design / Coding Controlled Environment Implementation Testing
Systems Design and Build Iteration	Security Design / Coding Controlled Environment Implementation Testing
Implementation	Implementation in Production End-User Evaluation

9.4 eXtreme Programming (XP)

The WES methodology could be implemented among the various stages and levels of the XP development process so that it looks something like Table 28. The exploration and the planning stages are portrayed as more high-level stages whereas development, acceptance testing and small releases are a bit more granular. WES is very suitable to the XP process in that it supports the idea that the company should determine the amount of documentation that is relevant for the environment. It is very compatible with multiple short development life cycles as it increases the number of conversations that are relevant to the security of the application.

The exploration stage is where the project development risk assessment should take place. This is where the customer / business unit pulls together enough information to construct the story cards and developers explore possible architectures. This is a great time to bring up possible risk introduced by the proposed system. These risks can then be used to flush out application security requirements in order to mitigate the risk raised in the previous stage. The development stage is where the secure coding should take place in pairs. Utilize good coding practices; establish trust and accountability while implementing standards from a design and a coding perspective. Acceptance testing should include a controlled environment implementation, security testing and end-user feedback. A small release coincides with implementation in production.

Table 28 - XP and WES Compatibility

Exploration	Project Development Risk Assessment
Planning	Application Security Requirements
Development	Security Design / Coding
Acceptance Testing	Controlled Environment Implementation Testing End-User Evaluation
Small Releases	Implementation in Production

9.5 Agile Manifesto Core Principles Compatibility

The Department of Home Land Security (DHLS) provides a break-down of the Agile Manifesto core principles and their perceived effect on agile application development. The information provided by the DHLS is directly available in the first three columns of Table 29 [51]. The fourth column provides information on how WES addresses these issues.

Table 29 - Core Principles of the Agile Manifesto & Relevant WES Impact

The Department of Home Land Security *			WES Dissertation
No.	Principle	Implication for Security	Relevant WES Impact
1	The highest priority of agile developers is to satisfy the customer. This is to be achieved through early and continuous delivery of valuable software.	Negative, unless customer is highly security-aware. There is a particular risk that security testing will be inadequate or excluded because of "early delivery" imperatives.	All three principles impact this issue Security Education, Good communication and Cultural Support. WES attempts to mitigate this issue by bringing security into the development life cycle at an early stage. Early identification of the security risk should filter through quick iterations of the development life cycle improving design, coding and testing.
2	Agile developers welcome changing requirements, even late in the development process. Indeed, agile processes are designed to leverage change to the customer's competitive advantage.	Negative, unless customer is careful to assess the security impact of all new/changing requirements, and include related requirements for new risk mitigations when necessary.	The principle of good communication is critical in this circumstance. Due to the fact that it explicitly supports end-user involvement; the WES methodology is also conducive to short development cycles. The WES methodology also provides support by having a risk assessment early in the development life cycle, helping to mitigate risk through the development iteration.

3	Agile projects produce frequent working software deliveries. Ideally, there will be a new delivery every few weeks or, at most, every few months. Preference is given to the shortest delivery timescale possible.	Negative, unless customer refuses to allow schedule imperatives to take precedence over security.	The principles (good communication, security education and cultural support) help provide the organization with the foundation to support frequent software releases. As demonstrated earlier in chapter nine, the WES process integrates into agile development processes (DSDM, XP) augmenting the security aspect of the development process while continuing to support frequent code releases.
4	The project will be built around the commitment and participation of motivated individual contributors.	Neutral. Could be Negative when the individual contributors are either unaware of or resistant to security priorities.	The principles (good communication, security education and cultural support) help provide the organization with the foundation to support individual development and participation in secure code development. The WES process provides guidance during development.
5	Customers, managers, and developers must collaborate daily, throughout the development project.	Neutral. Could be Positive when all participants include security stakeholders (e.g., risk managers) and have security as a key objective.	The WES methodology provides the framework to encourage daily collaboration. This is accomplished through the principals (good communication, security education and cultural support) in conjunction with the WES process. The WES approach augments the ideals and process advocated in the agile manifesto.
6	Agile developers must have the development environment and support they need.	Neutral. Could be Positive when that environment is expressly intended to enhance security.	WES encourages active organizational support for security in the Web development process through the principle of cultural support.
7	Developers will be trusted by both management and customers to get the job done.	Negative, unless developers are strongly committed and prepared to ensure security is incorporated into their process and products.	The WES methodology provides the framework to encourage daily collaboration. This is supported through the principles of good communication, security education and cultural support. Enabling the WES process to help mitigate these types of problems in this environment.
8	The most efficient and effective method of conveying information to and within a development team is through face-to-face communication.	Negative, as the assurance process for software is predicated on documented evidence that can be independently assessed by experts outside of the software project team.	The WES methodology encourages good communication and cultural support for that communication. The amount of documentation required by an organization is dependant upon their specific business, industry and regulatory needs.
9	The production of working software is the primary measure of success.	Negative, unless “working software” is defined to mean “software that always functions correctly *and* securely.”	The WES methodology provides the basic framework to help establish the definition of working software as functionally correct and secure software.

10	Agile processes promote sustainable development.	Neutral	The WES methodology fits into existing application development methodologies promoting sustainable development. Allowing the development team to decide how much of the WES methodology is suitable to their organization.
11	The developers, as well as the project's sponsors and the intended users (either of whom could be the "customer"), should be able to maintain a constant pace of progress indefinitely.	Neutral	As demonstrated previously in chapter nine, the WES methodology fits into existing application development methodologies promoting constant development.
12	Agility is enhanced by continuous attention to technical excellence and good design.	Positive, especially when "technical excellence and good design" reflect strong expertise in and commitment to software security.	WES promotes technical excellence through the use of standards and code review. WES also promotes extensive testing along with an environment that supports technical excellence through the use of technology. WES supports technical excellence through security education as well.
13	Simplicity, which is defined as the art of maximizing the amount of work not done, is essential to successful projects and good software.	Positive, if simplicity is extended to the design and code of the software as this will make them easier to analyze and their security implications and issues easier to recognize.	WES supports this concept starting with the project development risk assessment, the capturing of the security requirements and the use of this information in the security design and coding stage along with the testing stage.
14	The best architectures, requirements, and designs emerge from self-organizing teams. At regular intervals, the team must reflect on how to become more effective, then tune and adjust its behaviour accordingly.	Neutral	WES is a process neutral approach to security enabling the security approach to support the organization's culture and existing development synergies. This allows WES to be customized on an ongoing basis to meet the needs of the organization.

* The Department of Home Land Security [51]

9.6 Summary

This chapter evaluated the compatibility of the WES methodology with four methodologies that cover both traditional and agile development processes used in Web engineering application development. The chapter also examined the compatibility of the WES methodology with Agile Manifesto core principles. The results of the analysis, based on the available literature, indicate that WES is compatible with both agile and traditional Web engineering processes. Chapter ten examines a practical implementation of the Essential Elements and the Security Criteria for Web Application Development (SCWAD) discussed in chapter five.

10 Hunterian Museum and Art Gallery Case Study

This chapter focuses on a case study carried out in the Hunterian Museum and Art Gallery (Hunterian) at the University of Glasgow, Scotland from February, 2005 to January, 2006. The focus of the Hunterian case study involved providing security recommendations to the Hunterian development team during the construction of the Hunterian Online Photo Library (HOPL) Internet application. The idea behind HOPL was to enhance the overall exposure of the Hunterian image collection while providing an avenue for increasing business capacity on the sale of the images over the Internet. Section 10.1 presents the initial case study information. Section 10.2 discusses the methodology and section 10.3 examines the Essential Elements. Section 10.4 covers the analysis of the project through the application of the Security Criteria for Web Application Development (SCWAD) and section 10.5 summarizes the chapter.

10.1 Initial Hunterian Discussion Summary

The Hunterian Museum wanted to increase the visibility of their products by increasing its presence on the Internet. The overall marketing approach strives to increase the visibility of the museum by increasing the museum’s asset exposure on their primary Web site as well as through merchants such as The Research Libraries Group (RLG) (http://www.rlg.org/) and The Bridgeman Art Library (http://www.bridgeman.co.uk). The imaging business is heavily integrated with the legal side of life due to the fact that each sale of an image is associated with a specific release and, hence, a specific copyright use. Therefore, the increase in exposure for the museum increases their potential points of sale generating the possibility for increased revenue. The aspect of the marketing campaign that is of particular interest to this case study involves all aspects associated with expanding their Web site so they can display watermarked thumbnail images and sell high resolution images on the Internet. An additional benefit to making the images available over the Internet is the increased availability to departmental personnel.

The initial design area of the discussion revealed the following information.

- The initial Web site resided on the University central UNIX servers. Capacity should not be an issue from an interactive Web site point of view or an image housing perspective. There was some debate as to whether the images will be housed on a new Storage Area Network (SAN) that the University is currently installing or whether the images will be housed on a server in the Hunterian. Several discussions with various departments on campus resulted in the images being stored on a server in one of the main server rooms on campus.
- The initial Web authorizing tool was Adobe Go Live.
- The database server is a Microsoft SQL server. It should be noted that the current database that houses the images was FileMaker Pro. The decision to move to the

SQL server is based on increased future development flexibility by the Hunterian. This brings up the issue of importing the images from FileMaker Pro to Microsoft SQL Server.

- Reports are desirable, if possible, that can provide insight into marketing information and trends.
- The museum is flexible as to the display of the images on the Web site. They may want to do some end-user feed back to the input of design. They may also want to implement a voluntary Web survey in an attempt to acquire end-user feed back on site usability.

The security policy aspects of the discussion revealed interesting information about the business and copyright side of life in the imaging business. The purchaser of the image has to state the way that the image will be used. The copyright that is sold by the Hunterian is for a specific use. If the buyer wants to re-use the image for another purpose or use the image for the same purpose on a different print run, then these details will need to be negotiated with the Hunterian museum. Hence, the form for stating the intended use will need to be available on the Internet.

The Hunterian wants to make the images visible on the Web and to display contact and payment information. There is discussion as to whether the digital quality image should be downloadable from the net or whether the image should be sent via File Transfer Protocol (FTP) to the buyer or whether it should be burned to a CD-Rom and mailed to the buyer. This issue prompted an interesting design question.

If the ability to download an image is used as the transfer medium, should the customer be limited to a single download or allowed many downloads within a restricted period of time? Are there security implications for either decision? A single download provides tighter security from the perspective of controlling access to the images on the server. Multiple downloads within a restricted time means that the customer could conceivably download the image several times within a short time span. The reality is that once the customer has successfully downloaded the image then it can be copied. Hence, the single download does not really provide a lot of extra security when considering the individual image. Multiple downloads within a restricted period has the added advantage of alleviating situations where the customer's connection drops for whatever reason and the download has to be attempted a second time. This reduces the Hunterian's system support effort. Due to the latter reasons, the museum decided to implement the multiple downloads in a restricted time period solution.

The security portion of the initial discussion reveals:

- The Hunterian's desire to maintain a high level of customer confidentiality through the protection of any data that is collected via the Internet. This level of data protection will need to be compatible with the Freedom of Information Act (FIA) and the Data Protection Act. Before Web site implementation, a specialist at the University of Glasgow should be consulted for compliance with FIA.

- The Hunterian also expressed a desire to have a level of system operation integrity which translates into a high confidentiality level in the system by the museum.
- The levels of security that the Hunterian indicated interest in protecting included defacement, communication and transaction.
- The Hunterian would like to look into the use of image watermarking
- The Hunterian would like to look into the use of digital marking high resolution images with something to identify the image with the customer.
- The Hunterian does have implicit procedures in place when examining disaster recovery. The University of Glasgow computing services is backing up the Web site and the low resolution images that are currently associated with the site. The high resolution digital images are backed up on different hard drives within the Hunterian. It should be noted that all of the hard drives are located in the same building, leading to a physical security issue. It should be noted that there is no formal disaster recovery plan in writing.

10.2 Methodology

As discussed in chapter two, the research strategy utilized was that of a case study. The five stages are listed below.

1. Case study design: objectives are defined and the case study is planned.
2. Preparation for data collection: procedures and protocols for data collection are defined.
3. Collecting evidence: execution with data collection on the studied case.
4. Analysis of collected data
5. Reporting [95, 215]

Case study design stage took place when the Hunterian museum decided that it wanted to produce a Web application for the purpose of selling images over the Internet and then proceeded to inquire about assistance from the Department of Computing Science at the University of Glasgow.

The preparation for data collection stage took the form of several meetings which typically happens during the course of software development. Ten project meetings were attended during the course of this case study where the project manager deemed security to be an issue that might need to be discussed. These meetings specifically discussed recommendations on the following topics: the tools and software that the developers would use, the conversion of older images to the new system, common security problems, the security issues involved with accepting payments over the Web, the design of the system around the payment verification, the need to test the application and the identification of bugs in the system. Not all of the recommendations that were proposed were accepted.

Collecting evidence stage took place when some of the recommendations were implemented during project development. It should be noted that the security recommendations were not implemented by the individual proposing the changes. Recommendations were implemented by various members of the Hunterian's development team.

The Analysis of collected data and the reporting of the effort to include security into the Hunterian's application development process are discussed through the establishment of the Essential Elements and the application of the Security Criteria for Web Application Development (SCWAD). The specific lessons learned are discussed in the summary section of this chapter.

10.3 The Essential Elements

The Essential Elements for security in a Web application development process are discussed in greater detail in chapter five. The Essential Elements are as follows:

1. Web Application Development Methodology
2. Web Security Development Process Definition
3. End-Users Feed Back
4. Implement & Test Disaster Recovery Plans
5. Job Related Impact

10.3.1 Web Application Development Methodology

The Hunterian implements an implicit traditional life cycle development methodology. The developers are assigned to specific projects. They are generally asked to contribute to the design of the project and then they are expected to develop the application as agreed upon with the project manager. The project manager then keeps track of the progress as the developers progress through the agreed upon stages of the project. The project manager also attempts to coordinate any additional outside assistance as needed. This approach is not ideal. The success of the project is dependent on the skills of the project manager. This approach encourages an environment that is generally conducive to the generation of minimal code and system documentation. This lack of documentation also has a ripple effect on training time for new employees.

In the real world, the Hunterian, as with many other businesses, has limited funds to contribute to application development. The developers for the Hunterian are generally Glasgow University computing science students who have been brought in for a specific project. The incentive for the students is the experience they gain while working with an actual organization on a real problem along with the fact that the project is associated with a course mark. Hence, the high turn over and limited availability of a student's time places restrictions on the development team. This means that the Hunterian may have multiple students working on specific aspects of a project. The high turnover in students, coupled with a high number of potential students working on a project for very short periods of time, creates a volatile environment that can be very difficult to ensure that accurate documentation is being accomplished. The Hunterian imaging project had at least fifteen different developers who worked on various aspects of the project over the duration of the development life cycle.

10.3.2 Web Security Development Process Definition

Organizations should attempt to define the following questions when considering security in the development process.

- What security means to the business?
- What it means to a Web application?
- What it means in the development process?
- What a Web Engineering Security development process entails?

Security to the business, in this context, means that images are not being used in publications without the consent of the Hunterian museum. Security to the Web application translates into the Web application being able to withstand attacks so that the images, which are displaced via the Web site, are not compromised. They also wanted a widely available solution where the customer could participate in a secure payment transaction for the image over the Internet. The mechanism for this transaction should protect both the customer and the Hunterian in terms of confidentiality, integrity and availability. In addition, the application should not allow intruders to compromise other applications operating on the same server.

The Hunterian's response to defining security is that they want the application to be as secure as possible with the least amount of cost and effort. This translates into the securing of outside sources for security advice during the application development process. The Web engineering security development process for the Hunterian entails addressing security during the process when the project manager deems it to be a necessary issue.

10.3.3 End-Users Feedback

This is probably the weakest section within the application of the Essential Elements to the Hunterian development process. While the Hunterian did provide other museums, such as the Smithsonian and Harvard**,** with a link to view and use the system, it can be argued that these individuals are not true end-users. They could be analyzing the system from the perspective of a competitor or from a power user's perspective. While neither is bad, it does not provide an accurate overall picture from the end-users' perspective.

As discussed in the paper presented to the 2007 ARES conference [81], if a development process does not attempt to acquire feedback from the end-users, this could signal potentially large problems with the development process alignment with the needs of the business. Strong support for end-user participation, in Web Application development, has been previously indicated in a journal article by McDonald and Welland [82, 130].

The business needs for small organizations, like the Hunterian, require balancing this necessity for end-user feed back with the availability of resources.

10.3.4 Implement & Test Disaster Recovery Plans

The importance of a disaster recovery plan can not be overstated in today's Web enabled environment. The Hunterian addressed this issue by installing the database and the application on servers in the Management Information Service (MIS) department and not, as originally planned, in the university server farm. The MIS technical staff has an instance of Microsoft SQL, the SQL data and the image data stored on mirrored servers.

Database and source files on the server are backed up nightly. Both the database and the source files are backed up on a weekly basis and a monthly basis. The weekly and the monthly backups are stored to tape. The first backup of every month is set aside for a year. The weekly backups are held for a month. The tapes are then stored off site in a temperature controlled environment. In an event that there is a problem, they can restore the information. The backup currently contains five and a half thousand images which totals to roughly one hundred and eleven gigabits out of a total drive capability of five hundred gigabits. It should be noted that, to the knowledge of the Hunterian staff, the backups have never been tested. Meaning that Hunterian staff has never restored any of the backups to be sure that they are operating properly.

10.3.5 Job Related Impact

The project manager and one technical staff person are the only people on this project who were permanent employees of the Hunterian. The majority of the coders were students from the Department of Computing Science. The idea of job impact is really propagated through the effect the project has on their individual grade and potential future references. While this is important and does impact the developer, it is only one grade or the loss of a potential reference in the future. It does not carry the same overall impact as a job review.

10.4 Security Analysis

The Security Criteria for Web Application Development (SCWAD) are discussed in greater detail in chapter four. Security Criteria for Web Application Development (SCWAD) consists of six essential security criteria that need to be met within methodologies that are used for application development. These criteria are:

1. Active organizational support for security in the Web development process
2. Proper Security Controls in the development environment
3. Security visibility throughout all areas of the development process
4. Delivery of a cohesive system, integrating business requirements, software and security
5. Prompt, rigorous Security testing and evaluation
6. Trust and Accountability

10.4.1 Active organizational support for security

The project manager instigated the initial contact with the Department of Computing Science for both the development and the application security aspects of the project. This initial contact demonstrates that the project manager is cognisant of security issues in the development process that need to be recognized and addressed. The project manger openly encouraged communication and questions from the developers in the area of security.

The project manger also has taken steps to help educate stakeholders on the importance of the security aspect of the application. Being a small organization, with limited financial resources, the Hunterian has relied on the Department of Computing Science to aid in this endeavour.

10.4.2 Proper Controls in the development environment

Proper controls provide structure to the development environment. This is accomplished by providing information that covers policies, necessary knowledge, technology and the process that is to be utilized in the development environment.

10.4.2.1 Policies/Standards/Procedures

Since the Hunterian is a small organization with a high turnover, in reference to its development staff, there is very little documentation on the policies, standards and procedures that are involved in the development process. The project manager is highly involved in the development process and handles these issues as they arise. While this approach has been very successful for the Hunterian, it does create a general security issue that has repercussions in the development environment. The dependency on a single individual to achieve project success is a dangerous protocol to pursue. If this individual leaves the organization, for whatever reason, then the completion of current projects and the practical achievement of future projects are likely to become jeopardized.

10.4.2.2 Knowledge

The idea is that organizations need to provide proper training in reference to coding and project management. Again, since the Hunterian is limited on resources, they depend on the Department of Computing Science for this type of training. Currently, the Department of Computing Science at the University of Glasgow does not offer a specific class on security for computing science students prior to their involvement in this project. It should also be noted that students undertaking the projects involve in the construction of HOPL did not receive any formal training in security. The lack of security in academia is a recognized issue in industry. According to the Department of Home Land Security, their draft report on Security in the Software Lifecycle quotes several industry leaders on the inadequacy of security education in computing science programs [51]. They go on to indicate that

> "most developers are not being taught how to recognize and understand the security implications of how they specify and design software, write code, integrate/assemble components, test, package, distribute, and maintain software" [51].

The Hunterian project does not go into the overall education of the developers in any detail. The project manager is the primary point of contact for any issue that arises during the development project. This places an emphasis on the criticality of the individual in this role for the success of projects within the organization.

10.4.2.3 Technology

The technology implemented for this project, as with many organizations, was determined by existing resources, financial constraints and donations. The Hunterian has a limited budget to spend for development and only one technical person. Since Microsoft donated the SQL Server application and the Visual Studio software for the project, the technical scope was established early in the development process. The use of the software did provide the Hunterian with up-to-date code libraries and professional quality development tools. Some of the security benefits according to a couple of articles [107, 112] include:

- Design analysis tools
- Application Verifier
- Buffer Security Check /GS (Visual C++)
- The Safe CRT Libraries (Visual C++)
- Static code checkers (C and C++ source code)
- Code Access Security/Least Privilege (.NET Framework applications)
- Debug in Zone
- Improved Security Exceptions during Debugging
- IntelliSense in Zone (Visual Basic feature)
- PermCalc (Calculate Permissions for application zones)[112]
- Develop and debug as least privilege
- Issue tracking
- New Testing Tools (Visual C++, Visual C#, or Visual Basic)
- Load testing [107].

The point is not to argue the validity or the usefulness of the tools from a security capabilities perspective, but to acknowledge that they exist and provide options to the developers. It is also useful to note that the Hunterian decided to code the application in Visual Basic which limited access to some of the security tools being offered in the 2005 Visual Studio.

One suggestion that was not implemented is the use of a source control system. Source control systems provide versioning control during code development. This allows for code role backs in cases where bugs are intentionally or unintentionally introduced into the code and provides developer accountability.

10.4.2.4 Process

The software development process is simply another form of a control. The software development process is used to control the development of the application. The process that the Hunterian implements to develop projects is an implicit traditional software development life cycle. The resource pool that the Hunterian utilizes and the project manager dependency creates potential security issues within the development process. The heavy dependency on the project manger is dangerous from a process perspective. The project manager, in this case, is the only person who sees the entire development life cycle. The Hunterian recruits students to work on specific aspects of projects. This means that few students actually see a single project completed from inception to production. This lack of developer consistency throughout the project introduces potential problems with process understanding and process compliance consistency. The high developer turn-over has the potential to create problems if code is not commented properly and documentation is not kept up-to-date. There is also no specific process for security within the Hunterian.

10.4.3 Security visibility throughout all areas of the development process

Security visibility was clearly discussed during the business analysis, requirements, design phase and the testing phase. Meetings were conducted between the Hunterian project manager and the Department of Computing Science (DCS) during the business analysis stage and the design stage to determine the security requirements. The basic security requirements can be summarized as follows:

- High level of customer confidentiality and integrity
    - Data Protection
    - Operation Integrity
    - Customer Communication
- Protection of Images via Water Marking
- Protection of Images via Customer Number Identification
- Compliance with existing disaster recovery procedures

These security requirements led to discussions over the design in terms of integrity, confidentiality and availability of the system. These high-level security requirements transformed into the following security design recommendations:

1. Implement logins to establish authorization and authentication
2. Implement / Integrate a secure payment system
    a. Encryption of the payment transaction if possible
    b. Confirmation of the transaction prior to end-user download
    c. Page monitoring for post-back information from payment system
    d. Make the discount request manual for the purpose of adding a layer of human verification
3. Web page protection of top ten coding vulnerabilities

4. From a security standpoint, code needs to be modularized as much as possible. This can be handled in one of two ways. The code can be broken down so that there is a separate security class for each type of problem or we can create a single security class and have multiple methods for each type of security problem. Either will work; the set up is really a design preference issue. The goal is to modularize as much as possible from an object re-use perspective. This cuts down on the odds of accidentally having two classes that perform the same job.
5. Install and use a professional source code management system.
6. Any data that is going to be passed via a URL will need to be encrypted.
7. Any sensitive data that is being stored on the database will need to be encrypted.

The recommendations that were implemented include numbers one, two, three, six and seven. It should be noted that recommendation numbers three, six and seven were limited in their implementations. The elements that were specifically tested for out of the top ten vulnerabilities in Web applications included: un-validated input, broken access controls, injections flaws, and improper error handling. As far as the sixth recommendation goes, the only data that is encrypted is the data going to the payment system and the user password. The only stored data that is encrypted in the database is the user password. The marking of images to record customer numbers was deemed out of scope for this project and tabled for later investigation. Due to the limited resources, the developers were trusted to implement the security requirements as requested. Although security solutions were discussed during design and testing, an in-depth code review was not conducted.

Additional items that were discussed and not implemented include locking the user out after a set number of log-in attempts and keeping a log of the user’s activities within the program. Even though the development team had access to a security specialist, there was minimal contact during the implementation phase. It should be noted that contact between the development team and the security specialist was always initiated by the project manager. There was no true end-user testing conducted for this project before the Web application went live.

10.4.4 Delivery of a cohesive system

This situation is unique in that the unit setting up the system is also defining the business requirements. Hence, from that perspective, there is definitely a cohesive integration of business requirements and the software. The system provides the amount of security that the Hunterian deems necessary for the application. As with most organizations, the Hunterian would like to have a system that has had every aspect of the system tested to the nth degree; however, security has to be realistically applied to applications during the development process. Practical security makes trade-offs with the cost associated with developing the solution and testing the successfulness of the solution. It also makes trade-offs with development timelines, human resources, employee skill levels and the probability for potential types of attacks. In the end, the level of security integrated with an application becomes a managerial decision based on a variety of inputs. In the case of the Hunterian, the project manger makes these decisions.

10.4.5 Prompt, rigorous testing and evaluation

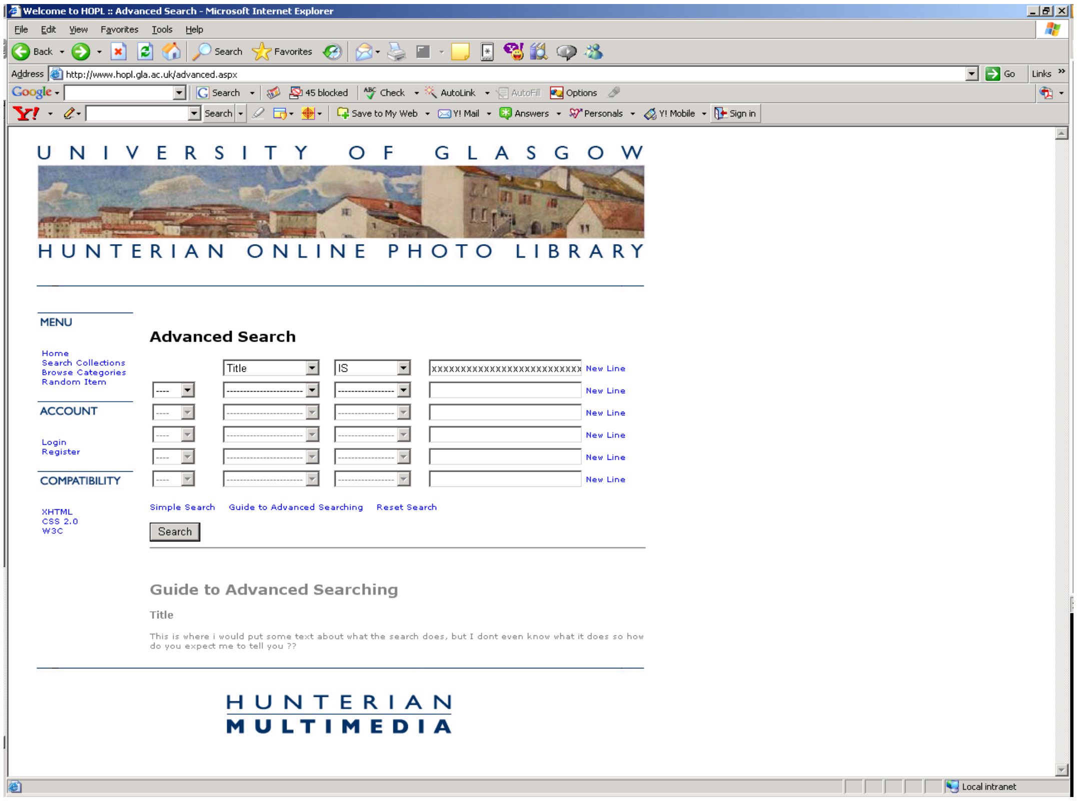
The idea of outsourcing penetration testing and load testing was discussed with the Hunterian project manager. The ideas were turned down when compared with the available resources. The testing for the application was handled primarily through the developers and outside testers. Three outside testers (including this author) were asked to examine the site. This author also discovered two major bugs in the system along with a couple of minor link errors and text display errors. The steps taken to identify the major bugs along with screen shots (Figure 8 and Figure 9) are as follows:

10.4.5.1 First Problem - Session State Problem

The steps are as follows:

- Select title
- Select IS from the drop down menu
- Enter xxxx to fill up the line
- Hit search twice - this is the root of the problem

Figure 8 - Hunterian Screen Shots Error Number One



Welcome to HOPL :: Advanced Search - Microsoft Internet Explorer

Address http://www.hopl.gla.ac.uk/advanced.aspx

UNIVERSITY OF GLASGOW

HUNTERIAN ONLINE PHOTO LIBRARY

Advanced Search

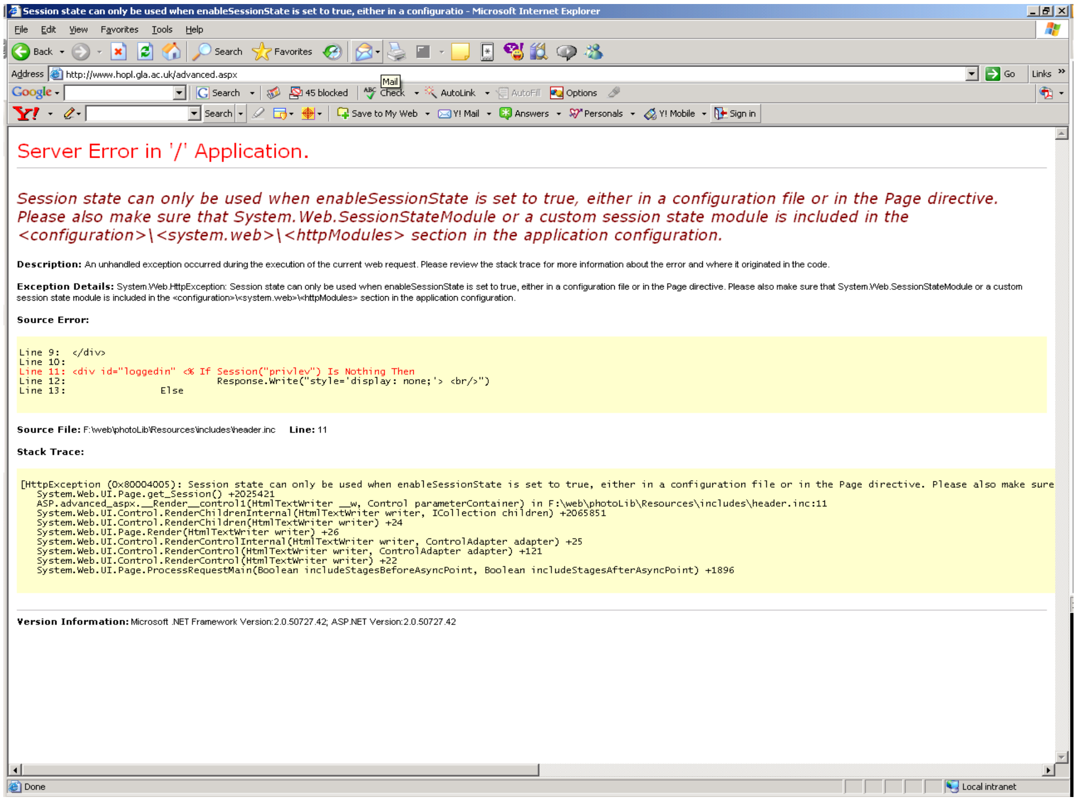
Title | IS | xxxxxxxxxxxxxxxxxxxxxxxxxxx

Guide to Advanced Searching

Title

This is where i would put some text about what the search does, but I dont even know what it does so how do you expect me to tell you ??

HUNTERIAN MULTIMEDIA


Session state can only be used when enableSessionState is set to true, either in a configuratio - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.hopl.gla.ac.uk/advanced.aspx
Go Links
Mail
Google Search 45 blocked Check AutoLink AutoFill Options
Search Save to My Web Y! Mail Answers Personals Y! Mobile Sign in
Done
Local intranet

Server Error in '/' Application.

Session state can only be used when enableSessionState is set to true, either in a configuration file or in the Page directive. Please also make sure that System.Web.SessionStateModule or a custom session state module is included in the <configuration>\<system.web>\<httpModules> section in the application configuration.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Web.HttpException: Session state can only be used when enableSessionState is set to true, either in a configuration file or in the Page directive. Please also make sure that System.Web.SessionStateModule or a custom session state module is included in the <configuration>\<system.web>\<httpModules> section in the application configuration.

