Spring 2015

An analysis of the effectiveness and cost of project security management

Robert E. Bott
Purdue University

Graduate School Form 30
Updated 1/15/2015

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Robert E. Bott

Entitled

AN ANALYSIS OF THE EFFECTIVENESS AND COST OF PROJECT SECURITY MANAGEMENT

For the degree of Master of Science

Is approved by the final examining committee:

Dr. Eric Dietz
Chair

Kevin Dittman

Raymond Hansen

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): Dr. Eric Dietz

Approved by: Jeffrey Whitten 4/6/2015

Head of the Departmental Graduate Program Date

AN ANALYSIS OF THE EFFECTIVENESS AND COST OF PROJECT SECURITY MANAGEMENT

A Thesis

Submitted to the Faculty

of

Purdue University

by

Robert E. Bott

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

May 2015

Purdue University

West Lafayette, Indiana

Any clime and place - Semper Fidelis

TABLE OF CONTENTS

Page

Page

Page

APPENDICES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABM	Agent-Based Modeling
CEO	Chief Executive Officer
CIT	Computer and Information Technology
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
COBIT	Control Objectives for Information and Related Technology
CRISC	Certified in Risk and Information Systems Control
CSC	Critical Security Control
CSM	Certified Scrum Master
ERM	Enterprise Risk Management
GMITS	Guidelines for the Management of IT Security
HIPAA	Health Insurance Portability and Accountability Act
ICP	ICAgile Certified Professional
IS	Information Security
IT	Information Technology
ITIL	Information Technology Library Infrastructure Foundations
IDS	Intrusion Detection System

ISG	Information Security Governance
ISM	Information Security Management
OA	Organization Agent
PA	Project Agent
PMI	Project Management Institute
PMP	Project Management Professional
PSM	Project Security Management
PMBOK	Project Management Body of Knowledge
RAT	Remote Administration Tools
ROI	Return On Investment
TA	Threat Agent

GLOSSARY

Control Objectives for Information and Related Technology (*COBIT*) - "Framework for the governance and management of Enterprise IT" (ISACA, 2014, p. 1)

Cyber Space - "The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information or communications systems, networks and embedded processors and controllers" ("Presidential Policy Directive / PPD-20," 2013, p. 2)

Generally Accepted Systems Security Principals (GASSP) - "Incorporate the consensus, at a particular time, as to the principles, standards, conventions, and mechanisms that information security practitioners should employ, that information processing products should provide, and that information owners should acknowledge to ensure the security of information and information systems" (Poore, 1996, p. 27)

Guidelines for the Management of IT Security (GMITS) - "An international standard that lays out guidelines for information security management. Associated with ISO/IEC standards"

Information Security - "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity and availability" (McCumber, 2005, p. xxiii)

Information Security Governance - "Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security program" (IT Governance Institute, 2006, p. 17)

Information Security Management - "Information security management is the process of administering people, policies, and programs with the objective of assuring continuity of operations while maintaining strategic alignment with the organizational mission" (Choobineh, Dhillon, Grimaila, & Rees, 2007, p. 959)

Intrusion Detection System - "A security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating

from outside the organization and also for system misuse or attacks originating from inside the organization" (SANS Institute, 2001, p. 4)

Managed Security Service Provider - "An [*sic*] managed security service provider (MSSP) provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. MSSPs use high-availability security operation centers (either from their own facilities or from other data center providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture" (“Managed Security Service Provider (MSSP) - Gartner IT Glossary,” 2013, p. 1)

Project Security Management - "The deliberate and detailed management of all aspects of security, physical and virtual, within a project. A component of risk management"

ABSTRACT

Bott, Robert E. M.S., Purdue University, May 2015. An Analysis of the Effectiveness and Cost of Project Security Management. Major Professor: Dr. Eric Dietz.

This research analyzes the idea of managing information security risk on projects, as well as the effectiveness and costs associated with this kind of management. Organizations today face a myriad of security risks given their increased use of information technology. New solutions to improve information security within organizations large and small need to be researched and analyzed. Review of relevant literature has determined that although organizations are managing security from the top down, there is a lack of security management at the project level and that most project managers and their teams rely on the organizational security measures to keep information secure. The concept of managing security risks at the project level is not well defined and there exists no concrete and widely accepted framework for it. This research examines if managing security at the project level within a multi-tiered defensive strategy can be effective and at what cost. It also seeks to determine if budgeting for security in projects will lead to more secure project assets and products. This qualitative study uses three sources of data to deduce conclusions and recommendations. One, literary sources, two, subject interviews of security and project management professionals, and three, a computerized model built to simulate a defense in depth strategy. The primary finding of

this research is that the concept of managing information security in projects is valid, and that doing so will lead to more secure project assets and products. This type of management will increase the security posture of the project itself and the organization as a whole. Recommendations are made by the researcher as to what steps a project manager and the organization above it must take to leverage the management of information security risks on projects.

CHAPTER 1. INTRODUCTION

This chapter will present an overview of the research topic, its scope, significance and the research question. Also, this chapter will include assumptions, limitations and delimitations.

1.1 Research Question

Given the increasing global threats to information technology (IT) infrastructure, should project managers focus more efforts on security in a comprehensive multi-tiered defense strategy? Would budgeting for security in projects result in more secure assets and products?

1.2 Problem Statement

Threats to information technology (IT) assets and the information they maintain and manage have been growing considerably over the years. Moreover, the quantity of information stored on various systems throughout the world, and its continuous use, has been steadily increasing. This gives threat actors, from single perpetrators to criminal gangs all the way to nation states, many more targets to exploit. Also, the wide dissemination of simple yet powerful remote administration tools (RAT) and other hacker-related applications has increased the ease at which threats can exploit vulnerabilities in many systems. Within this increasingly insecure global environment,

there is a considerable lack of qualified security experts throughout the IT industry. New methods and approaches must be found to maximize the security posture of organizations while minimizing costs. One such proposed method is to place more responsibility for managing security risks on project managers. This method will assist project managers to identify and manage security risks specific to their projects. This will enable a more robust security posture that will result in significantly safer project assets and a more secure product at project completion.

The intent of this case study will be to discover if security risk management for IT projects, within a comprehensive multi-tiered defensive strategy and budgeted for by project managers, will yield safer project assets during execution and a safer product after the project is concluded. Methods of inquiry will include grounded theory by collecting data from literary sources and interviews of security professionals and project managers. Also, data will be used to build a model for case studies to discover if the added management of security at the project level will yield significant positive results in security posture. The concept of study will at this point be referred to as project security management (PSM).

1.3 Scope

Security concerns for organizations using information technology (IT) has become a critical issue in daily operations. Both virtual and physical security must be managed at all levels within an organization in order to secure valuable assets. In an increasingly inter-connected world, security risks of all types are on the rise. One of the toughest challenges facing any organization is how to plan for mitigation of security risks

and respond to security incidents once they occur, or put more precisely, how to manage security risks. Given these challenges, the researcher proposed the question, should project managers focus more efforts on security in a comprehensive multi-tiered defense strategy, and would budgeting for security result in more secure project assets and products? The management of security risk at the project level is intended to add to the overall security posture of an organization, in particular ones that rely on projects in order to create or maintain market share.

With the research question defined above, it is necessary to understand the scope under which the researcher will attempt to answer the question. The intended audience for this research are IT project managers who manage projects of any size and type within a larger organization. This research is also applicable to projects within smaller organizations without large resource pools. Based on an initial inquiry, it was quickly determined that the research focus should be at the project level and not reach into the higher echelons of management, such as program management. The effects of security management at the higher organizational level have been considered and will be factored in as part of the research, in the form of a multi-tiered defensive strategy, though they are not the focus of this study. The focus on security at the project level is due to the fact that project managers and their teams are the primary innovators in most companies, and often handle the most important assets, including information, within the company.

1.4 Significance

With the increased use of information technology in all areas of life, and the steady march of globalization and interconnectivity, organizations today face daunting

security challenges, particularly in cyberspace. Several high profile data breaches in recent years have demonstrated the threats to organizations from many different types of bad actors, as well as the vulnerabilities in IT systems. Companies like Target and Home Depot have experienced attacks resulting in loss of customer information (Krebs, 2014a, 2014b). Government agencies and contractors are also vulnerable to attacks and potential loss of valuable information. According to Krebs (2014c), several Israeli military contractors were breached, and large quantities of critical information on their Iron Dome missile defense shield was lost to hackers based in China. According to one report, the cyber criminals involved are tied to the Chinese military (Mandiant, 2013), and this certainly paints a picture of a very specific and well-funded threat to companies and governments, with respect to their intellectual property and a nation's national security. Most recently, celebrity actresses had their personal pictures stolen from the Apple iCloud service, demonstrating that thieves are not just simply looking to steal financial information or company trade secrets (Bree, 2014). Any form of information is valuable to bad actors and can potentially be monetized.

Further, the increased use of technology and third party storage has dramatically increased the amount of information that can be compromised. These issues have companies attempting to find new ways to deal with security concerns, such as automation, outsourcing their security needs, or using managed security service providers (MSSP) to improve their security posture (Forrester Research, Inc. 2013). There is a clear need to look at the security issues of our time and find new ways to enhance the overall security posture of organizations. Some researchers advocate that an important area in which to enhance information security is not technological, but rather by educating

employees and involving leadership in a more direct way, while creating a certain culture that reduces the internal threats from employees (Nemati & Church, 2009). This approach recognizes that humans make mistakes or are sometimes not as well trained as they should be, and that establishing good processes to manage will yield a better security posture. Another, similar approach is to focus on the security of projects by creating processes that support a project manager in managing his or her own specific security concerns (Pruitt, 2013). These security management methods should interface well with established project management processes, and integrate into an overall organizational security process and add to a multi-tiered defensive strategy.

The research that will be conducted for this study is significant given the above discussed threats and vulnerabilities. The research will determine if managing security at the project level adds significant value to an organizational security posture, and will give insight as to how much a project manager should budget towards security. This study will enhance the understanding of the value of PSM within a risk management framework. The results will allow leaders to understand the importance of managing security at the project level within the organization.

1.5 Assumptions

Assumptions are a critical part of this study. They provide the basis for which it is conducted and are items that could potentially adversely affect the research. The following assumptions have been identified:

- There is a perceived need by IT project managers to help secure project assets and increase the security posture of organizations by managing security at the project level
- There is no substitute information security management scheme, framework, process or set of procedures or practices that answers the research question
- There is an adequate amount of data available, gathered from literature and from individuals in the information security and project management professions, that allows the researcher to answer the research question
- Review and approval of this study by committee members will be sufficient to validate the model and the research
- The assumption is made that if fewer successful attacks occur on projects, during various case studies executed by the model, that this will result in more secure project assets and products

1.6 Limitations

Limitations further refine the scope of the research by listing items that will be covered by the study. The following limitations have been identified:

- Due to the qualitative nature of this study, the author's bias in model design and implementation and the selection of relevant data points is inherent throughout the study
- Determination of which critical security controls to implement in the model was done through a subjective reasoning process by the researcher and is based on

literature and input from committee members as well as information security and project management professionals

- The model designed uses a risk management framework and treats security issues within an organization and a project as risks to be managed
- The model is intended to simulate an environment with projects nested within an organization that both have certain vulnerabilities that threats seek to exploit.
- This research is intended to determine the validity of the concept of security management at project level and its potential effectiveness and costs
- This research and the associated model is intended to act as a basis for possible further research in the area of project security management and its potential effectiveness and costs to information security within organizations

1.7 Delimitations

Delimitations ensure the further framing of the scope of the research by listing items that the study will not cover. The following delimitations have been identified:

- It is not the intention of this research to develop a practical and detailed project security management framework, under the risk management knowledge area, that can be implemented by IT project managers
- The study is not intended to produce detailed quantitative data on the benefits and costs of information security management at project level
- The study and its associated model will not result in data that is directly applicable to the use by organizations in order to improve their information security management at the project level

- The model used for the analysis is not intended to be a full-featured and generally applicable solution that can be used by any organization without further enhancements and modifications. It is specifically designed for the use in this research

1.8 Chapter Summary

This chapter covered the research question, the scope, significance and the problem statement. It also discussed the assumptions, limitations and delimitations of the research.

CHAPTER 2. REVIEW OF RELEVANT LITERATURE

The scope of this literature review consists of several topics that add to the relevancy of the research question. In order to properly address and build a case for the thesis, the researcher needed to investigate articles and books on enterprise risk management (ERM), information security (IS), information security governance (ISG), information security management (ISM) and information technology (IT) project management. News stories and journals regarding breaches of IT systems were also part of the relevant literature in order to provide context to the reader and make the case for the necessity of the research.

Given the scope and nature of the research question, there were few references regarding managing information security at the project level. The references that were available did not specifically address the effectiveness of such measures, or delve deep into the topic. There was however a large quantity of materials addressing topics that directly influence the research question and add to its legitimacy. Numerous articles touch on the subject of the research question and suggest it to be a valid concept within the larger framework of an organization.

Based on these findings, the researcher chose to concentrate largely on material related to ISG and ISM and how both fit within a larger organizational risk management

framework. Furthermore, significant materials on the concept of defense in depth were evaluated and contribute to the understanding and validity of the research question.

Finally, references on IT project management were utilized in order to demonstrate the need for the research question to be investigated. Articles and books selected to be reviewed by the following literature review were chosen based on the nature of the source and relevance to the research question, as judged by the researcher. The resulting review was a collection of materials related to security management at the project level and its need.

2.1 Search Areas for Literature Review

A detailed and thorough search of Purdue online libraries, Purdue e-Pubs and Google scholar was conducted. These resources consisted of databases covering a large variety of categories from the humanities to science, technology and engineering.

Given the topic of the research, certain databases were used more than others, among them Academic Search Premier (EBSCO), ProQuest Research Library and ScienceDirect. Furthermore, the researcher's committee members recommended relevant articles and books that provided valuable information to enhance the validity of the research. A search of websites representing professional organizations and individuals was also conducted. These sources added critical information from the professional domain to the already extensive research documents gathered from the academic libraries. Finally, a search of news websites was conducted to gather current news stories relating to the thesis topic in order to provide context and relevance to the research.

Of the resources mentioned above, the primary means used by the researcher to gather relevant material was a search of the databases listed. This resulted in higher quality articles and resources, most of which are peer-reviewed or published in well-known and respected journals. When using the above mentioned online search tools, an assortment of keywords was used to narrow the search to relevant topics. The primary keywords and phrases used were 'project security management', 'information security', 'information security governance', 'information security management', 'enterprise risk management', 'information technology', 'project management', and 'IT project management'. These key words and phrases were used separately as well as together in various combinations, searching in the title and body of texts. These searches were conducted exhaustively on all databases in order to retrieve as many relevant references as possible. The researcher then further discriminated by choosing only relevant materials based on a subjective assessment.

The articles chosen for review were obtained primarily by a number of reputable sources. These included *Communications of the Association of Information Systems, Computers and Security,* SANS Institute and the Council on Cyber Security. Also, conference proceeding from the *Association of Information Systems* AMCIS proceedings, and journal articles from the *Global Journal of Flexible Systems Management* were chosen for review.

The remainder of this literature review will be devoted to the topics of information security, information security governance, information security management, project security management and the concept of defense in depth within an organization. The researcher will discuss the current state of literature and thinking in security

management at the project level, after laying out an overview of information security at organizational level, followed by a discussion on the defense in depth concept.

2.2 Information Security Governance and Management

Before discussing the topic of project security management (PSM) and what it entails, literature regarding IS must be reviewed. Specifically, the current state of information security management (ISM) and information security governance (ISG) at enterprise level must be understood in order to better position project security management into the overall security management and governance framework within an organization.

This section will discuss information security from a technical and a human perspective and how policies, practices and procedures play a role in an organization's security management and governance framework. It will also lay the foundation for the following section by presenting information from sources on concepts and practices that can be used for project security management. The case will be made of the importance of IS governance and IS management to modern corporations, and how widely accepted and understood both are to senior and middle managers in most firms. Once an understanding exists regarding information security at organizational level, and a case has been made of the importance of IS governance and management, a clearer picture of PSM and how it fits into these security management systems will emerge.

According to the ISO/IEC (2014), information security is the "preservation of confidentiality, integrity and availability of information" (p. 4). The organization further notes that properties such as authenticity, accountability, non-repudiation and reliability

can also be involved. As is evident, information security covers a vast field of topics and affects every department and person within an organization.

Further, information has become the lifeblood of many organizations and is used to drive most business processes, involving employees from the top to the bottom of an organization (von Solms & von Solms, 2006). Therefore, companies have realized importance of securing their information from a variety of threats.

2.2.1 Information Security Governance

One well established framework that is deeply connected to information security is Information Security Governance (ISG). ISG occurs at the executive and board of directors levels of an organization and is directly related to corporate governance (von Solms, 2006). The author discusses ISG as being the fourth wave of IS development, pre-dated by the “technical wave, the management wave and the institutional wave” (p. 165). According to the author an increase in legal and regulatory statutes have forced top management and board of directors to pay closer attention to the proper management of their organization's information and its security. Von Solms (2006), makes the case that there is a "significant relationship between corporate governance and information security" (p. 166). The author also states that ISG “is an integral part of corporate governance” (p. 167) and consists of the following points (p. 167):

- The management and leadership commitment of the board and top management towards good information security
- The proper organizational structures for enforcing good information security
- Full user awareness and commitment towards good information security

- The necessary policies, procedures, processes, technologies and compliance enforcement mechanisms

Von Solms (2006) discusses the fact that IS issues cannot be solved with technological solutions alone, an idea echoed by others (Church & Nemati, 2009; Jahner & Krcmar, 2005; Khansa, Liginlal, & Sim, 2009) and discussed in more detail later in this chapter. The author finishes with the idea that the maturing of the concept of ISG is signified by the process of explicit inclusion of information security into corporate governance. Johnston and Hale (2009) claim that ISG is an essential element of corporate governance. The authors also mention the importance of ISG due to the fact that information security is brought to the attention of Boards and the Chief Executive Officers (CEOs), and that it enables firms to align business strategy with security.

According to one author, the increase dependence on IT systems throughout all modern industries has brought about the "criticality of information security" (p. 61) and therefore bringing about "the need for information security governance" (Williams, 2001, p. 61). Further, given the rapid change in technology, the speed at which risks emerge and the nature of human users of information systems, security must be dealt with in a timely and proactive manner. This reinforces the need for high level governance in order to secure information and protect executives and board members who are increasingly responsible for the security of corporate information (Williams, 2001).