Source Error:

```
Line 9:  </div>
Line 10:
Line 11: <div id="loggedin" <% If Session("privlev") Is Nothing Then
Line 12:                           Response.Write("style='display: none;'> <br/>")
Line 13:                 Else
```

Source File: F:\web\photoLib\Resources\includes\header.inc   **Line:** 11

Stack Trace:

```
[HttpException (0x80004005): Session state can only be used when enableSessionState is set to true, either in a configuration file or in the Page directive. Please also make sure
   System.Web.UI.Page.get_Session() +2025421
   ASP.advanced_aspx.__Render__control1(HtmlTextWriter __w, Control parameterContainer) in F:\web\photoLib\Resources\includes\header.inc:11
   System.Web.UI.Control.RenderChildrenInternal(HtmlTextWriter writer, ICollection children) +2065851
   System.Web.UI.Control.RenderChildren(HtmlTextWriter writer) +24
   System.Web.UI.Page.Render(HtmlTextWriter writer) +26
   System.Web.UI.Control.RenderControlInternal(HtmlTextWriter writer, ControlAdapter adapter) +25
   System.Web.UI.Control.RenderControl(HtmlTextWriter writer, ControlAdapter adapter) +121
   System.Web.UI.Control.RenderControl(HtmlTextWriter writer) +22
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +1896
```

Version Information: Microsoft .NET Framework Version:2.0.50727.42; ASP.NET Version:2.0.50727.42

The first issue that needs to be addressed is the restriction of the amount of input that the end-user is allowed to enter into the search field. As displayed in Figure 8, the first bug was found in the advanced search page. One of the text fields for the advanced search allowed the user to input more text than the field could handle. This generally causes the system to overwrite memory space that is being used to hold other information. In this case, the system then produced a session information error.

The second issue that needs to be addressed is the error message. The session error in turn caused the Web page to produce an error page that provided information which included the technical explanation for the problem, the line on which the error occurred, the drive path along with indications as to the language in which the system had been written and the platform on which the system was running. The system is giving away too much information when it does crash. This information could be useful for future malicious attacks. All messages should be changed so that a generic error message is displayed when a problem is encountered.

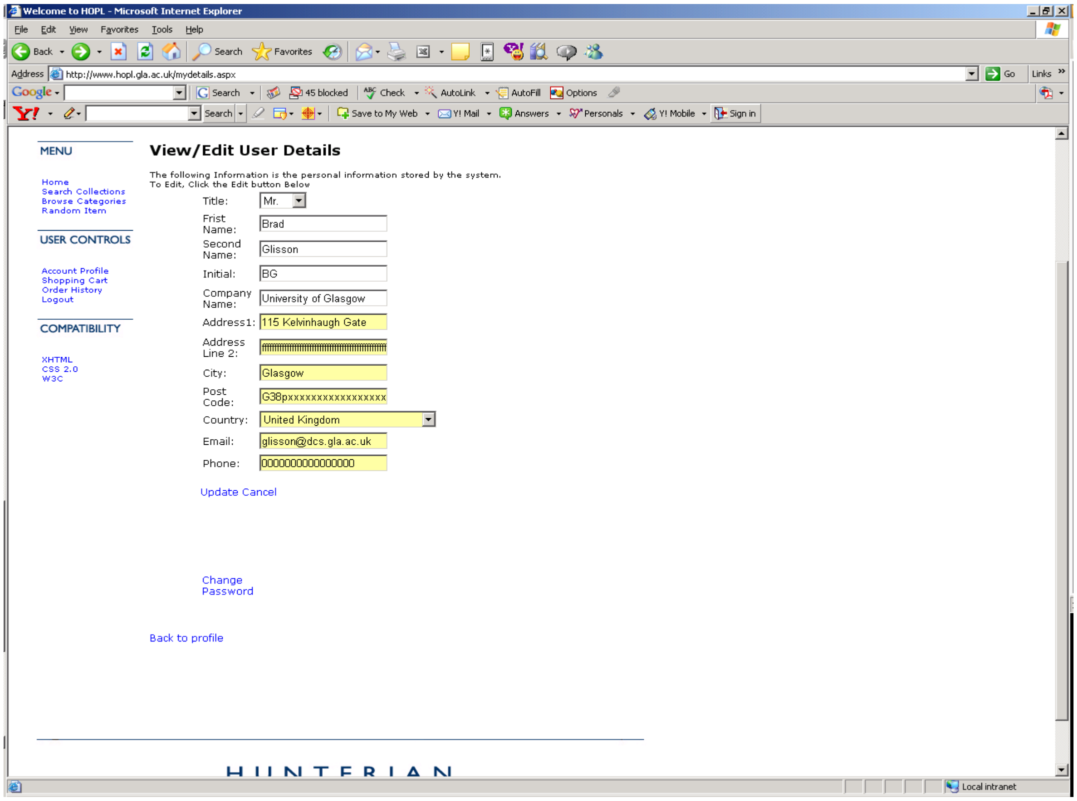
10.4.5.2 Second Problem - Unhandled Expression

The steps are as follows:

- Registered
- Modified the post code line

- G38pxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx; select * from user;
- Clicked update

Figure 9 - Hunterian Screen Shots Error Number Two



Welcome to HOPL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.hopl.gla.ac.uk/mydetails.aspx
Go Links
Google Search 45 blocked Check AutoLink AutoFill Options
Y! Search Save to My Web Y! Mail Answers Personals Y! Mobile Sign in
MENU
Home
Search Collections
Browse Categories
Random Item
USER CONTROLS
Account Profile
Shopping Cart
Order History
Logout
COMPATIBILITY
XHTML
CSS 2.0
W3C
HUNTERIAN
Local intranet

View/Edit User Details

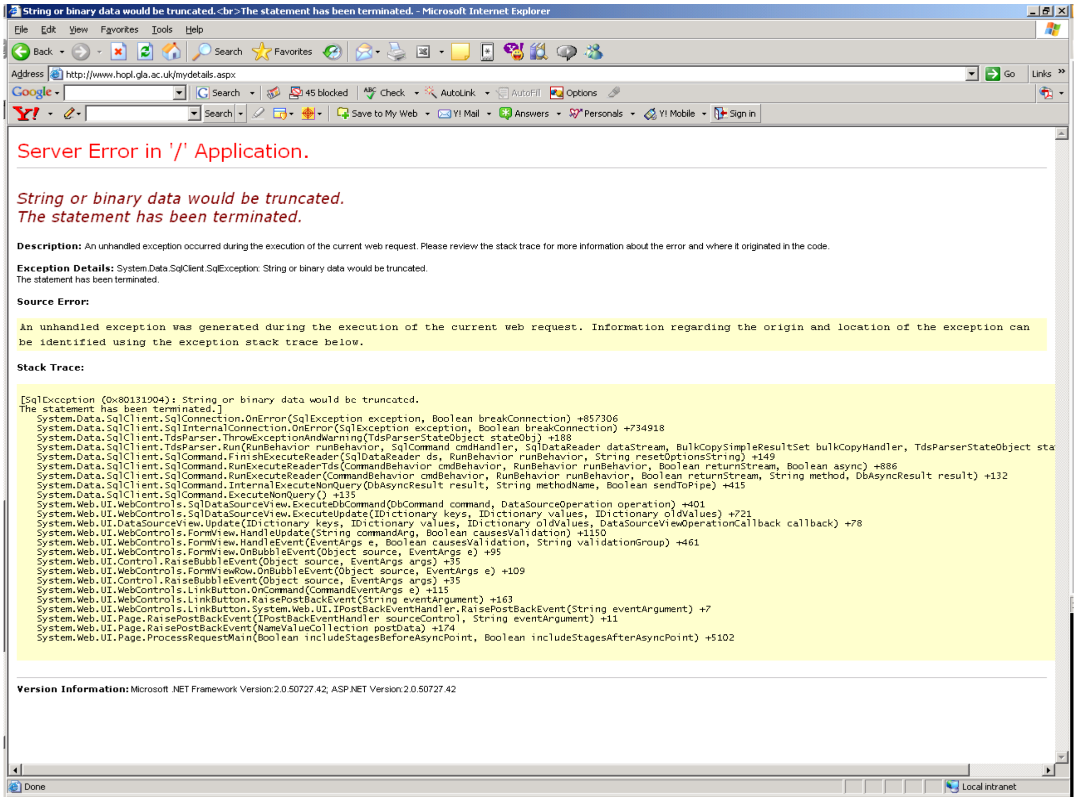
The following Information is the personal information stored by the system.
To Edit, Click the Edit button Below

Title:	Mr.
Frist Name:	Brad
Second Name:	Glisson
Initial:	BG
Company Name:	University of Glasgow
Address1:	115 Kelvinhaugh Gate
Address Line 2:	ffffffffffffffffffffffffffffffffffffffffffff
City:	Glasgow
Post Code:	G38pxxxxxxxxxxxxxxxxxx
Country:	United Kingdom
Email:	glisson@dcs.gla.ac.uk
Phone:	0000000000000000

Update Cancel

Change Password

Back to profile


String or binary data would be truncated.
The statement has been terminated. - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://www.hopl.gla.ac.uk/mydetails.aspx
Go
Links
Google
Search
45 blocked
Check
AutoLink
AutoFill
Options
Y!
Search
Save to My Web
Y! Mail
Answers
Personals
Y! Mobile
Sign in
Done
Local intranet

Server Error in '/' Application.

String or binary data would be truncated.
The statement has been terminated.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: String or binary data would be truncated.
The statement has been terminated.

Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can
be identified using the exception stack trace below.
```

Stack Trace:

```
[SqlException (0x80131904): String or binary data would be truncated.
The statement has been terminated.]
   System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) +857306
   System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) +734918
   System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) +188
   System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject sta
   System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString) +149
   System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async) +886
   System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, DbAsyncResult result) +132
   System.Data.SqlClient.SqlCommand.InternalExecuteNonQuery(DbAsyncResult result, String methodName, Boolean sendToPipe) +415
   System.Data.SqlClient.SqlCommand.ExecuteNonQuery() +135
   System.Web.UI.WebControls.SqlDataSourceView.ExecuteDbCommand(DbCommand command, DataSourceOperation operation) +401
   System.Web.UI.WebControls.SqlDataSourceView.ExecuteUpdate(IDictionary keys, IDictionary values, IDictionary oldValues) +721
   System.Web.UI.DataSourceView.Update(IDictionary keys, IDictionary values, IDictionary oldValues, DataSourceViewOperationCallback callback) +78
   System.Web.UI.WebControls.FormView.HandleUpdate(String commandArg, Boolean causesValidation) +1150
   System.Web.UI.WebControls.FormView.HandleEvent(EventArgs e, Boolean causesValidation, String validationGroup) +461
   System.Web.UI.WebControls.FormView.OnBubbleEvent(Object source, EventArgs e) +95
   System.Web.UI.Control.RaiseBubbleEvent(Object source, EventArgs args) +35
   System.Web.UI.WebControls.FormViewRow.OnBubbleEvent(Object source, EventArgs e) +109
   System.Web.UI.Control.RaiseBubbleEvent(Object source, EventArgs args) +35
   System.Web.UI.WebControls.LinkButton.OnCommand(CommandEventArgs e) +115
   System.Web.UI.WebControls.LinkButton.RaisePostBackEvent(String eventArgument) +163
   System.Web.UI.WebControls.LinkButton.System.Web.UI.IPostBackEventHandler.RaisePostBackEvent(String eventArgument) +7
   System.Web.UI.Page.RaisePostBackEvent(IPostBackEventHandler sourceControl, String eventArgument) +11
   System.Web.UI.Page.RaisePostBackEvent(NameValueCollection postData) +174
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5102
```

Version Information: Microsoft .NET Framework Version:2.0.50727.42; ASP.NET Version:2.0.50727.42

Unhandled expressions suggest that there is the possibility for successful SQL injection attacks. As mentioned in chapter four, SQL injection attacks are one of the more popular vulnerabilities that hackers like to exploit. The second address line in the user detail page was flooded with text; however, text entered at the end of the input field was not random text. This part of the input was constructed using the Structured Query Language (SQL) and attempted to retrieve data from one of the database tables. The actual query was not successful. However, the page that was returned to the user of the system provided information that could be used against the system in future attacks. This information included the error statement, information that could be used to help determine the database platform and to what extent the system executed the SQL code. Hence, code that explicitly handles specific exceptions and general Web errors needs to be implemented in all production code to alleviate this issue. Again as noted in the first problem, there is too much information being given away when the application fails.

10.4.6 Trust and Accountability

The Hunterian accepted and implemented the suggestion to implement the payment solution via PayPal. There are several reasons for using PayPal as the payment service provider. These reasons range from marketability, to code practicality, to security. PayPal is a world wide organization that is recognized as a legitimate payment service by the global public with over one hundred million account members worldwide [145]. PayPal has been very successful at establishing itself as a technology leader in the area of payment solutions, receiving several awards for technical excellence [145]. Since HOPL is geared to the general public it is wise to use such a provider.

More importantly, it is an even wiser decision from a coding and a security perspective. PayPal provides excellent reference materials along with a development center for developers. The development center is a sandbox area constructed so that developers can test their code before going live. The developer documentation also goes into detail on the encryption of Website payments. This information even provides a reference link to developers for creating their own certificates. The recommendation was for the Hunterian, if they had time, to encrypt the payment. If they did not have the time to figure out the encryption piece of the code, then they should use the PayPal configuration for the exchange of the payment information and the encryption could be added later. The developers took the security issue on board and implemented an encrypted payment system with PayPal.

Overall, the PayPal services were highly utilized by Hunterian's developers in the design of the payment aspect of the HOPL system. This includes developing the code necessary to encrypt the transaction information before it is sent to PayPal and configuring HOPL to act accordingly upon the automated response from PayPal. The way HOPL is constructed it actually waits for a real-time response from PayPal before allowing a customer to proceed. This is an excellent feature for HOPL and provides a level of security in the payment transaction that is beneficial for the organization. Another security feature that was built in, from the perspective of accountability, is the notification to the developer when anyone other than PayPal attempts to post to the PayPal response page. The use of the public and private keys helps establish trust between the Hunterian system and the PayPal system. This trust is supported by the fact that the Hunterian system enforces accountability through the system log-in process that has to take place prior to an order being placed. This meets the SCWAD for trust and accountability.

10.5 Summary

The business idea behind the project is to enable the Hunterian to display water marked images on the Internet and sell high quality versions of those images over the Internet. This includes the ability to conduct payment transactions on-line and, on successful payment, allow the end-user to download images. The application of the Essential Elements establishes the context of the development environment. All of the elements revealed potential areas of improvement.

The application of the Security Criteria for Web Application Development (SCWAD) demonstrates that there are strengths and weaknesses in the Hunterian's application development process. The strengths and weaknesses can be viewed as lessons learned. SCWAD identified Active Organizational Support, Security Visibility, and Trust and Accountability as overall strengths within the current application development process. The organization supports the implementation of security and it is visible through most of the development process. Minor improvements can be made in the security visibility in that the developers could initiate contact without the prompting of the project manager. The organization did very well with the Trust and Accountability aspects of the project. They established the need in the requirements phase, designed the solution appropriately and tested the trust and accountability aspects of the solution to the best of their ability from a resource perceptive.

SCWAD also recognized areas within the development process that provide an opportunity for improvement. The opportunity for improvement exists within Proper Controls in the Development Environment and Prompt, Rigorous Testing and Evaluation. There is the opportunity for improvement in the policy, knowledge and process sections of the Controls segment of SCWAD. The organization needs to consider moving from an implicit style of operation to an explicit style of operation. Vast improvements can be made in the Testing and Evaluation segment through the involvement of end-users. Another area in which there is opportunity for overall improvement is the delivery of a cohesive system integrating business requirements, software and security. While the museum does a good job of integrating the business requirements into the software, the previous issues demonstrate that there are improvements that can be made with the integration of the business requirements, the software and security.

This exercise illustrates the fact that security is a trade-off with financial resources, human resources, the employee knowledge base and time resources during the development project. The use of the Essential Elements and the Security Criteria for Web Application Development (SCWAD) can help identify potential security tradeoffs. Hence, the use of the Essential Elements and SCWAD can be used to establish the environmental context and analyze a development process helping organizations to make informed secure managerial decisions. The next chapter discusses the implementation of WES in a commercial environment.

11 Global Fortune 500 Financial Service Case Study

Chapter five presented evidence that the financial service sector organization, that employed the author during his PhD internship, faces multiple issues with application development security integration. The financial organization presented an excellent opportunity for testing the WES methodology due to the natural concern for security in the financial industry. Section 11.1 presents the initial background information for the commercial implementation of WES via a Security Improvement Initiative (SII) in a Global Fortune 500 financial organization. Section 11.2 demonstrates how WES was applied to the organization's existing application development environment. Section 11.3 presents the SII implementations that were executed within the organization. Section 11.4 examines the quarterly analysis of the assigned security conditions within the development process. Section 11.5 presents the results of a follow up survey with that organization's staff. Section 11.6 examines the Design Architecture Documents (DAD) versions along with the information that was actually captured in the documents. Section 11.7 examines the implementation obstacles that were experienced during this case study and section 11.8 summarizes the chapter.

11.1 Security Improvement Initiative (SII)

An internship was accepted, from July 2005 through August of 2006, with a Global Fortune 500 financial services organization with the objective of conducting a Security Improvement Initiative (SII) in a commercial environment. As of July 2004, the company was listed in the top fifty Global Fortune 500 financial services organizations [69]. The internship agreement consisted of examining the organization's security practices throughout the development process and making recommendations to the organization on how to strengthen process security. Although the organization appeared to be supportive of the security initiative, there was no guarantee that the organization would accept the recommendations or implement the changes into the production environment.

The SII was conducted in the following manner. As discussed in 5.3, in order to gain a better understanding of the security within the organization's development process a survey was conducted. The analysis of the survey responses provided answers to the Essential Elements and established the Security Criteria for Web Application Development (SCWAD). The WES methodology was applied to the observed development process. Several recommendations were made to the organization and some of the recommendations were accepted. The accepted recommendations were implemented into the production environment. This directly affects all large application development projects implemented by the United Kingdom arm of the organization. In order to acquire data, changes to this process were held to a strict minimum from October, 2005 through August of 2006.

In order to encourage open communication during the SII, the name of the organization is being withheld to ensure organizational anonymity. Following this idea, the names of the documents, the names of the processes and the names of the groups have all been altered. The results of all interviews are presented anonymously. Maintaining organizational anonymity facilitates the exchange of accurate information and creates an environment where all parties are comfortable presenting commercially sensitive information.

The organization develops and supports Web applications. As noted in chapter nine, there are a variety of methodologies that can be used to develop Web applications that range from agile processes to traditional plan driven software engineering processes. This organization uses a customized plan driven document centric waterfall approach when conducting Web application development and all other forms of software based initiatives. Within this process approach the business comes up with an idea and develops a business case to support the project. Once the business case is accepted, then, a project manager is assigned to the project.

The project manager contacts the necessary personnel to have resources assigned to the project. In general, these individuals include the architect and possibly a project risk analyst. The architect is responsible for completing a Design Architecture Document (DAD) and presenting it to the Design Architecture Committee (DAC). There are eight voting members on this committee, all have veto authority. If any of the members on the committee vetoes the project, then, the design is rejected and has to be resubmitted with identified committee objections addressed. It should be noted that all of the members had established their seats on the board months before the SII was initiated. It should also be noted that a preliminary DAD (PDAD) could be constructed in the Initial Design stage for early feed back, however, this was rare. Most projects skipped the PDAD in the design phases going straight to the construction of the DAD.

Based on member voting, there are three possible outcomes when a DAD is submitted to the DAC. First, the DAD could be accepted by the committee. Second, the DAD could be accepted by the committee with conditions, or third, the DAD could be rejected. Once the design is approved, then the coding teams produce a Detail Design Document (DDD) based on the DAD. The DDD in this organization was actually completed by the programmers and then the design was built, tested and implemented into the production environment under the governance of the architect.

All of the voting members have the right to assign conditions within their area of expertise. If a DAD is accepted with conditions, then these conditions must be satisfied prior to progression into the next stage, which in this case would be the build stage. An interesting gauge to examine the effects of security on the overall development process is the quarterly analysis of the assigned security conditions.

11.2 Web Engineering Security (WES) Methodology Implementation

Seamless security integration into an organization's existing development process and environment is desirable in order to maximize existing core competencies while providing a road map for areas that need to be strengthened. As discussed in chapter seven, the Web Engineering Security (WES) methodology is a development process independent solution designed to address the lack of security that is inherent in application development methodologies. The initial survey conducted in the Global Fortune 500 organization, discussed in chapter five, helped to attain an understanding of the development process and the role security plays within that process. The recommended changes were based on the application of the WES methodology.

The organization has customized the individual phases within this approach by subdividing them into stages. The application of the WES developmental methodology to the current environment is shown in Table 30. This table reveals how the process should operate by outlining the project phases of the application development life cycle, the associated generic project stages, and the phases of the WES methodology. The section of the table titled 'WES Applied Project Stages' specifically details the integration of the WES methodology with the company's generic project stages. The application of the WES methodology is conducted in conjunction with the knowledge derived from the survey. Since WES is a flexible methodology it can be tailored to suit the needs of an existing organization. In this case, aspects of the WES stage Security Design / Coding were split into two separate stages which were Security Design and Security Coding.

The application of WES reveals the opportunity to investigate and possibly propose multiple changes in the development process. The group most receptive to the idea of changes to the development process was the architecture group. The Design Architecture Document (DAD) is the primary instrument utilized by the architecture team in the organization. Hence, the logical place to implement changes is the DAD.

It should be noted that the WES methodology does not mandate deliverables from the individual areas within the methodology. The methodology lets the organization determine what is appropriate based on the size of the organization, the application development methodology that is being utilized and the corporate culture. In this particular case study, the organization is already pro-documentation. Hence, the feasible approach is to expand the current documentation so that it incorporates the new security functionality. The organization already produces a Business Case Document (BCD), Design Architecture Document (DAD), a Detail Design Document (DDD) and Testing Documentation (TD).

11.2.1 Project Development & Risk Analysis

During concept development, the Project Risk Analyst conducts a risk analysis. The Project Risk Analyst should also be speaking with the architect and the appropriate coding teams in order to determine the project risk and help the business unit develop the project's business case. The results of the survey support the need for early interaction between the business unit and the technical side of the organization. An issue that should be addressed during the risk analysis is the risk compatibility.

The application of the WES methodology indicates that the risk analysis should be determining critical functionality within the application, determining appropriate service levels, identifying all possible threats, the probability of attack, the probability of success and the cost associated with the desired level of protection [154]. All of the stakeholders, i.e., the architect, project manager, coding team representative, sponsor, and business unit representative should have input into the creation of the business case document. Realistically, the business unit representative should probably be the driver for this interaction.

11.2.2 Application Security Requirements

One of the ideas behind generating the risk assessment in the very beginning is so that this can be used to stimulate the conversations around requirements gathering. When the business requirements are being gathered, members of the business unit should be interacting with the project manager, the architect, a project risk analyst, and members from appropriate coding teams. The thought behind this diverse group interaction is to facilitate the gathering of a fairly comprehensive listing of the security requirements. Specific security requirements explicitly recognize all of the security requirements from the business unit so that they can be addressed successfully. The security requirements should identify specific environmental requirements along with addressing confidentiality, integrity and availability. Once the security requirements are gathered, they should be examined from a critical perspective in order to determine how they will comply with the organization's security policy, corporate culture and technology compatibility.

Table 30 - WES Application

Project Phases	Generic Project Phases	WES Stages
Initiate & Assess	Idea	**Project Development Risk Assessment** *(Cost / Risk / Effort / Probability of Success)* • Data Protection Legislation, Attack Trees • Risk Analysis Techniques
	Concept Development	
	Business Case (BCD)	
Design	Business Requirements	**Application Security Requirements** *(What needs to be secured & for how long for this specific project?)* Organizational Compatibility • Security Policy Compatibility • Corporate Culture Compatibility • Technological Compatibility
	Initial Design (PDAD)	**Security Design** *(Effectively Secure Individual Security Requirements)* • Satisfactorily address risk identified in risk assessment and application security requirements • Verify security requirement compliancy with organizational compatibility • Establish intended use of W3C Standards, Coding Practices • Describe the Establishment of Secure Data, Establishment of Accountability & Trust • State the use of Standards (Encryption, Architecture, Infrastructure) • Security verification of project viability
	Initial Technical Evaluation (DAC)	
	Design Architecture Document (DAD)	
	Technical Evaluation (DAC)	
Build	Construction (DDD)	**Security Coding** *(Effectively Secure Individual Security Requirements)* • Implement W3C Standards, Coding Practices, Code Reviews • Secure Data, Establishment of Accountability & Trust, • Utilization of Re-usable Components
	Testing	**Controlled Environment Implementation** • Application Environmental Compatibility • Regression testing • Load Testing
		Testing *(Prompt, Rigorous, Security Testing and Evaluation)* • Application Testing • Verification of risk and requirements satisfaction • Incident Management • Disaster Recovery Management
Implement	Implementation	**Deployment in Production** • Personnel Availability • Production Deployment Verification
Feedback	Feedback	**End User Feed Back** • Usability Feedback • Appropriateness Feedback • Patching

11.2.3 Security Design

Once the security requirements have been ascertained and they have been examined in reference to the security policy, corporate culture and technology compatibility, then the design should take place with this information in mind. The proposed design improvements concentrated on the architecture team's main instrument for creating solutions, which is the Design Architecture Document (DAD). The following changes were proposed to the design process and some of which are reflected in the DAD.

1. Owner / Creator Contact Information
2. Conversation Checklist for Security Requirements Gathering
3. Signature Section
4. Risk Compatibility Section
5. Identity Management
6. Threat Management
7. Trust Model
8. DAD Socialization

Owner / Creator Information

The idea behind capturing the owner-creator information, the conversion checklist for security requirements gathering, and the signature section, is not only to expedite communication but to assign accountability. Regardless of the existence of questions around various topics in the document, it is necessary to assign ownership of the proposed architecture solution. The owner / creator information tells anyone, who picks up the documented solution, who created the solution's architecture.

Conversation Checklist for Security Requirements Gathering

The conversation check list, for security requirements gathering, helps aid the project manager to ensure that all of the necessary parties are involved in the creation of the DAD and in the overall project. This should be the responsibility of the project manager. However, the survey and observation alludes to the fact that the skill level among the project managers in the organization varies widely. The goal of having the conversation checklist for the security requirements is that there is increased communication with the project members encouraging a higher level of security awareness.

Signature Section

The proposed signature section consisted of three names: the project manager, the individual in the business unit who was responsible for signing off on the business requirements, and the individual on the DAC who is responsible for matching the design to the actual production product. The project managers should be included in the DAD since the document is being created at their request. The inclusion of the project manager in this process will help educate management on the design process and help foster solution buy-in; including the name and the contact information for the individual who is responsible for providing approved user requirements helps to encourage communication when there are questions and to assign responsibility. The DAC signature should list the individual (and their contact information) who has agreed to follow up on the proposed application to verify that the application being delivered is the same as the application that was proposed in the design submitted to the DAC. This signature provides member and application accountability to the DAC.

Risk Compatibility Section

The idea behind the Risk Compatibility section stage is to ensure that the security design proposed by the architect is compatible with the Risk team's policy requirements. A Risk Compatibility section examines tier trust policy compatibility, proposed low level security practices, and data security.

> "A trust model is a tool that helps one visualize and understand the degree of confidence that is intentionally or unintentionally granted to individuals, computer networks, and systems, based on the associated risks that are inherent with granting this confidence" [181].

A tier trust model is a model that consists of one of more levels such as an Internet tier, a DMZ tier, and an intranet tier. The model would then state the interaction between the defined tiers. The trust model contributes to the foundation for the policies that are put into place in an organization. Hence, applications can be applied to the policies or the trust model in order to determine compliancy where trust is concerned. The reality is that both should be checked for each solution so that there is a system of checks and balances. This ensures that the solution is compatible with the organization trust model and policies, while verifying that there are no discrepancies between the policies and the trust model.

The trust model compliance can be examined from two perspectives. The first is the network architecture perspective and the second is the application architecture perspective. The architect would need to learn the organization's network architecture trust model and the application trust model. An assessment of an organization's trust models naturally leads to a discussion about new application integration into both architecture models making sure to identify any violations to the model and the acquisition of appropriate exception authorizations.

Figure 10 provides a network model for discussion purposes. An example of an Internet network trust model could look something like this:

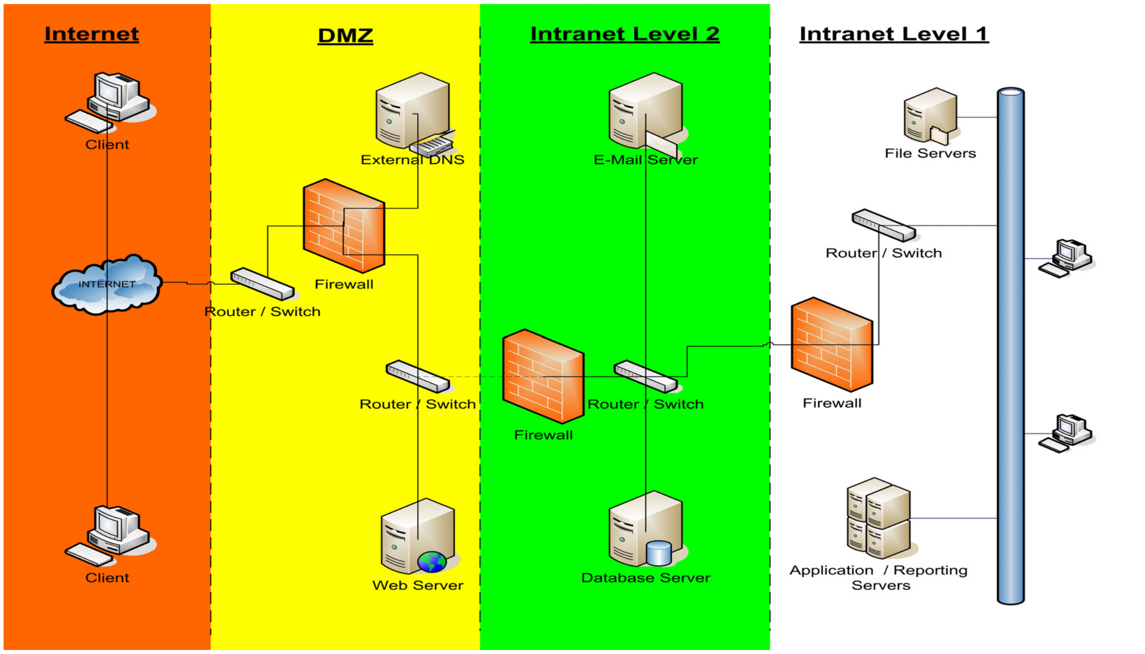
- Outside Internet traffic must pass through approved ports
- The Internet network must implement direct trust.
- All users must be identified and authenticated.
- Trust and authentication can never be implied or assumed.
- No transitive or assumptive trust can exist between any component of the organization's computing environment and any external system.

- Uniquely identified and authenticated entities may only be trusted to access data and resources on a predefined need-to-know basis.
- All data transferred between the organization and an authenticated user must be encrypted.
- Internet clients can only access DMZ servers
- DMZ servers can only access specifically defined Intranet Level 2 servers
- Data must be pulled from all Level 2 Servers to Level 1 Servers and Clients, i.e., no data can be pushed lower than Intranet Level 2.
- Application users on the network are established and maintained via the organizations' Identity Management (IM) System

Examples of the issues that the application should address would include:

- Assurance that the application does not violate the Internet network trust model
- That the applications use the organization's Identity Management (IM) system and, if not, explains why not and acquires the necessary exception
- How does the application establish direct trust?
- How does the application maintain trust?
- Does the application implement proper encryption policies? Do these policies comply with the Internet network trust model?

Figure 10 - Network Model



Another point that surfaced with the application of the WES methodology is an overview of the application and the impact on the organization's low level security practices. The idea behind identifying the proposed low level security practices is to ensure that the application's low level practices are compatible with established security policies. If they are not compatible, then, they have to be acknowledged appropriately. Example: An application that has to have access to the kernel level of a UNIX box would need to be acknowledged via an appropriate risk analysis. If the risk is deemed a necessary risk then the appropriate exceptions would have to be sought and granted within the organization.

The thought behind data security is that the organization needs to identify any sensitive data held within the proposed system design. The organization also needs to document that this data is being protected by successfully addressing appropriate risk in reference to encryption policies, transaction policies and storage policies.

Identity Management

Identity is a key factor in establishing and maintaining the security of a system. The physical world places multiple meanings on the term ‘identity’ depending on the context to which it is applied [137]. These meanings include everything from names, to addresses, to financial information, to citizenship [137]. “ ‘Digital identity’ is, at the core, an effort to recreate, organise, automate and integrate all those aspects in the online electronic world and (increasingly) link them to existing ‘offline’ identities”[137]. Hence, Identity Management (IM) has the potential to impact business processes, policies and the organization’s technology in order to attempt to provide access and user control to Web applications.

> “In this context, identity management is also a key e-business enabler: being able to recognize the digital identity of people and Web services, to understand, manage and validate their profiles and rights is fundamental in order to underpin accountability in business relationships and enable commercial transactions” [137].

As far as the organization is concerned, IM should be viewed as a re-useable component within the organization. Under the IM heading, architects should be addressing issues such as role based access and controls, authentication and authorization, user provisioning, access and control to environments, and audit and archive design.

Threat Management

Threat Management attempts to identify all of the known threats to the proposed solution and how these threats are being mitigated. This solution should also take into consideration interaction with existing software like host-based intrusion detection systems, network-based intrusion detection systems, firewalls, and antivirus software. Another area that needs attention is the use of any compliance tools that are being utilized by the organization and the solutions compatibility.

Trust Model

Trust is critical when establishing security. The architect should describe how trust will be established and maintained between the various application tiers. Another issue that needs to be addressed is how deep a user’s identification (id) can be traced within the application. This helps the organization identify a level of risk that it is willing to live with when it comes to identifying the actions of a user.

DAD Socialization

The organization has an interesting environment where the architect is supposed to formalize their solution with all of the members of the group. To formalize a solution with the members of the Design Architecture Committee (DAC) means that the architect meets with each member individually to discuss the proposed solution. This gives the architect and the group member the opportunity to work out any issues prior to the formal DAC meeting. However, observation indicated that this was not taking place effectively. The proposed solution to the problem is built on the idea that improved communication improves overall security. Hence, a mandatory socialization table that included the names and titles of all of the voting members of the DAC was implemented in the Design Architecture Document (DAD).

11.2.4 Security Coding & Controlled Environment Implementation

In the area of secure coding, the following recommendations were made: capture authentication and authorization techniques, implementation of coding standards and practices, identification of re-usable components and recognition of the information that needs to be secure along with the proposed encryption solution. Controlled environment implementation takes place in the testing area of this organization.

11.2.5 Testing & Deployment in Production

The organization, overall, appeared to be pretty adept at testing Web facing applications. The issue raised by the survey was in regard to the time involved to complete this task. The survey indicated that there are potential gains to be made by the organization from a time-to-market perspective. Hence, implementing dual testing units to shorten time windows would be advantageous from a time-to-market perspective.

11.2.6 End-User Feedback

End-user feed back, in the case of application security, is critical to the success of the application. The survey indicated that, realistically, there was very little feedback from end-users on the success of an application and no feed back specifically on security. The recommendation was made that the organization needs to start interfacing with the end-user to establish the effectiveness of the security implemented in their applications.

11.3 Security Improvement Initiative Implementations

As discussed in the previous section, several recommendations were made based on the application of the WES methodology. Some of these recommendations included identifying areas for additional in-depth analysis. The group that was receptive to process improvements and exploring the information attained from the application of the WES methodology was the Architecture Design group. The main tool used during the development of a design is the Design Architecture Document (DAD). Recommendations were made to the organization to improve the DAD. The changes to the DAD went through the same formalization and DAC approval process as all other projects. Some of the recommendations were accepted and implemented. Updates to the DAD template were frozen from October of 2005 to August of 2006 with two exceptions. A paragraph was added to the document in April. This paragraph specifically asked the architects to identify any situations where a new design touched a system that was being sold to another financial institution. This paragraph is available in Appendix IX. One line was added to the document in May notifying architects that the security non-functional requirements and documentation were now available in the Organization's General Site (OGS). It should be noted that this information was previously available from the risk group; it was just not in the OGS. Nothing else was changed in the document. The recommendations that were accepted and implemented include:

- A new security section that specifically recognizes the following security areas:
  - Identity Management
  - Threat Management / Compliance
  - Trust Model
- A new table to record assigned DAC Conditions
- A modified record of DAC Socialisation

The sections that were added to the document are included in Figure 11.

Figure 11 - DAD Updates

Security Design (Security Model Overview)

The purpose of this section is to describe the Security Model with direct reference to Identity Management, Threat Management and Trust Model between each tier of the proposed solution. See Contact Name (Architecture Team Member) and the Information Security Analyst's Team for guidance throughout this section. Each section requires attention regardless of the implementation of an internal or external solution.

Identity Management

The purpose of this section is to describe how the proposed solution will utilise the organization's Identity Management infrastructure for Access Control and User Credential management. Describe how the user identities are being managed and used within the solution. Reference should be made to the relevant Identity Management components, i.e. IBM's Tivoli Access Manager (for Access and Control); IBM's Tivoli Identity Manager (for User Provisioning) and Computer Associates' eTrust Directory (for directory services). For more information regarding the Identity Management infrastructure and its capabilities, refer to the "Identity Management Architecture: Principles, Policies & Standards" document or contact Employee Name (Title).

- Role Based Access and Control (RBAC)
- Authentication and Authorisation
- User Provisioning
- Access & Control to Environments
- Audit and Archive Design.

Note: Identity Management should not be limited to browser based applications.

Threat Management / Compliance

- List any known threats to the proposed solution and how these are being mitigated. Reference where relevant Threat Management software can help to counteract or reduce known or perceived threats, i.e., state how these interface with existing software like Network Intrusion Detection System (NIDS), Host based Intrusion Detection System (HIDS), Anti-Virus, Application and OS firewall, patching routers, and network appliances, etc. See *Employee Name* (Security Team for more details on the Threat Management systems portfolio).
- List all of the compliance tools in this section that are being utilized

Trust Model

- Within and between each tier, in the proposed architecture, describe how trust will be established between each application component.
- Describe how the trust model will be maintained.
- Layer Traceability

Figure 11 - DAD Updates - Continued

DAC Conditions

List all of the conditions assigned by the DAC in the current DAD document.

Condition Number	Description	Stakeholders	DAC Due Date / Progress
e.g. C#	*A brief description of the design challenge to be addressed.*	*List the technology and business stakeholders required to resolve and agree solution to design challenge. e.g. Engineering rooms, etc.*	*DAC date for resolution and follow-up DAC presentation.*

Record of DAC Socialisation

Date	Stakeholder List	Summary	Actions
DD/MM/YYYY	*e.g. Brad Glisson*	*Overview of discussion.*	*Briefly list outcomes and any agreed actions*
Mandatory Socialization			
	Security - *Contact Name*		
	Infrastructure - *Contact Name*		
	Architecture - *Contact Name*		
	Networks - *Contact Name*		
	Vendor Relations *Contact Name*		
	Testing Services - *Contact Name*		
	Business Relations - *Contact Name*		
	Sarbanes-Oxley - *Contact Name*		
Additional Socialization			

11.4 Security Conditions Analysis

As a general indicator of the effectiveness of the Security Improvement Initiative (SII), all of the conditions assigned to new and existing projects from December of 2004 to August of 2006 have been captured for analysis. The numbers used in the observations are simply very general indicators as to the impact of the SII and nothing more. As discussed earlier, the internship consisted of five main stages that included an initial survey / process analysis design stage, a recommendation stage, an implementation and data gathering stage, a data analysis stage and a write up stage. The first two stages and the implementation aspect of the third stage were conducted from July, 2005 to October, 2005. The data gathering portion of the third stage was carried out from November, 2005 until the end of the project in August of 2006. The data analysis stage and write up stage ensued from that point. The security condition data collected during the data gathering stage can be analysed from two perspectives. The first perspective examines all of the security conditions that were assigned to projects that had a Web interaction. The second perspective examines all of the security conditions that were assigned to all projects regardless of Web interaction.

11.4.1 Web Interaction Project Analysis

The phrase ‘Web interaction’ is broadly used in this text to include projects that acknowledged the Web in some form or fashion. This would include everything from intranet applications, to Internet applications, to systems that connect to support back-end processes, to transferring data over the Internet, to data functionality for Web systems. There were a total of one hundred and twenty-five projects that were presented to the DAC during the life of the SII. Out of these projects, there were ninety-six projects that interacted with the Web.

The raw numbers indicate that the number of security conditions being assigned to projects declined in the period from December, 2004 to June, 2005. A possible contributor to the decline could be a decreased number of projects between the second and third periods. The number of projects that came through the Design Architecture Committee (DAC) during the June, July, August, 2005 period was less than half of the number of projects submitted in the immediately preceding and post periods. This could be a result of vacation schedules. Other possible reasons for the variation could include a decrease in the complexity of the projects that were being submitted, to variations in the skills of the individuals preparing the DAD, to substitute representatives participating on the committee for stakeholder groups. It should be noted that, even though there was a large dip in both the total conditions and the security conditions, the security conditions represent more than half of the total conditions that were assigned for that period. None of the other periods have security conditions representing half of the total conditions.

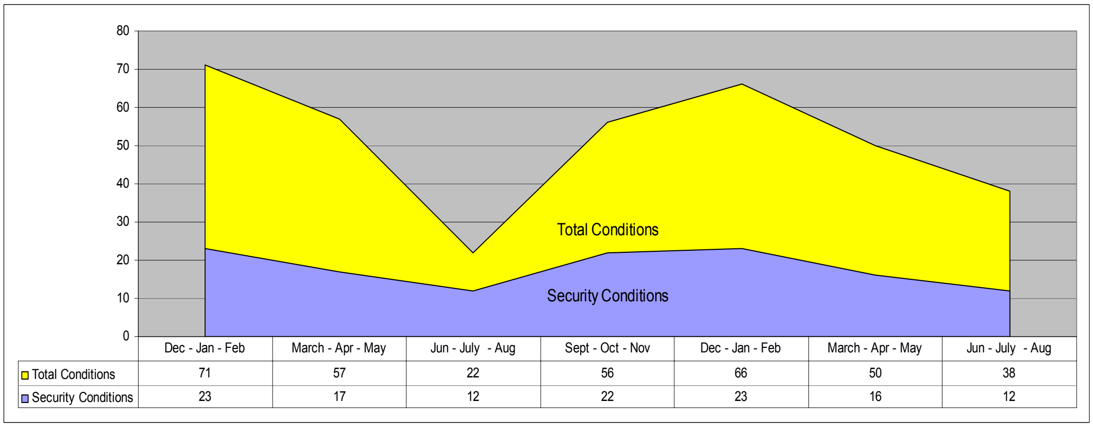
The security condition assignment climbs back into the twenties for the next two periods. Speculation on the return of the increased security conditions assignment for these two time frames could be that the Security Improvement Initiative (SII), which was started in July of 2005, raised the awareness of security to a level where more employees are making inquiries on the subject. An interesting observation is that the number of security conditions assigned to projects during the internship period appears to decline for the last two periods. The individual period numbers are given in Table 31 - Period Number of DAC Security Conditions to Web Interaction Projects and a graphical representation is available in Figure 12 - Period Number of DAC Security Conditions to Web Interaction Projects.

Table 31 - Period Number of DAC Security Conditions to Web Interaction Projects

Period	**3 Month %**	**Security Conditions**	**Total Conditions**	**Project Totals**
December 2004 January 2005 February 2005	32%	23	71	16
March 2005 April 2005 May 2005	30%	17	57	24
June 2005 **Started - July 2005** August 2005	55%	12	22	9
September 2005 October 2005 November 2005	39%	22	56	13
December 2005 January 2006 February 2006	35%	23	66	12
March 2006 April 2006 May 2006	32%	16	50	13
June 2006 July 2006 August 2006	32%	12	38	9

Note: Percentages are rounded to the nearest whole number

Figure 12 - Period Number of DAC Security Conditions to Web Interaction Projects

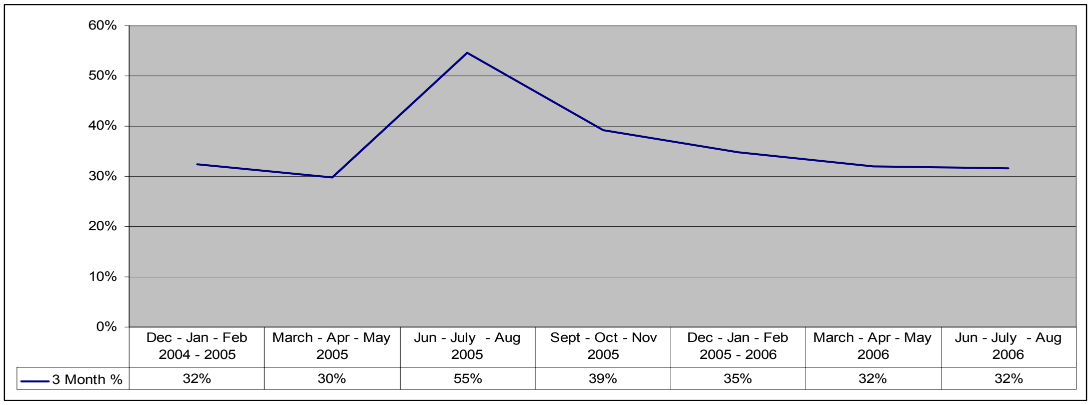


	Dec - Jan - Feb	March - Apr - May	Jun - July - Aug	Sept - Oct - Nov	Dec - Jan - Feb	March - Apr - May	Jun - July - Aug
🟨 Total Conditions	71	57	22	56	66	50	38
🟦 Security Conditions	23	17	12	22	23	16	12

Examining the security conditions as a portion of the total conditions presented an interesting perspective on the information. The numbers suggest that there was a slight decline and then a sharp rise in the assignment of security conditions in proportion to the overall conditions during the first three periods. The security conditions during the June, July, August, 2005 period represent over half of the total conditions that were assigned during that period. The security conditions, at this point, represent the highest proportion of the total conditions throughout the life of the SII. From the June, July, August, 2005 periods, the portion of security conditions, in comparison with the total conditions, declines through the May, 2006 period. The conditions appear to level off for the last period June, July and August of 2006. A graphical representation of this data is available in Figure 13 – Period Percentage of Security Conditions to Web Interaction Projects.