Corriss (2010) advocates corporate governance of information security through organizational culture. The author references the Department of Homeland Security and its systemic culture of security woven into the fabric of the organization. According to Corriss (2010), this influence on culture is created from the top leadership positions, such

as the CEO, and security professionals in these firms can take advantage of this by advocating a culture of security. This evidence demonstrates again how ISG plays an important role in information security for enterprises by governing the security of information from the top down.

Further reinforcing the validity of information security governance, (von Solms, 2005) compares two internationally recognized ISG frameworks that can be used by organizations to govern their information security. These are the COBIT framework for enterprise IT governance and the ISO/IEC 17799 information security management standard. Of importance to this research paper is not the results of the comparison, rather the fact that the concept of ISG is so well established that the need exists to find frameworks and standards to effectively conduct ISG on a day to day basis. This adds validity to the thesis question as will be seen later in this paper.

2.2.2 Information Security Management

Looking closer at how information security is managed within an organization today, the research will now define Information Security Management (ISM) and communicate its importance and value to enterprises of all types.

Cazemier, Overbeek, and Peters defined ISM as "the process of administering people, policies, and programs with the objective of assuring continuity of operations while maintaining strategic alignment with the organizational mission" (as cited in Choobineh, Dhillon, Grimaila, & Rees, 2007, p. 959). Further, Choobineh et al. (2007) stated that ISM "activities should be driven by organizational objectives so that no resources are expended" (p. 959) without understanding how they support the organizational mission. The authors detail some of the components of ISM by citing

examples of specific solutions businesses have implemented while performing ISM. Some of these are vulnerability assessment, developing an intrusion detection capability for IT systems, and periodically auditing information systems. This demonstrates that ISM is regarded as a lower level management function within an organization, as opposed to the high level governance as discussed in the previous section of this paper. Choobineh et al. (2007) finally argue that a risk management approach to information security might be a valid approach to ISM, yet there are some issues with properly understanding the nature of risks involved and the activities undertaken to manage them. This concept will become important when project security management is discussed later in this paper.

According to Gupta, Kranz, Ojha, Picot, and Singh (2013) a balanced mix of technical, procedural and human aspects of information security are necessary to building an overall ISM system in an organization. Their definition of ISM states that it is a set of activities involved in configuring resources in order to meet information security needs. Gupta et al. (2013) explain that ISM requires the active participation of employees across the hierarchy of an organization in order to be successful. This partly validates the discussions above regarding ISG and how it ties into ISM. Information security is a responsibility at all levels within an enterprise and though the executives are primarily responsible for setting the tone, lower level management is always responsible for planning, implementing and managing information security at their level.

Gupta et al. (2013) also recognize the importance of the culture in an organization by stating that an information security culture is about shared values and attitudes of employees towards the systems and information assets they use daily. The authors also

make mention of accepted international standards of ISM such as COBIT, GMITS and GASSP that provide best practice guidelines for managing information security in organizations. This is more validation that ISM is a well understood concept for managing information security in modern enterprises.

Some of the literature discusses what not to do within ISM. Von Solms and von Solms (2004) again discuss with vigor the importance of the corporate level of leadership that directly affects ISM by listing 10 deadly sins of IS. Not "realizing that information security is a corporate governance responsibility, not realizing that information security is a business issue not a technical issue and not realizing the core importance of information security awareness amongst users" (p. 372) are just three of these points. These points hammer home the importance of ISM at the mid and lower levels of an organization as well as the continuous effort required to manage the systems.

2.2.3 Information Security Measures

There are several factors that contribute to the effectiveness of Information Security Governance (ISG) and Information Security Management (ISM). These are technology, human factors and what are generally termed policies, practices and procedures. These three concepts are defined by McCumber (2005) as safeguards or security controls. The author states that:

> Security controls are defined as the management, operational and technical controls (safeguards or countermeasures) prescribed for an information system that, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity and availability of the system and its information. (p. xxiv)

When information security is mentioned, most people think first of technology (King, 2000). Technological controls are in part solutions such as Intrusion Detection Systems (IDSs), firewalls, anti-virus software, or data encryption algorithms.

Many organizations rely heavily on technology for their IS needs. The Council on Cyber Security (n.d.) published a list of 20 critical security controls for cyber defense, of which most are technological solutions, or involve technology in some way. Of course, many of the controls involve human factors as well as policies, practices and procedures, however the fact that a large number of the controls involve technology demonstrates the extensive focus on technological controls organizations rely on to keep information assets secure. This should make sense given the nature of modern IT use in nearly every industry around the world.

It is important to remember however that in the past many companies have made the mistake to rely too heavily on technology, as Choobineh et al. (2007) describe in a security breach example. In that case, ISM failed because improper policies existed that oversaw the technical solutions that were implemented. Many authors make the point that though technological solutions are important, the sole focus should not just be on technology and that good ISM also involves policies, practices and procedures as well as a considerations for human factors (Jahner & Krcmar, 2005; King, 2000).

Khansa, Liginlal and Sim (2009) move the ball further in this direction by focusing on human error as the cause of breaches in IT systems. The authors demonstrate well how human factors contribute significantly to data breaches occurring and privacy data being stolen. Khansa et al. (2009) conducted an empirical study gathering information from 1046 data breaches from January 2005 through June 2008. The results

demonstrate how human error is a significant determinant of IS. They report that 67% of all breaches were human error related and 33% were due to malicious acts. The authors also discuss the difference between slips and mistakes that human being are prone to make. Slips are defined as the "incorrect execution of a correct action", and mistakes as the "correct execution of an incorrect action sequence" (Khansa, Liginlal, & Sim, 2009, p. 216). Mistakes are in essence planning failures given that the individual executes the wrong action correctly. They might be trained well on the action to be performed, however have been instructed to execute something that is incorrect and not fitting the situation. Slips could be termed execution failures, where the proper action is not performed correctly. This could be due to the lack of appropriate training of the individual. The person has been instructed to execute the correct action, but fails to do it correctly. Slips and mistakes are clearly human factors in information security that must be addressed by all levels of leadership within an organization.

Other authors have investigated the human factors aspects of IS. Nemati and Church (2009) have argued for a human centered framework for ISM. They lay out the case using the healthcare industry, specifically highlighting the effects of the Health Insurance Portability and Accountability Act (HIPAA) on hospitals and other healthcare providers. The authors present a framework for managing the human element of organizational information security in a way that maximizes data security while also increasing efficiency (Nemati & Church, 2009). They make the convincing case that a law like HIPAA is impossible to manage with technological solutions alone. The exposure this law creates must be met with a broad program of education and effective management that involves every employee. The authors argue that the key to responding

effectively to a mandate like HIPAA is to use organizational culture to create an environment with the security and flexibility to handle various threats to the system. Nemati and Church (2009) effectively demonstrate how human factors play a key role in ISM.

Jahner and Krcmar (2005) advocate implementing an IT risk culture in organizations to assist in ISM. They state that much effort has been put into mitigating IT risks (in this case security risks) by means of physical, procedural or technological solutions. However, "the socio-cultural perspective of managing these risks has largely been ignored" (Jahner & Krcmar, 2005, p. 3327). The human factors that affect information security cannot be ignored and are a large part of ISM at the organizational level.

As already mentioned, on top of technological solutions and human factors, appropriate policies, practices and procedures are critical in effective ISM. Jahner and Krcmar (2005) mention policies and processes as described above. Gupta, Kranz, Ojha, Picot, and Singh (2013) make extensive references to policies and procedures and their absolute necessity as part of an effective information security management system. Policies that cover various issues such as data privacy, electronic media usage, external devices etc. are some of the policies mentioned in their work. These policies and procedures are implemented at organizational level covering all or many of the groups and departments of such firms. They govern and guide the people and the technology that they use in order to enhance the security posture of an organization and manage risk.

In this section a review of the literature with respect to information security governance (ISG) was discussed. How high level leadership such as the board of

directors or the CEO use ISG as a subset of corporate governance to ensure information security is maintained in their companies was discussed. Also, ISM was outlined in relevant literature. It was revealed how ISM is used at lower levels of the organization to manage daily information security issues. The three security controls of technology, human factors and policies, practices and procedures were discussed in detail by referencing relevant literature. The next section of this literature review will discuss the case for PSM by demonstrating how it fits into the overall information security apparatus described by ISG and ISM.

2.3 A Case for Project Security Management

At this point in the literature review it is clear how organizations manage their information security (IS). Given the factors discussed above, companies are forced to manage all aspects of security from top down, involving all levels of leadership all the way to the lowest level employee. This being the case, it stands to reason that organizations that execute IT projects for various reasons should consider allowing the project managers of these endeavors to manage specific security aspects of their projects.

Given that IT projects are unique, temporary and progressively elaborate (Brewer & Dittman, 2013), the security aspects of these projects are potentially different from the rest of the company (unique) and can be expected to change as time goes by (progressively elaborate). The higher level organizational manager of IS cannot keep track of and stay focused on the daily progression of a multitude of projects being planned and executed within an organization. Therefore, it would be wise for project

managers to execute their own information security management plan within their domains.

Little has been written regarding this specific topic. The standard for project management today is set by the Project Management Institute (PMI) and its Project Management Body of Knowledge (PMBOK). This organization has a myriad of training courses through which they and their associates produce Project Management Professionals (PMPs) and other trained professionals in the area of project management. However, nowhere in the PMBOK document does it reference security management (Project Management Institute, 2013). Even under the risk management knowledge area there is no specific mention of managing security risks on projects. This is not to say that some PMPs do not identify security risks in order to manage them during the project life cycle. However, there is no framework or standards set within this PMBOK document for managers of IT projects to manage their security risks, or any internationally accepted framework for IT project managers to reference. Further, there is no discussion in the literature reviewed at this point that specifically mentions project managers and their teams as being part of ISG or ISM.

2.3.1 Critical Security Controls and Risk Management

Pruitt (2013) is one notable reference discussing the topic of managing information security in IT projects. The author outlines the use of 20 critical security controls to be used as best practices for IT project managers. These however are the same controls published by Council on Cyber Security (n.d.). The important distinction between the two authors is that Pruitt incorporates the 20 security controls in a framework to be used by project managers to manage their information security during

project initiation, planning, execution and closing. As an example of how vulnerabilities are different and more dynamic at the project level vs. the higher organizational level, Pruitt (2013) suggests:

> IT project managers often handle intellectual capital that is the equivalent of the keys to the kingdom. IT project records are a rich source of valuable documents and due to the temporary and fast-moving nature of project work, access controls and records systems may not be maintained after the project closes and the team moves on. (p. 11)

This is just one of many examples discussed in the paper of how project security management differs from organizational security management given the various vulnerabilities and the factors that influence them on projects.

Further, the author references the PMI PMBOK and pulls information security management into the risk management knowledge area (Pruitt, 2013). This is a critical idea for the concept of PSM, given that many believe security should be managed as a risk (Bedi, Gandotra, & Singhal, 2009), and it lends itself to easier execution and understanding by the project managers since he or she will be managing other risks within the project life cycle. If information security is managed by project managers through risk management within the already well established PMBOK framework of the risk management knowledge area, this will surely lead to a more secure project and a secure product.

Others have discussed the need for project security management in the past. Emory (2003) discusses the security of projects during their life cycles making a clear distinction of securing information of the project, not the security of the product that is

created. The author states "A project may also have a unique set of security challenges that an organization may never have encountered or envisaged and that test the bounds of organizational policy" (p. 1), reinforcing the truth that organizations cannot predict or effectively manage all aspects of security in every project in their domains. Also Emory (2003) makes the case that project based organizations may have a hard time to propagate security policies, practices and procedures through all projects, team members and sub-contractors. This is an important point and well worth considering. Leaving some core security controls up to the project managers to oversee, while supporting him or her in those efforts, through proper funding and oversight, can potentially yield a better security environment for the entire organization.

2.3.2 Security Management as a Process

Another viewpoint on PSM and how it can improve information security in projects and the organizations as well as produce a more secure product is derived from quality management. Behara, Derrick, and Hu (2006) suggest that if security management is viewed similar to how quality management is in project management, then perhaps more secure products will result. The authors discuss some of the history of the quality revolution which changed industry in the United States in the 1980's. They make the case that similar methods and a care for managing security during a project's life cycle can result in better return on investment and a more secure product. Behara et al. (2006) use Deming's theory of profound knowledge to link quality management to security management. One element they discuss is regarding variations in systems. The authors tie common cause variation and assignable cause variation from the quality domain to the information security domain. Given that quality management of IT projects is a

universally accepted part of project management, as well as one of the PMBOK's knowledge areas, it would not be out of line to suggest that managing information security similar to quality aspects can yield a better product and a more secure project environment.

2.3.3 Defense in Depth

Finally, a method that reinforces the need for PSM is the defense in depth concept. Bedi et al. (2009) outline a defense in depth strategy for organizational information security. They speak of security layers surrounding an asset that needs to be protected and threats of a certain type and with a certain probability of realization. The more security layers are implemented the lesser the probability of the asset being compromised by a threat. When comparing the literature already reviewed and the concepts discussed therein, it becomes clear that PSM could be viewed as another layer of a defense in depth strategy. As explained above, an organization deals with information security at all levels, with each level adding certain specific aspects to the security posture. A project could be viewed as another level of this form of security strategy.

Having outlined the overall literature regarding PSM, it is clear that there are few if any accepted standard for managing information security specifically for projects. Although there are several papers regarding this topic, none outline a clear framework or are universally recognized as being a standard to follow. Further, none of the references specify what effectiveness or costs are associated with managing information security on projects. Therefore, it is vital to investigate the concept of PSM and if implementing a

framework to manage security within projects will yield more secure project assets and products.

2.4 Summary

This chapter has described the review of relevant literature. Starting with reviewing the concepts of ISG, through ISM to the idea of PSM. The focus was on explaining how ISG and ISM are used in organization today to provide information security and how they are structured to provide this security through higher level management. Also discussed were factors influencing information security such as technology, human factors and policies, practices and procedures. Finally, the idea of PSM was discussed and how it can fit into ISG and ISM in order to increase the security posture of an organization. A clear gap exists in literature in articulating a concept like project security management and how it might be effective at increasing information security for organizations by fitting into the well-established management structures that exist. It is believed by the researcher that a well thought-out framework, used within a risk management process on IT projects, can result in more secure project assets and make their resulting products safer.

CHAPTER 3. METHODOLOGY

This chapter will discuss the framework and research methodology used for this thesis. Researcher bias and data collection methods will also be articulated.

3.1 Framework

The review of relevant literature demonstrated the need for a focused view of security management at project level within the overall efforts of a larger organization. It presented a background on the current threats and vulnerabilities organizations are facing, a clear view of the different facets of information security management, a detailed look at current information security efforts within organizations, and the present state of thinking on managing security within projects.

Given the information presented in the literature review, it is clear that managing information security risk has become of great importance to organizations. Due to the increase in threats and the persistence of vulnerabilities in virtual and physical systems, it is necessary to improve the security posture within an organization in order to prevent loss now and in the future.

Given the complexity of the problem, security measures cannot be a concern for only one department or group within an organization. All members of an organization must be involved in managing the risks associated with security issues, including project managers and anyone engaged in producing new products and services within an

entity. This is especially true when information technology (IT) projects are being managed that are considered an important part of a company's portfolio.

Consequently, the question of whether IT project managers should focus more efforts on security in a comprehensive multi-tiered defense strategy, and would budgeting for security result in more secure project assets and products, becomes valid. The previous research question is what this thesis attempts to address. The objective of this thesis is to take information and recommendations from literature and professionals in the IT project management and security fields, build a computerized model based on a security framework design containing a set of vulnerabilities and threats being simulated, and investigate if project level security risk management yields a stronger security posture within the IT project, resulting in safer assets and a more secure product. This thesis will also look at the costs on the budget of projects for the added security posture.

3.2 Researcher Bias

In order to enhance the researcher's credibility, the impact of his bias on this thesis will be discussed. The motivations of the researcher are important to understand. First, the researcher is pursuing a master's degree in Computer Information Technology (CIT). Second, he has focused his curriculum on IT project management and studied risk management and cyber security issues outside of institutional learning. Lastly, he is a veteran with a military mindset that puts him in a unique position to look at information security in a different light than most other civilian professionals would. The history and experience of the researcher is important to note, given that it influences his belief that issues like security management are best left to the leaders at the lowest level of an

organization, or "at the point of friction". Bias will play a role in the way the model will be developed and how the results will be analyzed. This bias however will benefit the study because the researchers' mindset, interests and experience will help produce valid and useful conclusions and recommendations.

3.3 Methodology

An analysis of literary sources was conducted to determine which information security components should be modeled. This included areas in technology, policies, practices and procedures, and human factors. The researcher relied heavily on other published works in order to determine which security areas would best reflect a real world situation where an IT project manager could benefit from managing security risks within his or her project. The process involved the following steps:

1) Analyze the current state of security risk management, specifically as it pertains to information security, in order to determine if certain security risks could be mitigated by project level security management
2) Derive a list of topics in security risk management, specifically in the area of information security, that would significantly improve security posture at any level of an organization
3) Determine which components of information security are important for IT project managers to manage within their project's life cycle and which have the potential to significantly improve the project's security posture

   a. Note the components of security that are managed primarily or exclusively at organizational level for use in modeling the environment a project will be operating in within the model
   b. Base the list on a subset of the 20 Critical Security Controls (CSCs) published by the council on cyber security (Council on Cyber Security, n.d.)

4) Derive a list threats, based on the chosen CSCs, that organization face for use in the model
5) Design and build an agent based model within the AnyLogic® system that simulates a real world environment with threats present, as well as the security risk management solutions applied by IT project managers (based on the subset of CSCs)
   a. The model reflects specific threats that may attack an organization's information assets in order to cause damage
   b. The model reflects specific management actions taken to improve the security posture within projects
   c. The model collects data on the cost and effectiveness of specific critical security controls implemented by the organization and the projects for use in analysis

Figure 3.1 is a high level representation of how the data collected from literature and professional sources was applied to test the various security measures managed by IT projects. A threat agent will attack the organization and the project and have a certain chance to succeed based on the chosen CSCs. The

researcher assumed, based on literary review, input from professional subjects and his own experience, that a well-managed project security scheme will increase the security posture of the project and therefore the organization as a whole.

The model allows for the selection of specific security controls. These controls can be used at the organizational level as well as the project level, depending on the scenario the researcher wishes to run. All threats are directly associated with the selected controls, since the controls are linked to particular types of attack. Threats are based on the attack types articulated in The Critical Security Controls for Effective Cyber Defense (Council on Cyber Security, n.d.). For example, CSC #5 Malware Defenses protects against the introduction and spread of malware on the organization's assets, therefore the threat will be associated with attempts to introduce malicious software into the organization or its projects. During the simulation run, the threat continuously attacks the organization and its projects in order to cause damage. In this research, damage is not specifically defined and will not be quantified. Each security control implemented will increase the cost for the project, yet provide a certain level of enhanced security, thereby reducing the likelihood that an attack is successful, and reducing the risk level for organizations and projects. After each simulation run, the effectiveness and cost of the overall security strategy is measured and the results are used for analysis.

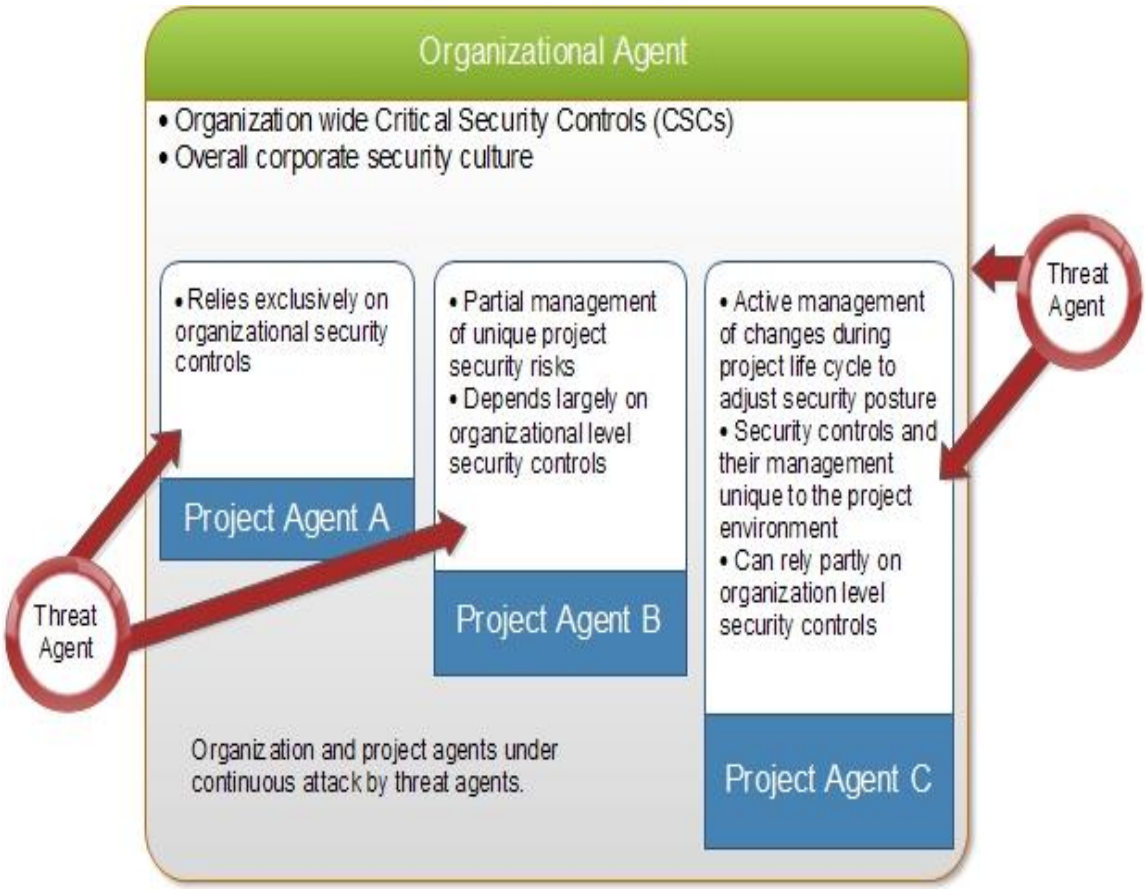

Figure 3.1 - High Level Agent-Based Model Design

6) Conduct simulation runs in order to produce relevant data to be analyzed.
    a. Simulation runs were conducted comparing projects with security risk management and without, based on a selection of specific security controls
7) Analyze the data produced by the simulation runs
    a. Determine if there is a significant improvement in the security posture of an IT project in which the manager implements his or her own security risk management
    b. Determine the costs of the added security controls

8) Conduct research of relevant literature to find information regarding managing information security in projects
9) Collect information regarding managing information security in projects from relevant professionals in IT management and security fields
10) Provide recommendations based on the results of the analysis of the simulation data and any related information from literature or from professionals

The steps above illustrate the process the researcher followed during this study. It was assumed that this methodology would create a clear understanding of the effectiveness of IT project managers actively managing their own security risks within a larger organizational framework, as well as the costs associated with the added security controls and their management.

The deliverables of this methodology are information gathered through simulation runs of the model, literature and professional interviews that was analyzed in order to determine an answer to the research question. Also, recommendations as to if IT project managers should or should not engage in active project security management (PSM) are part of the deliverables. Finally, the model itself delivers a foundation for further expansion and use by other researchers. Success is measured by the determination, through data collection from the model, literary and professional sources, if PSM is effective at increasing the security posture of a project or not, and what costs are associated with the added security controls.

3.4 Credibility of the Research

Given the qualitative nature of this study it was necessary that the assertions and suggestions discussed by the researcher be reviewed in order to increase the validity and credibility of the research. The suggestions and the findings of this study have been reviewed by three faculty members with experience in IT project management, cyber security, homeland security and computerized modeling.

3.4.1 Validity of the AnyLogic® Modeling Tool

Given the use of the AnyLogic® modeling tool for this research, it is important for establish the validity of the tool.

One way to assist in this task is to highlight other work and research that has been done with AnyLogic®. The power and flexibility of the tool is demonstrated by one model in particular. It was developed to analyze the most efficient staffing levels for a regional hub evacuation center. Dietz, Kirby, and Wojtalewicz (2012) demonstrated that a well-designed AnyLogic® model can produce valid results that are applicable to real world situations. The authors modeled a complex environment of thousands of agents, in this case people and their pets, being moved through a reception center for evacuation. Each agent had different properties and had to be treated in a unique way within the system. The large numbers of agents and the many simulation runs that occurred produced valid, usable data. The authors were able to refine the use of staff at the reception center within the model and produce results for decision makers to use for disaster preparation and planning.

Another example of the use of the AnyLogic® tool for agent-based modeling is demonstrated by Ciarallo, Heath, and Hill (2013). The authors utilize the tool in order to

implement an agent-base model for improving the costs and operating efficiency of drivers in warehouses and warehousing strategies. Their model captures, categorizes and quantifies traffic congestion in the warehouse and the cost due to the congestion (Ciarallo, Heath, & Hill, 2013). The model presented in the paper is an excellent example of the power and validity of using AnyLogic® to implement a theoretical model and produce useful results that gives decision makers critical information.

3.5 Data Collection

The data used to build the computerized model was gathered from literary sources and interviews of information security and project management professionals.

The information gathered from literary sources includes the 20 CSCs published by the council on cyber security (Council on Cyber Security, n.d.) that have also been mentioned by one author and applied to the project management environment (Pruitt, 2013). A subset of these controls was selected by the researcher in order to model a real-world environment. For the sake of scope of the model, the selected controls represent the full breadth and depth of an organization's security control implementation. The selected critical security controls include technical, human factor and processes, practices and procedural controls. These CSCs were selected based on the following criteria:

- CSC use in industry. Propagation of use and perceived usefulness by security professionals
- Data availability for use in model. Does sufficient information exist to appropriately model the CSC within the AnyLogic® model?

- Appropriate and realistic use of CSC within an organization and a project. The CSC should have a high likelihood of use within an individual project and not just at the organizational level
- The chosen CSCs cover technological, human factor and policy, practices and procedural security measures

The following six critical security controls are modeled:

- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 7: Wireless Access Control
- CSC 15: Controlled Access Based on Need to Know
- CSC 17: Data Protection
- CSC 18: Incident Response and Management

Data gathered from professionals consisted of opinions and anecdotes of various security and management topics related to the research. Also, when possible, specific data on cost and effectiveness of various security controls was gathered. A total of six professionals were questioned via email, starting with specific questions and often leading to follow on conversations. All conversations occurred between early November 2014 and mid-March 2015. The information provided by these professionals will be used throughout this paper to reach conclusions and in order to assist in the analysis of the model output data. Every email sent and received by the researcher is listed in Appendix A.

The following individuals were consulted for the research:

- Subject A: Chief Information Security Officer (CISO) for a large public university; Organizational Structure: Functional; Relevant certifications: CISSP, CRISC
- Subject B: Project Manager, responsible for Security & Policy for a large public university. Organizational Structure: Functional; Relevant certifications: PMP
- Subject C: Project Manager and Technical Lead for a commercial software company that developed cloud-based communications services for active content websites. Organizational Structure: Functional, project-based for current department/project;
- Subject D: Program Manager for a commercial software company that develops software for government agencies. Organizational Structure: Projectized; Relevant certifications: PMP, CSM
- Subject E: Project Manager, for a government agency. Organizational Structure: Functional; Relevant certifications: PMP, CSM, CISSP, CISM
- Subject F: Information Systems Security Manager for a commercial software company that develops software for government agencies. Organizational Structure: Projectized; Relevant certifications: CSM, CISSP, ITIL, ICP

At first, the subjects were asked a particular set of questions relating to the topic of information security and managing security risk on projects. This lead to more follow up questions to either clarify points or to gain more detailed answers. The questions asked initially of all subject are listed as follows:

- Do you think project managers who manage security, including information security, for their project above and beyond what the organization mandates

(assuming vulnerabilities have been considered and a threat assessment made) add to the security posture of the organization? Do you have any examples from past or current projects where you or others have done this, or similar management?

- Would you consider information security management a part of risk management?
- Do you think that project security management, in particular looking at information security, could lead to more secure project assets and products?
- How does your organization handle information security, in particular for projects? How are you organized, who is responsible for what tasks? In general, what technology do you use (does not have to be specific), how do you deal with human factors (ex. training) and what policies and practices are there in your organization regarding information security?
- Do you have any hard numbers of budget expenditures for information security and its effectiveness (ROI perhaps)? Any percentage numbers of information security expenditures per budget for projects would help. (If you do and it is propriety/secret information you don't have to divulge it of course - this is understandably the most difficult information to obtain)

All email correspondence with each subject is listed in Appendix A for reference.

Also, critical thinking and input from the researcher's committee members has been used in the design of the model in order to appropriately leverage the various data collected from literature and professionals. Researcher bias, as discussed previously had the largest impact during the design of the model and its implementation. The design reflects a system that is based on the researcher's listed biases.

The computerized model and the data obtained from it through a series of simulation runs was a vital part to obtain the data required to answer the thesis question. Also, information gathered from literary sources and professionals was used to highlight and provide context for the data from the model, as well as support the overall conclusions and recommendations. The data gathered from each simulation run included the number of attacks perpetrated by a threat, how many attacks were defeated and by which level (organization or project). Also, the cost, as a percentage of total IT security budget, of implementing each security control and its relative effectiveness was part of the output. The data from all simulation runs was compared and analyzed and conclusions drawn from it. All of the data produced and outputted by the model runs is included in its entirety in Appendix B.

3.6 Model Design

Several important pieces are part of the model design. The core of the model centers on the CSCs that are intended to model the real-world implementation of security controls. As discussed above, several of these were selected from the total list of 20. They were selected to provide coverage for technical, human factor and policies, practices and procedural security measures. Each CSC has one or more attack types associated with it, as listed by the council on cyber security (Council on Cyber Security, n.d.). Also, each CSC has a cost and a risk mitigation or defensive effectiveness rating associate with it. The cost values for each CSC represents the percentage cost added to an IT security budget. The effectiveness value of each CSC is the relative effectiveness that it provides against a single attack by a threat. So, the effectiveness value represents the percentage

chance the CSC has to defend against an attack. By designing the model to include these CSCs it allows for a more robust analysis of the effectiveness of the various security layers in an organization, including the project level security.

Given that the model is agent-based, numerous agents are modeled that interact with each other during a simulation run. The first agent is the Organization Agent (OA). This agent is designed to have all CSCs available and active at all times, and is intended to model the organizational level security structure. These CSCs provide one layer of security from threats at a certain cost.

Another agent is the Project Agent (PA) that represents a project within an organization with its own CSCs based on the uniqueness of the project and its environment. These CSCs provide the lowest layer of security within an organization and are the most important part of the research. These CSCs and their modeling are important to answering the research question of this study.

The last agent is the Threat Agent (TA). This agent models an attacker who seeks to exploit a vulnerability that a CSC is associated with. The TA attacks the organizational and project levels in order to exploit this vulnerability. One TA is modeled within the simulation and represents the totality of threats in a real world environment.

The model design is intended to produce a simple way to measure the effectiveness of project level security management. It is not intended to create a full-featured model that takes into account every aspect of a real-world scenario. It is based on accepted security principles that are being used in many organizations today.

3.7 Summary

Determining the validity of security management at the project level and its cost and effectiveness is the primary purpose of this study. The means to determining the answer to the research question is through analysis of literature, input and opinions of professionals in the project management and security fields, and the analysis of data generated by a computerized model. The analysis should shed light on the validity and effectiveness of the concept of project security management and its associated costs. The researcher hopes that project management and security professionals can use the findings and recommendations presented in this paper to the benefit of their organizations.

CHAPTER 4. MODEL DESIGN AND IMPLEMENTATION

4.1 Introduction

In today's highly connected and data-driven world where information is a key asset to organizations, the threats to the confidentiality, integrity and availability of such information is enormous. Recent, highly visible attacks on various businesses and government agencies have highlighted to more than security experts the threats that organizations face in protecting information (Krebs, 2014a; Krebs, 2014d; Mandiant, 2013). Information security issues, and the results of attacks and breaches, are increasingly being published in main-stream media outlets, for better or for worse (Collins, 2015; Dawson, 2015). Certainly, these publications are resulting in an increased awareness of the effects of poor information security to the general population, contributing to more pressure on organizations to improve and optimize their overall security posture and manage the risks associated with information security more effectively. It is no longer just financial or trade secrets that organizations lose from security incidents and breaches. Prestige, customer trust and the very jobs of senior leaders are at stake.

Looking at the current state of information security, Symantec (2014) reports that total breaches were up in 2013 by 63% from 2012, a trend which is likely to continue. Cybercrime cost to the global economy ranged from $375 to $575 billion dollars

annually, with an average estimated loss of $2.7 million per cybercrime incident (PwC, 2014). Further the same author reports that larger organizations incur higher costs from security incidents. Threats from cyber espionage by government entities, terror groups, businesses, criminal gangs and other sources will continue to increase in frequency (McAfee, 2015). In this environment, organizations of all types and sizes need to plan for and implement new forms of protections and risk management practices in order to keep their valuable data as secure as possible, and deal with negative events and their impacts. One way to assist in the planning, and to make the implementation of security controls more efficient and effective, is the use of computerized modeling. Using computerized models, based on real-world environments, leaders and decision-makers can more accurately predict the effectiveness of various security controls and their costs. If the model incorporates technological, human factor, and policies, practices and procedural controls in its design, the result would be of value to an organization. The data gathered from the simulation runs can be used to predict current and future effectiveness of the security controls and their costs. These methods will aid organizations in their information security related risk management endeavors.

This paper will use a unique model in order to demonstrate the usefulness and validity of this approach. Agent-based modeling (ABM) will be used in order to implement a simple design based on a defense in depth strategy using a sub-section of the 20 critical security controls (CSCs) published by the Council on Cyber Security (Council on Cyber Security, n.d.). The data resulting from simulation runs will demonstrate the relative effectiveness of various CSC implementation strategies and their budgetary costs.

4.2 Agent-Based Modeling

According to Gilbert (2008), "Formally, agent-based modeling is a computational method that enables a researcher to create, analyze, and experiment with models composed of agents that interact within an environment." (p. 2).

Agent-based modeling (ABM) was chosen for the design and implementation of the model based on the properties of the organization, its embedded projects and the threats which will interact with both. As the name suggest, this method of modeling makes use of autonomous agents where each has a set of attributes and behaviors that define how the agent will behave in response to changes in its environment (Palgrave Connect (Online service) & Taylor, 2014). In agent-based modeling, the relationships and connections between agents are also of importance as well as the environment in which the agents operate in (Palgrave Connect (Online service) & Taylor, 2014). Therefore, the system in an agent-based model consists of the agents, their relationships and the environment where they exist in.

One can see now that in order to achieve valid and useful results for the information security issues spoken about above, using the agent-based model methodology is a wise choice. Having multiple agents autonomously interacting with each other is arguably the most effective way to simulate real-world environments and behavior in the context of information security. It also allows for greater flexibility in choosing different courses of action for various simulation runs, as the reader will see below.

4.3 Model Design

This section will discuss the model design in detail. The approach taken in the design was based on a course-of-action (COA) decision making process. That means the results of the model runs are intended for managers and leaders to make important decisions regarding security control effectiveness and costs. These individuals are able to select certain COAs in order to determine which of these was most effective and at what cost. This methodology is very much grounded in the effective military approach to planning and decision making in a unit's staff planning. The staff will create three specific COAs for the commander to choose from and let him or her decide on the best one for the execution of an operation. The Department of the Army (2012) lays out the Military Decision Making Process (MDMP) in its doctrinal publication *ADP 5-0 The Operations Process* (p.8). It explains the process taken by military leaders and their staffs to determine the best COA for any one particular operation. This falls in line with the decisions an organization needs to make regarding information security. Certain actions must be taken to defend the organizational assets in the future and any tools and methods that can help in this planning are valuable. Hence, the reason for looking at the design of this model in these terms. Allowing certain COAs to be chosen by the user and then run within the simulation in order to determine the most effective security controls to implement in an organization and its projects.

4.3.1 The Critical Security Controls

At the core of the design are the 20 Critical Security Controls (CSCs), published by the Council on Cyber Security (Council on Cyber Security, n.d.). These form the basis of effectiveness and cost values used to determine the validity of the COA chosen for a

simulation run. A user may select a certain number of these to explore a specific security strategy, run the simulation and observe the overall effectiveness of the strategy chosen, and its relative cost. In order to properly scope the project, only six out of the 20 CSCs were selected in the design. It was also determined by the researcher that it would not be unnecessary at to include all 20 CSCs at this point, given that the ones chosen properly represent the whole. All choices were based on the following criteria:

- CSC use in industry. Propagation of use and perceived usefulness by security professionals
- Data availability for use in model. Does sufficient information exist to appropriately model the CSC within the AnyLogic® model?
- Appropriate and realistic use of CSC within an organization and a project. The CSC should have a high likelihood of use within an individual project and not just at the organizational level
- The chosen CSCs cover technological, human factor and policy, practices and procedural security measures

All 20 security controls were evaluated and studied in detail using *the critical security controls for effective cyber defense (version 5.0)* (Council on Cyber Security, n.d.). Also, *Security best practices for IT project managers* (Pruitt, 2013) was consulted in order to tie in relevancy of the CSCs for projects and their managers. A summary document of the evaluation process the author used to choose the six CSCs for the model can be found in Appendix C. It contains relevant details on each CSC gathered from the documents mentioned above and assisted in focusing the researcher's thoughts in regards to the CSCs.