It should be noted that the examination of Figure 13 identifies another possible interpretation. It is equally possible that there is no increase in the overall assignment of the conditions over the life of the SII with a summer spike in the June, July, August period of 2005. This could be due to a raised awareness of security within the DAC or other activities taking place within the organization during that period. If it was simply a summer spike due to vacations, substitutions, etc., it is interesting to note that it does not appear to have happened in the same period in 2006.

Figure 13 - Period Percentage of Security Conditions to Web Interaction Projects



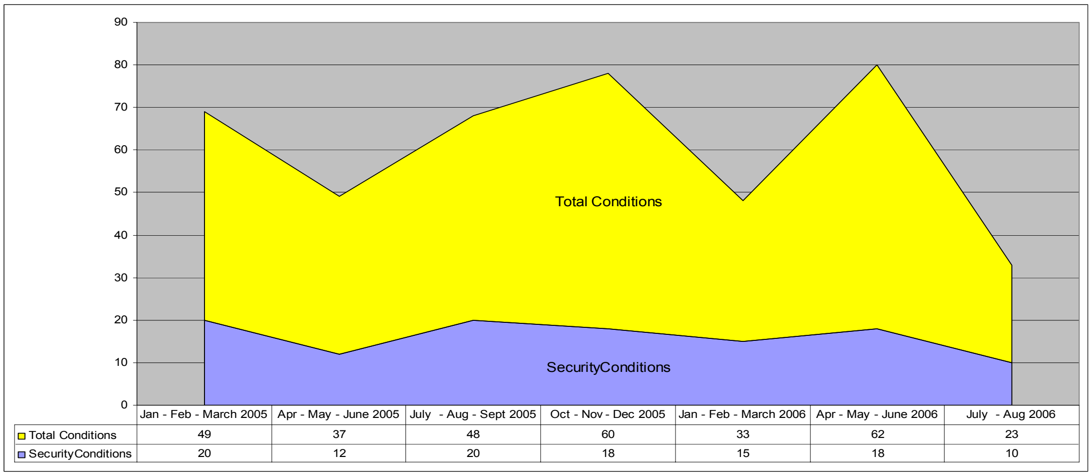
	Dec - Jan - Feb 2004 - 2005	March - Apr - May 2005	Jun - July - Aug 2005	Sept - Oct - Nov 2005	Dec - Jan - Feb 2005 - 2006	March - Apr - May 2006	Jun - July - Aug 2006
3 Month %	32%	30%	55%	39%	35%	32%	32%

If the data are examined from a traditional quarterly perspective, meaning that the December, 2004 data would not be included in the analysis, then the data tell a slight variation of the information previously presented. Also, it should be noted that there is no data for September in the third quarter of 2006. The lack of data for September means that the picture is incomplete from a quarterly perspective and that the period information probably presents a more accurate picture of the trends in the environment. The trends are less pronounced in the quarterly analysis of the data. The data are in Table 32 - Quarterly Security Conditions assigned to Web Interaction Projects. Graphical analyses of the data are available in Figure 14 - Quarterly Web Interaction Analysis and Figure 15 – Quarterly Percentage of Security Conditions to Web Interaction Projects. The quarterly percentage data present a more sporadic picture of the security conditions from period to period. It is interesting to note that there is an indication that the overall assignment of security conditions has actually risen during the life of the SII.

Table 32 - Quarterly Security Conditions assigned to Web Interaction Projects

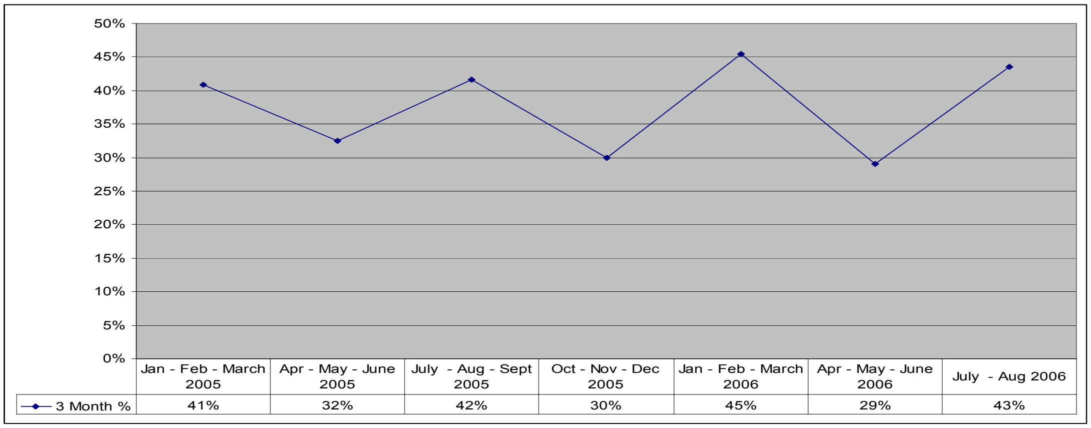
Quarter	3 Month %	Security Conditions	Total Conditions	Project Totals
January 2005 February 2005 March 2005	41%	20	49	20
April 2005 May 2005 June 2005	32%	12	37	13
Started - July 2005 August 2005 September 2005	42%	20	48	13
October 2005 November 2005 December 2005	30%	18	60	12
January 2006 February 2006 March 2006	45%	15	33	10
April 2006 May 2006 June 2006	29%	18	62	13
July 2006 August 2006	43%	10	23	6

Figure 14 – Quarterly Web Interaction Analysis



	Jan - Feb - March 2005	Apr - May - June 2005	July - Aug - Sept 2005	Oct - Nov - Dec 2005	Jan - Feb - March 2006	Apr - May - June 2006	July - Aug 2006
🟨 Total Conditions	49	37	48	60	33	62	23
🟦 SecurityConditions	20	12	20	18	15	18	10

Figure 15 - Quarterly Percentage of Security Conditions to Web Interaction Projects



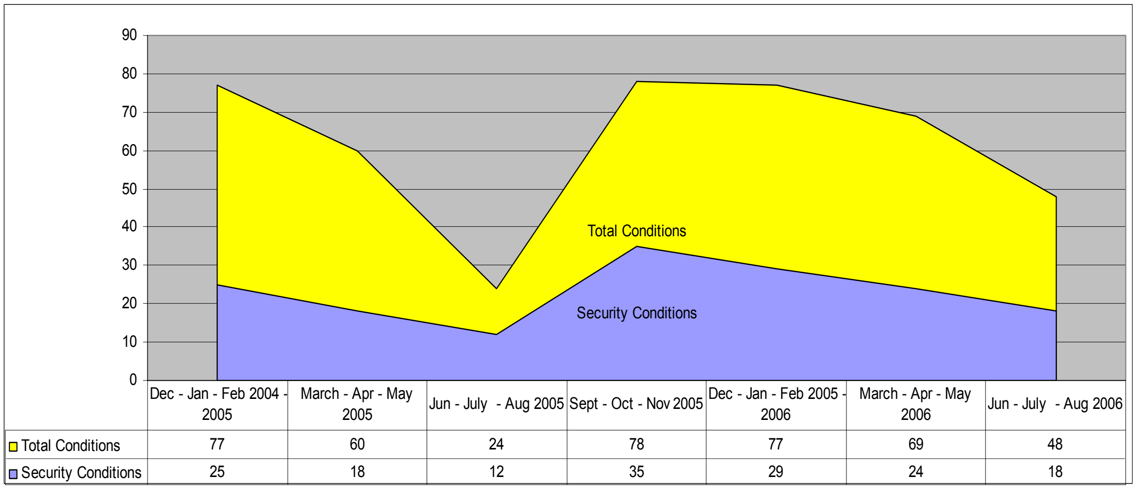
11.4.2 Overall Projects Analysis

The reality of the situation is that the changes that were introduced into the organization affected all of the projects that were brought before the DAC. Couple this information with the fact that the majority of the projects (96 out of 125) had some form of Web interaction indicates that it is appropriate to examine the overall impact of the changes implemented through security condition analysis. The first three periods mimic the information provided by the Web interaction analysis in that there is a decline and then a rise in both the number of security conditions and total conditions assigned to projects. The rise in both conditions is more pronounced in the overall analysis. An interesting observation is that the number of security conditions assigned to projects over the internship period appears to continuously decline starting with the September, October, November, 2005 period. The individual period numbers are given in Table 33 - Period Number of Security Conditions assigned by DAC to Projects and a graphical representation of the numbers is available in Figure 16 - Period Number of Security Conditions assigned by DAC.

The implication is that the security conditions were having an impact on projects prior to changes being implemented into the development environment. The changes that were introduced into the development environment were initiated as a result of the SII. The impact of the SII changes to the development process started in the September, October, November period of 2005 which corresponded with the start of a trend in decreasing security conditions being assigned to projects by the Design Architecture Committee (DAC) and that this appears to be a positive indicator of the impact of the SII.

Examining the data from the perspective of comparing the number of security conditions to the total number of conditions assigned for each period indicates that the impact of the SII actually started prior to the introduction of the changes to the DAD. A graphical representation is provided in Figure 17 - Period Percentage of Security Conditions assigned by the DAC. Again, due to the qualitative nature of the data and small sample sizes, it is stressed that this information provides a general indication of the impact of the SII and nothing more. Examining the information presented in Figure 17 indicates that there could actually have been an increase in the overall number of security conditions assigned to the projects by the DAC for the life of SII.

Figure 16 - Period Number of Security Conditions assigned by DAC to Projects

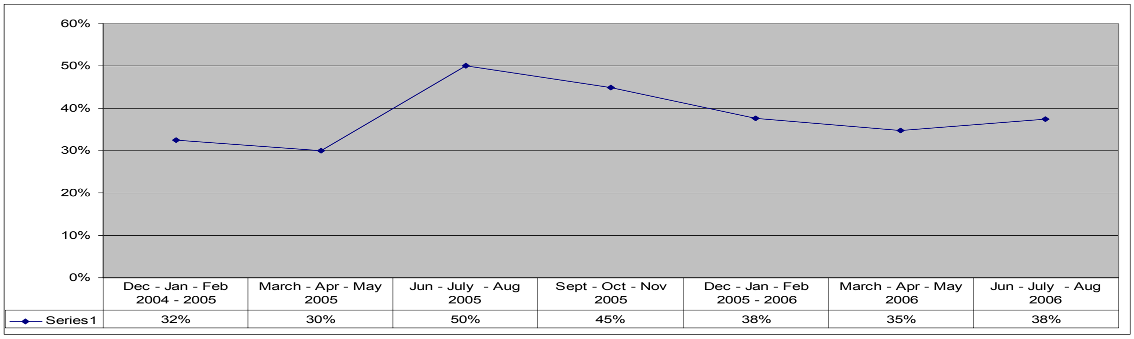


	Dec - Jan - Feb 2004 - 2005	March - Apr - May 2005	Jun - July - Aug 2005	Sept - Oct - Nov 2005	Dec - Jan - Feb 2005 - 2006	March - Apr - May 2006	Jun - July - Aug 2006
🟨 Total Conditions	77	60	24	78	77	69	48
🟦 Security Conditions	25	18	12	35	29	24	18

Table 33 - Period Number of Security Conditions assigned by DAC to projects

Period	**3 Month %**	**Security Conditions**	**Total Conditions**	**Project Totals**
December 2004 January 2005 February 2005	32%	25	77	22
March 2005 April 2005 May 2005	30%	18	60	29
June 2005 **Started - July 2005** August 2005	50%	12	24	12
September 2005 October 2005 November 2005	45%	35	78	17
December 2005 January 2006 February 2006	38%	29	77	16
March 2006 April 2006 May 2006	35%	24	69	17
June 2006 July 2006 August 2006	38%	18	48	12

Figure 17 -Period Percentage of Security Conditions assigned by the DAC



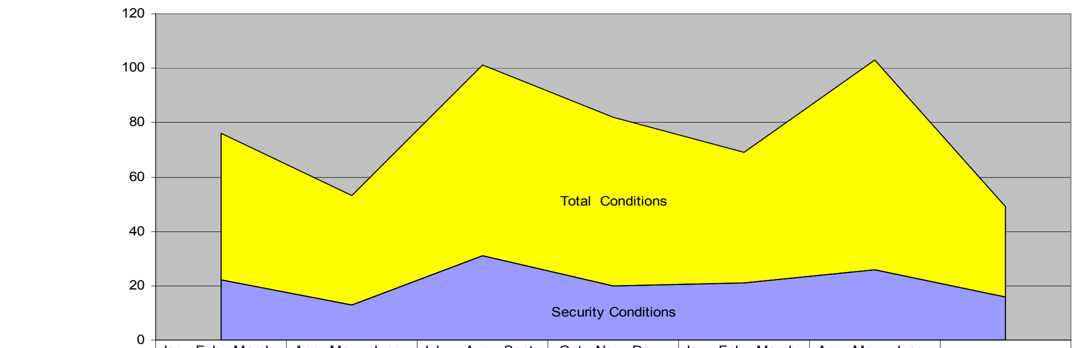
As in the Web interaction analysis, a traditional quarterly analysis of overall data tells a slight variation of the information previously presented. Again, as pointed out in the WEB interaction analysis, this overall increase in conditions could have taken place with a summer spike during the June, July, August 2005 period. It should also be noted that the upward trend in the June, July, August period of 2006 is not as high as the same period in 2005. The quarterly numbers are presented in Table 34 - Quarterly Security Conditions assigned by DAC to Projects and a graphical representation of the numbers is available in Figure 18 - Quarterly Security Conditions assigned by DAC to Projects.

The trends are not as pronounced as in the previous representation of the data. The increase in conditions takes place between the second quarter and the third quarter and the decreasing trend visible in the previous represenation of the data is shorter in duration and even shows a slight increase in the second quarter of 2006.

Table 34 - Quarterly Security Conditions assigned by DAC to Projects

Quarter	**3 Month %**	**Security Conditions**	**Total Conditions**	**Project Totals**
January 2005 February 2005 March 2005	40%	22	54	26
April 2005 May 2005 June 2005	33%	13	40	17
Started - July 2005 August 2005 September 2005	44%	31	70	19
October 2005 November 2005 December 2005	71%	20	62	13
January 2006 February 2006 March 2006	44%	21	48	16
April 2006 May 2006 June 2006	33%	26	77	15
July 2006 August 2006	48%	16	33	9

Figure 18 - Quarterly Security Conditions assigned by DAC to Projects

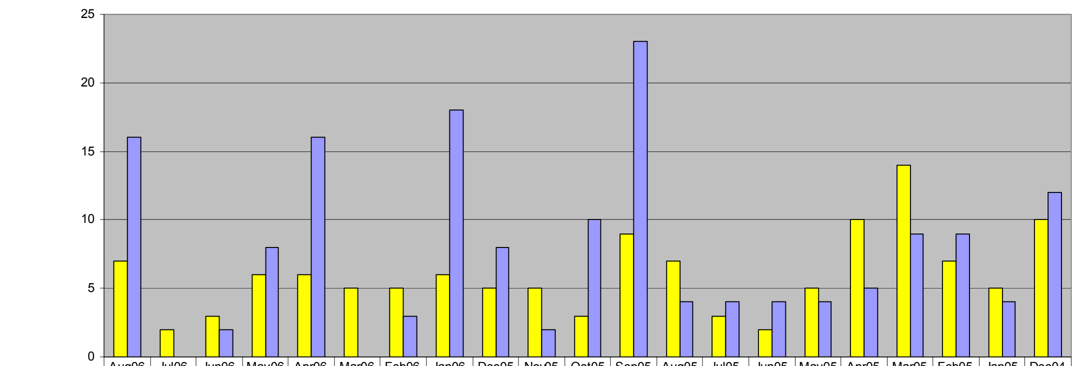


	Jan - Feb - March - 2005	Apr - May - June - 2005	July - Aug - Sept - 2005	Oct - Nov - Dec - 2005	Jan - Feb - March - 2006	Apr - May - June - 2006	July - Aug - 2006
🟨 Total Conditions	54	40	70	62	48	77	33
🟦 Security Conditions	22	13	31	20	21	26	16

A closer examination of the numbers reveals a slightly different story. Specifically, extracting the monthly security conditions from the data reveal an interesting observation. There appears to be a greater disparity in the number of security conditions after the security section has been made available in the DAD template at the beginning of October, 2005. The total number of projects and the total number of security conditions for each month used in this observation are avaiable in Figure 19 - Monthly Security Conditions.

Even though the new template was available in October there were no DADs submitted to the DAC with the new template in October. The first DAD that was submitted to the DAC with the correct template was in late November. Hence, October is counted in the time period before the changes.

Figure 19 - Monthly Security Conditions



	Aug06	Jul06	Jun06	May06	Apr06	Mar06	Feb06	Jan06	Dec05	Nov05	Oct05	Sep05	Aug05	Jul05	Jun05	May05	Apr05	Mar05	Feb05	Jan05	Dec04
🟨 Project Totals	7	2	3	6	6	5	5	6	5	5	3	9	7	3	2	5	10	14	7	5	10
🟦 Conditions	16	0	2	8	16	0	3	18	8	2	10	23	4	4	4	4	5	9	9	4	12

If the number of security conditions assigned to projects for the first eleven months is compared to the security conditions assigned to projects starting in November, there are slightly fewer security conditions assigned after the security section has been added to the DAD template. The monthly average for the number of conditions is slightly lower after the change. However, it should be noted that the number of projects presented to the DAC decreased drastically during the second half of the study. The number of conditions assigned to the projects did not decrease proportionally. The number of security conditions actually increased slightly during the second half of the study. It should also be noted that the number of conditions introduced by the service provider also increased; indicating that there were other factors encouraging the increased project condition assignment. This information is available in Table 35 – Condition Data. It should be stressed that the conditions captured during a DAC are somewhat subjective. There are multiple factors that affect a specific DAD that is submitted to the DAC. These factors include:

- the knowledge of the architect creating the DAD
- the individual members who show up to participate in the DAC
- the knowledge of the members participating in the DAC
- the political power struggles within the committee
- the capability of the individual capturing the minutes

The knowledge of the architect creating the DAD has a reasonable impact on the success of the DAD that is being presented to the DAC. The author observed a fairly high employee turnover and utilization of contractors in the organization under discussion. The individual members who showed up to participate in the DAC did change from time-to-time for reasons that ranged from employees being off work for medical reasons, to promotions. The working knowledge of the committee and the individual's personality could affect the assignment of conditions to a project. Other factors include power struggles and support staff. If one group thought it was not being properly recognized and consulted on a project, they could create problems for current and future projects presented by the offending group. The capabilities of the support staff would directly affect the reporting of the conditions since they are captured in the minutes. Even though the architects are responsible for capturing their project conditions, less than attentive architects would likely call on the support staff for condition verification after the meeting.

Understanding these issues, it is only practical to take the data on project conditions as a very general indicator as to the methodology's impact on the organization. There are additional factors that logically could have had an impact on the projects that were being presented to the DAC during the later part of the study to which the author was not privy. These factors include the monetary amounts assigned to projects, the project profiles and the demands on human resources for the projects that were being submitted to the DAC. The overall project analysis that examines the period security conditions assigned to projects is probably the best overall indicator of success or failure of the SII. This is due to the fact that it contains a more complete data set and that it helps to keep the information in context.

Table 35 - Condition Data

Security condition count before November, 2005	88
Security condition count after October, 2005	73
Months before November	11
Months after October	10
Average monthly security conditions before November	8.0
Average monthly security conditions after October	7.3
Total project count before November	75
Total project count after October	50
Average number of security conditions per project before November	1.17
Average number of security conditions per project after October	1.46
Service Provider condition count before November	85
Service Provider condition count after October	97
Average number of Service Provider conditions per project before November	1.13
Average number of Service Provider conditions per project after October	1.94

11.4.3 Condition Analysis Summary

The Web interaction and the overall analysis of the data indicate that the security conditions were having an impact on projects prior to the initiation of the SII in July of 2005. Even during the unexplained dip identified in both the Web interaction analysis and the overall condition analysis, there was still a problem with the assignment of security conditions. This is due to the fact that the security conditions represented at least half of the overall conditions assigned during that period; the highest ratio of security conditions to overall conditions during the entire case study.

Fewer projects were brought to the DAC during the second half of the case study. Even thought the total conditions that were assigned to projects during that time frame were elevated, the overall condition analysis indicates that the assignment of overall security conditions experienced a steady decrease for the period from September, October, and November, 2005 to the end of the case study. The Web interaction projects experienced a decrease in security conditions starting in the December, January and February, 2005 – 2006 period.

The monthly breakdown of the data reveal that there were five months that experienced fewer security condition assignments than any of the months in the first part of the case study. While these results are by no means conclusive, they provide a general indicator as to the positive effect of the SII, driven by the WES methodology, on the development process within the organization. This initial indication encourages future implementation testing of the WES methodology. Due to the wide range in the number of projects submitted to the DAC and the subjective nature of the conditions, additional data analysis was deemed to provide little value.

The important information to ascertain is that the SII appears to have had an overall positive effect on the organization. This could be due to either providing a decreasing trend in the overall analysis of period security conditions assigned to projects starting in the September, October, November, 2005 time frame. It could also be due to raising the awareness of security within the organization. However, it can not be claimed that the SII is the sole cause for the change in the trend. This is due to the fact that, it is impossible to totally control a business environment where multiple groups interact and link results to a single action.

The implication is that the security conditions were having an increasing impact on projects on at least two of the four periods prior to changes being implemented into the development environment. The changes that were introduced into the development environment were initiated as a result of the SII.

The new DAD associated with the SII was available in October of 2005. A possible decreasing trend in security conditions being assigned to projects by the Design Architecture Committee (DAC) can be identified in the data along with a possible overall elevation of security condition assignment. Both results are perceived to be a positive indicator of the impact of the SII on Web related projects.

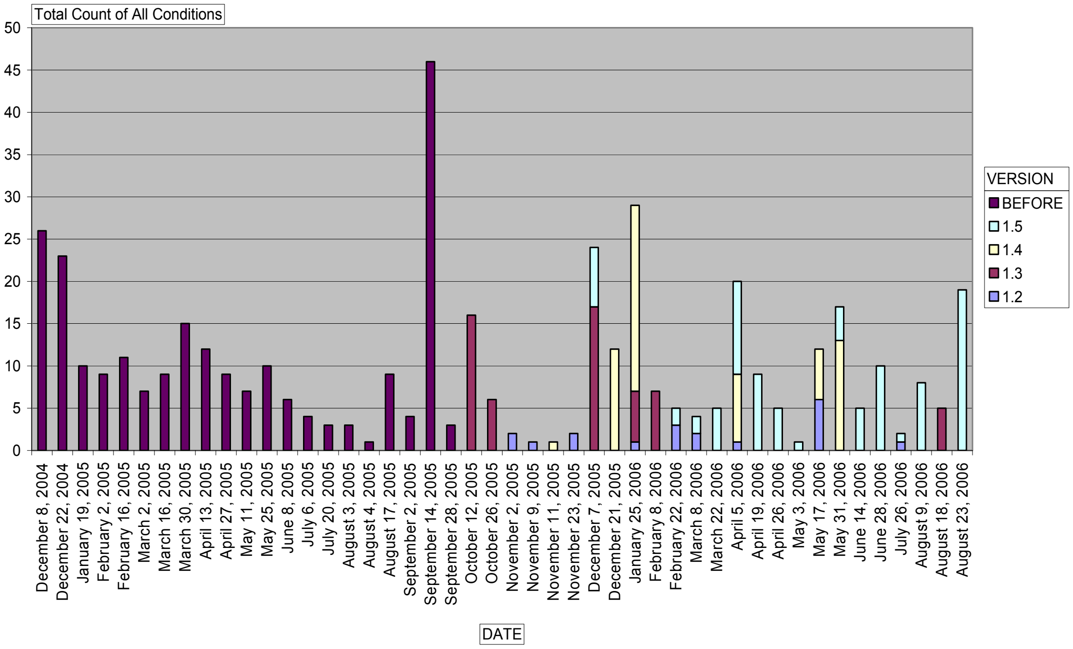
11.5 Design Architecture Document (DAD) Analysis

All of the Design Architecture Documents (DAD(s)) that were submitted to the Design Architecture Committee (DAC) were examined from November, 2005 through August, 2006. The purpose behind this exercise was to acquire an understanding of how much information was actually being recorded in the security sections of the DAD. Past DADs were examined based on expected information. The criteria for determining the version of the DAD that was submitted is as follows:

- Version 1.2 - Previous Template
- Version 1.3 - Added a Sarbanes Oxley Paragraph to the DAD
- Version 1.4 - Added the Security Section to the DAD
- Version 1.5 - Added a paragraph on the sale of a division to the DAD

Although version 1.4 of the DAD was available in October of 2005, the changes to the template were not utilized immediately. The DAC did not mandate that architects utilize the new template. In fact, the DAC has not enforced the changes to the template to date. The older templates are simply not available anymore unless they are taken from previous copies of the DAD. The earliest that the changes were observed in DAD’s is November of 2005. However, the adoption of new templates, by the architects, in the organization was very slow. This is demonstrated by the fact that the architects continued to submit older versions of the template to the DAC as late as July of 2006. It also shows that they submitted documents to the DAC that were not DADs throughout the life of the SII. Figure 20 - DAD Versions and Total Conditions depicts all of the conditions that were assigned for specific dates in conjunction with the version of the DAD that was being submitted to the DAC. This highlights the distribution of the used DADs and the delayed acceptance of the new DADs within the organization. This information provides some insight into the difficulties involved with implementing changes in large organizations. These changes have to have the full support of upper management and there has to be some employee repercussion for not complying with the new changes. That said, be it right or wrong, most businesses will not stop a several thousand pound project that is in motion in order to update its documentation so that it is compliant with a new template.

Figure 20- DAD Versions and Total Conditions



The overall numbers for the submission of DAD’s to the DAC from November, 2005 through August, 2006 are as follows:

- There were a total of 50 project documents submitted to the DAC
- Forty-seven of these documents were DADs.
- Three of these documents were not DADs.
- Eleven of these DAD’s were version 1.2
- Six of these DAD’s were version 1.3
- Seven of these DAD’s were version 1.4
- Twenty-three of the DAD’s were version 1.5

A practical analysis of the numbers indicates that there were seventeen DADs that were submitted to the DAC with the incorrect template version. Out of the seven DADs that were submitted with version 1.4 which originally contained the security section, four of the DADs either had sections deleted or the entire section was left blank. There were six 1.5 versions of the DAD with at least one of the sections within the new security part of the document that was either left blank or deleted. Three more DADs had at least one section completed with the line “n/a for all components” and two had at least one section completed with “Solution to be discussed with security”. In other words, fifteen DADs, out of twenty-nine, were submitted to the DAC with the correct template version and ignored some aspect or all of the security section of the document. Meaning that only fourteen documents were submitted with something semi-relevant written in the all of the sections. The competency of the answers varied in these sixteen documents. The information used in the version analysis is available in Appendix XI. Some of the answers were very detailed providing specific information addressing the needs of the applications in terms of identity management, threat complicacy and trust models. For example, one even provided a detailed diagram displaying a high level overview of the trust model while another provided detailed information about the establishment of trust for individual components. Examples of DAD answers for IM, Threat Management and Trust are available in Appendix VI. These answers provide enough information to recognize that the subject area has been acknowledged and addressed to some degree for these projects. It also opens the door to last minute questions from DAC if necessary. However, there were several DADs where this level of detail was not present.

There were also DADs that were completed with a minimum understanding of the purpose of the section. One example is the completion of the IM section with the following statement: *“Identity Management will not be used within this solution*”. This is the only information that was completed for the Identity Management section. This statement offers no explanation as to why IM is not being used for this solution. It offers no information on whether IM is needed or not. If it is not needed, an explanation as to why it was not needed would be helpful. On the other hand, if it is needed from a security perspective, what is the proposed solution and what is the justification for not using the in-house IM configuration? The author of this document missed the point behind this section either through a willingness to ignore the section or through a lack of security education and understanding. Another example of a poorly completed section has been provided in the Threat Management section with the answer: “No threats currently identified”. The first thought that springs to mind is why are no threats currently identified? Also, will there be any threats identified in the future? This answer implies that the author again either did not care about the section or does not understand how to accurately address the security issue.

11.6 Follow-Up Survey Analysis

The follow-up survey was conducted in August of 2006. The participants in the survey consisted of individuals who had a direct experience with the development process changes implemented in the organization. The goal of the survey was to assess stakeholder perception of the changes that were implemented. The survey questions are available in Appendix VII and the individual answers are available in Appendix VIII. The answers to the survey questions are summarized below.

11.6.1 Foundational Information

Questions 1 & 2:
The first two questions established the interviewee's current role in the organization and provided a brief idea of his/her history. These questions revealed that the interviewees are highly qualified IT professionals who have direct experience in the architecture aspect of the organization.

Questions 3 - 6:
These questions attempted to ascertain how important security is to the organization, the impact security has on the respondent's job, if they are involved in the architecture design process and, if so, how much experience they have in the field.

The result is that most of the respondents feel that security is very important and that it has a large impact on their daily jobs. All of the respondents are involved in the architecture design process and, together, the respondents have a rough average of approximately seven years experience.

Questions 7 & 8:
These questions determine if the respondents have actually created a DAD and if so, what version they used and the document's source. Eleven out of thirteen of the respondents have created a DAD and one of the respondents indicated that they contributed to high level designs. Nine of the respondents indicated that they have used the latest version of the DAD and that they retrieved this version from the local team room or from the organization's general site (OGS). The OGS is a document repository for the organization. The local architecture team room provides a link to OGS. Hence, in reality, everyone is getting the latest version of the document from OGS. It should be noted that two of the respondents indicated that they got the versions that they were using from the architects and one did not remember where they got the version they were using. Another interesting point is that the two people who do not create DADs both knew where to get the latest version.

Questions 9 & 10:
The purpose behind these questions is to determine if there have been any major differences in the way security is addressed over the past few years and, if so, gain an understanding of those differences. The majority of the respondents (eleven) indicated that major changes had taken place in the design process. While only two of the respondents indicated that it had not. The general consensus appears to be that security is more visible, more focussed and appears to be tighter than in the past. There is more involvement from the security team, more guidance in the DAD template and more representation in the organization.

Question 11:
Question eleven simply attempts to determine if the respondent was aware of the security initiative in the architecture group. Just over half of the respondents (7 out of 13) were aware of the security initiative and the rest were not (6 out of 13).

Question 12:
Question twelve attempts to ascertain the respondents' opinion of the organization's design process and its applicability to security. The results were almost fifty - fifty. Six of the respondents gave fairly positive answers in regard to the current development process and its applicability to security, while seven of the respondents gave negative responses to question twelve. A closer evaluation reveals that one of the negative responses was really not about the process but the people involved in the process and a general lack of knowledge.

Question 13:
The motivation behind question thirteen was to ascertain the depth to which the original white paper that this author submitted to security had come to the attention of the employees within the organization. The result is that most of the interviewees did not even know (eleven out of thirteen) of its existence.

Question 14:
Question fourteen attempted to determine whether the interviewees were familiar with the security sections that were added in version 1.4 of the DAD. The answer was a unanimous 'Yes' with one interviewee volunteering that they 'liked the fact that it was all in one section - helped with discussions with security'.

11.6.2 Identity Management (IM)

Question 15:
Question fifteen attempts to determine any problems with the completion of the new Identity Management (IM) section that was added to the DAD. The initial thought is that seven of the respondents indicated that they did not have a problem with the section. However, a closer examination of the responses reveals a slightly different story. One interviewee indicated that they had previous experience with IM. The reason three of the individuals did not have a problem with the section is that they were simply not using it. One of the respondents' jokingly said "Not applicable works quite nicely in that section of the DAD".

Four individuals stated that they had problems with the section; one said that it was not relevant to the interviewee's area due to the fact that each application has its own IM solution and one had no experience with the section.

So, in reality, there were five negative answers to the question. Along with one individual who clearly does not understand IM. The purpose for the creation of a specific IM group was to prevent the financial organization from having to support multiple applications with custom IM solutions. Hence, re-inventing the IM solution for every architecture solution would not be passed by the DAC.

One of the most positive answers to the section started out as a negative response - 'in the beginning, (the respondent had a problem) trying to understand (the) scope of the IM (section) and what was expected but, by the end, there were no problems. The guidelines from the IM group and the ones in the DAD template were very helpful".

Question 16:
This question attempts to determine any benefits from the completion of the new IM section in the DAD. The result is that eight of the respondents see the added value of having the section in the DAD. One respondent does not think that it is currently helping but indicated that it should be helping. This respondent thinks there is an education issue around IM and why it is worth while. Three of the respondents indicated that it was not relevant to the projects on which they were working and one did not have any experience.

Question 17:
Question seventeen attempts to determine the overall effect that adding the IM section has on the overall development process. Seven of the respondents think that it assisted the development process. Five think that it did not have an effect either way and one thinks that it both assisted and hindered the process. One respondent thinks that it helps internally but creates problems externally.

11.6.3 IM Summary:

In summary, the survey indicates that the IM section appears to have been helpful overall. It forces a conversation between the architect and the security team that may or may not have been happening previously. The reasoning behind this conclusion is based on the fact that most of the interviewees, logically, see the benefit of the section. The majority of the interviewees indicated that it assisted overall or indicated that it did not hinder the development process.

11.6.4 Threat Compliance

Questions 18 - 20:
Questions eighteen through twenty attempted to determine any problems and/or any benefits with the completion of the threat compliance section along with its effect on the overall design process. Six of the individuals indicated that they did not have a problem with this section. One of the five positive respondents indicated that they went to the security group for help and one indicated that they used the guidance notes in the template. There were also five individuals who indicated that they had problems with the section. One respondent indicated that it had no effect and one did not have any experience. The re-occurring theme is a general lack of understanding of what the section is asking or the topic in general.

When the respondents were asked if there is any benefit to the section, there were really six positive answers to the question. The non-committal answers were positive, in that they forced the respondents to think about the issues and determine if it was relevant to the project. There were five negative answers to the question and one 'did not affect' answer.

When asked if the addition of the section hindered or assisted the overall process, six respondents indicated that it did not have an effect, four indicated that it assisted, one had no experience and only two indicated that it hindered. One of the hindered responses went on to caveat the response with the comment that there was not a lot of clarity around the security area but that the security section will benefit the organization overall.

11.6.5 Threat Compliance Summary:

As a result of the summary, the threat compliance section did not hinder the development process. How much it actually helped is debatable. If anything, at best, it forced the architects to consider the issues. A point that was echoed by six of the respondents and, at worst, five respondents indicated that it was a non-event.

11.6.6 Trust Models

Questions 21 - 23:
Questions twenty-one through twenty-three attempted to determine any problems and/or any benefits with the completion of the trust models section, along with its effect on the overall design process. Four individuals indicated that they did not have a problem with the trust model section. Four of the respondents indicated that they did have a problem with the section. Four individuals did not provide a clear yes /no response to the question. However, a critical reading of the responses indicates that two of the four vague responses were not positive responses and two indicated the responses could be taken as initially positive. In fact, the two initially positive responses support the idea that there is a lack of understanding on trust models.

Seven of the respondents did indicate that they either experienced or perceived benefits to the completion of the trust model section. Five respondents gave negative responses to the question and one respondent did not have any experience.

As far as the overall effect on the design process, five individuals indicated that it assisted the overall process; five respondents indicated that it had no effect, one responded negatively, one did not have any experience and one indicated that it did not hinder but did clearly question the necessity of the section and whether it helps with the understanding of the architecture.

11.6.7 Trust Model Summary:

The responses indicate that there is a clear need for education on the subject of trust models. The majority of the respondents see a benefit in the completion of the section and there were four individuals who indicated that it assisted the process. There were also four individuals who indicated that there was no effect on the design process. Hence, from a survey perspective, it was neither a glowing success nor an outright failure.

11.6.8 Condition

Questions 24 - 26:
Questions twenty-four through twenty-six attempted to determine any problems and/or any benefits with the completion of the condition section along with its effect on the overall design process.

Eight respondents indicated that they did not have a problem with the completion of this section in the DAD. One respondent wanted clarification on the terminology of a condition vs. a comment. One indicated that adoption of the section has been a problem along with voicing discomfort about modifying a document that has been approved. Three of the respondents indicated that they had not gotten that far in the process and one of them went on to elaborate that they did not feel that the DAD was the appropriate vehicle for this issue.

When the respondents were asked if they received any benefit from the completion of the conditions section, twelve respondents gave positive answers to this question. One respondent gave a negative answer and then went on to add a positive comment.

When asked if the conditions section hindered or assisted the overall processes there were eight strong assist responses. There was a response that indicated that it did not assist. There was also one response that indicated that it did not hinder except when conditions were really project conditions and not design conditions. One respondent did not have any experience in the area and there were two ‘neither’ responses.

11.6.9 Condition Summary:

This questioning reveals that there is some misunderstanding as to the operation of the overall process and as to how the conditions section fits into the process. Overall, the condition section was well received and appears to be adding value to the design process.

11.6.10 Socialization

Questions 27 - 29:
Questions twenty-seven through twenty-nine attempted to determine any problems and/or any benefits with the completion of the modified socialization section along with its effect on the overall design process.

Eleven respondents indicated that they did not have a problem with the modified socialization section of the DAD. One respondent did say that it has not been used in all of the DADs and one respondent indicated that they issued the DAD before doing the socialization. This indicated that there is a practical timing issue with the completion of the socialization section and issuing the final version of the DAD.

Twelve respondents indicated that they either experienced or perceived benefits to the completion of the modified socialization section in the DAD. One of the positive respondents went so far as to say that they knew of one DAC meeting that it basically saved. One respondent indicated that they had not completed the section and basically had no experience with the section.

Ten respondents indicated that the modified socialization section assisted in the overall design process. One indicated that it did not have an effect either way; one respondent did not notice a change in the section and one respondent had no experience with the section.

11.6.11 Socialization Summary:

Overall, the survey revealed that the majority of the respondents felt that the modified socialization section assisted in the design process.

11.6.12 Template & Process

Question 30:
Question thirty attempts to determine the overall security weaknesses in the current version of the DAD template. Only two respondents indicated that there were no weaknesses in the document template. The weaknesses that surfaced as a result of this question ranged from the coordination of the information being asked for in the DAD with the security group, to the DAD not being compatible with external software builds, to repetition in the document, to the use of stock answers. One issue that did surface twice is that of the security education of the people completing the security section of the DAD. The lack of education could help explain the lack of respondent answers in the security section. It could also help explain the use of repeated / stock style of answers in the security section.

Question 31:
Question thirty-one attempts to determine the overall security strengths in the current version of the DAD template. The general theme that appears to be prevalent through the majority of the ten respondents who provide strengths is that it highlights explicit security information. There is better documentation and guidance to the security section along with prompting appropriate questions. One respondent did indicate that they were not sure what the organization was trying to establish with the DAD template. One respondent indicated that a fully completed document has not been presented for assessment and one respondent indicated that there was an overlap between the security section and the security non-functional requirements.

Question 32:
Question thirty-two attempts to determine if there were other factors that contributed to the successful or unsuccessful attempt to integrate security into the design process. Four individuals indicated access to security personnel support is important from a resource perspective. Two mentioned the loss of two employees within the architecture group

who were very strong in security. Three mentioned the importance of education. One mentioned the fact that highlighting security brought it to everyone's attention. One respondent mentioned that the security group is perceived, generally, as a hindrance by the project teams. The same respondent indicated that this perception is changing in the organization so that security is viewed in a better light.

11.6.13 General Survey

Question 33:
Question thirty-three attempts to determine if any of the questions were vague or difficult to follow. Eight of the respondents indicated that there were no problems with the questions. One said that number two was vague. One said that it was difficult to answer number thirty-two. This was due to the fact that the project they worked on expanded a solution that already had security in place. One said that number three was difficult to answer. The respondent was not sure if the question was from an organization's perspective or a personal perspective. One respondent indicated that number four could be examined from a design and from an everyday work perspective. One respondent indicated that it had been a while since they had completed his last DAD and had to stop to remember some of the information.

Question 34:
Question thirty-four gave the interviewee the opportunity to add any additional comments to the survey. Four of the respondents had nothing to add. One mentioned the need for standards, one indicated that the organization has document management issues, one thinks that the interaction with the infrastructure team is not as clear now as with the security team, one would like to see the same type of work that was conducted on security expanded to the other components of the DAD, one thinks that the conditions section should become the responsibility of the release managers and one stressed the need for education in security, infrastructure and tools. Another respondent also indicated that there is a high turnover in the architecture group which contributes to the education problems and puts more pressure on the security team. An interesting comment was made about the survey itself, one respondent indicated that they would like to take the survey again in a year after the changes had time to penetrate the organization.

11.7 Implementation Obstacles

The obstacles experienced during the implementation of the WES methodology can be summarized as inertia, political scope and lack of cultural ownership.

1. *Inertia*. The author experienced a great deal of resistance to the modification of the Design Architecture Document (DAD) which is the primary instrument utilized by the architecture team in the organization. The survey reveals that several of the architects acknowledged the benefits in the changes and the focus on security. However, when it came to actually filling in the sections of the DAD there was obvious resistance to actually completing the revised document.

2. *Political Scope*. Individual recommendations were dismissed during the application of the WES methodology due to the lack of support and interest from other groups within the organization. Modifications to the DAD had to be approved by the individual groups that were represented by various sections within the DAD. Some groups used the opportunity to attempt to assert political influence on the approval process and others attempted to use the approval of the security changes as an opportunity to insert additional changes, which they desired, into the DAD.
3. *Lack of Cultural Ownership*. The organization intuitively fostered a culture that continually decreases ownership of activities and processes within the organization. This lack of ownership for activities and processes contributes to an environment where everyone is trying to defend their actions leading to a lack of initiative. This lack of initiative is visible through high turnover rates in the organization and a high dependence on contractors. This leads to a situation where people want "cookie cutter" styles of answers to problems. Hence, there appears to be a lack of understanding of the project approval process and a lack of knowledge in the security area. The architects appear to want a resource that is available to answer their security question in the design arena so that they do not have to concentrate on learning that aspect of the job.

11.8 Summary

While no development process is going to suit everyone, the chosen deployment process needs to meet the business requirements for security. The surveys and the application of the WES methodology, as a guide to addressing their security problems, appears to have had a positive effect on the security of the organization.

The follow-up survey also brought to light the general lack of understanding of how the architecture process is supposed to work. Comments were made like: '…lot of discomfort with changing a document that has been approved'. If a condition is assigned to a project, it is suppose to be brought back to the DAC for final approval after the condition has been satisfied. This comment indicates that there is either a lack of understanding about the process or a breakdown in the operation of the DAC.