The following six critical security controls, taken from the council on cyber security (Council on Cyber Security, n.d.), were selected and are modeled (p. 19 – 95):

- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 7: Wireless Access Control
- CSC 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 15: Controlled Access Based on Need to Know
- CSC 17: Data Protection
- CSC 18: Incident Response and Management

Now that the topic of the CSCs has been conveyed, the author will discuss the high level conceptual model before explaining the COA decision and comparison process.

4.3.2 Describing the High-Level Conceptual Model

Before delving into the details of the COA decision making process inherent in the model, or the details of its design, it is worthwhile to discuss the high level conceptual model upon which all of it is based. The figure below gives a quick glimpse of the concept on which the model is built. At its center is the idea that a project (or a team of some size) is the lowest level of leadership or management in the organization that can affect the security posture of the organization as a whole, and of course its own internal security posture. This idea can be broadly defined as Project Security Management (PSM). Therefore its leaders must take security related risk into account, and in the case of this research, information security in particular. This conceptual model is built primarily on the simple defense in depth concept, viewed in the context of a management

and leadership hierarchy. As an example of defense in depth applied to information security, (Bedi, Gandotra, & Singhal, 2009) outline a defense in depth strategy for organizational information security. They speak of security layers surrounding an asset that needs to be protected and threats of a certain type and with a certain probability of realization. The more security layers are implemented the lesser the probability of the asset being compromised by a threat. This concept is also well understood by military professionals and examples of such practice are many throughout human history. The figure below demonstrates the use of agent-based modeling inherent in the design and implementation of the model, and describes at a high level the defense in depth method.

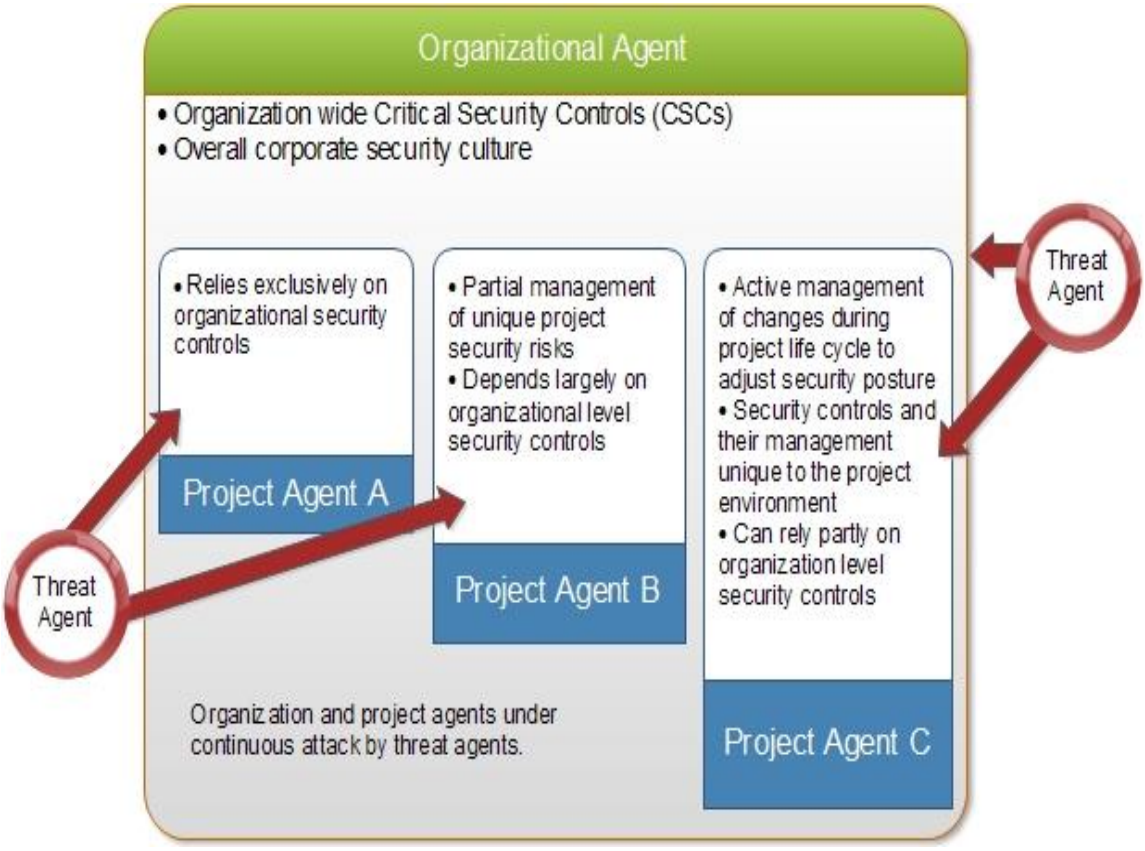

Figure 4.1 – High Level Model Design

The basic idea is that projects with various levels of CSC implementation are part of an organization with its own CSC protections. The threat agents, representing real-world threats, continuously attack the organization and its projects, seeking to exploit vulnerabilities. Given the use of the defense in depth strategy (or put in other terms, a multi-tiered defensive strategy, each tier being a management level), threats must first penetrate the defenses provided by the organization before being able to attack project assets directly. As discussed above, the Critical Security Controls are a vital part of the equation. They provide not only the defense against threats, but also point us to the type of asset and the method of attack the threats might use. A CSC is built to defend specific assets against one or more types of attacks. Effectiveness of defense and costs are also directly tied to each CSC, data which we will see is most critical.

4.3.3 COA Decision Making Process

In this section, the course of action (COA) decision making process will be discussed. As mentioned above, the model implementation is built around it and the process is meant to feed the model with decisions from the user. For obvious reasons, it is a shortened and more simplified decision making process than what is outlined in *ADP 5-0 The Operations Process* (Department of the Army, 2012). The following figure demonstrates the process taken in order to determine an appropriate COA.

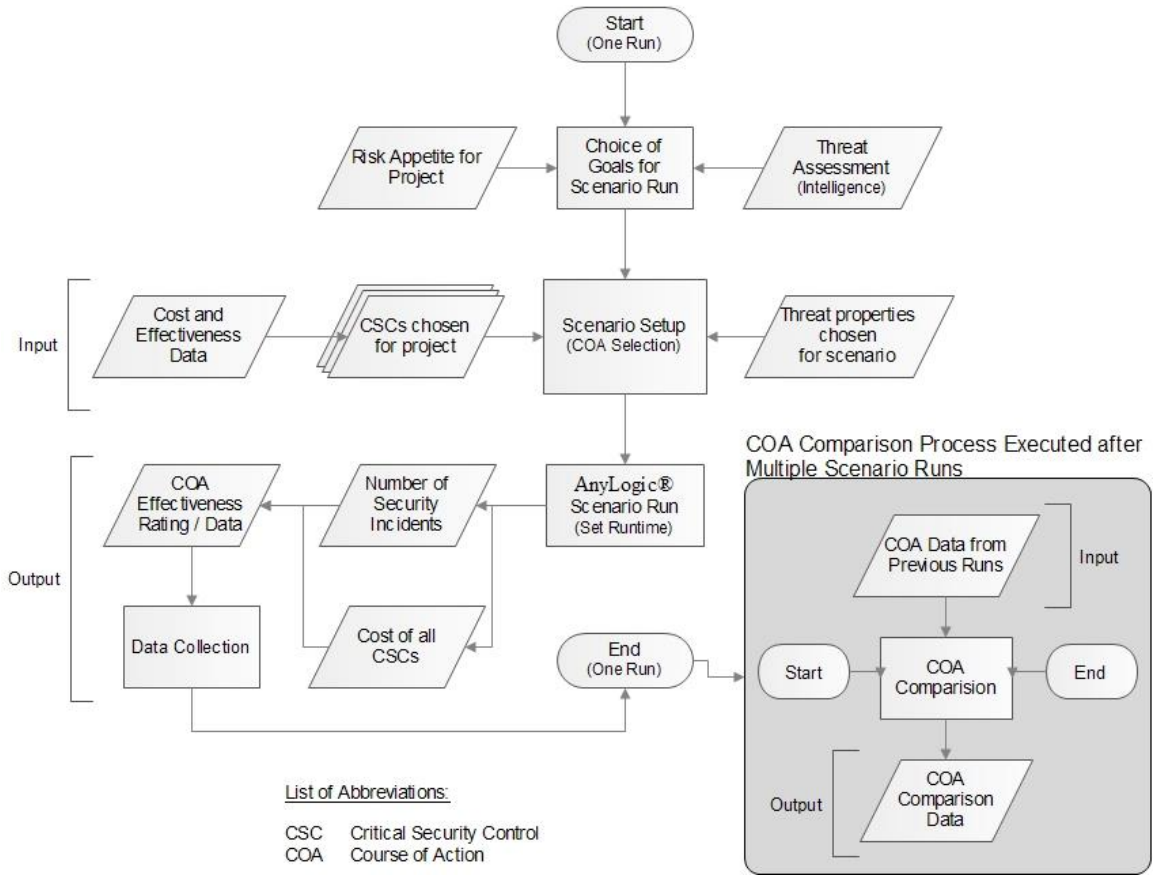

Figure 4.2 – Model COA Decision Making Process

For the scenario setup the user performs a threat assessment and determines the risk appetite of the organization overall, and the project specifically. This is similar to evaluating capabilities and limitations of friendly and enemy forces before battle. Next, the user will set up a scenario using the available information. This includes what threats exist to the organization and its projects and what critical security controls (CSCs) are needed in defense. The effectiveness and cost values are directly associated with the chosen CSCs and can be configured easily in the model, as we will see later in the implementation section of this paper. For example, if there is a threat from bad actors using wireless access points, CSC #7: Wireless Access Control can be implemented and

the effectiveness and cost values of this control will be considered in the scenario. Other inputs include the scenario runtime which represents one budget cycle. The cost of each control is measured in percentage of project budget for the budget cycle, be it a year or the length of the project. Also, multiple runs with the same data can be selected in order to later extract and analyze mean effectiveness values for the overall COA selected. During the simulation run, data is collected and written to a spreadsheet. The specific data collected from the model during runtime is the following:

- Total Number of Attacks
- Number of Attacks on the Organization
- Number of Successful Attacks on the Organization
- Number of Successful Defenses on the Organization
- Number of Attacks on the Project
- Number of Successful Attacks on the Project
- Number of Successful Defenses on the Project
- Total Cost to Project

After the completion of each scenario, the data that was written to the file can be analyzed in the COA comparison process. If, for example, one scenario has three of the six CSCs implemented vs. another scenario that had all six in use, a comparison of the number of successful attacks and defenses can be made. This process is denoted in the grey box in Figure 4.2.

4.3.4 User Input and Scenario Run Design

Next this paper will discuss the process the user follows in order to input the above discussed information and how to set up a scenario. Figure 4.3 below displays the

process of selecting the various inputs for a scenario run.

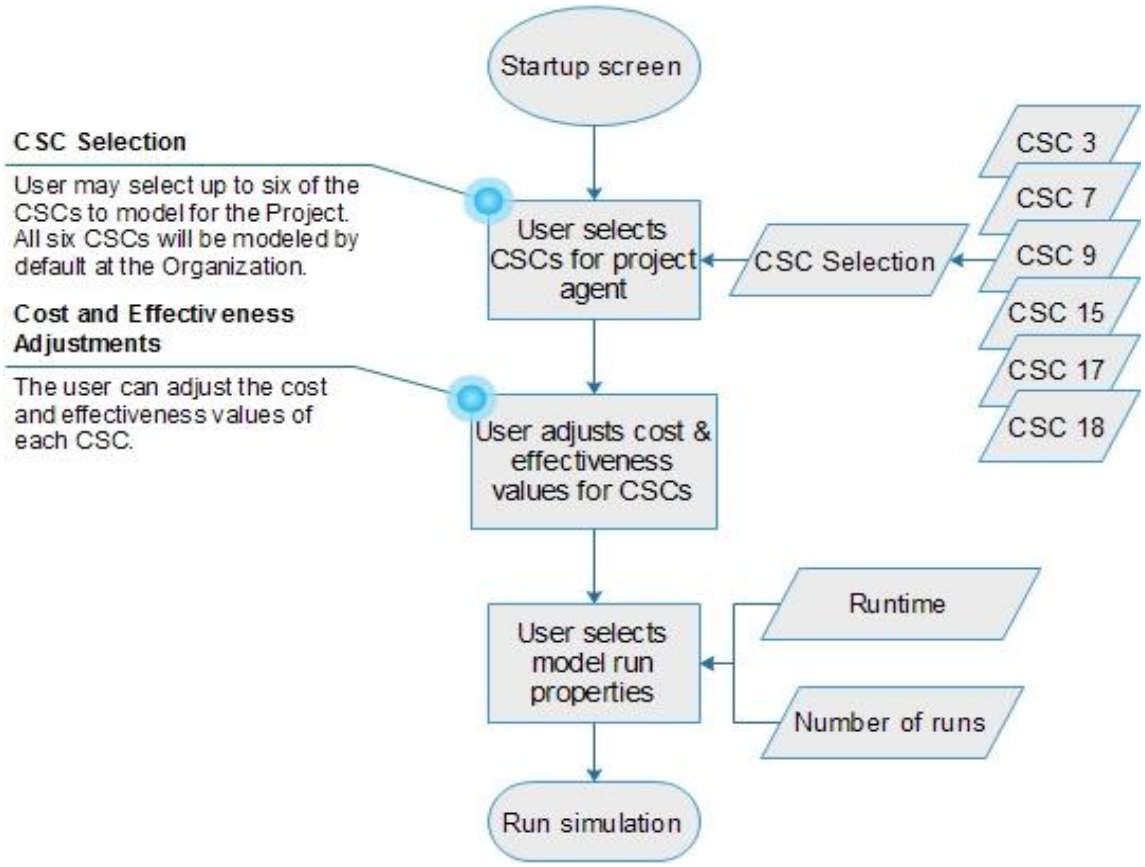

Figure 4.3 – Scenario Setup Process

The user is presented with a startup screen where all information is entered. He or she may select which CSCs are needed at the project for the scenario and adjusts the specific cost and effectiveness values. As mentioned above, the cost numbers entered represent percentage cost of each CSC of total security budget expenditure. The effectiveness numbers are the percentage chance each CSC has to successfully defend against a single attack. These values and how they are used in the system will be discussed in the model implementation section. After these selections have been made, the user can then determine the length of each scenario run and how many times the

scenario shall run in one session. As already stated, the length of each run represents one project budget cycle and is not designed to be a certain real-world time. After the information is entered, the simulation is run. Figure 4.4 demonstrates the process the model executes during a run.

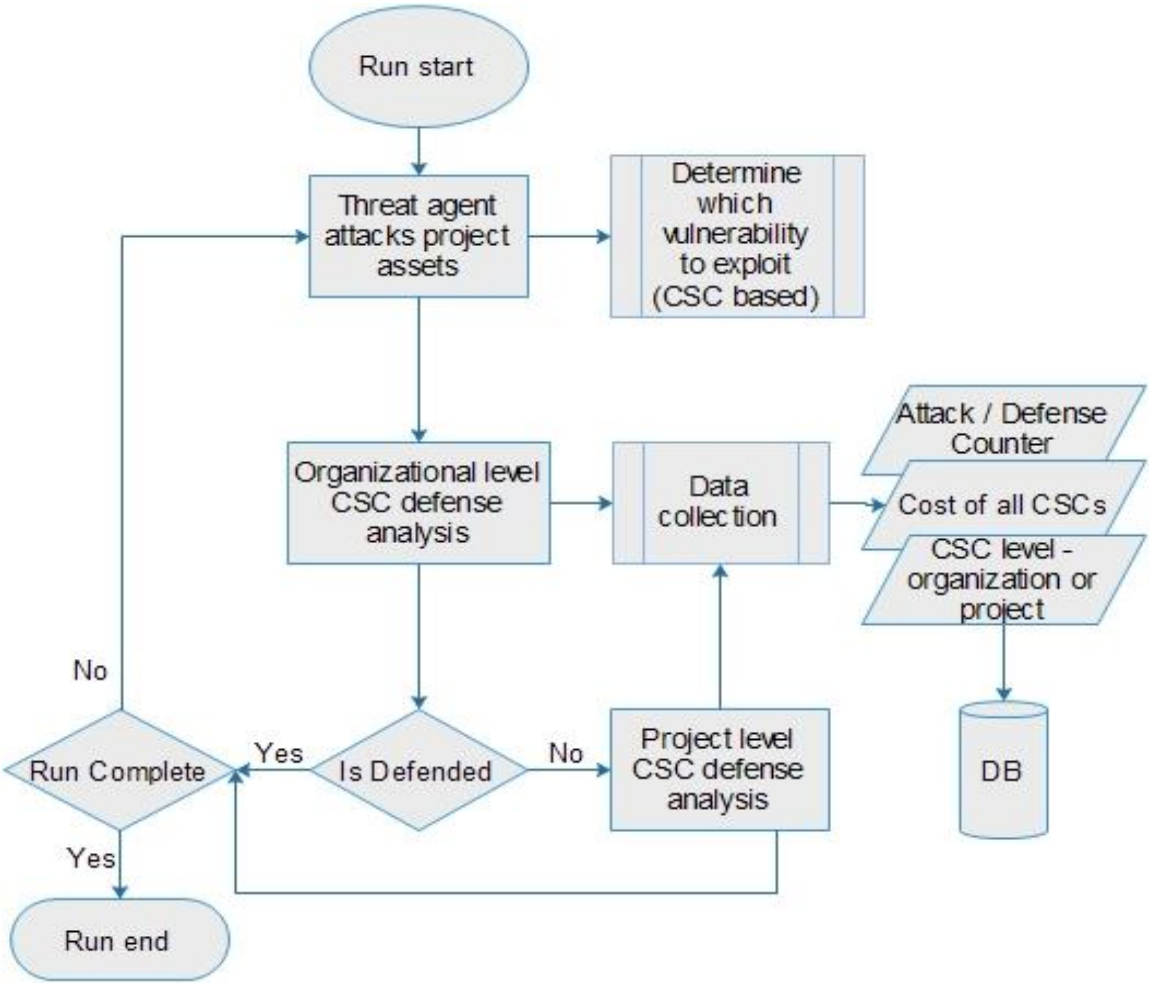

Figure 4.4 – Model Runtime Diagram

When the simulation starts, the threat agent immediately starts to attack the organizational CSCs and whichever project CSCs were implemented. First, the threat will determine which vulnerability to exploit. Once this has been determined, the organization will be attacked and the probability of a successful attack or a successful defense will be

determined. If the model calculates that a successful defense occurred, the logic will then test if the run is complete or not, and if the scenario needs to continue, the process will repeat and the threat will once again attack the organization. If a successful attack occurs on the organizational level, the threat will then attack the project level security control. Once again, a process will be executed to determine a successful attack or defense and the logic will proceed further to check if the run is complete or not. While all of this processing is occurring, the data on attacks and defenses is being collected. As mentioned in section 4.3.3, several metrics are gathered for later analysis and written to a spreadsheet.

Now that the design of the model and what concepts it is based on are explained, the detailed implementation will be discussed.

4.4 Model Implementation

The creation of the model was accomplished within the AnyLogic® Multimethod Simulation Software. The two main parts of the implementation were the user interface (UI), and the underlying logic using an agent-based finite state machine (FSM). Using the FSM was the best method to model the interactions of agents and their various states. Also, a state machine implementation lends itself for possible model expansion in the future, which is a large part of the motivations behind developing this base model. This particular topic will be discussed in more detail at the end of this chapter.

The overall goal of the implementation was of course to achieve the desired design as described in the previous section in regards to the course of action selection,

and to provide the data in order to come to conclusions as to which COA is the most effective.

4.4.1 The User Interface

The user interface was the first piece to be developed and was created to allow the user to enter the information needed for a simulation run. Figure 4.5 below is the final implementation of the interface called the PSM Simulation Configuration Screen.

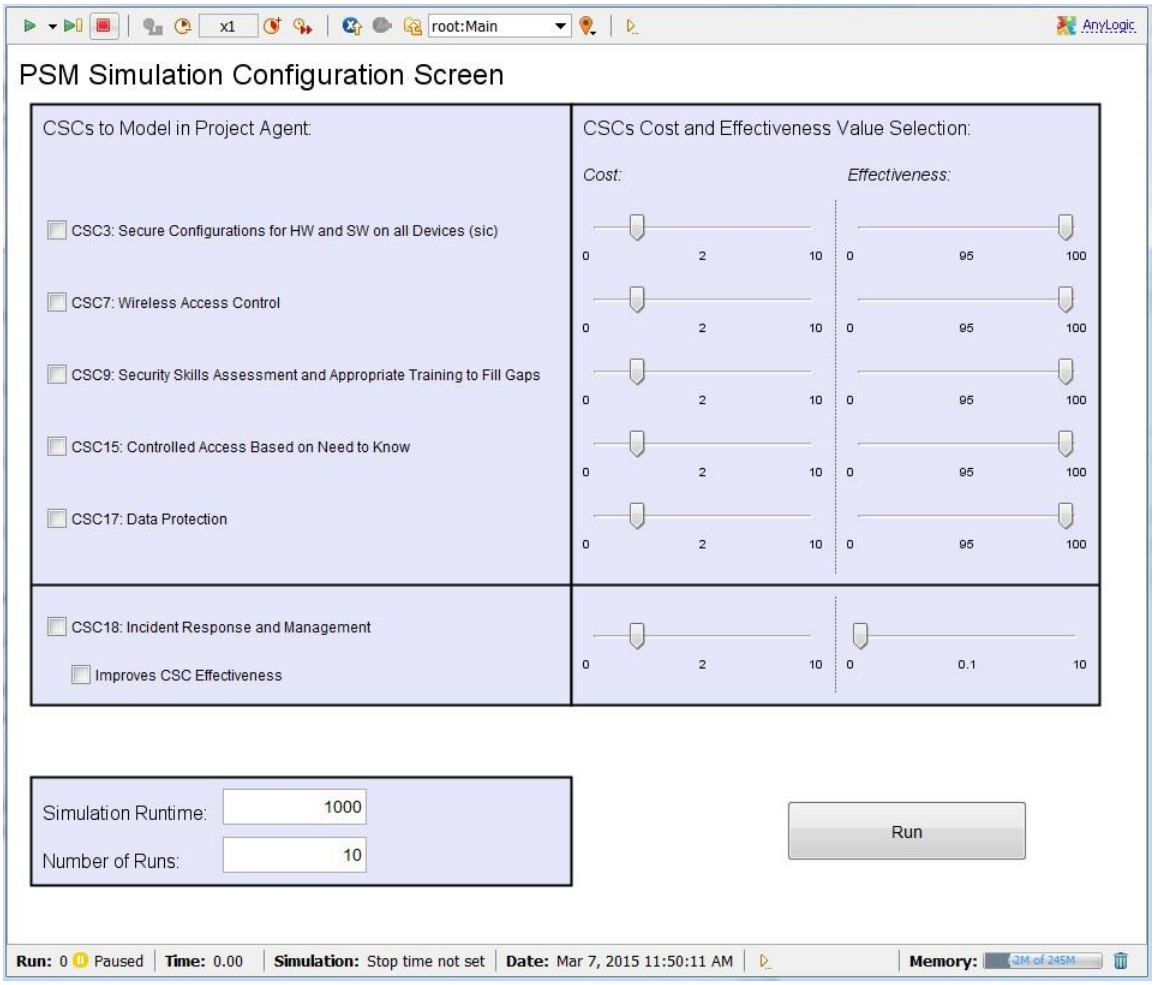

Figure 4.5 – PSM Simulation Configuration Screen

As one can see, the interface provides all the necessary input mechanism in order to fulfill the design's intent. On the left hand side of the screen the user may select,

through a series of check boxes, which critical security controls shall be used in the project during one simulation run. The details of each CSC, what they are and what protections they should provide to an organization or its projects are outlined in Appendix C. Note that a total of six CSCs are implemented. On the right hand side of the screen is where the user may enter the cost and effectiveness values for each specific CSC.

Note that CSC 18: Incident Response and Management is unique in that it affects the other five's effectiveness values during the simulation run. If this CSC is used in a run, it will enhance the effectiveness of the other controls by the percentage value selected, after a threat successfully breaches the project defenses. This implementation is based on the principle that if security incidents are properly responded to and managed, the organization and project members will learn from it and their overall security posture will improve. Although the primary focus of the incident response and management control is to mitigate the impact of a security incident (Ahmad, Hadgkiss, & Ruighaver, 2012), one could make the argument that going through the process improves the security posture, given the knowledge gained by the team regarding the attack. Ahmad et al. (2012) also state that "organizational learning is paramount, enabling organizations to learn effectively from the past and not suffer repeat incidents or mistakes" (p. 651). The improvement modeled is directly related to the type of attack, which is related to the specific CSC that is implemented to provide protections from that attack type.

Finally, the user can adjust the runtime and the number of runs to conduct. The runtime reflects one project budget cycle. The number of runs determines how many runs to conduct with the same inputs and at the selected runtime. This allows for multiple runs

to be averaged, later in analysis. When all information is entered, the user can proceed with the scenario execution by clicking the run button.

Figure 4.6 below shows the execution view of the simulation.

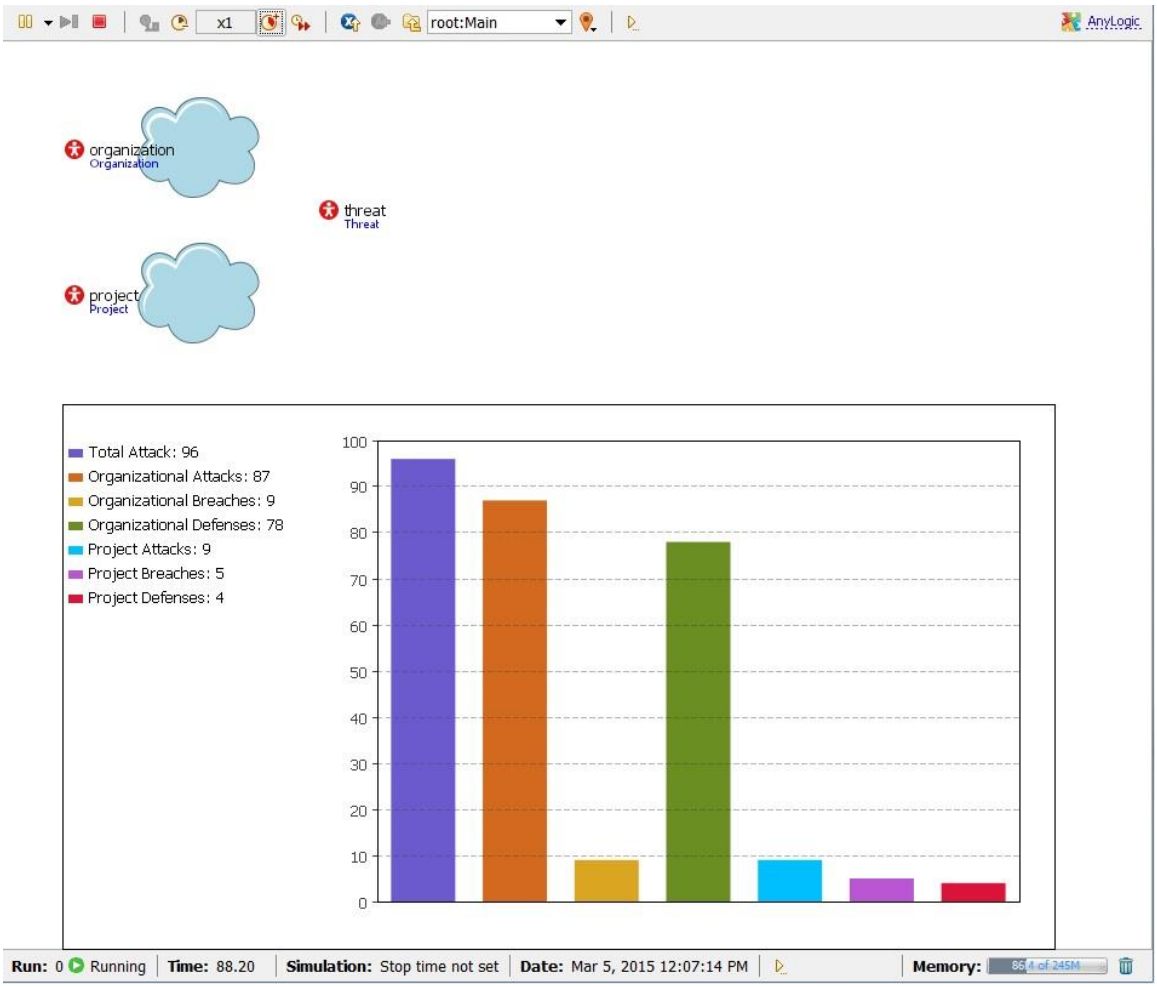

Figure 4.6 – Simulation Execution View

As the simulation runs, the bar chart continuously updates. The legend displayed all relevant information on the left of the chart. As with all other AnyLogic® models, execution time can be controlled with the run controls on the top. This particular screen is not intended to be more than a quick visual display of what is occurring "under the hood". To obtain output data quickly, the user can fast-forward the simulation and the

system will write all of it to the database, in this case a spreadsheet. Depending on how long the runs are and how many are executed, the file will contain a certain number of records that can be analyzed.

Now that the user interface has been presented, the important underlying functionality will be explained.

4.4.2 The State Machine Logic

As already mentioned, the core of the system is based on state machine within the threat agent. Since the determination was made by the researcher that critical security controls protect certain assets, and these CSCs are associated with particular types of attacks, it made perfect sense to have the threat agent contain the bulk of the functionality and logic. In its current version, the model is focused on what actions the threats take during the simulation, and not what counter-actions the organizations or projects take. The actions of the latter are perfectly well simulated by the selection of the CSCs by the user. That is, if a user select a specific critical security control, this means the threat agent now has it as a choice to attack during the run and the CSC has a certain chance to defend against the attack, simulating the actions of an organization or a project team defending against the attack. In the future, more extensive and granular modeling can be accomplished by giving organizational agents and project agents their own state machines. These expansions of the model will be discussed later. For now, this concise implementation suffices for what needs be accomplished in a simulation run. The following diagram, figure 4.7 presents the threat agent state machine, which is the core of the model.

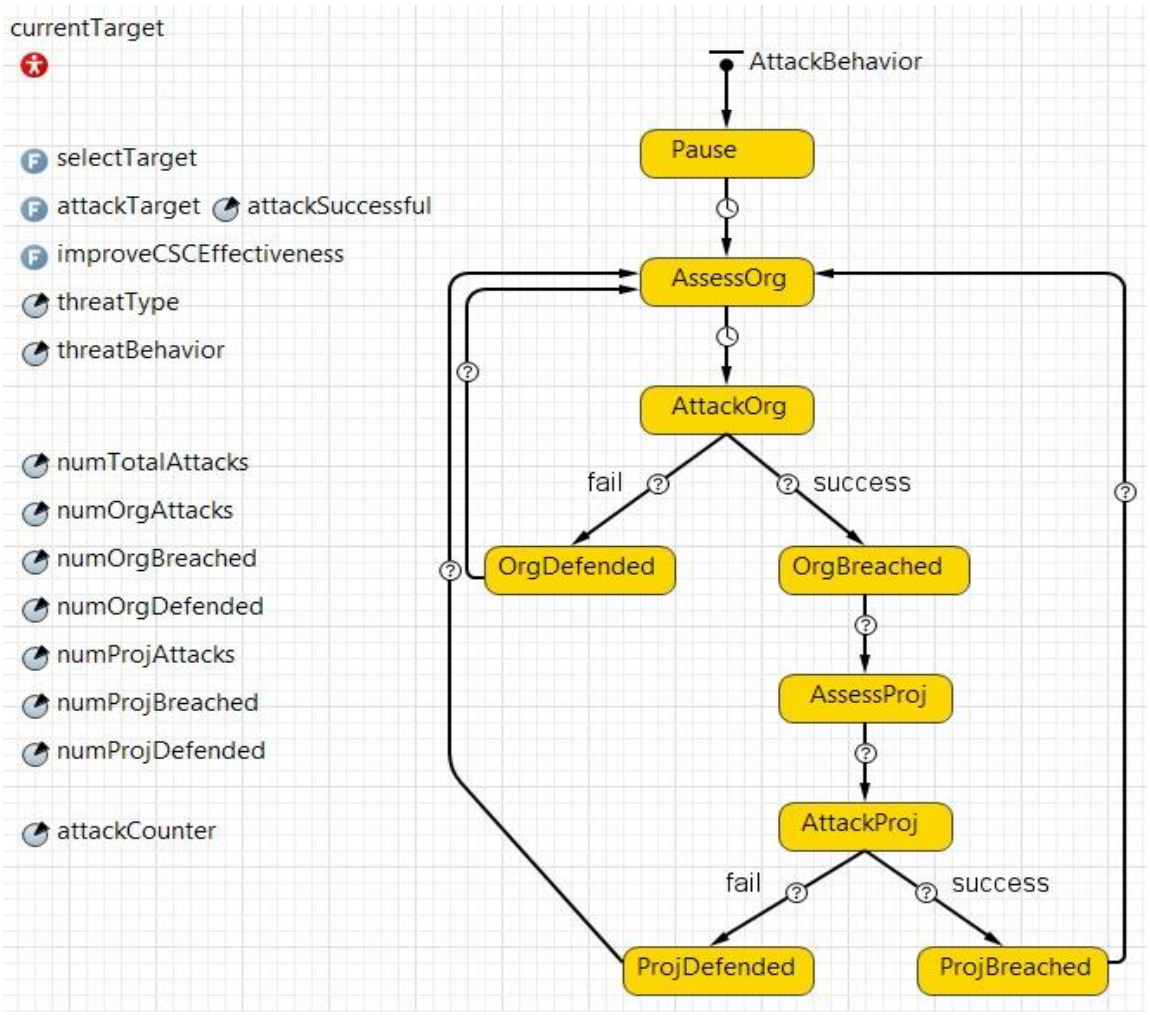

Figure 4.7 – Threat Agent State Machine

This figure is a screen capture from the AnyLogic® development environment. The many states the threat can take are represented and each relevant transition is labeled. The initial state the threat enters is the pause state. This state was created to solve a technical implementation issue and is not of significance to the logic.

The first relevant state the threat takes is the AssessOrg state. As the name suggests, the threat will assess the organization and its vulnerabilities. It is intended to combine reconnaissance and target selection. Currently, the model does not detail real

world threat behavior since it is out of the scope of this paper, therefore the implementation is basic in nature. In the AssessOrg state, the threat will randomly select a target in the organization to attack, which is one of the five CSCs implemented in the model. Note again that CSC 18: Incident Response and Management is not a control that should be selected for attack given its special purpose, which is to positively affect the other controls after a breach occurs.

After a target has been selected, the threat enters the AttackOrg state where the threat agent will attempt to exploit a vulnerability. The CSC is the focal point, since it has cost and effectiveness information associated with it. In this state, the attackTarget function is called and a determination is made if the attack was successful or not, and the organization is breached or not. The core of the implementation is the randomTrue method provided in the AnyLogic® library. This function is passed a probability value p from 0.00 – 1.00 and generates a true response with the given probability. It generates a false response with 1 - p probability. The purpose of this state is to simulate the effectiveness of a certain CSC. Each control has a chance to defend against its associated attacks. After the determination is made if the attack was successful or not, the state will change back to the AssessOrg state if unsuccessful, or to AssessProj if the attack resulted in a breach. Before doing so, the threat will enter either the OrgDefended or OrgBreached states, depending on which holds true. These states are primarily for data collection and to provide a means to include the incident response and management control.

When the threat state enters the AssessProj state, the same process that occurred in AssessOrg is launched. However, the threat will now assess the CSCs implemented in the project (selected by user in the configuration screen). As with the organization, a

control is randomly selected. The determination was made by the researcher that a breach relating to any organizational CSC opens the door for any other vulnerability to be exploited in a project. For example, if wireless access control fails at the organizational level, it does not mean that the project is only vulnerable to wireless access control related threats. This property of the model is easily modifiable if it does not accurately reflect any one organization's realities.