The surveys and the document analysis clearly support the need for education. The architects, referenced in this research in the financial institution, are considered the elite of the banking IT staff. Gather all of these people in a room and they should be able to tell you about all of the systems in the organization. Even though most of these individuals clearly understand the importance of security and see the benefits in having security in the development process, there is clear resistance to the practical implementation of this in the development process. The case study also demonstrated that security knowledge is lacking among the elite IT staff in the organization. Security was added into the design process along with general guidance notes. However, this information was not enough, as a general rule, to help the architects complete the new security section. This case study results provides support for the necessity of the practical implementation of a security education program along with the practical implementation of security into the development process.

Another idea that the case study supports is that security in the development process is really a product of heightened awareness and the promise of a conversation. The conditions that were being assigned did decrease over the life of the Security Improvement Initiative (SII). Although the security section was either not filled in or filled in very poorly in a lot of cases, the fact that these sections were not being mandated in the conditions section of the DAD indicates that there is the probability that there were some security conversations taking place. It also indicates that these security conversations were not being properly recorded in the DAD.

12 Conclusion

My hypothesis is that developing a process impartial security methodology applicable to different Web Engineering development processes will help organizations strengthen security in their Web application development process. Therefore, a flexible process neutral security methodology is required for Web Engineering application development. This process neutral methodology should explicitly integrate security throughout existing Web engineering application development methodologies. The first four sections of this chapter address the research questions that were presented in chapter one and to what extent they have been answered. The fifth section examines the WES methodology in conjunction with Siponen's criteria for fifth generation methodologies [171] and the final section of the chapter examines areas for future work.

12.1 Thesis Research Question 1

The answer to the first research question 'Is it possible to define a set of criteria that a Web Engineering Security process must fulfil?' is yes. Chapter five established the empirical evidence and discussed in detail the criteria entitled Essential Elements (EE) which need to be established prior to implementing a Security Improvement Initiative (SII) and the Security Criteria for a Web Application Development (SCWAD). The empirical evidence for both criteria is based on surveys. The Essential Elements are based on a Web survey and are as follows:

1. Web Application Development Methodology
2. Web Security Development Process Definition
3. End-Users Feed Back
4. Implement & Test Disaster Recovery Plans
5. Job Related Impact

The empirical evidence presented in chapter five for SCWAD is based on a survey conducted in a Global Fortune 500 financial organization. Chapter five also discussed, in detail, the six criteria for a Web engineering security process:

1. Active organizational support for security in the Web development process
2. Proper Security Controls in the development environment
3. Security Visibility throughout all areas of the development process
4. Delivery of a cohesive system, integrating business requirements, software and security
5. Prompt, Rigorous Security Testing and Evaluation
6. Trust and Accountability

SCWAD is used in chapter six to assess Web engineering application development processes and to scrutinize established security processes. Chapter ten presents a practical application of both the Essential Elements and SCWAD in the development of the Hunterian Online Photo Library (HOPL).

12.2 Thesis Research Question 2

The answer to the second research question ‘Can a new development process be defined to meet the criteria for a Web Engineering Security process?’ is yes. The WES methodology is constructed from empirical research that consisted of two surveys. The empirical research for both of these studies and the criteria that resulted from the analysis of the results is discussed in chapter five. The WES process was designed to address both sets of criteria which included the Essential Elements and the Security Criteria for Web Application Development (SCWAD).

The WES developed in this research process is described in chapter seven. The WES methodology was designed to complement Web software development through customer communications, short development cycles, and practical security solutions to business problems. The WES process life-cycle is designed to integrate with traditional and agile development processes that are used specifically for Web application development. Realistically, WES defines a security specific communication approach for management and developers that spans the Web application development life-cycle. The WES methodology advocates the foundation principles which include security education, good communication and cultural support. WES supports heavy end-user involvement throughout the security development process. This is due to the fact that end-users are the ultimate security assessment in the execution of an application.

12.3 Thesis Research Question 3

The answer to the third research question ‘Can it be argued that the introduction of this new process strengthens security within Web Engineering application development processes?’ is yes. The WES process was developed from an analysis of industry surveys that were discussed in chapter five. The WES process, discussed in chapter seven, establishes the benefit of a project development risk assessment, the acquisition of application security requirements and determination of organizational compatibility.

The WES process then filters the risk and security requirements through the development process, attempting to mitigate possible security breaches through security focussed design, coding activities, testing implications and end-user feedback. The WES methodology promotes industry best practices while providing structure to the integration of the practices into the Web application development methodology and with the policies of the organization.

Chapter eight examines the WES methodology alongside existing security methodologies. In doing so, chapter eight identifies several deficiencies within existing security methodologies that WES attempts to address. These issues include acknowledgement of security during the business analysis; security policy - cultural - technological compatibility (also known as organizational compatibility); controlled environment implementation and end-user feedback.

Chapter nine demonstrates the compatibility of the WES methodology with both traditional and agile application development methodologies. The process neutral approach provides the necessary flexibility for organizations to capitalize on existing expertise while improving security integration in their existing Web application development methodology.

The level of security that an organization attains through the implementation of the WES methodology is dependent upon the Web application security needs of the executing organization. These needs will vary between businesses within industries and between various industries. No organization is going to construct code that is 100% secure, nor do most organizations have a need to construct code that is totally secure. Realistically, organizations will implement the degree of security required by the local business environment, the industry or the governmental regulations. Most businesses do not have an unlimited budget which means that the security decisions will also be tempered by financial resources. The idea behind WES is to improve the security focus of the organizations conducting Web application development. The improvement of the security focus will allow organizations to mitigate security risk where it is deemed appropriate for the business. There are a number of elements to be considered. These elements can be mitigated through the components of the WES methodology which include the identified risk, the acquisition of specific security requirements; organizational compatibility acknowledgement; security design, coding and testing best practices; and the attainment of end-user feedback. The elements of the WES methodology specifically focus on the security aspects of the application which improves security during Web application development.

12.4 Thesis Research Question 4

The answer to the fourth research question ‘Is it possible to demonstrate that this new Web Engineering Security Process can be successfully used in industry?’ is yes within the scope of this research which includes resources, opportunities, corporate obstacles and time constraints. Both the components of the process and the overall process can be used in industry. The recommendations embraced and implemented by organizations is dependant on the needs and the culture of the implementing business. Chapter ten discusses the implementation of the individual components which include the Essential Elements (EE) and the Security Criteria for Web Application Development (SCWAD). The Essential Elements and SCWAD were applied to a project being implemented by the Hunterian Museum and Art Gallery at the University of Glasgow. The application of both of the Essential Elements and SCWAD revealed development process strengths and opportunities for improvement in the development process that was used to develop the Hunterian Museum’s Online Photo Library (HOPL).

Chapter eleven discusses the limited implementation of the WES methodology into a Global Fortune 500 financial organization and the obstacles that the implementation encountered. The Security Improvement Initiative (SII) consisted of a pre-WES implementation survey, WES implementation, a post-WES implementation survey and an analysis of relevant data. The evidence presented in chapter eleven indicates that SII appears to have had a positive effect on the organization by reversing an increasing trend in security conditions assigned to projects and raising security awareness within the organization. The catalyst for the recommendations proposed during the SII was the WES methodology. The application of the WES methodology in the organization resulted in several recommendations. Financial organizations, by their very nature, are averse to a lot of changes. Some of the proposed changes were accepted and implemented within the organization. Hence, the implementation of the WES methodology in the organizations affected the development process for all large applications being implemented in the United Kingdom. The obstacles that the author encountered during the implementation of the WES methodology are discussed in chapter eleven and included inertia, political scope and a lack of cultural ownership.

12.5 Scope and Validity

Scope and validity issues of the research should be specifically recognized and discussed at this point. The majority of the respondents to the Web survey probably originated from the greater Glasgow area due to the email request from the local chapter of the British Computing Society (BCS). While this is not negative, due to a diverse industry base in Glasgow, it should be recognized as having a potentially bias affect on the results. Although this should not impact the case study, it should be acknowledged that the initial industry survey, used to help create WES, was conducted in the same company where WES was implemented. This does raise the question of applicability in other organizations and should be investigated through future work. The fact that the industrial case study was implemented in a Fortune Five Hundred organization does help to mitigate this concern due to the fact that most of the organizations in this category broadly share common attributes in terms of size, bureaucracy and legislative concerns. These concerns lead to a broadly similar application process being developed in these organizations.

Also, the author worked visibly within the Fortune Five Hundred organization to implement WES. This visibility naturally raises the question of the author's impact on the results of the study. As with any empirical study, it becomes difficult to know how much influence the author had over the success of the experiment. The fact that there was a new face in the organization, that the new individual was asking security related questions around the development process, etc., all need to be acknowledged in reference to potentially impacting the study. It should also be noted that the opportunities presented by both of the case studies supported plan driven development of Web applications. While chapter nine does successfully address WES compatibility with agile application development, there was no empirical case study to support this analysis. This issue of conducting an empirical case study with an agile development process should be explored in future work.

12.6 Fifth Generation Analysis

As discussed in chapter three, Siponen identified five generations of information security methodologies. He proposed four criteria that fifth generation methodologies should strive to achieve. WES meets all of these criteria making it a fifth generation methodology. The criteria are the use of social ideas and techniques ensuring congruent design and user expectations; integration with all types of software development methodologies; painless adaptability of security methods with practitioners; and empirical evidence of their usefulness [173].

WES addresses the first criteria through the implementation of the foundational principles, as discussed in chapter seven, which include security education, good communication and cultural support. WES also involves the end-user from the beginning of the process and strives for security visibility throughout the entire development process. Chapter nine demonstrated the compatibility of the WES methodology with both traditional and agile development methodologies.

The last two criteria are addressed in chapters ten and eleven. Chapter ten demonstrates that aspects of the WES methodology can be applied successfully in a business environment. Chapter eleven demonstrates that the WES methodology can be applied in industry with relative ease. The empirical evidence gathered from the condition analysis and the follow-up survey, as discussed in chapter eleven, indicates that SII driven by the application of the WES methodology had a positive effect on the organization.

12.7 Further Work

The research reported in this dissertation identified several areas for future research in Web engineering, security, business, cultural and legislation. Future work in this area of Web Engineering and security should include an attempt to drill down into the various interpretations of the definition of security among an assortment of organizations. It should also attempt to acquire more detailed information on an organization's in-house development process approaches to security, examine implicit approaches to security and their effectiveness in 'real-world' environments.

Future research should investigate WES implementations in other financial companies and organizations in other industries. This should include specifically working with a financial organization that implements an agile development process in order to strengthen or disprove the theoretical argument proposed in the dissertation that WES is compatible with agile processes. Future implementations of the WES methodology should examine refinements of the individual stages of the methodology. Interdependencies should be examined between the WES methodologies and security activities that are currently being conducted in organizations. These interdependencies could provide opportunities for capitalization of reusable components within organizations.

The business perspective should be explored in future research to determine any interdependencies between the Essential Elements and the actual and/or perceived Return on Investment (ROI) for the individual stages of the development life cycle and specific ROI for security within each stage of the life cycle.

Additional work should include investigations into the creation of tools to help developers and managers implement the WES methodology. Some of these tools could include the development of configurable applications that capture a variety of security related issues experienced in the application development process in tailorable databases. These tools could capture information on everything from coding bugs, to process development issues, to organizational specific security requirements. The capturing of this information could be mined to provide organizations with an abundance of practical information for developing secure Web applications. These tools should be researched and developed in a manner that utilizes feedback from individual iterations of the development process capitalizing on "Lessons Learned" and maximizing reusable components of the process.

In the future, cultural research needs to be conducted into the barriers and aids to methodology adoption in industry which concurs with results stated in previous research [129]. The implementation of the WES methodology encountered resistance in the form of cultural change, i.e., inertia, political scope, and a lack of cultural ownership. Investigations into the reduction and/or elimination of organizational resistance to methodology implementations could provide valuable information to businesses.

The legislative perspective in future research should examine the practicality and productivity of the processes and procedures implemented, by individual organizations, to address the legislative requirements that are being imposed on organizations. This research should examine the practical effectiveness of international and domestic cyber legislation from a successful prosecution perspective, in respect to the deterrence of cyber crimes and the practical effects on the business environment. Research may also want to investigate any legislative conflicts between countries and the possible resolutions to any such conflicts. The Web engineering perspective should investigate and identify the role in the development team where the responsibility for the legislative aspect of the application development project should be placed.

12.8 Summary

The research presented in this dissertation achieved several goals. The results of the research defined criteria, the Essential Elements (EE) and the Security Criteria for Web Application Development SCWAD, which a Web Engineering Security process must fulfil. The EE and SCWAD provided the foundation for the development of a Web Engineering Security (WES) methodology which is a fifth generation information security process that strengthens Web Engineering Application development processes. The research then confirmed that the WES methodology, within the scope of the research, can be successfully implemented in industry.

Appendix I - Web Survey Questions

Question Number	**Question**	**Answer**
10	If necessary, would you be available to respond to a few specific questions?	YES - NO
20	Does your organization have an Internet site?	YES - NO - DO NOT KNOW
30	Does your organization develop any of its Internet applications in-house?	YES - NO - DO NOT KNOW
40	Does your organization have a defined Internet application development process?	YES - NO - DO NOT KNOW
50	What type of Internet development process does your organization implement?	• Agile Development Process (Extreme Programming, Dynamic Systems Development Method) • Traditional Systems Development Processes (Water Fall Approach, Spiral Model) • A process that is a combination of Traditional and Agile Development Processes • Use both Agile and Traditional process depending on the nature of the project. • In-House
60	Where does security design fall in your Internet application development process?	• During the initial design phase • During the coding & testing phase • During the implementation phase • Not at all
70	Does your organization have a defined application development Internet security process?	YES - NO - DO NOT KNOW
80	Does the process contain a risk analysis phase?	YES - NO - DO NOT KNOW
90	Does the process contain application security requirements phase?	YES - NO - DO NOT KNOW
100	Does this process contain a security design phase?	YES - NO - DO NOT KNOW
110	Does this process contain a controlled implementation environment phase?	YES - NO - DO NOT KNOW
120	Does this process contain a testing phase that is specific to security?	YES - NO - DO NOT KNOW
130	Does the process attempt to acquire feedback from the end-user?	YES - NO - DO NOT KNOW
131	Is the Internet security process followed by the employees?	YES - NO - DO NOT KNOW

132	Is there an individual on the team or in the organization that is responsible for insuring that the Internet security process is followed?	YES - NO - DO NOT KNOW
133	Is there any job related impact for not following the Internet security process?	YES - NO - DO NOT KNOW
134	In your opinion, is the Internet security process effective?	YES - NO - DO NOT KNOW
140	Does your organization contract out any of its Web site development?	YES - NO - DO NOT KNOW
150	At what point does security become an issue when considering outside applications?	• During the initial design phase • During the coding & testing phase • During the implementation phase • Not at all
160	Does your organization have plans to develop or implement an Internet site in the next 12 months?	YES - NO - DO NOT KNOW
170	Does your organization have an intranet site?	YES - NO - DO NOT KNOW
180	Does your organization develop any of its intranet applications in-house?	YES - NO - DO NOT KNOW
190	Does your organization have a defined application development process for intranet applications?	YES - NO - DO NOT KNOW
200	What type of intranet development process does your organization implement?	• Agile Development Process (Extreme Programming, Dynamic Systems Development Method) • Traditional Systems Development Processes (Water Fall Approach, Spiral Model) • A process that is a combination of Traditional and Agile Development Processes • Use both Agile and Traditional process depending on the nature of the project. • In-House
210	Where does security design fall in your intranet application development process?	• During the initial design phase • During the coding & testing phase • During the implementation phase • Not at all
220	Does your organization have a defined application development intranet security process?	YES - NO - DO NOT KNOW
230	Does the process contain a risk analysis phase?	YES - NO - DO NOT KNOW
240	Does the process contain application security requirements phase?	YES - NO - DO NOT KNOW

250	Does this process contain a security design phase?	YES - NO - DO NOT KNOW
260	Does this process contain a controlled implementation environment phase?	YES - NO - DO NOT KNOW
270	Does this process contain a testing phase that is specific to security?	YES - NO - DO NOT KNOW
280	Does the process attempt to acquire feedback from the end-user?	YES - NO - DO NOT KNOW
281	Is the intranet security process followed by the employees?	YES - NO - DO NOT KNOW
282	Is there an individual on the team or in the organization that is responsible for insuring that the intranet security process is followed?	YES - NO - DO NOT KNOW
283	Is there any job related impact for not following the intranet security process?	YES - NO - DO NOT KNOW
284	In your opinion, is the intranet security process effective?	YES - NO - DO NOT KNOW
290	Does your organization have plans to develop or implement an intranet site in the next 12 months?	YES - NO - DO NOT KNOW
300	Does your organization have an extranet?	YES - NO - DO NOT KNOW
310	Does your organization develop any of its extranet applications in-house?	YES - NO - DO NOT KNOW
320	Does your organization have a defined application development process for extranet applications?	YES - NO - DO NOT KNOW
330	What type of extranet development process does your organization implement?	• Agile Development Process (Extreme Programming, Dynamic Systems Development Method) • Traditional Systems Development Processes (Water Fall Approach, Spiral Model) • A process that is a combination of Traditional and Agile Development Processes • Use both Agile and Traditional process depending on the nature of the project. • In-House
340	Where does security design fall in your extranet application development process?	• During the initial design phase • During the coding & testing phase • During the implementation phase • Not at all
350	Does your organization have a defined application development extranet security process?	YES - NO - DO NOT KNOW

360	Does the process contain a risk analysis phase?	YES - NO - DO NOT KNOW
370	Does the process contain application security requirements phase?	YES - NO - DO NOT KNOW
380	Does this process contain a security design phase?	YES - NO - DO NOT KNOW
390	Does this process contain a controlled implementation environment phase?	YES - NO - DO NOT KNOW
400	Does this process contain a testing phase that is specific to security?	YES - NO - DO NOT KNOW
410	Does the process attempt to acquire feedback from the end-user?	YES - NO - DO NOT KNOW
411	Is the extranet security process followed by the employees?	YES - NO - DO NOT KNOW
412	Is there an individual on the team or in the organization that is responsible for insuring that the extranet security process is followed?	YES - NO - DO NOT KNOW
413	Is there any job related impact for not following the extranet security process?	YES - NO - DO NOT KNOW
414	In your opinion, is the extranet security process effective?	YES - NO - DO NOT KNOW
420	Does your organization have plans to develop or implement an extranet site in the next 12 months?	YES - NO - DO NOT KNOW
430	How important does your organization consider security in its Internet, intranet, and /or extranet applications?	• Unimportant • Somewhat important • Important • Very Important
440	How important does your organization consider security in the development process?	• Unimportant • Somewhat important • Important • Very Important
450	Does your organization take any actions to educate employees about computer security?	YES - NO - DO NOT KNOW
460	Does your organization have a disaster recovery plan that includes individual applications in the security design requirements?	YES - NO - DO NOT KNOW
470	Has your organization tested (by execution) this disaster recovery plan within the last 12 months?	YES - NO - DO NOT KNOW
480	What position/title in the company is responsible for monitoring information and computer security within your organization?	Short Answer

Appendix II - Web Survey Answers

Table 36 - Web Survey Abbreviations

Abbreviation	Meaning
Nbr	Question Number
Rspdts	Respondents
DKN	Do Not Know
A.D.P.	Application Development Process

Table 37 - Web Survey Answers

Nbr	Abbreviated Question	Rspdts	YES	NO	DKN
10	Available to respond to a few specific questions?	53	43	10	
20	Does your organization have an Internet site?	53	51	2	
30	Develop any of its Internet applications in-house?	49	39	6	4
40	Have a defined application development process?	36	14	19	3

Nbr	Abbreviated Question	Rspdts	Agile	Traditional	Combination	Both A&T	In-House
50	Internet development process	13	2	3	2		6

Nbr	Abbreviated Question	Rspdts	Initial Design	Coding & Testing	Implementation	Not at all
60	Security design falls in your Internet A.D.P.?	13	11	1	1	

Nbr	Abbreviated Question	Rspdts	YES	NO	DKN
70	Defined application development Internet security process?	35	17	14	4
80	Does the process contain a risk analysis phase?	16	12	2	2
90	Contain application security requirements phase?	16	14	0	2
100	Contain a security design phase?	16	13	2	1
110	Contain a controlled implementation environment phase?	16	14	1	1
120	Does this process contain a testing phase that is specific to security?	16	12	4	0
130	Attempt to acquire feedback from the end-user?	16	9	6	1
131	Internet security process followed by employees?	16	14	1	1
132	Individual responsible for Internet security process is followed?	16	15	0	1
133	Job related impact for not following the Internet security process	16	4	6	6
134	Is the Internet security process effective?	15	13	2	0
140	Org. contract out any of its Web site development?	44	17	19	8

Nbr	Abbreviated Question	Rspdts	Initial Design	Coding & Testing	Implementation	Not at all
150	Point security becomes an issue when considering outside applications?	17	13	1	1	2

Nbr	Abbreviated Question	Rspdts	YES	NO	DKN
160	Plans to develop or implement an Internet site in the next 12 months?	2	1	0	1
170	Does your organization have an intranet site?	42	32	9	1
180	Develop any intranet applications in-house?	31	27	2	2
190	Defined A.D.P. for intranet applications	27	13	11	3

Nbr	Abbreviated Question	Rspdts	Agile	Traditional	Combination	Both A&T	In-House
200	Type of intranet development process	13	1	6	2	0	4

Nbr	Abbreviated Question	Rspdts	Initial Design	Coding & Testing	Implementation	Not at all
210	Security design falls in your intranet A.D.P?	13	10	1	0	2

Nbr	Abbreviated Question	Rspdts	YES	NO	DKN
220	Application development intranet security process?	27	10	12	5
230	Does the process contain a risk analysis phase?	10	6	2	2
240	Application security requirements phase?”	10	9	1	
250	Does this process contain a security design phase?	10	9	0	1
260	Controlled implementation environment phase?	10	7	2	1
270	Testing phase that is specific to security?	10	5	4	1
280	Acquire feedback from the end-user	10	6	2	2
281	Intranet security process followed by employees?”	10	9	0	1
282	Individual responsible for insuring that the intranet security process is followed?	10	9	0	1
283	Job related impact for not following the intranet security process?	10	5	2	3
284	Is the intranet security process effective?	10	8	1	1
290	Plans to develop an intranet site next 12 months?	9	2	7	
300	Does your organization have an extranet?	41	12	18	11
310	Develop any of its extranet applications in-house?	12	11	0	1
320	Have a defined A.D.P. for extranet applications?	11	6	4	1

Nbr	Abbreviated Question	Rspdts	Agile	Traditional	Combination	Both A&T	In-House
330	Extranet development process your org implement?	6	0	2	2	0	2

Nbr	Abbreviated Question	Rspdts	Initial Design	Coding & Testing	Implementation	Not at all
340	Security design falls in your extranet A.D.P.?	6	5	1	0	0

Nbr	Abbreviated Question	Rspdts	YES	NO	DKN
350	Does your organization have a defined application development extranet security process?	11	5	3	3
360	Does the process contain a risk analysis phase?	5	3	1	1
370	Does the process contain a risk analysis phase?”	5	5	0	0
380	Does this process contain a security design phase?	5	5	0	0
390	Controlled implementation environment phase?	5	5	0	0
400	Testing phase that is specific to security?	5	4	1	0
410	Acquire feedback from the end-user?	5	5	0	0
411	Is the extranet security process followed by the employees?	5	5	0	0
412	Individual responsible for insuring that the extranet security process is followed?	5	5	0	0
413	Job related impact for not following the extranet security process?	5	3	1	1
414	Is the extranet security process effective?	5	5	0	0
420	Plans to develop or implement an extranet site in the next 12 months?	18	3	13	2

Nbr	Abbreviated Question	Rspdts	Unimportant	Somewhat Important	Important	Very Important
430	Importance of security in Internet, intranet, and /or extranet applications?	37	2	4	8	23
440	Importance of security in the development process?	37	3	7	11	16

Nbr	Abbreviated Question	Rspdts	YES	NO	DKN
450	Actions to educate employees about computer security?	37	27	5	5
460	Disaster recovery plan that includes individual applications in the security design requirements?	37	19	9	9
470	Tested disaster recovery plan within the last 12 months?	19	10	4	5

Appendix III - Pre -WES Implementation Industry Survey Questions

1. What is your current job title/role?

2. Briefly describe the key areas of your job function/role?

3. How many years have you worked in IT?

4. Briefly describe your career history in IT?

5. Does the company have a defined (documented) application development process? YES/NO/DNK

    a. If YES, briefly describe the company's development process.

    b. If YES, in your opinion, what are the **good** points of the application development process?

    c. If YES, in your opinion, what are the **bad** points of the application development process?

    d. If YES, Is the application development process used on all projects? YES/NO/ DNK

        1. If NO, What are some of the reasons that it might not be used?

        2. If NO, Are there multiple application development processes used in the company? YES/NO/ DNK

            1. If YES, please list the type of application and the corresponding development process and their exception criteria.

    e. If the company does not have a defined (documented) application development process? Why not?

6. From these Generic categories, in what areas of the process life-cycle are you engaged:

    a. ___Business Analysis

    b. ___Requirements

    c. ___Design

    d. ___Implementation

    e. ___Testing

    f. ___Evaluation

    g. ___Deployment

    h. ___Maintenance and Evolution

7. In your opinion, is the application development process effective? YES/NO/SOMETIMES/ DNK
    a. If NO, why not?
    b. If SOMETIMES, when is it effective?
    c. If SOMETIMES, when is it not effective?
8. How long does it currently take to get a project from inception to delivery?
9. In your opinion, do you feel that the time-line for project delivery should be longer, shorter or no different?
    a. Why?
10. Do development projects exceed the estimated time frames? YES/NO/ DNK
    a. If YES, How often do development projects exceed the estimated time frame?
    b. If YES, What are the reasons for exceeding the estimated time frame for development?
    c. If YES, Are any of the reasons listed in 10.b. security related?
11. Do development projects exceed the estimated budgets? YES/NO/ DNK
    a. If YES, How often do development projects run over budget?
    b. If YES, What are the reasons for exceeding the estimated budget for development?
    c. If YES, Are any of the reasons listed in 11.b. security related?
12. Is there a documented corporate recommendation for an optimal overall development timeline? YES/NO/ DNK
    a. If YES, what is it?
    b. If YES, Is that recommendation for a specific type of project? YES/NO/ DNK
        1. If YES, What type of project is it?
        2. Does that project have a specific number of requirements?
13. Do Projects always follow the in-house development process? YES/NO/ DNK
    a. Why?
14. What do you feel a security development process should contain?
15. In your experience of the company's development process, in what parts of the life-cycle does security play a role? (In other words, how does security affect the development process?)
    a. Business Analysis ____
    b. Requirements____

c. Design____

d. Implementation____

e. Testing____

f. Evaluation ____

g. Deployment ____

h. Maintenance and Evolution________________________________

16. Does the company have a defined (documented) **security** development process? YES/NO/ DNK

a. If YES, Briefly describe the company's development security process.

b. IF YES, Does the security development process apply to all types of application development? (ex. Web development, mainframe, ATM, stand alone applications) YES/NO/ DNK

1. If YES, What are the types of applications that the security process has to support? ___Internet

___Intranet

___Extranet

___Standalone Applications

___Distributed Applications

___Other – Please Explain

2. If NO, to what type of application development process does it not apply?

3. If NO, to which ones does it apply?

4. IF NO, why does it not apply to all forms of application development?

c. If YES, in your opinion, what are the **good** points of the SECURITY application development process?

d. If YES, in your opinion, what are the **bad** points of the SECURITY application development process?

e. If YES, in your opinion, are there currently any problems with the security process? Or, is there anything you would like to see changed?

f. IF YES, is there any point, in your opinion, at which the Security development process breaks down?

g. IF does the company does **NOT** have a defined (documented) **security** development process, Why Not?

17. How are applications measured from a security perspective; i.e., how is an application deemed secure?

a. Do the same security criteria apply to all applications? YES/NO/ DNK

b. If NO, please describe the difference(s) in the criteria between the different Security application development processes?

18. How is security measured from a development perspective; i.e., how is it tested?

    a. Do the same security tests apply to all applications? YES/NO/ DNK

    b. If NO, what tests apply to which applications?

19. Which stakeholders are responsible for ensuring security is represented and in what phases?

    a. Business Analysis____

    b. Requirements____

    c. Design____

    d. Implementation____

    e. Testing____

    f. Evaluation ____

    g. Deployment ____

    h. Maintenance and Evolution____________________________________

20. Is there an individual in the security area or in the organization who is responsible for insuring that the security process is followed from a development standpoint? YES/NO/DNK

    a. IF YES, what is his/her title?

21. Do conflicts arise between stakeholders responsible for security and application developers during the application development process? YES/NO/DNK

    a. If so, what are the conflicts?

22. Do you contract out any of your development work? YES/NO/ DNK

    a. If YES, are Contractors held to the same application development process requirements as employees? YES/NO/ DNK

        1. If NO, Why not?

    b. If YES, are contractors held to the same security process requirements as employees? YES/NO/ DNK

        1. If NO, Why not?

23. What is your opinion on the emphasis security plays within the organization’s development process?

24. Do you think that the elements of the existing security development process are always followed? YES/NO/ DNK

    a. Why?

25. In your opinion, do you think security should play a larger role in the development environment, a smaller role, or is the current role accurate? Why?

26. Is there a job related impact for an employee not following the development security process? YES/NO/ DNK
27. What areas do you feel require more or less emphasis on security within the company process? Why?
28. From your perspective, what are the major security threats during application development?

    a. Which of these issues are successfully addressed by the current security development process?

    b. Which of these issues are NOT successfully addressed by the current security development process?
29. Were any of the survey questions vague or difficult to follow?
30. Are there any additional comments that you would like to make about the questions?

Appendix IV - Pre - WES Implementation Industry Survey Answers

Questions 1 – 4: The first four questions were used to establish the interviewee's current role in the organization, their number of years experience and a brief idea of their history. These questions revealed that the interviewees who were selected are highly qualified IT professionals who have a variety of backgrounds and, in general, several years experience. The average number of years among the 16 responders is 13.9.

Question 5 – 5.e: Question 5 firmly established the existence of a documented application development process with fourteen 'Yes' responses and two 'Do Not Know' responses. There was some discrepancy on the process specifics but the general idea is that the organization uses a customized plan driven version of the waterfall approach. The good points ranged from providing structure to the environment, to being well understood in the organization, to providing accountability, to flexibility at the granular level. The bad points of the process generally focused on business time-to-market, heavy documentation, and one-size-fits all (non-flexible) approach. Eleven out of fourteen indicated that the process was used on all projects. Out of the remaining three answers, two indicated that it was not used on all projects and one did not answer. The reasons for not using the process ranged from individual choice, to experimentation, to time pressures, to a lack of overall business strategy and cohesiveness. The two who indicated that the development process was not used on all projects did say that multiple development processes are used in the organization. The two people who indicated that they did not know of a process, in the initial query, could not offer an explanation as to why the company did not have one.

Question 6: Question six indicates the areas in which the interviewees are engaged in the product life cycle. The Answers are summarized in Table 38 – Interviewees Life Cycle Engagement.

Table 38 - Interviewees Life Cycle Engagement

STAGE	YES	NO	OTHER
Business Analysis	8	6	2
Requirements	15		1
Design	16		
Implementation	11	2	3
Testing	11	3	2
Evaluation	10	3	3
Deployment	12	4	
Maintenance and Evolution	8	6	2

Question 7 – 7.d: Only six out of sixteen indicated that the application development process is effective. The balance, of the respondents, obviously thinks that there are some problems with the current application development process. Four indicated that it was not successful and six indicated that it was successful “Sometimes”.

Out of the four who indicated that the development process is not effective, these individuals indicated that the process was not cost effective; too heavy on the documentation, too slow, and applications are chosen based on business need and not organizational fit.

Out of the respondents who indicated effectiveness “Sometimes”, they thought that the application development methodology was good for project structure and repeating projects. They thought it was not effective when considering time-to-market issues and rapid application development needs, introduction of new technology, and a lack of efficiency.

Question 8: There was a range of answers to the inquiry about the amount of time it takes to get a project from inception to delivery. The reality of the answer is that it depends on the project requirements but the average appears to be a year, give or take a couple of months. Taking a very subjective view of the numbers from the answers the mathematical average appears to be 10.9.

Question 9 – 9a: Thirteen out of sixteen respondents indicated that they feel that the project time-lines should be shorter. Two respondents feel that it really depends on the business / project requirements and one feels that it should be longer. The reasons behind the desire for a shorter process range from the loss of potential business opportunities, market competitiveness, and the need to take advantage of new technologies.

Clarifying the longer time frame response reveals that the respondent works a lot on reactive types of projects where the business unit appears with a product and the technical group has to make it work. Hence, the respondent would like more time for the implementation of the product. The underlying desire is really for the technical side of the organization to be engaged earlier in the project life cycle.

Question 10 – 10c: Question ten returned a unanimously positive result, indicating that projects exceed estimated time frames within the organization. Ten out of the sixteen indicated that it is a very frequent occurrence for projects to run over allotted time frames. Two individuals indicated that it was rare. Three individuals, including the two rare respondents, indicated that scope-cut and an increase in man-days and hours per day is a common counter measure in the organization. This common counter measure is implemented in an attempt to stay on track from a project time frame perspective. One individual indicated that he did not know how often projects exceeded time scales and one indicated that he was new to the company but was sure that it happened. One individual indicated that highly complex projects exceed time frames due to a lack of skills at all levels.

The reason for exceeding time scales ranged from changing business requirements, to complex technical environments, to a lack of technical expertise, to inadequate estimation techniques, and to inexperienced project managers. Only one respondent indicated that security did not contribute to elongated timeframes. Fifteen respondents indicated that it contributed to the issue in some form or fashion.

Question 11 – 11c: Fifteen out of sixteen respondents indicated that projects exceed the estimated budgets. Nine of the respondents indicated that projects run over budget on a regular basis. Three responded that they did not know and three responded that it was rare for projects to exceed the budget. The reasons ranged from poor managerial planning, to resource issues, to changing business requirements.

Seven of the respondents indicated that security issues have contributed to budget over-runs and three indicated that it is possible that security contributes to over-runs. Three indicated that it does not make such a contribution to overruns. There was effectively one "Do Not Know" answer and one answer that placed the emphasis on the project manager.

Question 12 – 12b.2: The purpose of this question is to determine the existence of any corporate recommendations in terms of optimal overall time frames for development. The effective answer to this question, in the organization, is that one does not explicitly exist. That there may be expectations from various business units and time frames exist within specific pieces of the overall development cycle processes.

Question 13 – 13a: Eight individuals indicated that projects always follow the in-house development project. One of the "Yes" respondents did indicate that this was a presumption. Five of the respondents indicated that all projects did not follow the development process. One of the respondents indicated that he did not know, but he suspected that they did not. Two of the respondents indicated that it happened "Sometimes".

The reasons behind the "Yes" indicate that the interviewees were responding to the extent of their knowledge. Even though some of the responders initially indicated that all of the projects followed the in-house development life cycle; further discussion reveals some underlying doubt. Two of the individuals who answered yes would not elaborate any further. One indicated in a post answer that this was to his knowledge and another one indicated that things happen out of order, i.e., start building before the design is complete.

The "No" responders indicated that reasons ranged from people attempting to circumvent the process, to critical time scales, to poor project planning. One point of interest that did surface during this line of questioning is the fact that after the design approval by Design Authority Committee (DAC), the development process has the potential to break down and be discarded in the name of project completion.

The individuals who answered "Sometime" indicate that it is up to the project manager to follow the development process and that exceptions have been made in the past in order to get around following the methodology.

Question 14: Question fourteen attempted to ascertain what individuals, in the industry, feel a security development process should contain. There were a wide range of answers for this question with several answers indicating the security development process should contain specific stages of the development life cycle. Additional answers also indicated best practices, guidelines, communication, training and accountability. All of which are valid responses, however, the lack of a clear, straightforward answer indicates a potential discrepancy in the definition of the term 'security' and the interpretation of the phrase "a security development process" within the organization.

Question 15: The idea behind question fifteen is to determine areas where security is not engaged in the development life cycle. The answers are summarized in Table 39 – Security in the Development Life Cycle.

Table 39- Security in the Development Life Cycle

STAGE	YES	NO	OTHER
Business Analysis	4	9	3
Requirements	10	1	5
Design	13	3	
Implementation	9	4	3
Testing	9	3	4
Evaluation	5	5	6
Deployment	9	4	3
Maintenance and Evolution	6	5	5

The results, in the table, indicate that there are clear deficiencies in the overall development process security visibility. Security is severely lacking in the business analysis stage. Clearly, there are issues with security in the evaluation, maintenance and evolution stages. Since the numbers are relatively close in the testing and deployment stages, it could be argued that there is a potential problem or perception of a problem, in these stages as well. In fact, the only two stages where security is clearly perceived to be involved in the development process are the requirements and the design stages.

Question 16 – 16g: This question ascertains the number of people who think there is a documented security development process. The company does actually have a document security process in the Project Security team. Their responses reveal that the knowledge of the document is restricted to specific groups. Three of the five responses indicated that the security development process was really part of the development life cycle. There were five "Yes" answers, ten "No" answers and one "Do Not Know".

Of the five "Yes" answers, it was unanimous that the security development process applies to all types of application development. The general response to the application support question is all / everything. However, one individual did indicate that the company does not have an Intranet or an Extranet. There was one individual who indicated that only the large projects actually go through the process. However, they did say that those who do not go through the process have an approved exception.

The good points of the security development process include high structure which helps to provide documentation. The highly structured process creates an environment that is conducive to audits and future reference needs.

The documentation was also listed as a draw-back to the process along with explicitly making one group responsible for security verses making everyone responsible for security. Security awareness was one point that was mentioned that still needs to be developed within the organization.

The problems that were discussed with the current security process included a lack of emphasis on the employee; a lack of utilization of the current process, a lack of security involvement after the design has been signed off, a lack of security awareness and a lack of stakeholder buy-in to security.

The point of break down appears to be around the entire development process. The process takes too long. The business has the power to circumvent the process to keep projects on track from a time-line and budget perspective; while a shortage of personnel and problems around post implementation and change management need to be addressed.

The general thought behind the lack of a security process within the organization seem to be around the fact that the individuals involved in security do not record the process; they just go do what needs to be done. These people are viewed as a resource and are accessed as needed during the development process. However, there is some confusion over when and where the Security Team actually gets involved in the process. This is taken to the point that it is viewed as the architects' problem. There is also the view that security is a bolt-on issue that is addressed after the coding is complete. Hence, the organization is only giving security lip service and not truly pursuing a security architecture infrastructure.

Question 17 – 17b: Question seventeen attempts to determine how applications are deemed secure within the organization. There were a variety of answers to this query. The answers ranged from requirements, to policies, to security standards, to processes, to testing, to audits and reviews.

The requirements, in the previous paragraph, refer to the business and technical application requirements. The policies and standards are set by the Security team and industry standards that are used to help insure security within the organization. The process refers to the creation of the DAD and submitting it to the DAC. The testing refers to internal penetration testing and third party testing.

Within individual areas there definitely would be similarities and, across the board, there might be similarities in certain policies, but as to the criteria applying to all applications, the general consensus was that it depends on the environment; the amount of risk presented and the application-facing that determines the security criteria that would be applied.

Question 18: Question 18 attempts to determine how an application is deemed secure from a development perspective. The result is that testing is subjective and tailored around the needs of the application based on the functional and non-functional requirements. The general rule is that high risk applications require more testing and third party testing.

Twelve respondents indicated that the same tests do not apply to all applications. There were also two “Yes” answers, one “Yes” / “No” and one “Do Not Know”. One of the “Yes” answers indicates two different possible paths negating that answer. Again the answers indicate that the tests used on specific applications depend on the needs of the application. Outwardly facing applications are more rigorously tested than inwardly facing applications.

Question 19: The idea behind question nineteen is to determine the stakeholders who are responsible for security at the various stages of the development life cycle. The results are displayed in Table 40 - Stakeholder Consistent Answers and Table 41 - Stakeholder Inconsistent Answers.

Table 40 - Stakeholder Consistent Answers

Survey	Answer
Number 2	Project Manager and Head of Security
Number 6	Security Team – Project Manager – Release Manager
Number 7	Project Manager
Number 11	Everyone
Number 14	Security Team

The results displayed in Tables 40 – Stakeholder Consistent Answers and 39 – Stakeholder Inconsistent Answers indicate that there is a lot of confusion about who is responsible for what and at what stages of the life cycle. An analysis of the information in Table 41 - Stakeholder Inconsistent Answers reveals that the Security Team is perceived to have the most responsibility through the various stages of the development life cycle. This is due to the recurrence of various responses to question number nineteen. This information is available in Table 42 - Response Occurrence. The ‘Blank’ response reveals that the respondent did not know the answer, indicating that there is an educational issue within the organization. An interesting observation is that the developer is number six down the list if the data from Table 40 - Stakeholder Inconsistent Answers is analysed alone and it is 8th if the data from Table 41 - Stakeholder Inconsistent Answers is taken in conjunction with Tables 40 – Stakeholder Consistent Answers. This information is useful in providing some insight to the importance of security within the culture and who is perceived to be responsible for security within the organization. The point is that the individuals responsible for developing the code are not the primary parties being held responsible for creating secure code!

This confusion over which stake holders are responsible for security supports the results obtained from question fifteen where there were clearly areas in the development life cycle where security is not involved in the process. If you do not know which stakeholders are responsible for security, it stands to reason that it would be difficult to know where security is involved in the process.

Question 20 – 20.a: Question twenty is designed to try to pin point a specific individual title that is responsible for security within the organization. Eleven of the respondents indicated that there was an individual responsible for security within the organization. There were two “Do not Know”, two “No” answers, and one blank. Out of the eleven positive responses some form of the Security Team was identified by name six times.

Question 21 – 21a: Question twenty-one attempts to determine if conflicts arise between the stakeholders and the individuals responsible for security. Fourteen of the respondents indicated that conflicts arise between the two groups. There was one “Do Not Know” answer and one “No” answer. It should be noted that the one “No” answer indicated that the conflicts arise between the individuals responsible for security and the business unit; not between those responsible for security and the developers.

Table 41 - Stakeholder Inconsistent Answers

Survey Nbr	Business Analysis	Requirements	Design	Implementation	Testing	Evaluation	Deployment	Maintenance & Evolution
1	Blank	Blank	Architecture Team	Architecture Team	Architecture Team	Blank	Architecture Team	Blank
3	Project Originator	Author Business Requirements & Project Manager	Security Team – Architecture Team – Project Manager	Infrastructure Team	Testing Manager – Project Manager	Project Manager	Infrastructure Team – Project Manager	Security Team – Architecture Team – Business Unit
4	None (No One)	Project Manager	Architecture Team - Security Team	Infrastructure Team – Security Team	Infrastructure and Security Team	Project Manager – Infrastructure Team	Security Team – Project Manager – Release Manager	Everyone
5	None (No One)	Security Team	Security Team	Security Team	Security Team	Security Team	Security Team	Security Team
8	Business Analysts	Business Analysts - Designer	Architect	Programmers - Infrastructure Team	Testers	Programmers - Infrastructure Team	Programmer – Infrastructure Team	Infrastructure Team
9	Business Project Manager	Release Manager	Architecture Team	Architecture Team	Test Manager	Architecture Team	Security Team	Security Team

10	Business Unit	Blank	Security Team – Architecture Team	Blank	Blank	Blank	Blank	Blank
12	Blank	Development Team	Security Team – Architecture Team – Infrastructure	Security Team	Testing Services	Blank	Security Team - Infrastructure Team	Security Team - infrastructure Team
13	Sponsor	Sponsor	Architecture Team – Specific coding teams	Specific Coding Teams	Tester	Sponsor	Infrastructure Team	Testers – Infrastructure Team – Specific Coding Teams
15	No One	Security Team & Identity Management Team	Security Team	Security Team	Project Team - Security Team	Architecture Team	Security Team	Security Team
16	No One	Security Team and Business Unit	Specific Coding Teams	Security Team	Testing Team	No One	Infrastructure Team	Infrastructure Team

The types of conflicts range from financial and time constraints, to conflicts over security solutions. The disagreement over the security solution appears to have its roots in the perception of the level of risk that is perceive with an application. Hence, a higher level of risk would necessitate a stronger security solution. This disagreement in risk could logically take place between both the business unit and the application developers.

Table 42 - Response Occurrence

Response Grouping	**Number of Occurrences Table 41**	**Number of Occurrences Table 40**	**Total Number of Occurrences**
Security Team / Head of Security	28	24	52
Infrastructure Team	16	0	16
Architecture Team / Architect / Designer	16	0	16
Blank	12	0	12
Project Manager (IT) / Project Team	9	24	33
Release Manager	*2*	*8*	*10*
Every One	*1*	*8*	*9*
Development Team / Programmer / Specific Coding Team	**8**	**0**	**8**
Business Unit / Analysts / Author Requirements / Project Manager	7	0	7
Tester(s) / Test Manager / Testing Services / Testing Team	7	0	7
None / No One	5	0	5
Project Originator / Sponsor	4	0	4
Identity Management Team	1	0	1

Question 22 – 22.b: The questions in section twenty-two are designed to determine the extent contractors are used in the organization and to determine if they present a major risk to the organization. The initial result is that the company uses contractors very heavily. There was only one group that did not use contractors.

The majority of the respondents indicated that contractors are held to the same application development methodology as employees. If they do use a different process, then the process is examined and approved by the proper individuals within the organization.

The majority of the respondents indicated that contractors are also held to the same security requirements as employees. However, reading between the lines in conversation, the organization does not do the testing for them on the applications that they are building. Hence, there is the underlying possibility that there could be discrepancies in application testing. How effectively this is monitored appears to be up to the project manager.

Question 23: Question twenty-three seeks the interviewee’s opinion on the emphasis security plays within the organization. The answers to this question were widely varied. Some individuals think that the emphasis on security is strong, due to outside factors such as legislation, while others feel that the emphasis is weak. A couple of individuals feel that the emphasis has improved over the past several months while others feel that the security focus is mis-aligned. Some individuals feel that security plays a large role in the organization while others feel that the emphasis is small and that security is effectively seen as an inhibitor rather than an enabler in the development process.

Question 24 – 24.a: Question twenty-four drills down to the heart of the matter to determine if the elements of the existing in-house security process are always followed. The result is that seven out of the sixteen respondents indicted that it was not always followed. There was one “Sometimes” answer and the rest indicted that it was always followed.

The reasons for not following the development process range from time pressures, to bureaucracy, to lack of awareness, to a lack of security involvement in certain aspects of the process. Other reasons that were mentioned include the lack of a process all together and where the application sits, i.e., does the application face the Internet or is it internal.

Question 25 – 25a: Question twenty-five reveals that the majority of the individuals who were surveyed (11 out of 16) feel that security should play a larger role in the organization’s development environment. Four of the individuals’ surveyed feel that the current role security plays in the development environment is accurate and one feels that there are cases where it should play a smaller role. The individuals who feel that the role should be larger base their opinion on several different reasons. The reasons that seem to re-occur through out the answers to this question are around the business. They indicate that the organization is relatively small in the financial world and protection of the reputation is critical. In the current environment, security can be de-scoped due to numerous reasons; integrating security into the development process up front would cut development overhead and increase security awareness within the organization.

One of the individuals who thinks the role is accurate believes that there is a good balance in the organization between security and the development environment. One of them indicated that it would be good to see it extended throughout the development life cycle. However, another one indicated that there is a need to engage the Security Team as early as possible. The last one believes that the current role meets project needs.

The one individual who indicated a possible smaller security role in the development process was specifically targeting internal application development. He /she believed that the role was accurate on outwardly facing business critical systems.

Question 26: Eight of the individuals surveyed feel that there is not a job related impact for not following the development security process. Two of the responders indicated that they do not know if there is an impact and the balance of the responders (6) feel that there is a job related impact.

Question 27: There were a variety of answers to question twenty-seven which attempted to determine the areas that require a greater or reduced emphasis on security within the company process. However, there were some re-occurring themes as briefly outlined as follows: four interviewees talked about business requirements, four interviewees talked about education, and five interviewees talked about testing. These themes indicate that there are problems with these areas in the organization.

Question 28 – 28b: There were a variety of answers to question twenty-eight, which asked about the major security threats during application development. Common themes include – 7 mentioned code/design/testing /requirements – 3 mentioned People and behaviour – 2 mentioned policy circumvention and enforcement – 2 mentioned viruses. There were a variety of answers to the question inquiring which of these issues are being met by the existing process, which ranged from “None” to “All”. A theme that did surface in a few of the answers is that separation of duty, code reviews and testing is sufficient within the organization. There were several “None” responses to the question asking which issues were not being satisfied by the existing process. Other answers ranged from a lack of documentation to internal and external coding issues, to a lack security in the solution design.

Question 29: The purpose behind question twenty-nine was to analyse the survey instrument. Eight individuals indicated that there were no questions that were vague or difficult to follow. Three individuals indicated that there was some confusion over the term application development versus the term that the organization uses which is product life cycle. One individual thought that question twenty-three was difficult to follow and prevented him from delivering a clean concise response. Two individuals thought that there were a lot of questions about a security development process that does not exist.

Question 30: The purpose of the last question is to provide a forum that allows interviewees to add any additional comments that they feel are relevant to the survey. Five of the interviewees did not have any additional information to offer. The answers from the balance of the responders were extremely varied. Their answers ranged from discussing interviewee backgrounds, to general discussions abut the survey, to the definition of security, to the skill sets and training of employees. The results of the study indicate that there are areas within the organization's development process that are experiencing deficiencies in security and need to be addressed, hopefully, in the near future.

Appendix V - Legislative Guidance

	US Legislation
	Electronic Communications Privacy Act
	Federal Information Security Act (FISA) of 2002
	Executive order - National Strategy to Secure Cyberspace
	Homeland Security Act of 2002
	Homeland Security Presidential Directive No. 7 (HSPD-7)
	Cyber Security Research and Development Act
	Check Clearing for the 21st Century Act
	The Economic Espionage Act of 1996 (EEA)
	The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
	The Graham-Leach-Bliley Act of 1999
	The Sarbanes-Oxley Act which was passed into law in July of 2002 [216]
	The Fair and Accurate Credit Transaction Act of 2003
	The Family Rights and Privacy Act (FERPA)
	Identity Theft Penalty Enhancement Act of 2004.
	Electronic Signatures Act
	The Computer Fraud Act of 1984
	The National Information Infrastructure Protection Act of 1996
	The USA Patriot Act of 2001
	The US Safe Harbor Act
	United Kingdom Legislation
	The Theft Act 1968 - applicable to fraud
	The Forgery and Counterfeiting Act 1981
	The Criminal Damage Act 1977
	The Protection of Children Act 1978
	The Telecommunications Act 1984
	The Public Order Act 1986 - applicable to racist materials
	The Criminal Justice Act 1988
	The Malicious Communications Act 1988
	The Copyright, Designs and Patents Act 1988
	The Computer Misuse Act of 1990
	The Criminal Justice and Public Order Act 1994
	The Data Protection Act of 1998
	Regulation of Investigatory Powers Act(RIP) 2000
	Electronic Communications Act 2000
	The Telecommunications Regulations 2000
	The Electronic Signatures Regulations 2002

Appendix VI - IM / Threat Management / Trust Model Examples

Example Number 1

Identity Management

The organization's Identity Management solution will not be used for these applications.

Exemptions from IM were sought by the projects involved with the initial deployment of these applications i.e.:

AAA Investment Platform project for AAA Website
Phase 2 - Release 1 for Application 1, Application 2, Application 3, Application 4, Application 5
BBB Release

DAD is just concerned with rolling out these existing services to a new set of users

Threat Management / Compliance

Threat Management is not being specifically undertaken for this solution.

The outsourced providers of the external services have been engaged to perform their own threat management, i.e.:

Organization 1 for AAA Website
Organization 2 for Application 1
Organization 3 for Application 2,
Organization 4 for Application 4,
Organization 5 for Application 5

Organization's existing Network Intrusion Detection System is being used for internal system threat identification for Application 5, Application 3 and Web access.

Example Number 2

Identity Management
The solution will use a modified version of the IM mechanisms already in use within Internet banking. WebSEAL, as a reverse proxy, will authenticate the client using a remote call to the pilot project authentication infrastructure, passing the authentication credentials. It is expected that this infrastructure will be externally hosted.

The user identifier and the authentication result will then be propagated to the WebSphere environment, where the WebSphere TAM plug-in will be used to provide Role Based Access and Control (RBAC) for protected components.

Threat Management / Compliance
The primary threat for the project is the exposure to the Internet that it requires in order to function. The primary defences for the project are the same as for Internet banking since the threat is the same and the infrastructure used for each project will be the same.

See the XXXX banking DAD for more details.

Figure 17 - IM / Threat Management / Trust Model Examples - Continued

Trust Model
Trust will be established between each component in the system in the following way:

Browser to WebSEAL
SSL, 128 bit encryption.
This portion of the communication is most vulnerable; therefore, the channel is encrypted. The users provide their authentication credentials through the encrypted channel which allows us to trust the overall session.

WebSEAL to IHS
MA-SSL, MD5 Signed.
Internal communication. MD5 signed to allow for mutual authentication, null encryption used to allow for network IDS.

IHS to WAS Plug-In
MA-SSL, MD5 Signed.
Internal communication. MD5 signed to allow for mutual authentication, null encryption used to allow for network IDS.

*Note: the following information has been modified to ensure that the name of the company and the names of the applications involved are kept anonymous

Appendix VII - Post WES Implementation Industry Survey Question

Thank you, for participating in this brief questionnaire. The purpose of this exercise is to assess the company's development process. You are not being examined. As a result there is no right or wrong answers, it is your opinion that is being sought. Therefore, this questionnaire will be conducted with your anonymity ensured. Understand that the interviews are conducted in confidence and that I will not record or disclose any personal information.

I would request that participants do not discuss the survey with anyone else in the company as this may invalidate the survey results.

1. What is your current job title/role?
2. Briefly describe the key areas of your job function/role/responsibilities?
3. How important do you think security is to the organization?
   - Unimportant
   - Somewhat important
   - Important
   - Very Important
4. How much impact does security have on your job?
5. Are you involved in the solution design process? YES / NO
6. If "YES" to question #5 - How long have you been involved in the overall design process?
7. Do you have experience in creating a DAD? YES / NO
8. If "YES" to questions #7 - What version of the Design Template did you use and where did you get that version?
9. In your experience, have you noticed any major differences in the way that security has been addressed over the past few years in the design process? YES / NO
10. If "YES" to question #9, - What differences?
11. Were you aware of the security initiative that has been taking place in the solutions design group?
12. What do you think of the organization's design process and its applicability to security?
13. Have you read the security white paper (Solutions Design's 2005 Security Initiative) that I submitted to the Solutions Design group? YES / NO
14. Are you familiar with the sections of the DAD that were added in version 1.4? YES / NO (Security - IM, Threat Compliance, Trust Model, Conditions, Socialization Modification)

If YES to question 14, questions 15-29 refer to that answer; if question 14's answer was "NO", please go directly to question # 30

15. Did you experience /perceive any problems with the completion of the new **Identity Management (IM)** section within the DAD?
16. Did you experience /perceive any benefits with the completion of the new **Identity Management (IM)** section within the DAD?
17. Did the addition of the **Identity Management** (**IM)** section hinder or assist with the overall design process?
18. Did you experience /perceive any problems with the completion of the new **Threat Compliance** section within the DAD?
19. Did you experience /perceive any benefits with the completion of the new **Threat Compliance** section within the DAD?
20. Did the addition of the **Threat Compliance** section hinder or assist with the overall design process?
21. Did you experience /perceive any problems with the completion of the new **Trust Model** section within the DAD?
22. Did you experience /perceive any benefits with the completion of the new **Trust Model** section within the DAD?
23. Did the addition of the **Trust Model** section hinder or assist with the overall design process?
24. Did you experience / perceive any problems with the completion of the **Condition** section within the DAD?
25. Did you experience / perceive any benefits with the completion of the **Condition** section within the DAD?
26. Did the addition of the **Condition** section hinder or assist with the overall design process?
27. Did you experience / perceive any problems with the completion of the modified **Socialization** section within the DAD?
28. Did you experience / perceive any benefits with the completion of the modified **Socialization** section within the DAD?
29. Did the modification of the **Socialization** section hinder or assist with the overall design process?

---

30. What do you perceive as the overall weaknesses in terms of security in the current version of the DAD template?
31. What do you perceive as the overall strengths in terms of security in the current version of the DAD template?
32. What other factors contributed to the successful or unsuccessful attempt to integrate security in the design process?
33. Were any of the survey questions vague or difficult to follow?
34. Are there any additional comments that you would like to make about the questions?

Appendix VIII - Post WES Implementation Survey Answers

Question 1 - What is your current job title/role?

Nine of the respondents indicated that they worked in the architect area of the organization. One indicated that he was a business designer who worked as an architect when needed. Another respondent is a Lead technology consultant and portfolio lead. One respondent was an infrastructure architect and two were security analysts.

Architecture Responses:

- Technical Consultant within the architect team
- Architect
- Architect
- Technical consultant - I take business requirements and turn them into designs – conforming to architecture and security standards.
- Technology Consultant in Architect group
- Infrastructure Architect – Design hardware component end-to-end for a given solution
- Architect
- Architect
- Architect

Other Responses:

- Business Designer but working as a solutions designer when needed
- Lead Technology Consultant and Portfolio Design Lead
- Security analyst within the security project team
- Security Analyst

Question 2 - Briefly describe the key areas of your job function/role/responsibilities?

Eight of the respondents are directly involved with the architecture design of new systems. Two of the respondents work in security, one works with data, one works with the business and one respondent provided a very general answer to the question.

Solutions Architect / DAD Creation Responses:

- High level Design - which leads to the DAD creation and later design governance (in terms of the detail design that is produced by the individual engineering rooms)
- Creating DAD, input into technology and solutions that are being implemented into the organization, working with 3rd parties and ensuring that they adhere to our standards. Coordinate the design with different departments such as security and architecture standards.
- Analyze and evaluate solutions, i.e., solutions architect
- Producing DADs providing governance for engineering rooms

- Proposing solutions architecture for projects run by the organization - syndicating and seeking approval for the proposed solutions.
- Shaping Architecture in the early stages of a project, providing a high level costing of the project, governances of designs (in my auspice) and line management, and resource responsibilities.
- Lead project role – responsible for design and delivering technical solution for Large scale projects
- Producing High level Designs for high level development

Security Personnel Response:

- Responsible for making sure solutions meet internal policy, standards, external regulation and, in general, good security practices. Also, responsible to raise security risk where appropriate if first bit is not met.
- Analyse solutions to find gaps in analysis - contents – and reduce risk

Business Perspective Response:

- Take Business requirements and come up with business solutions within the business application suite.

Data Management Response:

- Working in the regulatory and compliance space – dealing a lot with data management and data mapping

General Response:

- Ensuring that existing or newly deployed systems are capable of providing performance, resiliency and security to meet the needs of the solution.

Question 3 - How important do you think security is to the organization?

Eleven out of the thirteen respondents indicated that security is ‘Very Important’ to the organization. One said that it was ‘Somewhat Important’ to the organization but personally thought it was Very Important. One indicated that it was ‘Important’ to the organization but that it should be ‘Very Important’.

Question 4 - How much impact does security have on your job?

Eight out of the ten respondents indicated that security affected their jobs a significant amount. One respondent indicated that it was not a lot, one said some, one respondent answered by using project experience and one indicated that security has become more focused. One respondent discussed the role of security in design work.

Not a Lot Response:

- On a day-to-day basis, not a lot – security is a focused activity that takes place during design.

‘A Lot / Significant /Pretty High/Huge’ Responses:

- A lot - everything has to be compliant – using secure methods – it is something that is always there and you have to be aware of.

- A lot - everything you do has to consider the security impact
- A lot – realistically it is a key factor in any design
- Significant in design role – I spent a lot of time with security working on security issues. A lot of my work involves working with development work conducted in external organizations which requires a lot of coordination with the security team and external organizations on security issues.
- Pretty High - every solution considered needs to include security requirements – if not meeting all of the requirements - detail how risks are mitigated
- Huge impact, it is what I do.
- Large Part - Can not design system that is not secure - same as robustness in design – equally problematic - All NFRS are there for a reason, ignore at your peril – security/ scalability/robustness – pain in the ass
- 100% Total impact

Some Response:

- Some. The respondent tries to ensure that the shaping he/she is doing from a (Design Perspective) is within (what they think are the) general security principals.

By Project Response:

- First project very little impact - Second project - Third party company interactions where they are administrating customer data – security in this case was massively important. Hence, it is really project dependant.

More Focused Response:

- More focus now than before and, in some respects, it is easier; the requirements are more clearly defined (in terms of what security is looking for - it is put into writing more than in the past and there is more policing)

Discussion Response:

- Good security should not have any impact - it should just be there. Secure enough to do the job – not intrusive. No real impact - day to day perspective. Important part of the design work

Question 5 - Are you involved in the architecture design process?

The result is a unanimous ‘Yes’.

Question 6 - If “YES” to question #5 - How long have you been involved in the overall design process?

There was a wide range of responses to this question that included as little as three and a half months to as much as sixteen years. A very lose average of the number of years the ten interviewees have in the architecture design field calculated to be roughly, seven years.

Question 7 - Do you have experience in creating a DAD?

Eleven responders indicated ‘Yes’, one said ‘High Level Design - Yes’ and one said ‘No’. The ‘No’ respondent did indicate that they provided plenty of input into the security sections of the DAD.

Question 8 - If “YES” to question #7 - What version of the Design Architecture Document (DAD) Template did you use and where did you get that version?

Nine respondents indicated that they have used a new version of the Design Architecture Document (DAD). One respondent indicated that he/she had used an older version of the template; one indicated that they did not know the version number and that he got it from the architects with the skeleton filled in. Two respondents indicated that they do not fill out DAD’s and both of them knew where to get the latest version.

New Template Responses:

- The last templates that I worked with are 1.4 for the final DAD and 1.3 for the preliminary DAD. The templates were gathered from the DAC team room or the architecture team room - do not remember which.
- Version 1.5 got it off of the organization’s general site (OGS).
- Used several different versions and I am currently up to 1.5 – I have used up to 3 or 4 versions - Got the latest from the organization’s general site (OGS)
- DAC Team room until it went to the organization’s general site (OGS) - started working with version 1 ish – last version used 1.4
- 1.5 for the last DAD – got it from the architects’ team room
- Got the latest version from an architect – they had done the preliminary DAD and the interviewee picked it up from there. Other-wise, got it form a team member.
- Have used the last four or five versions – the latest version was 1.5 and got it out of the organization’s general site (OGS).
- Last version used was 1.5 – from the DAC team room
- Organization’s General Site (OGS) - Latest version 1.5

Other Template Responses:

- Last DAD that I wrote was version 1.3 - I do not remember where I got it.
- Do not know version – but do get it from the architects – get it with skeleton filled in.
- N/A – I do not create DADs, but would get it from the organization’s general site (OGS).
- N/A – but knows where to get the information - organization’s general site (OGS) and version 1.5

Question 9 - In your experience, have you noticed any major differences in the way that security has been addressed over the past few years in the design process?

Eleven respondents said ‘Yes’ to question nine. However, one of the ‘Yes’ responses did change the years to months in his/her response. Two respondents said ‘No’.

Question 10 - If “YES” to question #9, - What differences?

Out of the eleven who responded ‘Yes’ to question number nine, there were five respondents that indicated that security has increased in some form or fashion. It should be noted that one of the ‘No’ respondents also gave an answer for this question during a discussion after question nine. There were five general discussion responses to the question; one of which is a ‘No’ response who went on to elaborate. Two responses implied that security is having a greater impact now than in the beginning.

Higher/Tighter/Increased Focus Responses:

- Much higher profile - there are more team members that are involved in security in the various projects that are taking place in the bank in our team (there is a person that is security specific) and more resources are available from the security team.
- Security has been tightened up - the interviewee is experiencing more kick-back to look at items.
- Mainly focus – there is a lot more. An example is the increased focus on the type of data and the level of security around the data.
- More significant - more involvement from security and more information being required from external vendors – the organization is a risk averse organization which focuses on this type of activity.
- Guidance in DADs more specific - there are additional sections that need to be filled out - in general has improved, i.e., more regular – more consistency - from a security perspective.

General Responses:

- In that the way security has been addressed in general - but there have been changes to the design template in the solutions design group. (One of the NO responses that went on to elaborate)
- Responsibility for design of security moving from security to the architect - more use of formal security reviews taking place. 14 to 18 months ago, not aware of formal security reviews taking place - now regularly - also - now do not get as much opposition to budgeting man days for security as in the past.
- Now security is represented on the DAC with the ability to reject /accept/condition designs – non-functional security requirements now exist - there is a dedicated team to make sure projects meet security requirements and a review process to make sure an external organization meets security requirements. Security Project team now has a frame work for consistency of security analyses of a project.
- A little more security through the NFR addition to the DAD - a lot more organized now.
- One employee left the organization – another employee transferred to the infrastructure design group – the architecture group does not have in-department coverage as far as personnel are concerned. Culture is changing and influence is there; issues are currently being addressed as a result.

Implied Impact Response:

- Impact of legal issues SOX, etc., the emergence of autonomous hackers, i.e., virus and worms – systems being compromised by automated code. In the beginning security started with fire-walls, then went to policies, then back doors, and then into RAS, etc. Best practices from governments along with some commercial drivers. ITDL – UK Web site – governs things - expanded to cover standards and methods.

- The introduction of fire walls / virus checkers for Web based systems (Started in the late 80's early 90's) last few years Java based systems / Web browsers. Regulatory influences been around for a few years – as well as hackers.

Question 11 - Were you aware of the security initiative that has been taking place in the architecture group?

There were four 'No' responses and one 'Not really' response to this question. There were seven 'Yes' answers and one respondent indicated that he/she was aware more people were focused on it in the group but not aware of a specific project. He/she also indicated that there is still a gap to having it done properly in the group.

Yes Responses:

- Yes
- Yes
- YES – I have been involved in the surveys and aware of changes to the design template but, otherwise, would have said no.
- Yes
- YES – aware of DAC process improvement attempts
- Yes
- Yes

No Responses:

- NO - not specifically – there has been a continual beefing up of the group in terms of security and it has been gradual over time.
- No
- Not Really – Started before Arrived
- No
- No

Other Responses:

- Aware more people were focused on it in the group but not aware of a specific project – there is still a gap to having it done properly in the group.

Question 12 - What do you think of the organization's design process and its applicability to security?

Six respondents gave fairly positive responses and seven respondents gave fairly negative responses.

Positive Responses:

- OKAY – with the extra resources being assigned to the projects there is more involvement from a high level and a low level design perspective.
- The process is constantly **enveloping** - learning and modifying appropriately - security is involved in the process – overall the process is reasonably applicable to security.