Now, the AttackProj state is entered and again the attackTarget method is called. The exact same calculations occur as did on the organizational agent, yet now they are related to the probability of a successful attack occurring to the project agent. If an attack fails or succeeds, the threat will revert back to the AssessOrg state. Before this state however, it will enter either the ProjDefended or ProjBreached states. Both states are currently used for data collection and in the case of ProjBreached to run routines which are related to the incident response and management control. As described above, this control is intended to simulate the improvements in defenses that are typically achieved with good incident management. It is important to note that in any future version of the model, these states will be included in the project agent or in the case of the organization, in its agent. For this version of the model these states were included in the threat agent for simplicity sake.

Next sample data from a simulation run will be discussed.

4.4.3 Sample Run

When a simulation is run, the data is pushed to a spreadsheet for analysis. The following section includes output from two separate runs with different configurations in order to demonstrate how the model can be used to set up and choose various COA's.

First, a discussion on the basis of the selected cost and effectiveness values needs to occur. The author found enough relevant data to be able to estimate the cost of IT security measures and can deduce percentage budget cost per critical security control implemented. The choice of cost as a percentage of budget was made, given the wide monetary figures reported by various organizations. It was necessary to normalize the data and the best approach was using percentage figured related to IT security budgets as opposed to any range of monetary values. Everett (2010) reports that IT security spending is around 10-15% of IT budgets. This out of a total IT budget ranging from 1.0% to 8.1%, depending on industry (Gartner, 2013). Further, IT budgets will grant an estimated 11% to security projects (Brocklehurst, 2014). These figures give a good reference to how much a single CSC should cost as percentage of budget for any scenario run. A choice of 2 – 2.5% would suffice to be valid for the six security controls implemented in the model.

Obtaining accurate effectiveness values was however not possible given the apparent confidentiality of this information to organizations. No specific data was found in literature or by interviewing professionals that was usable for this particular model. General figures to help assess relative effectiveness were discovered, such as 71% of system compromises not being immediately detected (Trustwave, 2014). Further, according to the same author, 31% of compromises were related to weak passwords. Given these statistics, it is not clear however that we can make an absolute determination of the effectiveness of any one CSC related to these numbers, in particular given the variability of organizations and their unique structures and CSC implementation. Finding specific probability-based numbers for the 20 Critical Security Controls was difficult, so certain judgment-based decisions had to be made.

In the end, the researcher believes that although it would be positive to have exact figures, it is not necessary to demonstrate the value of the model and its potential, nor to come to a conclusion based on the inputs. This is because one can run numerous configurations with different cost and effectiveness values based on whatever specific metrics that were gathered, be they confidential or not. An organization can utilize their own data to feed the model. Further, one can optimize them to determine important facts about the relationship between costs and related effectiveness. What is important is the concept the model implements. Being a defense in depth based model allowing an individual to create multiple defensive strategies and determine which one is best suited for the situation.

With this in mind, the following two courses of action will be presented in order to demonstrate the value of the model. The two COA's were set up with the following inputs:

- Cost for each implemented CSC is 2% of project budget
- Effectiveness for each CSC is 95, meaning a 95% chance of defending against any one attack
- Model run time: 1000 simulation seconds
- Number of Runs: 10
- Run #1: Implement five CSCs
- Run #2: Implement two CSCs

Run #1 Output:

Total Attacks	Organizational Attacks	Successful Organizational Attacks	Organizational Defenses	Project Attacks	Successful Project Attacks	Project Defenses	Total Cost of CSCs to Project (% of budget)
1046	999	47	952	47	5	42	10
1035	1000	35	965	35	2	33	10
1065	1000	65	935	65	2	63	10
1052	1000	52	948	52	2	50	10
1071	1000	71	929	71	4	67	10
1051	1000	51	949	51	1	50	10
1041	1000	41	959	41	2	39	10
1051	1000	51	949	51	3	48	10
1049	1000	49	951	49	0	49	10
1046	1000	46	954	46	1	45	10
1051	**1000**	**51**	**949**	**51**	**2**	**49**	**10**

Figure 4.8 – Run #1 Output Example

Run #2 Output:

Total Attacks	Organizational Attacks	Successful Organizational Attacks	Organizational Defenses	Project Attacks	Successful Project Attacks	Project Defenses	Total Cost of CSCs to Project (% of budget)
1035	999	36	963	36	20	16	4
1041	1000	41	959	41	25	16	4
1049	1000	49	951	49	37	12	4
1046	1000	46	954	46	30	16	4
1053	1000	53	947	53	28	25	4
1051	1000	51	949	51	30	21	4
1041	1000	41	959	41	25	16	4
1060	1000	60	940	60	37	23	4
1043	1000	43	957	43	29	14	4
1053	1000	53	947	53	31	22	4
1047	**1000**	**47**	**953**	**47**	**29**	**18**	**4**

Figure 4.9 – Run #2 Output Example

For both COA's, each run was conducted ten times and the output from each individual run was averaged. The model allows for the running of as many simulation runs as the user deems necessary to achieve desired results.

As one can see, the first COA implements all five CSCs and shows a reduced amount of successful project attacks (two attacks) vs. the second COA which only used two separate CSCs for defense, resulting in 29 successful attacks on the project. The cost for the first COA is measured at 10% of the project budget, vs. only four percent for the second COA.

Depending on the specific data available to the researcher using the model, the cost and effectiveness values that feed the model will be more detailed and reflect the specific case that he or she is looking into. This will provide a more robust and valid result upon which leaders can make certain decisions about CSC implementation.

4.4.4 Future Model Expansion

Although this base model and its implementation in AnyLogic® can serve a useful purpose, it is the hope of the author that the model be expanded to fit the needs of different organizations. Some of the suggestions are presented now.

4.4.4.1 Threat Behavior

Some organizations might have a need to model the behavior of threats in more detail. The current model provides the baseline of an agent-based approach to modeling these threats. Expansion in the threat state machine would allow for more realistic and granular implementation of the various threat behaviors. The model implementation could expand to include numerous types of threats that get data input from the user interface or a database to allow threats to exhibit different actions during the simulation runs in order to better serve the needs of specific organizations in their threat related research.

4.4.4.2 Adding Multiple Project Agents and Adding Program Agents

The model can also be expanded to include multiple project agents. Also, the program management level in an organization can be added to more realistically model certain organizational structures. Of course, any agent can be included in the implementation in order to model whatever structure is needed to give a more accurate representation of reality. The basic hooks have been placed into the model in order to allow a simpler transition to this kind of expansion.

4.4.4.3 Detailed State Machine for Project Agents

In line with the expansion of the model for multiple project agents, these agents can be modeled with their own separate state machine and functionality to accurately reflect actions taken by project management and staff to ward of whatever attacks are committed against the project assets (detailed project security management modeling). Also, state machines can be included for any other agents deemed necessary, such as Program agents. The expansion of these agents will allow a more seamless tie-in with the following point regarding Asset agents.

4.4.4.4 Integrate Asset Agents

In order to come closer and closer to a real-world system and its encompassing environment within the model, it is suggested that an Asset agent be created. This agent will represent any asset that an organization or its projects own. Examples include routers, laptops, desktops, mobile devices or wireless access points. The reasoning behind including this type of agent is to allow for finer granularity in the modeling of how assets are attacked and defended, as well as how attacks can propagate through IT networks. If a

project owns an asset and implements a critical security control meant to protect it, this would more accurately represent the true nature of the system. When the asset is attacked by a threat, the interactions between the project agents with its implemented CSCs, the asset agent and the threat will produce a more accurate modeling. The value in this to an organization will be a much increased confidence in the validity of the output data.

4.4.4.5 Use of Real Time

In order to tie the cost and effectiveness outputs to an organization's real-world operations, real time must be used in the model. In the future, it will not suffice to represent a budget cycle with relative time. Managers and decision makers will want to know what the costs and effectiveness of controls are for a real budget cycle or project life cycle. Also, implementing real time will allow for more realistic modeling of threats. The model will be able to simulate threat attacks over time by using data on how many attacks of which type occur in a real time period.

4.4.4.6 Detailed Critical Security Control Implementation

There is a lot more to the CSCs than the current model implements. It is recommended that the details of each control be represented in the model. This will have to tie into the improved threat behavior and the Asset agent in future versions. Of course, if this expansion becomes a reality it will provide a more accurate representation of the effectiveness and costs of each CSC, leading to better decisions by the users of the model output.

4.4.4.7 Full Critical Security Control Use

The last recommended expansion is the full inclusion of all 20 Critical Security Controls. This will enable organizations that have not yet implemented certain controls to estimate the cost and effectiveness of these controls before effort is spent on them in a real environment.

4.5 Summary

This chapter presented a unique modeling approach for choosing certain courses of action relating to critical security controls. The model, implemented using AnyLogic® Multimethod Simulation Software, provides the means to estimate the effectiveness and costs of certain CSC implementation strategies. It allows for the user to build these defensive strategies and utilize the resulting data from numerous simulation runs. It is possible to expand the model beyond the current baseline to be more granular and valid for the needs of specific organizations. The output from this model was used, in part, to deduce the following conclusions and recommendations.

CHAPTER 5. PRESENTATION OF DATA, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

In today's highly connected and data-driven world where information is a key asset to organizations, the threats to the confidentiality, integrity and availability of such information is enormous. Recent, highly visible attacks on various businesses and government agencies have highlighted to more than just security experts the threats that organizations face in protecting information (Krebs, 2014a; Krebs, 2014d; Mandiant, 2013). Information security issues, and the results of attacks and breaches, are increasingly being published in main-stream media outlets, for better or for worse (Collins, 2015; Dawson, 2015). Certainly, these publications are resulting in an increased awareness of the effects of poor information security to the general population, contributing to more pressure on organizations to improve and optimize their overall security posture and manage the risks associated with information security more effectively. On top of monetary, trade secret and intellectual property loss, organizations are subject to loss of customer trust and prestige. Further, the positions and livelihoods of senior executives are increasingly at stake.

Looking at the current state of information security, Symantec (2014) reports that total breaches were up in 2013 by 63% from 2012, a trend which is likely to continue. Cybercrime cost to the global economy ranged from $375 to $575 billion dollars

annually, with an average estimated loss of $2.7 million per cybercrime incident (PwC, 2014). Further the same author reports that larger organizations incur higher costs from security incidents. Threats from cyber espionage by government entities, terror groups, businesses, criminal gangs and other sources will continue to increase in frequency (McAfee, 2015). In this environment, organizations of all types and sizes need to plan for and implement new forms of protections and risk management practices in order to keep their valuable data as secure as possible.

This chapter will present means to improve security risk management for an organization by focusing on the projects within them. Specifically, on the project managers and their efforts to provide better security of their assets during the project life cycle and therefore improve the safety of the product.

The idea that all levels of management in an organization are responsible for information security is not new or novel. However, the author has not found many concrete sources in literature that specifically define or articulate this idea. Certainly, there are organizations that permeate a strong security culture throughout all levels of the enterprise, though as we will see below, it is often through an informal process based chiefly on the expertise and knowledge of current leadership within the organizational structure. Also, given the author's bias and experience in military matters, he strongly believes in the concept of mission tactics where the lowest level subordinate is allowed freedom of command in order to accomplish a mission. The higher levels of leadership will support in the endeavor, yet not dictate the exact means of achieving mission success. This equates in better results given the fact that the lowest level of leadership knows its environment and needs best, and can act on them more effectively and

efficiently. This also breeds a sense of trust and loyalty within these junior leaders, which is an important component in any successful organization.

This chapter is divided into three major components. One, the literary sources supporting the idea of formal project security management. Secondly, interviews of several professionals in the information security and project managements fields. Lastly, results from the running of the agent-based model discussed in the previous chapter demonstrating the effects of a defense in depth strategy involving organizational level and project level security management.

After the presentation of all data sources, conclusions and recommendations will be made. Analysis of the data provided will be made where needed within each separate section.

5.2 Presentation of Data

This section will present the information gathered from the three sources, which are literary, subject interviews and computerized model. The structure is intended to build an understanding in the reader of the overall concept this thesis paper presents, and what sources were consulted before any conclusions or recommendations are made. Given the qualitative nature of this research, the method of triangulation was used in order to deduce conclusions and recommendations. The intent behind the literary research in this chapter was to create a foundation in the understanding of the concept proposed in this paper and to present valid sources. The reasoning behind the subject interviews was to confirm or deny the sources in literature and build on them if similarities can be found. Finally, the intent behind building a foundational model was one, to back up the two

other sources for the establishment of conclusions and recommendations, and two, to create a model that can be built upon and used by organizations in the future to assist in determining cost and effectiveness of various security strategies involving project security management. Once this section is presented and an understanding is created in the reader's mind, the author will present his conclusions and recommendations on the topic discussed.

5.2.1 Literary Sources

5.2.1.1 Mission Tactics

In order to successfully move forward, the author must explain his reasoning for approaching the problem faced by organizations regarding information security in a particular way. Having a military background, the author has a certain bias towards how successful organizations operate. His experience has taught him that placing trust and responsibility in subordinates, while properly supervising them, is an approach that will most often lead to successful outcomes. This approach in the realm of war is not unique to one present military force, though it is well defined by one service, the United States Marine Corps, as mission tactics. It is central to putting their doctrine of maneuver warfare into practice (Department of the Navy, 1997). The author states that "Mission tactics is … the tactics of assigning a subordinate mission without specifying how the mission must be accomplished" (Department of the Navy, 1997, p. 87), and also that "We leave the manner of accomplishing the mission to the subordinate, thereby allowing the freedom - and establishing the duty - for the subordinate to take whatever steps deemed necessary based on the situation." (p. 87). This form of practicing war on the tactical and

operational levels has been proven successful over many decades and continues to yield positive results for the service in accomplishing missions assigned.

From this perspective, the author approaches the problems faced in today's interconnected world with all of the threats to information technology (IT) systems and the information contained and used within them. Looking at the various management levels within organizations of all types and sizes, and seeing a need to think differently about the issue, the author took steps to research literature that would illuminate his suggestions and experiences. To be certain, there is and never will be a one to one mapping of a military organization with a civilian one. However, the researcher believes that there are enough similarities, and that in most cases at least some of the ideas can transfer. This is mainly because, both war and information security are and will remain innately human affairs no matter how advanced technology becomes. The reason war exists is because of human nature, and the reason we build IT products and services is because of human need. Human factors like skill, morale and leadership must be taken into consideration in both arenas and not just the technology associated with both.

5.2.1.2 Managing Security Risk on Projects

For project managers, assessing and then managing risks to projects is an important task that runs throughout its life cycle. Managing risks to budget, logistics, personnel and other areas of the project are critical to success. Within the overall structure of risk management are also security related risks to consider. These might be physical in nature, such as the risk of theft of documents, or relating to information stored and transferred digitally. Unfortunately, the formal management of security risks during

the project life cycle does not appear well established or much acknowledged in literature or common knowledge. For example, the 5th edition of the project management institute's PMBOK (Project Management Institute, 2013), does not mention security in relation to managing risks in projects. Although it does speak of security of communications, which is a risk to consider, this is not involved enough to satisfy. Further, few documents exist that speak of managing security risks during the project life cycle, and in particular relating to information security. One can make the safe assessment that many project managers do manage security risks, and in particular those effecting information, though there does not appear to be a common understanding of the importance or benefits of it. This chapter will look at some of the literature researched that starts to set the path towards thinking about managing information security risks on projects.

Pruitt (2013) articulates the concept of managing project risks related to information security within the context of implementing the 20 critical security controls published by the council on cyber security (Council on Cyber Security, n.d.). The author suggests ways for project managers to properly manage information security risks using the controls presented, by integrating security into the project management methodology (Pruitt, 2013). Instead of making security an afterthought on a project, which unfortunately occurs all too often, properly integrating security considerations early on will avoid cost, scope and time issues on projects. Also, building in security checkpoints (or milestones) "during several key processes will ensure progress toward desired security" (Pruitt, 2013, p. 4). The author clearly puts the focus and the responsibility on the project managers to provide better security during the project life cycle and upon

product delivery. It is interesting to note that the author also addresses the differences between larger and smaller organizations. Pruitt (2013) determines that larger organizations might already have certain security stage gates that are required to pass on to the next phase in projects, but that smaller ones might have to assign a reviewer to affect the same. This is an important point for the overall thoughts of this research. The question of the lowest level manager taking responsibility for managing risks is given worth by acknowledging the needs smaller organizations have in this regard. If project managers increase their efforts to manage information security risks, using the 20 security controls or any other framework, the need for higher level support by the organization decreases. This will lower the burden on the upper leadership and information security management professionals in an organization, allowing them to focus on more pressing matters. It will also contribute to the overall security posture of the organization by hardening the project and its resulting product against risks relating to information security.

Another point made by Pruitt (2013) is a relationship drawn between security and the cost of quality on a project. The cost of quality being appraisal costs and the failure costs, both internal and external. In terms of security, appraisal costs might include preventative measures such as implementing the critical security controls during the project life cycle. For failure costs Pruitt (2013) correctly states:

> The costs of failure include the costs to recover from a cyber-security incident like a data loss or theft. Those recovery costs would include external failure costs like loss of goodwill, lost sales, fines, liability costs, investigation of incidents and

> remediation as well as internal failure costs like wasted work, rework, and failed handoff to operations. (p. 6)

It would be safe to say that since the quality revolution in the 1980's and its application to software development and the IT industry, managing quality within projects is well established. Quality management methodologies like CMMI and Six Sigma are known to be effective at improving the quality of delivered products. The axiom "Quality is Free" coined by Philip Crosby is well understood and claimed true by many. It is also understood that project managers have a direct and important role in managing the quality of the products their projects produce. So the question remains, why not the same formal processes and methodologies as well as general acceptance of the concept for managing security, specifically information security? Could the term "Security is Free" be valid now or in the future? Perhaps it is the difficulty of quantifying information security, whereas better and more quantitative metrics exists for measuring the quality of a product and process.

Progress however has been made in establishing security related metrics. For example, the Center for Internet Security (2010) has produced a set of metrics specific to security. These metrics are defined in several categories such as management, operational and technical metrics. Metrics like "Mean Cost of Incidents" or "Percentage of Configuration Compliance" are valuable for the management while "Number of Incidents" and "Number of Applications" are more of a technical nature. Also, the critical security controls mentioned above are heavy on validating implementation. Metrics that can be used to measure successful information security management. The point to make is that general accepted metrics exist that can be collected in order to measure the

effectiveness of managing information security within organizations and their subordinate projects. Similar to measuring quality metrics within a project, the project manager can apply these or metrics to measuring the effects of his or her project security management. Of course, the project is not an island and as with many other things within an organization, the backing of corporate leadership is critical. Given the increase of threats and attacks worldwide and the resulting breaches mentioned above, it would be in the best interest of the highest level of leadership to engage in these security related efforts just like their predecessors did during the quality revolution and beyond.