- Gotten better - Non-functional requirements are in a central place – in the past it has been ad hock, depending on who you talked to, you got a bit of opinion - they have formalized the process a bit.
- Overall the design process is very though - security elements being weak up until now - it is now very applicable to security.
- Design process is good if not circumvented – gated process which is what you want – but people are allowed to go through without satisfactorily satisfying gates or gates are not in the right place.
- It is certainly applied well enough during the design - sceptical that security input, i.e., encryption – actually implemented into production. Does anyone actually follow up to be sure we are compliant?

Negative Responses:

- Organization does not focus enough on it and uses it as an escape goat. Usually security is cramped into a specific project that is due by a specific date - projects are not clearly defined before it gets into a project mode – Security is not done early enough in the process. Generally, security is put around a product that meets the needs of the business.
- **Long winded & Convoluted Response:**
  - Long winded & Convoluted – DAD open to interpretation - it needs to be more specific – out of the sections, the security section does a better job of detailing what is expected via the guidelines.
- **Two Part Responses:**
  - Considers the question a 2 part question:
    Part 1 – The organizations design process could do with some improvement – generally it is very good.
    Part 2 – Security seems to be an add-on not the main focus. In other words, you look at a solution FIRST and then see if security is applicable. The two ways of approaching the problem include; the most secure solution to solve a problem vs. looking at the solution then examining the security aspects.
- At large the process could apply to security but we miss the start because we do not capture security requirements from the start. No business drive for security – could be fixed if security requirements are gathered from the start.
- Do not think the process is the problem / people are the problem (hindrance) – ex: people not knowing where to get the latest information.
- The design process is not very good - Major overhaul needed. Whole end-to-end needs to support governance and to be traceable from end-to-end. Needs a phased approach - there is a lack of stage gates. The lack of stage gates and lack of traceability is an issue for security as well. Seems to be a bit of disjoint between security section and the security non-functional requirements and what is used to decide on approval.
- Process slow – hoops that are required are time consuming and high cost –belts and braces too many times makes the delivery slow to market – too many tactical solutions - compromises across the board.

Question 13 - Have you read the security white paper (Architecture's 2005 Security Initiative) that I submitted to the Solutions Design group?

There were eleven 'No' responses and two 'Yes' responses to this question.

Question 14 - Are you familiar with the sections of the DAD that were added in version 1.4?

There were thirteen 'Yes' responses to this question with one interviewee volunteering that he/she 'liked the fact that it was all in one section - helped with discussions with security'.

Question 15 - Did you experience /perceive any problems with the completion of the new **Identity Management (IM)** section within the DAD?

There were seven 'No' responses to this question, four respondents indicated that they had problems; one said that it was not relevant to their area, and one did not have any experience in filling out the section.

<u>No Responses:</u>

- No – latest DAD that I created there was no IM impact. Interviewee did say that he had IM experience in the past and could tell that the project that he was working on did not have any IM relevance. He did indicate that the section may be a bit tricky for new people that did not have any experience with IM.
- NO – "Not applicable, works quite nicely in that section of the DAD"
- Projects building off existing infrastructure or not applicable - so there have been no problems – one issue is the level of detail that is needed from checking it off from a DAC or security perspective. An example would be to use IM in the standard way and not have to explain that in every DAD.
- No – DAD produced by the interviewee was built on existing IM solution
- NO
- No – might be good to split out specific components - how does the solution specifically address authentication and authorization and, if not, how are you going to address it?
- Something never paid much attention to before – had to get head around - made me think about security - ignored for years – but after I thought about it - everything was okay – did wonder once or twice if too rigorous.

<u>Problem Responses:</u>

- In the beginning, had a problem trying to understand scope of the IM and what was expected but by the end there were no problem. The guidelines from the IM shop and the ones in the DAD template were very helpful.
- Yes – general lack of understanding of what IM is and where and how it should be used by the architects. Section could be evolved to make sure what architect needs – but first need to understand & know what it is and how it is to be used.
- YES – general feeling that no one knows what is suppose to go in there - no understanding of the value.
- Not applicable to all Projects

Not Relevant Responses:

- Not relevant for applications in interviewee's area – each application has its own IM solution.

No Experience Response:

- No experience – too many projects are not embracing IM, is my perception.

Question 16 - Did you experience /perceive any benefits with the completion of the new **Identity Management (IM)** section within the DAD?

There was one 'No' response, two 'Not relevant' responses, one 'Not the way we are doing it' response, and one no experience response. There were effectively eight positive responses to the question.

No Responses:

- 'No' response - No – IM is not applicable to a lot of projects on which the interviewee has been working.

Not Relevant Responses:

- 'Not relevant' response number one - IM was not relevant for the projects that the interviewee has worked on but the section is important from a learning curve and understanding why IM is there and understanding the importance and defending the design decision in the DAC review process.
- Second 'Not relevant' response - IM is not relevant for applications in interviewee's area. Each application has it own IM solution

Not the way we are doing it Response:

- 'Not the way we are doing it' response - Not the way we are doing it just now. It should be adding value, there needs to be more education to make it worth while. There is value to be added but it is not sold from a European perspective. People are not seeing the benefit - cost etc.

Positive Responses:

- 1st positive response - It explicitly calls out IM - it is good to acknowledge it and state the impact - it is also query-able by members of the DAC during review.
- 2nd positive response - Provides effectively a check list for items to be covered or specifically not covered - it provides a level of comfort.
- 3rd positive response - It is a good section to have forcing designers to make a decision on whether IM is appropriate and documenting reasons (forcing information) for and against " Getting people to think – not easy to do"
- 4th positive response - YES makes people think of IM first - it focuses people into considering IM vs. thinking their own AAA (authentication, authorization and Audit) model is fine.
- 5th positive response - Forced you to recognize that IM was our strategic solution
- 6th positive response - Do not see more designs using IM – due to general miss conception of where IM can be used - architecture fault – they are not pushing

IM use in other areas. It is a benefit to know that it is there – it started the ball rolling - but need education program

- 7th positive response - Made me think about it, which had not done before which was good - if not explicitly called out would not have given it a second thought.
- 8th positive response - It is good that the section is there if you are changing it - in the respondent's opinion, securitization should be par for the course. Anything outside of the norm should require the architect to say how they are going to bolt it down.

No Experience Response:

- No Experience

Question 17 - Did the addition of the **Identity Management (IM)** section hinder or assist with the overall design process?

There were seven responses saying that it 'Assisted'. There were six other responses as follows: one 'Both', one 'No Change' one 'Non-Event', one 'Neither', one 'No effect', and one 'No Impact' response.

Assist Responses:

- Assist in the overall process - due to the fact that it explicitly calls it out.
- It did assist due to the fact that you have to give consideration and decide what to put into the section from a design perspective.
- Caused people to consider IM, more definitely raised awareness of IM – from that perspective, it is an assist.
- Assisted it
- Did not hinder - assisted posting IM question earlier - Assisted overall.
- Did not hinder – assisted in as much as thinking about a specific area
- Assist provides visibility and awareness for designers - raises profile

No Effect / No Change / Non-Event / Neither

- No Change
- Non-event – it is there for projects that require IM.
- Neither - just confirms existing solution fitted with the existing security package.
- No Effect
- No Impact

Both Responses:

- Both – Assist – forces design down a rout that is more acceptable to service provision and security, removing objections before they happen. Hinders, causing communication problems with external parties. The architect has to explain that they can not simply say no – you have to get them to explain in detail as to why.

Question 18 - Did you experience /perceive any problems with the completion of the new Threat Compliance section within the DAD?

There were six ‘No’ responses, five ‘Yes’ responses, one ‘Did not effect’, and one ‘No experience’ response.

No Responses:

- No - had a specific person from the security group that was assigned to help. – They helped with the completion of the area.
- No problems - straight forward – note the section to some extent is open to interpretation, ex., do you need 3rd party threats identified, i.e., **interviewee put non currently identified – to basically cover unseen threats.**
- No – Not application DADs that have been produced - most of the threat stuff is on external facing applications.
- No problems, used guidance notes in the template - just verified compliance tools.
- No problem with this section.
- No – been aware of for a long time - no problems at all

Yes Responses:

- Yes – No definition of threat management or how we should deal with it - put section in the DAD and expected people to know how to fill it in - far easer to not read the guidelines and moan.
- Yes – Much clearer definition of trust compliance is needed – I am a fully qualified security consultant and I had to look at it twice. Threat / Identification / Management might be clearer - More information on the back-end programs that are available within the organization is needed.
- Yes - no example given - more education is required around threat management. What is the organization’s standard for threat management? The designer needs to understand what is available.
- Yes – people still do not know what it is and how it should be used - section never completed - Needs to be backed up with education.
- Perceive a problem – threat management should be a service that should apply to all designs – “kind of like putting an electricity section in the DAD”

No Effect Response:

- ‘Did not effect’ response - It did not effect the completion of the DAD.

No Experience Response:

- No Experience

Question 19 - Did you experience /perceive any benefits with the completion of the new Threat Compliance section within the DAD?

There were in effect four positive answers, two non-committal answers that could be taken positively, one ‘No effect’ answer, one ‘No experience’ answer and five ‘No’ answers.

Positive Responses:

- Assist in the overall process - due to the fact that it explicitly calls it out.

- Specifically calling out what is expected makes the approval process better – process not as iterative as in the past – no problems.
- YES – focuses design effort in that area to be sure that it is actually being considered to ensure that there is a safety net there - Post IDS etc.
- YES - the fact that it flagged up a requirement that needs to be addressed in the design process.

Non-committal Responses:

- It made me think about the requirements in that area.
- Again – important to consider what to give thought to – always unforeseen issues exist.

No Responses

- No – Not applicable to the DAD's that have been produced - most of the threat stuff is on external facing applications.
- No – do not know anyone that has put anything meaningful in there.
- No benefit what-so-ever, never completed - Security needs to educate the designers.
- NO
- NO - it did not make the design or the document easier. It did help to define some of the design challenges.

No Effect Response:

- Did not effect the completion of the DAD

No Experience Response:

- No Experience

Question 20 - Did the addition of the Threat Compliance section hinder or assist with the overall design process?

There were four positive answers, six no effect style of answers, two hinders responses and one 'No experience' response.

Positive Responses:

- It assisted with the overall process
- It assisted; helped a lot.
- Does not hinder – does mean that there is more thinking up front and interaction with external vendors to get answers
- Did not hinder – assisted in as much as thinking about a specific area

No Effect Style of Responses

- No Change
- Non-event – it is there for projects that require IM.
- Neither
- Did not make a difference

- No – Impact – no interaction with threat management team. Question the usefulness of the whole section - if it needs to be in the DAD.
- No Impact - just a few extra words in the DAD.

Hindered Response:

- Hindered – Lack of info available on threat mitigation software available within the network or host file.
- At the moment it hindered - not a lot of clarity around the area – overall, it will benefit.

No Experience Response:

- No Experience

Question 21 - Did you experience /perceive any problems with the completion of the new **Trust Model** section within the DAD?

There were four positive responses, four negative responses, four answers that indicated there were issues with the section and one 'No experience' response.

Positive Responses:

- No difficulty - used security resources while writing the section – on the last DAD that this particular interviewee completed, there was more relevance to the trust section than the IM section, hence, there was more work done on this section.
- No
- No problems - having each section in there and forcing response makes the process better.
- Same as IM but more so - should really think about, but would have ignored totally if had not been there.

Negative Responses:

- Yes - understanding concept trust – confusing for one of the specific projects that the interviewee worked on because it did not appear to be a necessity from a design perspective due to the design that was being implemented.
- YES, trust mode led me to think of COM application objects at first, but did not take me long to dispel.
- "No trust at all" Basically not applicable for DADs completed or use standards.
- "Perceived as a pain in the ass" – If standard trust model exists apply it to all (internally).

Issues Responses:

- Language used was too specialist – level of knowledge expected is not there and the interviewee did not know anyone that has put anything meaningful in there.
- Built off existing trust model – however, not sure exactly what a trust model is or how it works.
- It would have helped with an example diagram. What trust is in place in the organizations at the moment? An example would be excellent – particularly

comparing external and internal infrastructure – standards would be good to include.
- Trust Model very important in today's solutions – there is a lack of understanding on where and when to use it.

No Experience Response:

- No Experience

Question 22 - Did you experience /perceive any benefits with the completion of the new **Trust Model** section within the DAD?

There were seven positive, five negative responses and one 'No experience' response to this question.

Positive Responses:

- Benefit is to call it out early and explicitly.
- If you have to implement, it helps with the reasoning from a review process perspective - Providing a defence etc.
- To help know what you should be looking at
- No problems - having each section in there and forcing response makes the process better.
- YES - Ensures enter that passing of authentication, authorization information is considered rather than add hoc.
- The fact that it flagged up the need to think about it is good.
- Made me think about it and call it out as an issue

Negative Responses:

- No, No, None, None what so ever – not completed, No.

No Experience Response:

- No Experience

Question 23 - Did the addition of the **Trust Model** section hinder or assist with the overall design process?

There were five positive answers to this question. There were five answers indicating no effect, one non-committal response, one negative response and one 'No experience' response.

Positive Responses:

- Assisted with the overall process
- Definitely assist – again knowing what you need to complete.
- YES – assisted, moved barriers to security and **S.P.**, created barriers when dealing with 3rd parties.
- Does assist in complementing non-functional requirements but the architects do not know what to put in that section. Security should have education of what to put into that section. The trust model issues needs to be examined from a high

level and discussion around who completes the section from a consistency perspective the SD or TRS.

- Same as IM - Did not hinder – assisted in as much as thinking about a specific area – certainly did not hinder.

<u>No Effect Responses:</u>

- No Difference, No Effect, Neither, Neither, No Impact

<u>Negative Response:</u>

- At the moment hindered - slows down production of DAD - especially if on shared infrastructure where everyone knows the trust model.

<u>Non-Committal Responses:</u>

- Did not hinder – question of weather the trust needs to be there and helps with the understanding of the architecture of the overall project being implemented.

<u>No Experience Response:</u>

- No Experience

Question 24 - Did you experience / perceive any problems with the completion of the **Conditions** section within the DAD?

Eight respondents indicated that they had no problem with the conditions section of the DAD; two respondents discussed the problem, and three respondents who had no experience with the section.

<u>No Problem Responses:</u>

- No problems - no conditions on projects that the interviewee has been working on as of yet – but sees the necessity – conditions appear regularly in the DAC process,
- No
- No - problems are with the conditions that are applied to the design – not always true conditions for design – some are really project conditions.
- No Problem
- No – but have to complete after DAC – would have thought it better to have a central log - can see the benefit form having it in the DAD from an audit perspective but better from a DAC management perspective to have the conditions in a central log. Architects are re-assigned after an approval creating time constraints.
- No
- No
- No – it is good

<u>Discussion Responses:</u>

- The section itself is straight forward - the big problem is really in the definition of true conditions vs. comments. The DAC suffers from a lack of a good definition of a good condition. The minutes are also a problem; there is no

differentiation on what is a condition and what is a comment or action – hence everything gets lumped under the condition section.
- Adoption of it has been the problem and the explanation of how it fits into the process – Lot of discomfort with changing a document that has been approved.

No Expertise:
- Do not think they go into the DAD – go to clinics update DAD – not condition section – if it gets to the DAC then it should be added to condition section and then taken care of before it goes live. However, it is not currently used by the interviewee – due to not gotten that far in the process.
- Still going through process – have not filled out.
- Have not gotten to it yet - not gone to DAC

Question 25 - Did you experience / perceive any benefits with the completion of the **Conditions** section within the DAD?

There was only one respondent that gave an initial negative answer. That same respondent also provided a positive comment after the initial negative response.

Positive Responses:
- It is a good place to record what has taken place – the problem is that it goes into the DAD after the DAC has meet – who reads it? And is it the right place to record the information?
- Collect everything needed and provides a complete document.
- Can see the benefit of having it there but did not use it.
- As a record it is good to help improve understanding for conditions in future DADs.
- Good addition from an audit-ability perspective.
- Having them already in a section where we could say how they were addressed is very helpful – interviewee picked up a preliminary DAD with the condition section filled in by architects and completed the final DAD.
- YES – it has more chance of getting them done.
- There is no other place where these issues are being tracked – so there is benefit in having them there.
- Use a lot - SD becomes responsible for conditions in the design because recorded in solution.
- Better that it is documented - it is a bit more formal now.
- It is good - back to continuity of governance.
- Good Idea - provides understanding of responsibilities

Negative Responses:
- No - could ensure conditions are not missed.

Question 26 -Did the addition of the **Conditions** section hinder or assist with the overall design process?

Eight interviewees indicated that the conditions section assisted in the overall design process. Two indicated that it hindered to some degree, two said ‘Neither’ and one did not have any experience.

Assisted Responses:

- Assists in keeping things in context with the DAD and provides an audit trail.
- Definitely assist on focusing on exactly what the conditions are and what the resolution to them is.
- Assisted
- Assist - YES – it has more chance of getting them done – formalizing and focusing on issues that are likely to get dropped.
- Assisted - overall - more concept of conditions but overall assisted
- Organization perspective assisted - audit compliance
- Assisted - definitely
- Assisted – formalized it - helps the document

Hindered Responses:

- Does not assist – considered after the design process and DAC meets. The conditions are added after the DAC.
- Did not hinder – except where the condition is not a design condition.

Neither Response:

- Neither
- Neither

No Experience Responses:

- Did not come across it

Question 27 - Did you experience / perceive any problems with the completion of the modified **Socialization** section within the DAD?

Eleven of the respondents indicated that they did not have a problem with the modified socialization section of the DAD. There were two respondents that had an issue with the section.

No Responses:

- No problems
- No - None
- No
- No
- No
- No problems
- No problems
- No
- No
- No
- No

Problem Responses:

- Not been taken up across the board – used in some DADs, not all.
- Issue the doc before you have done the socialization – no one reads, by the time it is issued to DAC, the final version is not socialized again.

Question 28 -Did you experience / perceive any benefits with the completion of the modified **Socialization** section within the DAD?

Twelve out of the thirteen respondents gave positive feedback to this question. One respondent did not have any experience with this section of the DAC.

Benefit Responses:

- It provides a double check to be sure that nothing has been missed.
- It is ideal to have due to the fact that it tells you who to socialize with and provides a place to record the conversations that took place. Hence it helps in the DAC process.
- Helps identify who is supposed to be going through.
- Big benefits provides audit trail to process - questions that were asked and the answers – publishing to a wide audience.
- Good record and reminder of who to socialize with - also good for people not completing the DAD regularly – good check list. Socialization group seems to be growing.
- YES – Mainly preventing socialized individuals claiming no socialization or making up new conditions after it has been socialized – know of one DAC meeting it basically saved.
- Definite improvement
- Good in that it keeps track
- We get to see the designs before going to the DAC - set up clinics that coincide with socialization section - improved a lot.
- Good addition - suggest project life cycle check list
- It is good - back to continuity of governance. Record who you socialized with and what happened.
- YES – it benefits because you see all points raised at meetings and go back to check to be sure they were covered.

Not Completed Section Responses:

- No perception of the completion of the socialization section.

Question 29 - Did the modification of the **Socialization** section hinder or assist with the overall design process?

Ten respondents indicated that the modification of the socialization section assisted with the overall design process. One respondent did not notice any changes, one did not notice a difference either way, and one indicated that he/she did not have any experience in the overall design process.

Assisted Responses:

- Assist - provides a good checklist
- Assisted to help get the right people socialized
- Assist
- Definitely assisted in term of a checklist
- Assisted the design process
- Assisted - know who you are talking too.
- Assisted overall
- Assisted
- Assisted
- Assisted

No difference:

- No difference either way

Did not notice:

- Did not notice the change in the section

No Experience:

- No experience

Question 30 - What do you perceive as the overall weaknesses in terms of security in the current version of the DAD template?

Eleven respondents indicated that there were some weaknesses with the DAD. Two respondents indicated that there no weaknesses.

No Weaknesses Responses:

- 1.4 version is the version that I am familiar with – no straight forward weakness – the DAD has got to be fairly non-specific due to the general nature of the DAD but at the same time it has to provide the general headings that need to be addressed when completing a DAD so that the architect can be provided with the opportunity to provide the necessary details as needed.
- Nothing springs to mind – the threat compliance section would be good to call out recommendations for tools with specific environments.

Weakness Responses:

- Coordination with the security group - they have been looking for different things than are specified in the template – it is difficult to meet the needs of the individual security specialist expectations of what they are looking for in the DAD.
- Weakness – stuff there assumed to be in place is not necessarily there – an example designing using Oracle or the networks – I expect there to be standard lock downs in places like roles, etc. The DAD requires the designer to call out all of that information every time - even when the exact same set up is used as in the past. Another example would be adding applications to a UNIX box – every time you put something on a UNIX box, security should be providing a list of things

to use instead of having to list all of the applications that you will be using every time - like using BMC to monitor the application etc.

- The security non-functional requirements are, in general, repetitious.
- Not in the template – most of the design process focus assumes it is an internal build –not as natural a fit at times when it is an external build situation.
- Lack of understanding of security by people completing the DAD and of what the security section is looking for.
- Stock answers - cutting pasting out of other DADs – ex. As per existing threat management guidelines - Interviewee has been told that “The only way to fill it in is to find another DAD and copy it” applies to the security section as well as the overall DAD.
- Data section - security data model – bits of security throughout the document; it might be better to consolidate into one security section and just refer to the security section for the security data model. In **section 5.6.1**, this section overlaps with the security non-functional requirements. Alignment of the non-functional security requirements needs to be considered.
- Biggest issues - SD not using current security non-functional requirements - Do not think needs anymore security section - Major issue – education issues on the IM/ Threat/ Trust sections
- No full filled out document has been presented for assessment
- Maybe data protection - otherwise not much missing - Data protection of personal records very important – maybe move data protection section into the security section.
- 1 – Threat management and trust model need to go

  2 – Need to put list of security items in the DAD and Delete what is not applicable to your project

Question 31 - What do you perceive as the overall strengths in terms of security in the current version of the DAD template?

Ten respondents gave various responses on the strengths of the DAD. One respondent does not understand what the architecture group is trying to accomplish with the DAD. Two respondents provided other answers.

<u>Strength Responses:</u>

- 1.4 - Pulling out explicit information security information and how it impacts various areas - it breaks down the areas that need to be addressed.
- The overall section (guidelines) is a bit clearer than other sections within the DAD - the example is the difference between the Architecture standards section and the security section
- Helps remember what you should be looking for.
- Having the heading there to promote the appropriate questions.
- Able to give the NFRs and security section to external organizations and say how are you going to do this? And it worked very well. The documentation is much better than in the past - due to ability to say this - is what we need.
- Forces people to give it some consideration and some documentation

- The way it focuses design to have to consider it – "if not there the level of consideration that security gets is directly relevant to the amount of security knowledge the designer has".
- Much better - more guidance on what is required - be great if we had an example security section to refer to for ideas.
- Socialization / sign off piece before DAC - Security section forces architect awareness - Reference to non-functional requirements is important to security
- Good template – clearly calls out issues that you need to think about - IM/Trust/Threat compliance makes you take it seriously.

Not Understand Response:

- No definitive answer – not 100% clear as to what they are trying to establish in the DAD template.

Other Response:

- No fully filled out document has been presented for assessment.
- Security non-functional requirements **– A bit like number 2 through 30.**

Question 32 -What other factors contributed to the successful or unsuccessful attempt to integrate security in the design process?

- The allocation of specific security specialists in the last project was a big help. Security is a specialist area of expertise – the interviewee admitted that he is not an expert in the area and that it was helpful to have the recourse while completing that DAD.
- Calling out security brought it more into the loop and to everyone's attention. Coordination with people from the security section to comment and help with that section - provided a point of conversation.
- Who you deal with - it is either hit or miss and getting them to understand what you are trying to establish – an example – it is not enough to say establish a secure connection – you need to understand the security in terms of each stage of the system - in other words the connection has to be secure to the Web page and any data that is involved can not be tampered with.
- Better teaching and lessons to help explain the point of what was being asked and expected.
- None
- Significant factor – access to someone in the security area to foster communication between then and the vendor – proved very helpful.
- Lack of clear requirements and ownership of requirements - "No one has explained to the business why it should care" - Losing two people that were doing security design (type of work) did not help the situation.
- Amount of information and support available to the designers who do not have a security background - If they have the support, they will fill it in correctly – if not, then they will not.
- Do not have a lot of people on the team with security experience; most people have moved to infrastructure design.

- People issue / where / how / why security is required – education, Perception of security - there to hinder – getting better, Security perception within the project team having confidence in what they are asking has improved
- Visibility /clear goals / simple / understandable / integral part of daily routine / has to be culturally accepted and facilitate change to be a success – the organization can not be scared to air dirty laundry to learn from our mistakes.
- Nothing else
- Input from the security team on what they want from specific security sections - ‘they give us input on what they want and we give them input on reality’.

Question 33 - Were any of the survey questions vague or difficult to follow? Out of the thirteen respondents only four mentioned questions that were difficult. None of the respondents mentioned the same question.

- No, not really – the biggest issue is that the last DAD the interviewee completed was before Christmas and he had to stop to remember some of the information.
- No
- No
- Number 2 was vague
- Difficult to answer number 32 – due to the fact that the DAD completed by the interviewee already had security basically in place – built on existing solution. Pretty straight forward - so the problem is with the content not the question.
- No
- #3 – To who is security important, the organization or the person – have had conversations with the business units in the past on this subject when I think they are being loose with security.
- No
- No
- Question #4 – Look at two ways - from design and form everyday work perspective - the others are okay
- No
- No
- No

Question 34 - Are there any additional comments that you would like to make about the questions?

- No
- There is no standardization as to the way that the DAD is completed - different sections of the DAD are completed differently by different individuals. Standardization of the DAD completion (as much as possible) would help the process.
- The organization has issues with effective document management due to the fact that documents are stored all over the organization. There needs to be one location for all of the documents that shows the progression through the development process.

- No
- No
- The DAD process is simpler this time than in the past. The interaction with the infrastructure team is not as clear now – when compared with the security area.
- No
- Issues with the IM – all - if you can not integrate please detail how you handle IM / threat / trust - Useful survey - needs to be expanded to the rest of the DAD sections including the non-functional requirements' specifically. They could use some tightening and explanation - Overall Process issues with design time table being conducted backwards i.e. end date, then testing, then design, vs. design time, then testing, then end date.
- Conditions need to become responsibility of the Release Manager (RM) after DAC approval - RM should be formally notified of conditions that have been raised at the DAC
- General lacking in education, in organization of tools and infrastructure IM /threat/trust – need architecture vision for the overall security area – currently do not have. High overturn of the architects - constantly educating architects because they do not know the process / TRS responsibilities or the whole shebang.
- More questions with a 1 to 7 range would help provide quantitative measures.
- Added a revisions table - see changes requested - suggestion for future DADs Questions are focused - Subject Boring - Life Sucks - Need for business analysis information (In particular - business process analysis) now and what is wanted in the future (2B) - the business analysis information drives the design.
- Would like to take the survey again in a year, once the changes have had time to penetrate the organization.

Appendix IX - Added Paragraph in DAD v1.5

Project Sell - Legal Obligation to Financial Organization

- *State whether the change will affect the data structure of the system.*
- *State whether the data is being migrated to the financial organization.*
- *State whether the change/upgrade is planned to implement before the end of April 2006.*

- *Where the above conditions apply, we have a legal obligation to obtain permission from financial organization prior to implementing any changes. The project team will be advised to go through the change control process in order to obtain financial organization approval.*

For further guidance on any of the points above, please contact the Project Sell Change Council. (Name on Phone number or Name on Phone Number).

- ***All** projects are required to socialise this document with the Sell Change Council prior to DAC approval. Details of the Socialisation Clinics are available in the DAC workroom.*

Appendix X - CLASP / WES Comparison

CLASP Activity *	WES (SCWAD) Analysis
Institute Security awareness program	Principle - Education **(Proper Controls in the development environment)**
Monitor Security Metrics	Principle Recommendation - Synergy
Manage Certification Process	Management Issue
Specify operational environment	Management Issue
Identify global security policy	Application Security Requirements **(Proper Controls in the development environment)**
Identify user roles and requirements	Application Security Requirements
Detailed misuse cases	Project Development Risk Assessment **(Trust and Accountability)**
Performance security analysis of requirements	Application Security Requirements **(Delivery of a cohesive system)**
Document security design assumptions	Security Design / Code
Specify resource-based security properties	Management Issue
Apply security principals to design	Security Design / Code
Research and assess security solutions	Security Design / Code
Build information labelling scheme	Security Design / Code
Design UI for security functionality	Security Design / Code
Annotate class designs with security properties	Security Design / Code
Perform security functionality usability testing	Testing **(Prompt, rigorous testing and evaluation)**
Manage System Security Authorization Agreement	Management Issue
Specify database security configuration	Security Design / Code
Perform security analysis of system design	Security Design / Code
Integrate security analysis of system design	Security Design / Code
Implement and elaborate resource policies	Management Issue
Implement interface contacts	Security Design / Code / Implementation
Perform software security fault injection	Testing **(Prompt, rigorous testing and evaluation)**
Address reported security issues	Security Design / Code
Perform sources level security review	Security Design / Code
Identify and implement security tests	Testing **(Prompt, rigorous testing and evaluation)**
Verify security attributes of resources	Testing **(Prompt, rigorous testing and evaluation)**
Perform code signing	Security Design / Code
Build operational security guide	Management Issue
Manage security issue disclosure process	Management Issue

* This information is from 'Security in the software development lifecycle' by John Viega, 2004 [203]

Appendix XI - Version Analysis

Date	Version	Security Section Completed
November – 2005		
4 - DAD	1.2	
1 - DAD	1.4	All three sections filled completed
5 - Total Projects November		
December – 2005		
3 – DAD	1.3	
1 – DAD	1.4	All three sections filled completed
1 – DAD	1.5	Identity Management Section was filled completed Threat and trust were completed with the statement: "Solution to be discussed with Security"
5 - Total Projects December		
January – 2006		
2 – DAD	1.2	
1 - DAD	1.3	
2 – DAD	1.4	*First DAD* • **Identity Management section was Blank** • Threat Management section was completed. • **Trust section was Deleted** ***Second DAD*** • **IM & Threat were Blank** • **Trust Deleted**
1 – DAD	1.5	Identity Management Section was filled completed Threat and trust were completed with the statement: "Solution to be discussed with Security"
6 - Total Projects January		
February – 2006		
1 - Not a DAD		
1 – DAD	1.2	
2 – DAD	1.3	
1 – DAD	1.5	IM and Threat completed with "n/a for all components" - Trust completed
5 - Total Projects February		

March – 2006		
1 – DAD	1.2	
4 – DAD	1.5	1. All three sections were completed 2. All three sections were completed 3. **IM left Blank** / Threat and Trust sections completed 4. IM and Threat completed with “n/a for all components” - Trust completed
5 - Total Projects March		
April – 2006		
1 - DAD	1.2	
1 - DAD	1.4	• **All three sections were blank**
4 – DAD	1.5	1. All three sections were completed 2. All three sections were completed 3. IM and Threat completed with “n/a for all components” - Trust completed 4. **Security section deleted**
6 - Total Projects April		
May – 2006		
1 - Non-DAD		
1 – DAD	1.2	
2 – DAD	1.4	1. All three sections were completed **2. Security sections blank**
2 – DAD	1.5	<u>**First DAD**</u> • IM section completed with “Identity Management will not be used within this solution.” • Threat compliance completed • **Trust section deleted** <u>**Second DAD**</u> • IM Filled in • Threat - “No threats currently identified.” • Trust Filled in
6 - Total Projects May		

June – 2006		
3 – DAD	1.5	1. All three sections were completed 2. IM modified heavily, threat and trust sections completed. 3. **All three section were Blank**
3 - Total Projects June		
July – 2006		
1 – DAD	1.2	
1 – DAD	1.5	**Security section deleted**
2 - Total Projects July		
August – 2006		
1 – Non-DAD		
6 – DAD	1.5	1. All three sections completed 2. All three sections completed **3. Security section deleted** 4. All three sections completed 5. IM - heavily modified / Threat and Trust completed with the statement that the systems will conform to existing... 6. IM completed with “reuse existing design” and Threat completed with the statement “reuse existing …infrastructure” / Trust model completed.
7 - Total Projects August		

Appendix XII – Hunterian Survey

Design Interview Questions

1. Where does the current web site currently reside?
2. What is the environment? I.e. UNIX, Windows?
3. Does it have ample capacity to handle interactive web pages?
4. What web authoring tools are currently being utilized in the museum?
5. What databases are currently being used in the museum?
6. Does the database have the capability to support the potential volume generated by dynamic web pages?
7. How is security currently handled in the museum for web applications?
8. As far as the web front-end design is concerned, is there a style sheet that the museum uses?

   ____ YES ____ NO

   If YES, can you provide the style sheets?

   If YES, and you can not provide a style sheet, who can?

   If NO, are there any rules that the museum follows, & where can I get a copy?
9. Do you have any additional advice or suggestions for the system?
10. Do you need any reports from the system?

    ____ YES ____ NO

    If YES, what kind of reports?
11. Does a testing environment currently exist in the museum?

    ____ YES ____ NO

    If YES, who do I need to speak with to gain access to the environment?

    If NO, can I get a copy of the current web environment and some sample pictures, so that I can set up a testing environment within the computer science department at the University of Glasgow?
12. Do you have any ideas on how you would like the images to be displayed on the web page?

Policy Questions

1. Are there any legal issues that need to be addressed such as:

    A. Copyright display issues____

    B. Copyright acquirement issues___________________________________

    C. Additional comments or issues that need to be addressed______________