Security management cuts across all process groups within a project. It is important during initiation, planning, execution, closing and of course controlling (Emory, 2003). This author talks about a Security Management Plan (SMP). If security risks are not considered on projects the results can effect scope, time, cost and quality. This plan can be viewed as falling under the overall risk management plan and brings together all security related aspects relevant to the project, including any organizational security requirements. Given the amount of information a project might produce, depending on type and size, it stands to reason that the location where this information is created is the first and best line of defense. If a project manager and his or her team conducts a robust security risk assessment and has put the proper controls into place, while managing them throughout the project life cycle, the assets of the project and its resulting product must be more secure than without these efforts.

Another point to be made for the adoption of more robust information security management on projects is the variability and uniqueness inherent in organizations. Choobineh et al. (2007) state that “organizations are as unique as human beings are” and

that “organizations are organic, dynamic entities that change over time” (p. 963). These are most true statements and it’s worth considering the impact these facts have on information security for an organization. Information security management (ISM) is harder to properly conduct within an organization when the security professionals are separated from the business-related segments. Inevitably, the chief information security officer (CISO) and his or her subordinates must find ways to effect the overall security posture of the organization while keeping in mind not to restrict the business itself. Security professionals must be enablers to the business, not disablers for the sake of security. This is where the management of security risks by project managers can assist in dealing with the dynamism inherent in any organization while assisting the CISO with increasing the security posture. Project managers and their teams create innovation, and are at the cutting edge for most companies, driving them forward to success. When the project managers conduct the management of their own information security risks, within the overall organizational framework, all of the information and innovation produced by the projects is secured at inception. Further, Choobineh et al. (2007) correctly state that “the best policies, procedures, and practices will have little or no value if they are not followed” (p. 963). Security professionals often have a difficult time ensuring that everyone in the organization follows established policies and practices. Even some security minded individuals are often lax with certain practices. Khansa et al. (2009) make the case that human errors in the form of slips and mistakes are a significant part of security breaches. Slips, being defined at “execution failures”, relate best to the above mentioned failure to follow proper policies, practices and procedures. A way to increase the chance that employees perform these guidelines appropriately is through proper

supervision or management. This can be accomplished best through the lowest level of leadership, namely through project managers. If project managers consider the security risks in human factors and plan towards them while managing them during the project life cycle, they are able to better effect the security posture of their project, product and the organization as a whole. A well-managed project information security plan will contribute to the organizational security posture managed by the CISO and his or her staff. In an organization that is smaller and that does not have the resources for an information security management staff, this concept becomes even more critical. With these smaller organizations, the need to manage security risks by the project managers becomes even higher since they will not have the benefit of the expertise of the security professionals. A formal process to manage these risks must be utilized in order to properly assess and manage the risks.

In order to summarize these thoughts, the author would like to point out another valuable statement by Pruitt (2013):

> PMs are not expected to be security experts, but by including security considerations in every phase and process of a project, especially in initiating and planning, communications and deliverables, PMs have the opportunity to deliver more secure systems in a more secure manner. (p. 18)

The above summarizes the potential benefits and organization will reap through emphasizing the management of information security risk in projects. Ultimately, the purpose of conducting projects is to produce something of value to the organization. Having this done in a secure manner will only benefit the organization by yielding a more secure product while keeping information secure during the project life cycle.

One aspect not mentioned in this section are the costs associated to the project with increased emphasis on security management. This item will be discussed in more detail in the following sections. It will become clear to the reader that costs will increase and project budgets might swell, though the benefits will outweigh the added costs.

5.2.2 Subject Interviews

The researcher conducted interviews via email correspondence with several professionals in the project management and security fields. Every individuals interviewed is employed in information technology (IT), serving organizations that develop and manage state-of-the-art IT solutions. The purpose of these interviews was to discover parallels to the literary sources and to either confirm or deny the validity of managing information security risks at the project level. Also, the intent was to provide input on the costs and effectiveness of having project managers involved in information security management within their projects.

All subject information and the questions asked of them are listen in chapter three above.

5.2.2.1 Security Management is Risk Management

One of the first questions asked of the subjects is if they considered information security management on projects as risk management. The author wanted to establish a clear baseline in thought for this paper in order to move forward in exploring the topic deeper. The answers given were unanimous. Every respondent considered information security risks as falling under risk management. When security issues are properly managed, the overall risk level for a project decreases. Subject D stated: “If I can mitigate

the information security risk, then my overall risk profile decreases." a simple and direct way of stating a widely accepted belief in regards to security risk management. Clearly, in any framework that manages information security at any level of management within an organization, it should be considered as risk management and fall under the risk management plan.

5.2.2.2 Security Management and Quality Management

One of the most important facets of the concept of actively managing security on projects is its potential parallels with quality management. As mentioned above in literature, there are advocates of this idea. It is not hard to see the similarities of quality management on projects, in order to produce a better product and reduce time and costs, with the management of information security. Many advocates of quality management in the past and present have made statements indicating that quality is everyone's responsibility. It is not just left up to executive leadership to advocate quality processes and project managers to follow them. Each employee within the organization and in particular on projects that create innovation have a role to play in ensuring the quality process produces a quality product. The same can be said in regards to security. As Subject A states "Everyone is responsible for security".

The parallels with the early quality movement in IT are also evident in the participants' answers. In the past, many developers and their managers on projects rejected any quality processes as "red tape" or extra work with no benefit to the employee or product. These thoughts have been disproved over time and most professionals understand the value that a well planned and executed quality management plan brings to

the project team and the resulting product. In regards to security management, there seems to be similar concerns at this point in time with the understanding of how information security management can help a project. Subject B claims that security mandates can be viewed by the project managers, and his or her staff, as red tape and that the importance of information security varies with project managers. The participant also suggests that collecting metrics that demonstrate the cost of loss of work or intellectual property due to security incidents will assist in convincing project managers and employees of the value of proper security management. As one can see, the similarities with the early quality movement are clear. Today's quality metrics are extensive and demonstrate clearly the advantage of managing quality throughout the project life cycle. Subject B also points out that a bottom-up approach in regards to introducing information security management on projects would be a wise direction to take. Again, as was with quality movement, simple directives by senior executives will not suffice. Buy-in by all members of the organization must occur. Subject D states that if developers were looking at their code with a mindset focused on current security vulnerabilities, their code would be safer. Also that most developers rely too much on the "outer castle" and rely too heavily on someone else to keep their work secure. This is a clear parallel in mindset to what project members, including managers, had before proper and effective quality processes were introduced. They relied too heavily on acceptance testing or other methods of testing after code was produced, instead of thinking quality while developing. So, if these developers can think quality during the development process, then they can think security also. It is up to the manager of the project to introduce effective security management processes during development to ensure the team can execute them

effectively. This might include certain tools and technology that automate periodic testing, as subject D also states. This is however not an absolute solution and at the very least will increase the instances of failed security testing, forcing developers to redo work, and at the very worst letting critical vulnerabilities slip though the tests which lead to security breaches once the product is delivered. A more effective way is to introduce information security management at the project level in order to increase the security posture of the organization and enhance the security of the final product, just like quality management and quality processes have contributed to better quality products over time.

5.2.2.3 Project Managers Improve the Security Posture of Organizations

One of the core elements of support for the question of project managers practicing information security risk management is if by doing so, do they and their teams increase the overall security posture of the organization. The security posture of an organization can be measured by the collective implementation of technology, human factors and policies, practices and procedures in regards to security. Technology such as anti-malware certainly increases this posture and so does a policy that directs administrators to update the virus definitions regularly. Human factors such as security awareness can be improved by training and experience. All of these contribute to the organization by raising the overall security level. Most of these efforts today are focused on the organization as a whole, usually managed by the CISO or another security-related professional. Projects and their managers are of course part of the organization and one would presume that they would benefit from the organizational level initiatives. The question before us is, would a project manager with increased focus on security as

described above add more value towards the security of the organization as a whole? This is an important question, in particular to executives seeking to maximize their expenditures towards information security measures.

According to the results of the questions, all subjects agree that project managers add to the security posture of the organization. Several subjects of course mention the balance between cost and security, which will be discussed in more detail below. The important part to note is that all subjects seem to understand the importance project managers play in any organization. Subject F states “I see Project Managers as the face of the Project”, correctly stating the importance of this individual to the project perception and outcome. So it is valid to think of the project manager as the lynchpin of the project. They must consider many things during the life cycle such as risk, quality and communications management, therefore he or she would be the best person to consider managing the information security aspect of a project. Another person interviewed commented in regards to certain units within an organization that “a robust cybersecurity program with highly engineered systems will likely have a reduced active threat count … compared to a less advanced engineered program”. If one considers a project a unit of sorts, then this statement hold true. Far from red tape, implementing and managing a robust security risk management plan would result in an increased security posture for the entire organization, and ensure the safety of project assets while producing a safer product.

5.2.2.4 Costs of Security and Return on Investment

In this last section on information gathered by relevant subjects, the author will discuss the comments made in regards to costs of implementing any security measure or security risk management framework.

Nothing is free and certainly security comes at a cost. Security risk management, as with any risk management, can only be justified if it returns something of value to the organization or its expenditure is balanced with the risk appetite of the organization. The problem has always been measuring the return on investment (ROI). As Subject E points out, some investments in security, and its management, is due to government mandates and considered a cost in that context. There is no direct return on investment as with other expenditures. However, some commercial companies protecting trade secrets or intellectual property could consider ROI, though this is still very difficult to measure. As mentioned above, the cost of security is no longer simply monetary or loss of trade secrets or intellectual property. Prestige, customer loyalty and reputation is also increasingly at stake for organizations. These intangibles are of course not easy to measure, however it is clear that they are important to some organizations. One subject mentioned that piece of mind is important in regards to knowing that organizational assets are protected, which is certainly a unique form of ROI.

Currently, very little tracking of direct expenditures on security is conducted in any of the subjects' organizations'. It would be hard to determine a direct dollar amount. Subject E stated that a previous employer spent 35-45% of their budget on security, though this was heavily dependent on the type of organization and the information to be protected. Just as with measuring certain security related metrics, expenditures that relate

directly to security activity must be taken if leaders want to gain insight into the cost of these actions. There are some expenditures which are easy to measure. Subject C notes that they contract outside security experts for regular audits on their developed software in order to detect vulnerabilities. This is an approach many organizations take and as far as projects, something that might fit well into a security management plan to reduce the likelihood and impact of security incidents. Though the author found a figure in literature regarding security expenditure of total IT budgets, which was 10-15% (Everett, 2010), this specific number was not conveyed by the subjects. This is due to the above mentioned issues with keeping track of security expenditures, and the variable types of the organizations the subjects are employed by. Given the knowledge gained from the subjects, it is therefore hard to accept numbers such as 10-15% referenced through literature. If organizations want to estimate the costs of project security management in more detail, better metrics must be gathered in order to do so.

5.2.3 Model Data

This section will present the model data and its effect on the following conclusions and recommendations. The detailed output of all model runs can be found in Appendix B.

5.2.3.1 Model Output

A total of seven runs with different COA's was conducted. The cost for each control was set at 2 percent of project budget and the effectiveness at 95 percent. These values are simply an estimate of cost and effectiveness and not related to any specific data gathered in research. They are figures produced by the researchers through general

analysis and thought process, and represent enough accuracy to be valid for the purpose of this chapter. Each run was set at 1000 seconds simulation time with a total of 10 runs per input data. All runs for each data set were averaged to produce results. Again, all of the simulation input data is selectable by the user to more accurately reflect the specific situation. The following summary output was produced:

Project Defenses - Number of CSCs	Total Attacks	Organizational Attacks	Successful Organizational Attacks	Organizational Defenses	Project Attacks	Successful Project Attacks	Project Defenses	Total Cost of CSCs to Project (% of budget)
None	1049	1000	49	951	49	49	0	0
One	1049	1000	49	951	49	41	8	2
Two	1047	1000	47	953	47	29	18	4
Three	1046	1000	46	954	46	20	27	6
Four	1051	1000	51	949	51	12	39	8
Five	1051	1000	51	949	51	2	49	10
Five with CSC 18	1021	1000	21	979	21	1	20	12

Figure 5.1 – Summary Model Output

As the reader can see, the data presents the total number of attacks by a threat agent within the runtime period, the total organizational and project attacks as well as how many were successful or not. This data is meant to demonstrate the defense in depth concept and how and increased emphasis on security by project managers can result in fewer breaches at a particular cost. As the number of CSC uses by the project staff increase, fewer attacks against the project are successful. This is demonstrated by the Successful Project Attacks column. The last row is a special case with the use of CSC 18: Incident Response and Management. The model simulates the improvement of security measures if a breach occurs, given that proper management of an incident results in learning that increases overall effectiveness of security staff.

Though this model is basic in its design and implementation it is valid in providing insight into how managing information security in projects can result in fewer security incidents. This is done via a simple defense in depth strategy. Of course, in a real environment there are many more variables to consider. This model has the potential to be expanded in many different and interesting ways to provide a more granular representation of the real world, as discussed in chapter four. This AnyLogic® model serves its purpose in the context of this research, though it is the hope of the author that the model will be expanded in meaningful way to assist organizations in their security risk management planning.

5.3 Conclusions

Given the information presented above, conclusions can be made regarding the validity of the concept of information security management on projects, as well as its potential effectiveness and cost.

The data presented from three sources point towards certain conclusions in favor of the proposed method, however there are still unknowns that need to be considered. To a degree, analysis of the information has occurred within the above sections, though a more detailed look at the data and the resulting conclusions will be made currently.

The doctrine of mission tactics and its application in war lends itself to the overall concept of pushing responsibility of leadership to the lowest possible level. Within the context of project managers and information security management this is no different. The reason for allowing such freedom of decision-making for junior leaders in war is not just communications problems on the battlefield. It is also the fact that these leaders

know the environment they operate in best, and when individuals are given responsibility and trust they tend to excel. When project managers are given the freedom to adopt information security management strategies of their own, tailored to their environment, better solutions to these problems result. Advantages of this kind of freedom in decision making leads to increased innovation in civilian enterprises, just as it results in unique solutions to problems in war.

Knowing the environment the project operates in is not the only advantage of pushing responsibility of leadership to the lowest level. Human factors are a critical part of information security organization-wide, and some argue the most vital factor. Most experienced project managers will attest that people are the most important asset to a project. Through them it either succeeds or fails. Empowering the project managers to create his or her own information security management strategy will leverage the knowledge gained by this individual of the project staff. Organizational security staff cannot know the expertise, talents and temperaments of each member on a project. Project managers should be knowledgeable in this area for many different reasons. The understanding he or she has of the project staff will allow for a better information security plan, adding to or surpassing any organizational level plan. Analyzing the responses from subjects the author believes that the majority of professionals agree with the belief that more involvement of project managers in security management is a net positive for the security posture of the organization and the project. Also that, in most cases, they will better be able to manage specific security strategies than the overall organization. The fact that project managers are not security experts is understood,

though they can contribute to this area just as they contribute to other knowledge areas of the project.

The similarities between project quality management and security management are undeniable and the data presented above make this clear. Information security management appears to be in a stage of development that quality management was in years ago. Professionals understand the worth of managing security organization-wide though there is resistance to its formal or detailed management in every segment of the entity. This resistance is slowly fading with every breach reported in the media and suffered in silence by many organizations. Just as project managers slowly adapted quality management processes, it is evident that they are increasingly adapting various forms of security management for their project. As literature and subject interviews pointed out, many project managers agree that more emphasis on information security on projects will add to the security posture of an organization, keep assets more secure and produce a safer product. If this was conducted in a defense-in-depth strategy it can yield positive results, as the computerized model suggests.

Although the effectiveness and potential benefits of information security management on projects has been well articulated, a critical piece in these conclusions to consider are the costs. As described above it was extremely difficult for the author to find exact, or even general costs of any implementation. The variables are far too numerous and a detailed analysis is out of the scope of this paper. However, if a particular organization were to explore the concept presented here with propriety budget information, accurate information could be gathered. To accomplish this, the environment needs to be analyzed, metrics need to be gathered and other factors such as

organizational risk appetite need to be considered. Once these tasks are complete, more accurate costs of project security management can be found and conclusions made on them specific to the organization.

The author can conclude that project managers should implement a formal information security management plan within the overall risk management plan. The benefits of such actions are more secure project assets and a more secure product. Recommendations on ways to implement such a plan are discussed in the next section.

5.4 Recommendations

The intent of this research was to determine if more attention should be paid by project managers in managing their information security risks on projects, and if these efforts might lead to more secure project assets and resulting products. Based on the sources of data and its analysis the author believes there is ample evidence that such methods should be pursued, and that project managers should be more involved in project security management.

It is recommended that project managers consider their information security risks in a formal process aided by the organizational assets. This might include security experts, other more experiences project managers, or members of the project team. They would be well served to manage these special risks with similar processes as quality controls, gathering metrics and making decision based upon the data. Project managers should interface with whatever organizational resources available and consider the security risk management framework the organization is using. If no set processes or frameworks are in use organization wide, and no support given, the author recommends

project managers familiarize themselves with information security control standards. Publications such as ISO/IEC 27002, NIST SP800-53, or the 20 critical security controls can give keen insight into what the project might require. These controls of course are subject to a risk assessment and analysis, and when used form part of the overall information security management plan. As mentioned above, the exact costs of such a plan is hard to determine and very dependent on the size, type and structure of the organization. Project managers must be cautious to balance the costs with the benefit of added security. In order to do this, proper metrics must be gathered and it will take certain time to accomplish this. It is recommended that the most critical controls be implemented first on the project and metrics tracked, including any added cost of managing them.

5.5 Future Research

This section will discuss possible future research that can be conducted on the topic of information security management on projects.

5.5.1 Quantitative Research

As discussed above, if proper security metrics were gathered, certain hypothesis regarding project security management could be tested. The research in this paper can be the qualitative foundation for such future endeavors. The author hopes that a future researcher will have the ability to gather such quantitative data and produce results that either support or deny the results from this particular research paper. Looking back at how quality management evolved can give us answers as to how to properly commit to this course of action. Once enough specific data existed, gathered from quality metrics, it

was shown that actively managing quality on a project was of value to an organization. The author believes, based on the information provided in this paper, that this will also hold true for security management.