2. If there are legal issues that need to be addressed in Question Number 1, in the form of permissions, how does the museum handle this process?

3. Do you want the images to be downloadable?

    ____ YES ____NO

    IF NO, why not____

4. If the answer to question 3 is YES, is the customer allowed to conduct multiple downloads?

    ____ YES ____ NO

5. How do you want to handle the payment? ________________________________

6. Can we implement a voluntary web survey for customers?

    ____ YES ____ NO

If YES, what types of questions would you like to ask? ____________________

IF NO, why not____

7. Does the museum adhere to any standards that need to be followed?

Security Questions

1. What is the desired level of customer confidentiality within the system?

    ____ High

    ____ Medium

    ____ Low

    ____ Other (____)

2. What is the desired level of the museums confidentiality within the system?

    ____ High

    ____ Medium

    ____ Low

    ____ Other (____)

3. What is the desired level of system availability?

    ____ 24 / 7 Availability

    ____ 8 to 5 - Monday –Sunday Availability

    ____ 8 to 5 - Monday – Friday Availability

    ____ Other (____)

4. What is the desired level of system operation integrity?

    ____ High

    ____ Medium

    ____ Low

    ____ Other (____)

5. What are the levels of security that need to be addresses from the museums standpoint?

    ____ Defacement

    ____ Communication

    ____ Transaction

    ____ Other (____)

6. What are the consequences for the Hunterian Museum of the most server security breach imaginable?

7. Based on the answer to number 1 how secure do you feel the web site needs to be?

8. Based on the answers to questions 6 and 7 do you want to investigate image water marking?

    ____ YES ____ NO

    If NO, why not?

9. Based on the answers to questions 6 and 7 do you want to investigate image security?

    ____ YES ____ NO

If NO, why not?

10. Does the Museum currently have procedures, roles and responsibilities defined for disaster recovery?

    ____ YES ____ NO

If YES, can you provide a copy of the disaster recovery plan?

If YES, and you can not provide a copy of the disaster recovery plan, who can?

If NO, are there any rules that the museum follows, & where can I get a copy?

11. Where will the production servers reside and who will maintain the servers from an update and configuration standpoint?

Testing and Evaluation Questions

1. Did you find the image that you were looking for?

   ____ YES ____ NO

2. If the answer to Question Number 1 is NO, please describe the image that you were trying to locate.
3. Do you have any additional suggestions or ideas for improvements to the Hunterian Museum's image purchase internet application?
4. Please assign an overall functionality rating to the Museum's image purchase internet application.

   ____ 5- Excellent

   ____ 4-Good

   ____ 3-Fair

   ____ 2-Poor

   ____ 1-Unacceptable

Abbreviations

Agile Web Engineering	AWE
American Depositary Receipts	ADRs
Automated Secure Systems Development Methodology	ASSDM
Availability, Reliability and Security Conference	ARES
Business Case Document	BCD
Business Continuity Plan	BCP
Common Criteria	CC
Comprehensive Lightweight Application Security Process	CLASP
Data Flow Diagrams	DFD
Department of Computing Science	DCS
Department of Home Land Security	DHLS
Design Architecture Committee	DAC
Design Architecture Document	DAD
Detail Design Document	DDD
Dynamic Systems Development Method	DSDM
Economic Espionage Act of 1996	EEA
Entity Relationship	ER
Essential Elements	EE
eXtreme Programming	XP
Extreme Security Engineering	ESE
Facilitated Risk Analysis Process	FRAP

Fair and Accurate Credit Transaction Act of 2003	FACTA
Family Rights and Privacy Act	FERPA
Feature-Driven Development	FDD
Federal Information Security Act	FISA
File Transfer Protocol	FTP
Freedom of Information Act	FIA
Global Fortune 500 Financial Organization Surveys Lessons Learned	GFFFOS
Homeland Security Presidential Directive No. 7	HSPD-7
Host Intrusion Detections Systems	HIDS
Hunterian Museum and Art Gallery's Online Photo Library	HOPL
Identity Management	IM
Information Systems	IS
Information Technology	IT
International Conference on Hypermedia and Interactivity in Museums	ICHIM
International Conference on Web Engineering	ICWE
International Organization for Standardization and International Electrotechnical Commission standard	ISO/IEC
Internet Service Providers	ISP
Management Information Systems	MIS
Mutual Legal Assistance Treaties	MILAT
National Institute of Standards and Technology	NIST
Network Intrusion Detection Systems	NIDS
Operationally Critical Threat, Asset, and Vulnerability Evaluation	OCTAVE

Organization for Internet Safety	OIS
Organization’s General Site	OGS
Preliminary DAD	PDAD
PricewaterhouseCoopers	PWC
Public Key Infrastructure	PKI
Rational Unified Process	RUP
Regulation of Investigatory Powers Act	RIP
Research Libraries Group	RLG
Return on Investment	ROI
Role Based Access and Control	RBAC
Sarbanes-Oxley	SOX
Secure Socket Layer	SSL
Securities Exchange Commission	SEC
Security Audit and Field Evaluation	SAFE
Security Criteria for Web Application Development	SCWAD
Security Development Lifecycle	SDL
Security Improvement Approach	SIA
Security Improvement Initiative	SII
Software Process Improvement	SPI
Storage Area Network	SAN
Structured Query Language	SQL
Structured Systems Analysis and Design Methods	SSADM

Systems Security Engineering - Capability Maturity Model	SSE-CCM
Testing Documentation	TD
The Open Web Application Security Project	OWASP
U.K. Government's Central Computing and Telecommunications Agency	CCTA
U.K. Government's Central Computing and Telecommunications Agency's Risk Analysis Management Method	CRAMM
Unified Modelling Language	UML
Unified Software Development Process	USD
United Nations	UN
Viable Information System	VIS
Viable System Model	VSM
Web Engineering Security	WES
World Wide Web	WWW
World Wide Web Consortium	W3C

Glossary

Agile Process	A term used to describe lightweight application development methodologies.
Availability	“The assurance that a computer system is accessible by authorized users whenever needed” [90].
Bell-LaPadula	An information security confidentially-based model that permits access modes based on a set security policy, i.e., Classification: Top Secret, Secret, Classified, Unclassified, & Public - Couple with Sensitivity Levels: Rank [91].
Cobra	Security risk analysis product developed by C&A Systems Security LTD [31].
Confidentiality	“The protection of information within systems so that unauthorized people, recourses, and processes cannot access that information” [90].
Cyberspace	Has been defined as “an interdependent network of information technology infrastructures” [201]. Realistically it is a term that has been created to describe the entire online community, i.e., internet and World Wide Web.
DAC	Design Architecture Committee approved designs for large projects in the Fortune Global 500 financial organization case study.
DAD	Design Architecture Document is the instrument used to submit large projects to the DAC.
End-User	The individual using the application
Facilitated Risk Analysis Process (FRAP)	Qualitative risk analysis process developed by Thomas Peltier [206].
Hackers	“Someone who bypasses the systems access controls by taking advantage of security weaknesses that developers have left in the system” [90].
Integrity	“The protection of systems information or processing from intentional or accidental unauthorized changes” [90].
HIS	IBM HTTP Server
Internet	A conglomerate of individual networks connected through a Transmission Control Protocol/Internet Protocol [90].
Masquerade	A type of security threat where an authorized or unauthorized user of the system who has obtained the id and password of another user and successfully pretends to be that entity [90].

Message Digest (MD) 5	One way hashing function that generates a 128 bit fixed length message [119, 153].
RBAC	Role Based Access Control
Risk Analysis	“Represents the process of analyzing a target environment and the relationships of it risk-related attributes” [144].
Risk Assessment	“Represents the assignment of value to assets, threat frequency (annualized), consequence (i.e. exposure factors), and other elements of chance” [144].
Risk Evaluation	“Evaluation of all collected information regarding threats, vulnerabilities, assets and asset value in order to measure the associated chance of loss and the expected magnitude of loss for each of an array of threats that could occur” [90].
Scientific Method	“A method of research in which a problem is identified, relevant data are gathered, a hypothesis is formulated from these data, and the hypothesis is empirically tested” [61].
Security Improvement Approach (SIA)	The SIA is the high level theoretical approach to making security improvements.
Security Improvement Initiative (SII)	The SII is the activity that takes place to achieve security improvements.
Social engineering	“Successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access, unauthorized use, or unauthorized disclosure, to an information systems, network or data” [22].
Secure Socket Layer (SSL)	“SSL protocol was originally designed by Netscape to protect communication between a web browser and server” [153].
The Web Engineering Security (WES) Process	A proactive, flexible, process neutral security methodology with customizable components that is based on the empirical evidence and used to explicitly integrate security throughout an organization’s chosen application development process.
Threat	“The occurrence of an event of which could have an undesirable impact of the well-being of the asset” [90].
Tivoli Access Manager	“IBM Tivoli Access Manager is an authorization and network security policy management solution that attempts to provide end-to-end protection of resources over geographically dispersed intranets and extranets” [99].

Tivoli Access Manager WebSEAL

"IBM Tivoli Access Manager WebSEAL is a resource manager responsible for managing and protecting Web-based information and resources. IBM WebSEAL is a high performance, multi-threaded Web server that applies fine-grained security policy to the Tivoli Access Manager protected Web object space. WebSEAL can provide single sign-on solutions and incorporate back-end Web application server resources into its security policy" [99].

Uncertainty

"Degree, expressed as a percent, to which there is less than complete confidence in the value of any element of the risk assessment" [144].

Value Chain

A series of activities to deliver low-cost or differentiated products [3].

Value Configuration

Configuration of activities in order to add value that can be grouped into three categories: Value Chain, Valued Network and Value Shop [3].

Value Network

A series of activities to deliver low-cost or differentiated products based on an intermediaries service and technologies to provide a connection between parties that wish to remain independent [3].

Value Shop

A series of activities to deliver low-cost or differentiated products based on intensive technologies through most types of services models [3].

Vulnerability

"The absence or weakness of a risk reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact or both" [144].

WebSphere

Software developed by IBM to integrate e-business applications using Web technologies [100].

World Wide Web a.k.a Web

"An extensive information system on the Internet providing facilities for documents to be connected to other documents by hypertext links" [10].

References

[1] Abrahamsson P, Salo O, Ronkainen J, Warsta J. Agile Software Development Methods: VTT Technical Research Centre of Finland; 2002.

[2] Abrahamsson P, Warsta J, Siponen MT, Ronkainen J. New directions on agile methods: a comparative analysis. In: 25th International Conference on Software Engineering; 2003 3-10 May 2003: IEEE; 2003. p. 244-254.

[3] Afuah A, Tucci CL. Internet Business Models and Strategies, Second Edition. International Edition ed. Boston: MacGraw-Hill; 2003.

[4] Agile Alliance Organization, *Agile Alliance*, Agile Alliance http://www.agilealliance.org/

[5] Alberts C. Introduction to the OCTAVE® Approach. In: Audrey Dorofee JS, Carol Woody, editor. Carnegie Mellon Software Engineering Institute: Carnegie Mellon Software Engineering Institute; 2003. p. 1-37.

[6] Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons, Inc.; 2001.

[7] Ardi S, Byers D, Meland PH, Tondel IA, Shahmehri N. How can the developer benefit from security modeling? In: The Second International Conference on Availability, Reliability and Security (ARES). 2007 April, 2007; Vienna, Austria: IEEE; 2007. p. 1017-1025.

[8] Armstrong H. Managing Information Security in Healthcare - an Action Research Experience. In: Proceedings of the IFIP TC11 Fifteenth Annual Working Conference on Information Security for Global Information Infrastructures; 2000; Deventer, The Netherlands: Kluwer, B.V.; 2000. p. 19-28.

[9] AskOxford.com, *Method*, AskOxford.com http://www.askoxford.com/concise_oed/method?view=uk

[10] AskOxford.com, *World Wide Web*, AskOxford.com http://www.askoxford.com/concise_oed/worldwideweb?view=uk

[11] AT&T, *AT&T Study Finds U.S. Businesses Unprepared For Disaster*. 2005, AT&T http://www.att.com/news/2005/09/12-2

[12] Balfanz D, Durfee G, Smetters DK, Grinter RE. In search of usable security: five lessons from the field. Security & Privacy Magazine, IEEE 2004;2(5):19-24.

[13] Baskerville R. Information systems security design methods: implications for information systems development. ACM Computing Surveys 1993;25(4):375-414.

[14] Baskerville R, Ramesh B, Levine L, Pries-Heje J. High-Speed Software Development Practices: What Works, What Doesn't. IT Professional 2006;8(4):29-36.

[15] Baskerville RL. Logical controls specification: An approach to information systems security. Systems Development for Human Progress 1989:241-255.

[16] BBC, *Penalty plea on cyber criminals*. 2005, BBC http://news.bbc.co.uk/1/hi/uk_politics/4676169.stm

[17] Beck K. eXtreme Programming eXplained Embrace Change. Boston: Addison-Wesley; 2000.

[18] Beck K. Extreme Programming Explained: Embrace Change. Second Edition ed. Boston: Addison-Wesley; 2005.

[19] Benington HD. Production of large computer programs. In: International Conference on Software Engineering Proceedings of the 9th international conference on Software Engineering; 1987 / 1956; Monterey, California, United States: IEEE Computer Society Press Los Alamitos, CA, USA; 1987 / 1956. p. 299-310.

[20] Berinato S, *The Bugs Stop Here*, in *CIO*. 2003 http://www.cio.com/archive/051503/bugs.html

[21] Berinato S, *Global Security, The Global State of Information Security 2005*, WARE LC, Editor. 2005, CIO Magazine: Framingham http://www.cio.com/archive/091505/global.html

[22] Berti J, Rogers M. Social Engineering the Forgotten risk. In: Tipton HF, Krause M, editors. Information Security Management Handbook. Boca Raton: Auerbach; 2004. p. 147 --154.

[23] Beznosov K. eXtreme Security Engineering. In: First ACM BizSec Workshop; 2003; Fairfax, VA: ACM; 2003.

[24] Boehm BW. A spiral model of software development and enhancement. In: ACM SIGSOFT; 1986 August: ACM Press; 1986. p. 14-24.

[25] Boehm BW. A spiral model of software development and enhancement. Computer 1988;21(5):61-72.

[26] Boman M. Conceptual Modelling. London: Prentice Hall; 1997.

[27] Booysen HAS, Eloff JHP. A Methodology for the development of secure Application Systems. In: Proceedings of the 11th IFIP TC11 International Conference on Information Security; 1995: IFIP/SEC'95; 1995.

[28] Bostrom RB, Heinen JS. MIS problems and failures. A socio-technical perspective: Part I: The causes. MIS Quartely, 1977;1(3):17-32.

[29] Boulton C, *Oracle Set to Stake Security Claim*. 2007, internetnews.com http://www.internetnews.com/security/article.php/3657531

[30] Byers D, Shahmehri N. Design of a Process for Software Security. In: The Second International Conference on Availability, Reliability and Security (ARES); 2007 April 2007; Vienna, Austria: IEEE; 2007. p. 301-309.

[31] C&A Systems Security Limited, *COBRA*, C&A Systems Security Limited: Cheshire http://www.riskworld.net/

[32] Civil Society Internet Rights Project (CSIR), *UK Internet Rights project: Fact Sheets: Computer crime*, internetrights.org.uk http://www.internetrights.org.uk/

[33] CNN, *Massacre in Madrid, Madrid bombings: One Year on*. 2006, CNN.com http://www.cnn.com/SPECIALS/2004/madrid.bombing/

[34] Coblenz M, *Federal Protection of Trade Secrets: The Economic Espionage Act of 1996*. 1997, Washington State Bar Association http://www.wsba.org/media/publications/barnews/archives/sep-97-federal.htm

[35] Common Criteria, *Common Criteria*, http://www.commoncriteriaportal.org/

[36] Compliance Home, *International Standards Organization (ISO) 17799*, Compliance Home Regulatory Compliance Portal http://www.compliancehome.com/topics/ISO-17799/

[37] Computer Crime Research Center Staff, *UN recommendations on fighting cybercrime*. 2005, Computer Crime Research Center http://www.crime-research.org/news/12.05.2005/1225/

[38] Consumer Guides, *Fact Sheet: President Bush Signs the Fair and Accurate Credit Transactions Act of 2003*, Consumer Guides http://www.consumer-guides.info/consumer-debt/fact_act.html

[39] Consumer Privacy Guide, *Financial Modernization Act (Gramm-Leach-Bliley Act)*. 2001, ConsumerPrivacyGuide.org http://www.consumerprivacyguide.org/law/glb.shtml

[40] Council of Europe, *Convention on Cybercrime*. 2004, Council of Europe http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm

[41] Couper MP, Lamias MJ. Web Surveys: Perceptions of Burden. Social Science Computer Review 2001;19(2):146-162.

[42] Couper MP, Traugott MW, Lamias MJ. Web Survey Design and Administration. Public Opinion Quarterly 2001;65(2):230-253.

[43] Cross M. Web Application Security. Rockland, MA, USA: Syngress; 2007.

[44] Cwarel Isaf Institute, *Methods & Models*. 2002 http://www.managementkybernetik.com/en/fs_methmod3.html

[45] Dacey RF. INFORMATION SECURITY Effective Patch Management is Critical to Mitigating Software Vulnerabilities: United States General Accounting Office; 2003.

[46] deJong J, *Slipping In The Side Door With App Security Message*. 2006, BZ Media LLC: Huntington NY http://www.sdtimes.com/article/special-20060815-01.html

[47] Deloitte. 2004 Global Security Survey. London: Deloitte Touché Tohmatsu; 2004.

[48] Deloitte, *Security Attacks On IT Systems More Than Double, According to Respondents of Deloitte & Touche LLP's Global Financial Services Survey*. 2004, Deloitte http://www.deloitte.com/

[49] Deloitte. 2005 Global Security Survey. London: Deloitte Touché Tohmatsu; 2005 2005.

[50] Deloitte. 2006 Global Security Survey. London: Deloitte Touché Tohmatsu; 2006 2005.

[51] Department of Homeland Security, *Security in the Software Lifecycle*. 2006, Department of Homeland Security: Washington, DC https://buildsecurityin.us-cert.gov/daisy/bsi/87/version/12/part/4/data/Draft+Security+in+the+Software+Lifcycle+v1.2.pdf?branch=main&language=default

[52] Department of Justice U, *Computer Crime and Intellectual Property Section (CCIPS)*, Department of Justice, USA http://www.usdoj.gov/criminal/cybercrime/ipmanual/08ipma.htm#VIII.C.3.

[53] Deshpande Y. Web Engineering Curriculum: A Case Study of an Evolving Framework. In: Web Enginering 4th international conference, ICE 2004; 2004 July 2004; Munich, Germany; 2004. p. 526.

[54] Deshpande Y, Hansen S. Web Engineering: Creating a Discipline among Disciplines. Multimedia, IEEE 2001;8(2):82-87.

[55] Deshpande Y, Murugesan S, Ginige A, Hansen S, Schwabe D, Gaedke M, et al. Web Engineering. Journal of Web Engineering 2002;1(No. 1):3-17.

[56] Devine J, Glisson WB, Welland R. Picture this: developing a museum online photo library. In: International Conference on Hypermedia and Interactivity in Museums (ICHIM); 2007; Toronto, Canada: ICHIM; 2007.

[57] Dhillon G, Backhouse J. Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal 2001;11(2):127-153.

[58] Dickson JB. Web applications have become IT's next security battleground. San Antonio Business Journal 2004.

[59] Dictionary.com, *Method*, Dictionary.com http://dictionary.reference.com/browse/method

[60] Dictionary.com, *Trust*. 2005, Lexico Publishing Group, LLC http://dictionary.reference.com/search?q=Trust

[61] Dictionary.com Unabridged (v 1.1), *Scientific Method*, Random House, Inc. http://dictionary.reference.com/browse/scientific%20method

[62] DSDM Consortium, *DSDM Consortium Delivering Agile Business Solutions on Time*. 1997-2007 http://www.na.dsdm.org/tour/overview.asp

[63] DSDM Consortium, *Guidelines for introducing DSDM into an Organisation*. 1998-2003 http://www.dsdm.org/products/white_papers.asp

[64] Ellis J, Speed T. The internet security guidebook: from planning to deployment. San Diego: Academic Press; 2001.

[65] Exler R, *Security and the Application Development Process*, in *CSO*. 2004, CXO Media Inc. http://www.csoonline.com/analyst/report3068.html

[66] Fernandez EB. Coordination of security levels for Internet architectures. In: Procs. 10th Intl. Workshop on Database and Expert Systems Applications; 1999: Procs. 10th Intl. Workshop on Database and Expert Systems Applications; 1999. p. 837-841.

[67] Fernandez EB. A methodology for secure software design. In: Procs. of the 2004 Intl. Symposium on Web Services and Applications (ISWS'04); 2004 June 21-24, 2004; Las Vegas, NV; 2004.

[68] Fingar P, Aronica R. The Death of "e" and the Birth of the Real New Economy: Business Models, Technologies and Strategies for the 21st Century. Tampa, Florida USA: Meghan-Kiffer Press; 2001.

[69] Fortune Global 500, *Industry: Banks: Commercial and Savings*. 2004, Fortune http://money.cnn.com/magazines/fortune/global500/2006/industries/Banks_Commercial_and_Savings/1.html

[70] Foster JC, *Five hidden tactics for secure programming*. 2004, Ounce Labs

[71] Fowler M, Highsmith J, *The Agile Manifesto*. 2001, Dr. Dobb's Portal: San Mateo, CA http://www.ddj.com/dept/architect/184414755#sidebar

[72] Gartner Research. Three Lenses Into Information Security. Research; 2006 10 January 2006. Report No.: G00136780.

[73] Ge X, Paige RF, Polack FAC, Chivers H, Brooke PJ. Agile Development of Secure Web Applications. In: International Conference on Web Engineering.; 2006; Palo Alto, California: Springer; 2006.

[74] Glass RL. Facts and Fallacies of Software Engineering. Boston, USA: Addison-Wesley; 2003.

[75] Glisson WB, Glisson LM, Welland R. Web Development Evolution: The Business Perspective on Security. In: Thirty-Fifth Annual Western Decision Sciences Institute; 2006; Hawaii: Western Decision Sciences Institute; 2006.

[76] Glisson WB, Glisson LM, Welland R. Secure Web Application Development and Global Regulation. In: The Second International Conference on Availability, Reliability and Security (ARES); 2007; Vienna, Austria: IEEE; 2007.

[77] Glisson WB, McDonald A, Welland R. Web Engineering Security: A Practitioner's Perspective. In: International Conference on Web Engineering; 2006; Palo Alto, California: Springer; 2006.

[78] Glisson WB, Welland R. Web Development Evolution: The Assimilation of Web Engineering Security. In: 3rd Latin American Web Congress; 2005; Buenos Aires - Argentina: IEEE CS Press; 2005.

[79] Glisson WB, Welland R. Web Engineering Security (WES) Application Survey Technical Report. Glasgow: University of Glasgow; 2006 2006.

[80] Glisson WB, Welland R. Web Engineering Security (WES) Technical Report: University of Glasgow; 2007.

[81] Glisson WB, Welland R. Web Engineering Security: Essential Elements. In: The Second International Conference on Availability, Reliability and Security (ARES); 2007; Vienna, Austria: IEEE; 2007.

[82] Glisson WB, Welland R. Web Survey Technical Report: University of Glasgow; 2007.

[83] Gordon LA, Loeb MP, Lucyshyn W, Richardson R. 2004 CSI/FBI Computer Crime Security Survey: Computer Security Institute; 2004.

[84] Gordon LA, Loeb MP, Lucyshyn W, Richardson R. 2005 CSI/FBIComputer Crime Survey: Computer Security Institute; 2005.

[85] Gordon LA, Loeb MP, Lucyshyn W, Richardson R. 2006 CSI/FBIComputer Crime Survey: Computer Security Institute; 2006.

[86] Graff MG, Wyk KRv. Secure Coding Principles & Practices. Sebastopol, CA: O'Reilly & Associates Inc.; 2003.

[87] Gross G, *Secret Service head calls for cybersecurity cooperation*. 2005, Computerworld http://www.computerworld.com/securitytopics/security/story/0,10801,101820,00.html?SKC=security-101820

[88] Guardian Unlimited, *The RIP Act*. 2004, Guardian Unlimited http://www.guardian.co.uk/theissues/article/0,6512,334007,00.html

[89] Gunn H, *Web-based Surveys: Changing the Survey Process*. 2002, http://www.firstmonday.org/ http://www.firstmonday.org/issues/issue7_12/gunn/

[90] Hansche S, Berti J, Hare C. Official (ISC)2 Guide to the CISSP Exam. Boca Raton: Auerbach; 2004.

[91] Hare C. Policy Development. In: Tipton HF, Krause M, editors. Information Security Managment Handbook. Fifth Edition ed. Boca Raton: Auerbach Publications; 2004. p. 925-943.

[92] Hargittai E. Second-Level Digital Divide: Differences in People's Online Skills. First Monday: Peer-Reviewed Journal of the Interne 2002;7(4).

[93] Hirschheim RA. Information Systems Epistemology: An Historical Perspective. In: Mumford E, Hirschheim R, Fitzgerald G, Wood-Harper T, editors. Research Methods in Information Systems. North-Holland, Amsterdam; 1985. p. pp.3-9.

[94] Hoo KS, Sudbury AW, Jaquith AR. Tangible ROI through Secure Software Engineering. Secure Business Quarterly 2001;1(2).

[95] Host M, Runeson P. Checklists for Software Engineering Case Study Research. In: Empirical Software Engineering and Measurement; 2007 20-21 Sept. 2007; Madrid, Spain: IEEE; 2007. p. 479-481.

[96] Howard M, *How Do They Do It? A Look Inside the Security Development Lifecycle at Microsoft*. 2005, MSDN Magazine http://msdn.microsoft.com/msdnmag/issues/05/11/SDL/

[97] Howard PD. The Security Policy life Cycle: Functions and Responsibilities. In: Tipton HF, Krause M, editors. Information Security Management Handbook. Fifth ed. Boca Raton: Auerbach Publications; 2004.

[98] Hurley E, *Security and Sarbanes-Oxley*. 2003, SearchSecurity.com http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929451,00.html

[99] IBM, *Introducing IBM Tivoli Access Manager and WebSEAL*, IBM http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1359-00/en_US/HTML/am51_webseal_guide11.htm#i1038108

[100] IBM, *WebSphere software*, IBM http://www-306.ibm.com/software/info1/websphere/index.jsp?tab=prodinfomgmt

[101] IBM, *Strenghting e-business security*. 2005, IBM: Raleigh NC, USA http://www-1.ibm.com/services/us/bcs/pdf/tivoli-strengthening-e-business-security.pdf

[102] IBM, *Security and privacy*. 2006, IBM: Armonk, NY http://www-1.ibm.com/services/us/index.wss/itservice/bcs/a1000405

[103] IBM Global Services, *Business Continuity: New risks, new imperatives and a new approach*. 1999, IBM Global Services: Somers, NY http://www-935.ibm.com/services/us/index.wss/summary/bcrs/a1000475?cntxt=a1000388

[104] ISO, *International Organization for Standards*, http://www.iso.org/iso/en/ISOOnline.frontpage

[105] Jacobson I, Booch G, Rumbaugh J. The Unified Software Development Process. Boston: Addison-Wesley; 1999.

[106] James HL. Managing information systems security: a soft approach. In: Proceedings of the 1996 Information Systems Conference of New Zealand (ISCNZ '96); 1996; New Zealand: IEEE Computer Society; 1996. p. 10.

[107] Johnson B, *New Security Features in Visual Studio 2005*. 2005, Microsoft http://msdn2.microsoft.com/en-us/library/ms364073(vs.80).aspx

[108] Jones T, Holden J, *Disaster recovery: no more excuses*. 2005, Computer Business Review Online http://www.computerbusinessreview.com/article_feature.asp?guid=D82839BB-8BD7-4C94-B06E-BF0B27968B6A

[109] Joshi JBD, Aref WG, Ghafoor A, Spafford EH. Security models for web-based applications. Communications of the ACM 2001;44(2):38-44.

[110] Kaplan R. A Matter of Trust. In: Krause HFTaM, editor. Information Security Management Handbook. Fifth ed. Boca Raton: Auerbach Publications; 2004.

[111] Karyda M, Kokolakis S, Kiountouzis E. Redefining information systems security: viable information systems. In: 16th International Conference on Information Security; 2001 June 11-13; Paris, France: Kluwer International Federation; 2001. p. 453-468.

[112] Kiely D, *New Security Tools in Visual Studio 2005 - The Permissions Calculator*. 2005, asp.netPro http://www.aspnetpro.com/NewsletterArticle/2005/11/asp200511dk_l/asp200511dk_l.asp

[113] King RON, *E-Business Growth Demands Security Spending*. 2004, Web Hosting Industry Review http://www.thewhir.com/features/security-spending.cfm

[114] Kitchenham BA, Pfleeger SL. Principles of survey research: part 1: turning lemons into lemonade. ACM SIGSOFT Software Engineering Notes 2001;26(6):16-18.

[115] Kitchenham BA, Pfleeger SL. Principles of survey research part 2: designing a survey. ACM SIGSOFT Software Engineering Not 2002;27(1):18-20.

[116] Kitchenham BA, Pfleeger SL. Principles of survey research: part 3: constructing a survey instrument. ACM SIGSOFT Software Engineering Notes 2002;27(2):20-24.

[117] Klein HK, Myers MD. A set of principles for conducting and evaluating interpretive field studies in information systems. MIS Quarterly 1999;23(1):67-93.

[118] Knight W, Thorel J, *G8 nations team up to fight cyber-crime*. 2000, ZDNet UK http://news.zdnet.co.uk/internet/security/0,39020375,2079018,00.htm

[119] Krutz RL, Vines RD. The CISSP and CAP Prep Guide. Indiananapolis, IN: Wiley; 2007.

[120] Landman J. Forensic Computing: An Introduction to the Principles and the Practical applications. Sydney, Australia: School of Computing and Mathematics, University of Western Sydney; 2002 April 15, 2002.

[121] Lemos R, *Microsoft developers feel Windows pain.* 2002, CNET News.COM http://news.com.com/2100-1001-832048.html

[122] Line 56, *E-Business Spending now exceeds 20 percent of all I.T. expenditure*. 2003, Line56.com

[123] Lipner S. The Trustworthy Computing Security Development Lifecycle. In: 2004 Annual Computer Security Applications Conference; 2004; Tucson, Arizona: Annual Computer Security Applications Conference; 2004.

[124] Lipner S, Howard M, *The Trustworthy Computing Security Development Lifecycle*. 2005, Microsoft Corporation http://msdn2.microsoft.com/en-us/library/ms995349.aspx

[125] Mayer, Brown, Rowe, Maw. The Sarbanes-Oxley Act of 2002 and its Impact on European Companies. Washington, DC: Mayer, Brown, Rowe, and Maw; 2002 September 2002.

[126] McCormick J, *Computer Security as a Business Enabler*. 2007, Baseline http://www.baselinemag.com/article2/0,1397,2152093,00.asp

[127] McCullagh D, *Senators propose sweeping data-security bill*. 2005, ZDNet News http://news.zdnet.com/2100-1009_22-5769156.html

[128] McDermott J, Fox C. Using abuse case models for security requirements analysis. In: Computer Security Applications Conference, 1999. (ACSAC '99); 1999; Phoenix, AZ, USA: IEEE; 1999. p. 55-64.

[129] McDonald A. The Agile Web Engineering (AWE) Process, Ph.D. Thesis. Glasgow: University of Glasgow; 2004.

[130] McDonald A, Welland R. Agile Web Engineering (AWE) Process: Perceptions within a Fortune 500 Financial Services Company. Journal of Web Engineering 2005;4(4):283-312.

[131] McKemmish R. What is Forensic Computing?: Australian Institute of Criminology; 1999 June.

[132] Microsoft. Trustworthy Computing: Microsoft; 2002 May 2002.

[133] Microsoft. Trustworthy Computing White Paper: Microsoft; 2003 September 12, 2003.

[134] Mimoso MS, *Top Web application security problems identified SearchSecurity.com*. 2003, SearchSecurity.com http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci873823,00.html?NewsEL=9.25

[135] Mitnick K. The art of deception : controlling the human element of security / Kevin D. Mitnick & William L. Simon. Indianapolis, Ind.: Wiley; 2002.

[136] Mobbs P, *Computer Crime The law on the misuse of computers and networks*. 2003, GreenNet Civil Society Internet Rights Project. http://www.internetrights.org.uk/briefings/irtb08-rev1-draft.pdf

[137] Mont MC, Bramhall P, Gittler M, Pato J, Rees O. Identity Management: a Key e-Business Enabler. Bristol: Trusted E-Services Laboratory, HP Laboratories, Bristol; 2002 June 12th , 2002.

[138] Moteff J. Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives. Washington, DC: Congressional Research Service [CRS]; 2004 April 16, 2004.

[139] Murugesan S, Deshpande Y, Hansen S, Ginige A. A New Discipline for Development of Web-based Systems. In: Proceedings of the 1999 International Conference Software Engineering; 1999; 1999. p. 693-694.

[140] Oates B. Researching Information Systems and Computing. London: Sage Publications; 2006.

[141] Office of the Press Secretary, *President Bush Signs Identity Theft Penalty Enhancement Act*. 2004, US Government: Washington, DC http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html

[142] Organization for Internet Safety, *Guidelines for Security Vulnerability Reporting and Response*. 2004, Organization for Internet Safety http://www.oisafety.org/guidelines/Guidelines%20for%20Security%20Vulnerability%20Reporting%20and%20Response%20V2.0.pdf

[143] Ounce Labs. Weapons for the Hunt: Methods for Software Risk Assessment: Ounce Labs, Inc; 2004.

[144] Ozier W. Risk Analysis and Assessment. In: Tipton HF, Krause M, editors. Information Security Managment Handbook. Fifth ed. Boca Raton: Auerbach Publications; 2004. p. 795-820.

[145] PayPal, *About US*. 2006, PayPal.com: California http://www.paypal.com/uk/cgi-bin/webscr?cmd=p/gen/about-outside

[146] Peltier Associates, *Peltier Associates Facilitated Risk Analysis Process (FRAP)*. 2005: Howell, MI http://www.peltierassociates.com/frap.htm

[147] Peltier T. Effective Risk Analysis. In: 23rd National Information Systems Security Conference; 2000 October 16-19, 2000; Baltimore, Maryland: National Information Systems Security Confrence; 2000.

[148] Pernul G. Security constraint processing during multilevel secure databasedesign. In: Computer Security Applications Conference, 1992. Proceedings., Eighth Annual; 1992 11/30/1992 - 12/04/1992; San Antonio, TX, USA: IEEE; 1992. p. 75-84.

[149] Pernul G, Quirchmayr G. Organizing MLS Databases from a Data Modelling Point of View. In: 10th Annual Computer Security Applications Conference; 1994 12/05/1994 - 12/09/1994; Orlando, Florida: IEEE; 1994. p. 96-105.

[150] Pernul G, Tjoa M, Winiwarter W. Modelling data secrecy and integrity. Data & Knowledge Engineering 1998;26(3):291-308.

[151] Pescatore J. Sanctum Buy Shows Security Is Key to Application Development: Gartner; 2004.

[152] Peytchev A, Couper MP, McCabe SE, Crawford SD. Web Survey Design Paging versus Scrolling. Public Opinion Quarterly 2006;70(4):596-607.

[153] Pfleeger CP, Pfleeger SL. Security in Computing. Third Edition ed. Upper Saddle River, NJ: Prentice Hall; 2003.

[154] Phaltankar KM. Practical Guide for Implementing Secure Intranets and Extranets. Boston: Artech House, Inc.; 2000.

[155] Plesser R, Halpert J, Cividanes M, *Summary and Analysis of Key Sections of USA PATRIOT ACT of 2001*. 2001, Center for Democracy and Technology http://www.cdt.org/security/011031summary.shtml

[156] Premkumar T. Devanbu SS. Software engineering for security: a roadmap. In: International Conference on Software Engineering Proceedings of the Conference on The Future of Software Engineering; 2000; Limerick, Ireland: ACM Press New York, NY, USA; 2000. p. 227 - 239.

[157] PricewaterhouseCoopers. The Information Security Breaches Survey 2004. In: PricewaterhouseCoopers; 2004.

[158] PricewaterhouseCoopers. Information security breaches survey 2006. In: PricewaterhouseCoopers; 2006.

[159] Public Law 104-191 104th Congress, *Health Insurance Portability and Accountability Act of 1996*. 1996, Congress: Washington http://aspe.hhs.gov/admnsimp/pl104191.htm

[160] Rakitin SR. Software Verification and Validation: A practitioner's Guide. Boston: Artech House; 1997.

[161] Redemtech I, *Data Security Regulations - U.S. Federal Legislation*, Redemtech, Inc. http://www.datasurelockit.com/data_security_federal.aspx

[162] Reed DW, *The Scientific Method*, Department of Horticultural Sciences TexasA&MUniversity http://generalhorticulture.tamu.edu/LearningCommunity/ScientificMethod.htm

[163] Rothke B. A Look at the Common Criteria. In: Tiption HF, Krause M, editors. Information Security Managment Handbook. Fifth ed. Boca Raton: Auerbach; 2004. p. 969-977.

[164] Royce WW. Managing the development of large software systems: concepts and techniques. In: International Conference on Software Engineering Proceedings of the 9th international conference on Software Engineering; 1987 / 1970: IEEE Computer Society Press Los Alamitos CA USA; 1987 / 1970. p. 328-338.

[165] RSA, *RSA Security Announces RSA ClearTrust Ready Partner Program*. 2002, RSA http://www.rsasecurity.com/press_release.asp?doc_id=1235&id=1034

[166] Saltzer JH, Schroeder MD, *The Protection of Information in Computer Systems*. 1975, University of Virginia, Department of Computer Science http://www.cs.virginia.edu/~evans/cs551/saltzer/

[167] Schjolberg S, *The Legal Framework - Unauthorized Access to Computer Systems*. 2003, Moss District Court, Norway http://www.mosstingrett.no/info/legal.html

[168] Schneier B. Beyond Fear: Thinking Sensibly About Security in an Uncertain World. New York: Springer-Verlag New York Inc; 2006.

[169] Secure Software. Why Application Security is the New Business Imperative - and How to Achieve It. McLean, Virgina: Secure Software; 2004 2004.

[170] Siponen M, Baskerville R, Kuivalainen T. Integrating Security into Agile Development Methods. In: Proceedings of the 38th Hawaii International Conference on System Sciences; 2005; Hawaii: IEEE; 2005.

[171] Siponen MT. Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. Oulu, Finland: Department of Information Processing Science, University of Oulu; 2004 November 19.

[172] Siponen MT. An analysis of the traditional IS security approaches: implications for research and practice. European Journal of Information Systems 2005;14(3):303-315.

[173] Siponen MT. Secure-System Design Methods: Evolution and Future Directions. IT Professional 2006;8(3):40-44.

[174] Sommerville I. Software Engineering. Wokingham, England: Addison-Wesley; 1989.

[175] Sommerville I. Software Engineering. Eighth ed. Essex: Pearson Education Limited; 2007.

[176] Standford University Law School, *US Information Technology Law*. 2006, Standford University: Stanford, CA http://www.law.stanford.edu/program/centers/ttlf/law/us/it/

[177] Stapleton J. DSDM Dynamic Systems Devleopment Method. Harlow, England: Addison-Wesley; 1997.

[178] Stapleton J. DSDM Business Focused Development. Second ed. London: Addison-Wesley; 2003.

[179] Steinke G. Data privacy approaches from US and EU perspectives. Telematics and Informatics 2002;19(2):193-200.

[180] Stewart TA. The Wealth of Knowledge. London: Nicholas Brealey Publishing; 2001.

[181] Stinson JA, Pellissier SV, Andrews AD. Defining and Applying Generic Trust Relationships in a Networked Computing Environment. North Charleston, SC: ATI; 2000 May 2000.

[182] Symantec, *Importance of Corporate Security Policy Defining corporate security policies, basing them on industry standards, measuring compliance, and outsourced services are*

keys to successful policy management., Symantec http://securityresponse.symantec.com/avcenter/security/Content/security.articles/corp.security.policy.html

[183] Systems Security Engineering Capability Maturity Model (SSE-CMM) Project. Systems Security Engineering - Capability Maturity Model (SSE-CMM) Model Description Document. Pennsylvania: Carnegie Mellon University; 2003 June 15, 2003.

[184] Telang R, Wattal S, *Impact of Software Vulnerability Announcements on the Market Value of Software Vendors - An Empirical Investigation*. 2005, Carnegie Mellon University http://ssrn.com/abstract=677427

[185] The Open Web Application Security Project, *The Ten Most Critical Web Application Security Vulnerabilities*. 2004, The Open Web Application Security Project http://www.owasp.org/index.jsp

[186] The State of Minnesota, *H.F. No. 2121, 3rd Engrossment - 84th Legislative Session (2005-2006)*. 2005, Minnesota House of Representatives http://www.revisor.leg.state.mn.us

[187] Tiller JS. Outsourcing Security. In: Tiption HF, Krause M, editors. Information Security Management Handbook. Fifth ed. Boca Raton: Auerbach Publication; 2004. p. 1061-1072.

[188] UK Parliament, *Malicious Communications Act 1988*. 1988, UK Government: London http://www.opsi.gov.uk/ACTS/acts1988/Ukpga_19880027_en_1.htm

[189] UK Parliament, *Computer Misuse Act 1990*. 1990, Queen's Printer of Acts of Parliament: London http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

[190] UK Parliament, *Data Protection Act 1998*. 1998, Controller of HMSO: London http://www.opsi.gov.uk/acts/acts1998/19980029.htm

[191] UK Parliament, *Electronic Communications Act 2000*. 2000, UK Government: London http://www.opsi.gov.uk/acts/acts2000/20000007.htm

[192] UK Parliament, *Regulation of Investigatory Powers Act 2000*. 2000, Queen's Printer of Acts of Parliament: London http://www.opsi.gov.uk/Acts/acts2000/20000023.htm

[193] UK Parliament, *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*. 2000, UK Government: London http://www.opsi.gov.uk/si/si2000/20002699.htm

[194] UK Parliament, *The Electronic Signatures Regulations 2002*. 2002, UK Government: London http://www.opsi.gov.uk/SI/si2002/20020318.htm

[195] United States Department of Justice, *Computer Crime Policy & Programs*. 2006, US Government: Washington, DC http://www.usdoj.gov/criminal/cybercrime/ccpolicy.html

[196] United States Department of the Treasury, *Office of Critical Infrastructure Protection and Compliance Policy*. 2007, United States Department of the Treasury, http://www.ustreas.gov/offices/domestic-finance/financial-institution/cip/

[197] US Department of Education, *The Family Educational Rights and Privacy Act (FERPA)*, http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[198] US Government, *Electronic Signatures Act*. 2000, US Government: Washington http://www.ecsi.net/help/help_esig.html

[199] US Government, *Mutual Legal Assistance Treaty Between the United States and Russia*. 2002, US Government: Washington, DC http://www.state.gov/r/pa/prs/ps/2002/7734.htm

[200] US Government, *Check Clearing for the 21st Century Act*. 2003, The Federal Reserve Board: Washington, DC http://www.federalreserve.gov/paymentsystems/truncation/

[201] US Government. The National Strategy to Secure Cyberspace. Washington: US Government; 2003 February.

[202] VentureLine, *MBA Glossary*. 1996-2005, http://www.ventureline.com/ http://www.ventureline.com/glossary.asp

[203] Viega J, *Security in the software development lifecycle*. 2004, IBM http://www-128.ibm.com/developerworks/rational/library/content/RationalEdge/oct04/viega/

[204] Viega J. Building Security Requirements with CLASP. In: International Conference on Software Engineering; 2005; St. Louis, Missouri: ACM Press New York, NY, USA; 2005. p. 1-7.

[205] Viega J, McGraw B. Building Secure Software. Boston: Addison-Wesley; 2005.

[206] Visintine V, *An Introduction to Information Risk Assessment*. 2003, SANS Institute http://202.113.72.6/Network/raw/paper_security/IT_risk.pdf

[207] Vliet HV. Software Engineering Principals and Practice. Chichester: John Wiley & Sons, LTD; 2000.

[208] W3C, *W3C World Wide Web Consortium*. 2005, W3C World Wide Web Consortium http://www.w3.org/

[209] Walden I. Harmonising Computer Crime Laws in Europe. Journal of Crime, Criminal Law and Criminal Justice 2004;12(4):321-336.

[210] Walden I. Crime and Security in Cyberspace. Cambridge Review of International Affairs 2005;18(1):51-68.

[211] Wang H, Wang C. Taxonomy of security considerations and software quality. Communications of the ACM 2003;46(6):75-78.

[212] Webster's Online Dictionary.org, *Method*, Webster's Online Dictionary.org http://www.websters-online-dictionary.org/definition/method

[213] Williams P, Shimeall T, Dunlevy C. Intelligence Analysis for Internet Security. In: Casey Dunlevy TS, editor. London • New York • Oslo • Philadelphia • Singapore • Stockholm: Routledge, part of the Taylor & Francis Group; 2002. p. 1-38.

[214] Wylder JO. Towards Enforcing Security Policy: Encouraging Personal Accountability for Corporate Information Security Policy. In: Tipton HF, Krause M, editors. Information Security Management Handbook. Fifth Edition ed: Auerbach Publications; 2004. p. 945-952.

[215] Yin RK. Case Study Research: Design and Methods. Third Edition ed. London: Sage Publications, Inc; 2002.

[216] Zameeruddin R, *The Sarbanes-Oxley Act of 2002: An Overview, Analysis, and Caveats*, University of West Georgia http://www.westga.edu/~bquest/2003/auditlaw.htm

[217] Zegarelli GR, *Computer Fraud and Abuse Act of 1986*. 1991, BookRags & Macmillan Science Library: Computer Sciences http://www.bookrags.com/research/computer-fraud-and-abuse-act-of-198-csci-01/

[218] Zelkowitz M, Wallace D. Experimental Models for Validating Technology. IEEE Computer 1998;31(5):23-31.

Index