5.5.2 Security Management Plan Framework

Future research should be conducted which suggests a project specific information security management plan. The author has not found any definite methods or useable frameworks that accomplish this. Of course, there are many organizations that have created ways in-house to deal with these and similar security issues, however a broader and more comprehensive framework that can withstand the scrutiny of professionals and academics would further this topic. Developing a practical framework for project managers to use in order to secure their projects would be of value, by suggesting ways to properly manage information security risks. This plan can include many different topics such as what security controls to use, or what processes are going to be in place to assist in security related management.

5.5.3 Security Process Improvement

There is a possibility to conduct research into security processes for projects, similar to quality management processes and process improvement. Future researchers can look into the viability of developing these processes and systems and how they might benefit the security posture of a project and the organization. If these security management process improvement methodologies are seen to be of benefit, similar to how quality processes have proven valuable, then researchers could suggest how to implement the security processes.

5.5.4 Computerized Modeling

One path to take for future research would be the expansion of the base model presented in this paper. The potential to create a proper tool that is able to accurately estimate the effectiveness and costs of an information security strategy implemented on a project is immense. If this model were expanded to reflect an organizations' true size, structure and type it would be a valuable asset in predicting future security strategies. Project managers could use this tool during initiation and planning phases to help in determining what the information security management plan consists of. They can predict which controls are the most effective for their specific environment and what their implementation would cost in time and budget. This lets them adapt their security strategy to the risk appetite of the organization with more accuracy. An accurate and detailed tool like this will support decision making in regards to security on projects and perhaps organization-wide.

LIST OF REFERENCES

LIST OF REFERENCES

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams – Challenges in supporting the organisational security function. *Computers & Security*, *31*(5), 643–652. http://doi.org/10.1016/j.cose.2012.04.001

Bedi, P., Gandotra, V., & Singhal, A. (2009). *Threat Mitigation, Monitoring and Management Plan - A New Approach in Risk Management* (pp. 719–723). Presented at the 2009 International Conference on Advances in Recent Technologies in Communication and Computing, IEEE. doi:10.1109/ARTCom.2009.38

Behara, R., Derrick, C., & Hu, Q. (2006). *A Process Approach to Information Security: Lessons from Quality Management.* Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1717&context=amcis2006

Bree, K. (2014). *iCloud celeb photo hack could be a disaster for Apple: Expert.* Retrieved September 22, 2014, from http://www.cnbc.com/id/101964319

Brewer, J. L., & Dittman, K. C. (2013). *Methods of IT Project Management* (Second Edition.). West Lafayette, IN: Purdue University Press.

Brocklehurst, K. (2014). 2014 IT Security Budget Forecast Roundup for CIOs and CISOs/CSOs. Retrieved from https://www.akat-t.com/wp-content/uploads/2014/01/IT-Security-Budget-Forecast-Roundup-2014-for-CIOs-and-CSO-CISOs.pdf

Cazemier, J. A., Overbeek, P. L., & Peters, L. M. (2000). *Security Management (IT Infrastructure Library Series).* UK: Stationary Office.

Center for Internet Security. (2010). The CIS Security Metrics. Retrieved from https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of information security: Challenges and research directions. *Communications of the Association for Information Systems, 20*(1), 57.

Church, M., Nemati, H. R. (2009). A Human Centered Framework for Information Security Management: A Healthcare Perspective. *AMCIS 2009 Proceedings*, 591.

Ciarallo, F. W., Heath, B. L., & Hill, R. R. (2013). An agent-based modeling approach to analyze the impact of warehouse congestion on cost and performance. *The International Journal of Advanced Manufacturing Technology, 67*(1-4), 563–574. http://doi.org/10.1007/s00170-012-4505-5

Collins, K. (2015). A Quick Guide to the Worst Corporate Hack Attacks - Business, Financial & Economic News, Stock Quotes. Retrieved March 12, 2015, from http://www.bloomberg.com/graphics/2014-data-breaches/

Corriss, L. (2010). Information security governance: Integrating security into the organizational culture. In *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies* (pp. 35–41). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1920326

Council on Cyber Security. (n.d.). *The critical security controls for effective cyber defense (version 5.0)*. Retrieved from http://www.councloncybersecurity.org/critical-controls

Dawson, F. (2015). What The Sony Hack Can Teach About Cyber Security. Retrieved March 12, 2015, from http://www.forbes.com/sites/freddiedawson/2015/02/27/what-the-sony-hack-can-teach-about-cyber-security/

Department of the Army (2012). *ADP5-0: The Operations Process*. Washington DC: Headquarters, Department of the Army.

Department of the Navy. (1997). *Warfighting*. Washington DC: Headquarters, Department of the Navy.

Dietz, J. E., Kirby, A., & Wojtalewicz, C. (2012). Modeling of a Regional HubReception Center to improve the speed of an urban area evacuation. *2012IEEE Conference on Technologies for Homeland Security*, (pp. 476-482). doi: 10.1109/THS.2012.6459895

Emory, D. (2003). The Need for Secure Project Management - SC Magazine. Retrieved October 6, 2014, from http://www.scmagazine.com/the-need-for-secure-project-management/article/30225

Everett, C. (2010). Information security initiatives: counting the cost. *Computer Fraud & Security*, *2010*(1), 6–7.

Forrester Research, Inc. (2013*). Surviving the technical security skills crisis: An assessment of the current security skills landscape and how to overcome it.* Cambridge, MA: Forrester.

Gartner. (2013). Gartner IT Key Metrics Data - 2013 IT ENTERPRISE SUMMARY REPORT.

Gilbert, N. (2008). *Agent-based models*. Sage. Retrieved from http://books.google.com/books?hl=en&lr=&id=Z3cp0ZBK9UsC&oi=fnd&pg=PR9&dq=%22and+theoretical+issues+and+explaining+what+%E2%80%98%E2%80%98agents%E2%80%99%E2%80%99+are.%22+%22of+resources+useful+to+agent-based+modelers+on+the+Web+and+in%22+%22or+another+type+of+space.+It+allows+modelers+to%22+&ots=T4GFAEnVnW&sig=aLpDdYn0B5ZUPV_5596Rh2SavHA

Gupta, M. P., Kranz, J., Ojha, A., Picot, A., & Singh, A. N. (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. *Global Journal of Flexible Systems Management*, *14*(4), 225–239. doi:10.1007/s40171-013-0047-4

ISACA (2014). COBIT 5: *A Business Framework for the Governance and Management of Enterprise IT*. Retrieved November 11, 2014, from http://www.isaca.org/cobit/pages/default.aspx?cid=1003566&appeal=pr

ISO/IEC. (2014). International Standard ISO/IEC 27000. Retrieved from http://standards.iso.org/ittf/licence.html

IT Governance Institute. (2006). *Information security governance guidance for boards of directors and executive management*. Rolling Meadows, Ill.: IT Governance Institute. Retrieved from http://www.books24x7.com/marc.asp?bookid=30815

Jahner, S., & Krcmar, H. (2005). *Beyond technical aspects of information security: Risk culture as a success factor for IT risk management*. Retrieved from http://aisel.aisnet.org/amcis2005/462

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129.

Khansa, L., Liginlal, D., & Sim, I. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, *28*(3-4), 215–228. doi:10.1016/j.cose.2008.11.003

King, G. (2000). Best security practices: An overview. In *Proceedings of the 23rd National Information Systems Security Conference, Baltimore, Maryland, NIST*. Retrieved from http://webpage.pace.edu/sp68870w/Security/022.pdf

Krebs (2014a). *Home Depot: 56M cards impacted, malware contained — Krebs on security.* Retrieved September 22, 2014, from http://krebsonsecurity.com/2014/09/home-depot-56m-cards-impacted-malware-contained

Krebs (2014b*). In Home Depot breach, investigation focuses on self-checkout lanes — Krebs on security.* Retrieved September 22, 2014, from http://krebsonsecurity.com/2014/09/in-home-depot-breach-investigation-focuses-on-self-checkout-lanes

Krebs (2014c). *Hackers plundered Israeli defense firms that built "Iron Dome" missile defense system — Krebs on security.* Retrieved September 22, 2014, from http://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system

Krebs (2014d). *Sony Breach May Have Exposed Employee Healthcare, Salary Data — Krebs on Security.* Retrieved February 22, 2015, from http://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/

Kunas, M. (2012). *Implementing service quality based on ISO/IEC 20000: A management guide.* IT Governanve Ltd. Retrieved from http://standards.iso.org/ittf/licence.html

Managed Security Service Provider (MSSP) - Gartner IT Glossary (2013). Retrieved September 23, 2014, from http://www.gartner.com/it-glossary/mssp-managed-security-service-provider

Mandiant (2013). *Exposing one of China's cyber espionage units. Mandiant.com.* Retrieved September 22, 2014,from http://intelreport.mandiant.com

McAfee. (2014). *McAfee Labs Threats Report.* Retrieved from http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2014.pdf

McCumber, J. (2005). *Assessing and Managing Security Risk in IT Systems*. Boca Raton, FL: CRC Press LLC.

NIST. (2005). NIST Special Publication 800-65. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf

Palgrave Connect (Online service), & Taylor, S. (2014). *Agent-based modeling and simulation*. Retrieved from http://public.eblib.com/choice/publicfullrecord.aspx?p=1779948

Poore, R. S. (1996). *Generally Accepted System Security Principles*. Taylor & Francis. Retrieved from http://www.tandfonline.com/doi/pdf/10.1201/1086/43306.8.3.19990901/31073.6

Project Management Institute. (2013). *A guide to the Project Management Body of Knowledge (PMBOK guide), fifth edition*. Newtown Square, Pa.: Project Management Institute.

Pruitt, M. (2013). *Security best practices for IT project managers.* The SANS Institute. Retrieved from http://www.sans.org/reading-room/whitepapers/bestprac/security-practices-project-managers-34257

Presidential Policy Directive / PPD-20 (2013). Retrieved from http://epic.org/privacy/cybersecurity/presidential-directives/presidential-policy-directive-20.pdf

PwC. (2014). Managing cyber risks in an interconnected world.

Symantec. (2014). *Internet Security Threat Report.* Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

SANS Institute (2001). *Intrusion Detection Systems: Definition, Need and Challenges.* Retrieved from http://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-definition-challenges-343

Symantec. (2014). *Internet Security Threat Report.* Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Trustwave. (2014). 2014 TRUSTWAVE GLOBAL SECURITY REPORT. Retrieved from https://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf

Von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376. doi:10.1016/j.cose.2004.05.002

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, *24*(2), 99–104. doi:10.1016/j.cose.2005.02.002

Von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security*, *25*(3), 165–168. doi:10.1016/j.cose.2006.03.004

Von Solms, R., & von Solms, S. H. (Basie). (2006). Information security governance: Due care. *Computers & Security*, *25*(7), 494–497. doi:10.1016/j.cose.2006.08.013

Williams, P. (2001). Information security governance. *Information Security Technical Report*, *6*(3), 60–70.

APPENDICES

Appendix A Data Collection Emails

Robert,
See response below. Also, I have added <REDACTED> to this thread. I have provided her with some background so please feel free to reach out to her when you are ready.
-<REDACTED>

From: Robert [mailto:rbott@purdue.edu]
Sent: Friday, November 07, 2014 1:30 PM
To: <REDACTED>
Cc: <REDACTED>
Subject: RE: Project Security Management Thesis

<REDACTED>,

I have replied to your answers below.

Robert

From: <REDACTED>
Sent: Thursday, November 06, 2014 4:25 PM
To: 'Robert'
Cc: <REDACTED>
Subject: RE: Project Security Management Thesis

Robert,
See my response inline below…

<REDACTED>, CISSP, CRISC
CISO, Interim
<REDACTED>
Office <REDACTED>

From: Robert [mailto:rbott@purdue.edu]
Sent: Thursday, November 06, 2014 12:05 PM
To: <REDACTED>
Cc: <REDACTED>
Subject: Project Security Management Thesis

Sir,

I want to thank you again for your time this morning. The information you shared will help me with my thesis work. As discussed, below are some of the questions I had regarding security management. I understand that some of the information I am asking

about is confidential, so it is not a problem if you cannot give me specifics. If you could still enlighten me in general it can still help greatly. I am also looking forward to talking to <REDACTED> regarding project management and security.

Questions follow:

1. What level of funding and how much effort by employees is spent on security specifically, in particular management functions (percentage of funding for operations and on projects)? The answer to this depends on the scope of your question. From an IT organization perspective, we just started tracking effort spent on security tasks. However, out of the total IT budget on all campuses, my group has approximately 4% of that budget. With that said, the old saying goes "everyone is responsible for security" so, for example, server admins would be responsible for patching. There is spend there but I honestly don't know what that is.

- To narrow the question, this scenario will work. If you consider patching as part of your technological security solution (even if it is also to improve performance, add new features etc.), then one could say the server admins are spending time on security management, correct? Yes. Adding all the time they spend on performing security patching and other security related tasks, what percentage of their total work week does this add up to? This is a very rough guess, but I would suggest they spend about 2% of their time on average per week if you consider tracking the patches, implementing, etc. If you apply this to a project and let's say the PM identified a particular security risk coming from the specific servers they use, then the patching they do would be a part of project security management (in a minor way at least). I know it is difficult to come up with a solid number for cost, and measuring the effectiveness of risk management is always tricky, but anything close to reality would be helpful at this point. I hope I have explained it a little better. Perhaps when PM's perform project security management in the future they can account for costs by putting tasks related to security management on the WBS and then on the Gantt chart etc. giving a full account of effort spent on it. Some PM's actually do this as part of their projects, but <REDACTED> can give you more specifics.

2. How effective are your information and physical security management efforts and how do you measure them? My scope is related to information technology security. We have just started to track some metrics (operationally), but the security management program is based upon risk measurements. We have done qualitative risk assessments in the past (just for the WL campus) to help build our roadmaps out, but it's not as effective as I'd like. We will soon be looking at an overall risk management program to help better measure security risk. I would also add that Audit assists with this as well…they audit against what is in place to help us measure effective controls. From a physical perspective, I can't really answer because that is not necessarily within scope of what I've been tasked to do. In reality, we have a card office (not part of my organization) that deals with physical access controls, safety and security that deals with cameras, etc. but no

one (that I know of) is really charged with "physical security". We have looked at processes related to data center access, however.

- So I guess the question is do you and your group feel like the security risk management program is effective, if viewed through your professional lens? I would say that based upon what we know and the constraints that we have it is effective. If I compare where we were 10 years ago to today, we have made great strides, but there is always more to do. With both questions one and two I am trying to relate a number of monetary and/or time expenditure with another that demonstrates the level of effectiveness. If your networks were constantly being breached and information lost, you might say "x% dollars spent on security is not effective", or if you rarely have security issues you could say "x% dollars spent is good enough for our risk appetite". Anything helps, I can always put on my qualitative and biased researcher glasses for my thesis and explain what I did to the model in the paper. I also have literary sources that can yield some helpful insights. I hope I am making sense. So for physical, I can't really answer that. From an IT perspective, our risk appetite changes depending on leadership. I'm not as risk adverse as some other are in the security field. Ultimately we are trying to protect data while balancing the business needs. We do have some data controls/policies in place, but the verification of the controls is where we stumble. I would say that for now (until we have a well-developed risk process in place) our spend is good enough for our risk appetite.

3. Do you and your security staff focus consciously on technological security solutions, human factors and processes, procedures and practices when creating security plans and/or managing security? Yes, we typically look at technology, process, and people from a risk perspective.

You briefly discussed how you involve project managers in security this morning. If you had the time to elaborate on this process and perhaps how things might be done more effectively by involving project managers it would help. Assuming I made my case well enough regarding security management at the project level, how do you see this concept working for you and your organization, if at all? This is a very interesting topic. When I think of project managers and what they are tasked to do, one of the components is risk identification. However, I don't think we do a security risk identification assessment with the project managers we have in our organization. I think, from a risk perspective, they focus on lack of resources, funding, etc. I think you'll gain more insight with this one when I connect you with <REDACTED>.

- I am looking forward to talking to her regarding project management and security. <REDACTED> seems to be just the right person to talk to. Thank you again for taking the time to answer my questions.

Again, I understand the sensitive nature of these questions so I will not be upset if you cannot answer them fully or at all. I am hoping I can get some general pieces of information on top of the literature I found that will help me build a more complete valid

computerized model. I could be completely in left field with your questions, so please feel free to ask more. □

Thank you,

Robert

From: Robert [mailto:rbott@purdue.edu]
Sent: Tuesday, November 11, 2014 1:45 PM
To: '<REDACTED>'
Cc: <REDACTED>
Subject: Questions on Project Security Management

Ma'am,

My name is Robert Bott and I am a graduate student here at Purdue. As I'm sure <REDACTED> has already mentioned, I have a few questions regarding project management and security for you. My thesis is on the topic of project security management. Specifically, if project managers would add to the security posture of their organization by managing security under their risk management plans. I am looking into the validity of this concept through literary review, questioning professionals such as <REDACTED> and yourself, and building a computerized model. If you have some time I would appreciate whatever information you are willing to share with me in regards to this. I'm sure you have already seen the correspondence I had with <REDACTED> on this topic. I will try not to repeat anything, while also attempting to explaining what I am doing a little better.

Hopefully my research question for my thesis will help provide some initial understanding of what I am researching. The question follows:

"Given the increasing global threats to information technology (IT) infrastructure, should IT project managers prioritize security risk management within a comprehensive multi-tiered defense strategy? Would budgeting for security result in more secure project assets and products?"

My questions for you are the following:

1. In your opinion do you think project managers who manage security for their project above and beyond what the organization mandates (assuming vulnerabilities have been considered and a threat assessment made) add to the security posture of the organization? Do you have any examples from past or current projects where you have done this, or similar management?
   Absolutely these PMs add to the security posture of the organization. Maybe of the challenges could be solved by a conversation or an improved communication plan; the

challenge we face is not that PMs don't want to provide adequate planning towards security, but rather those are unknown / unknowns risks. If a project team has no involvement from a security minded person, then there's no way they know that protecting themselves is a key element.

- Could you see a scenario where the organization is security conscious and has set policies, practices and procedures that ensure PM's take care of unknown/unknowns by mandating involvement of security personnel? A mandate stating "you will spend X hours doing security related planning" for example. Either these security experts are part of the team, or you involve them through the communications plan in order to get their expertise as it relates to the specifics of the project. I would classify this is project security management (PSM), which would most likely fall under risk management. You identify security risks using the security SME and then apply your mitigation strategies. This should yield a far higher security posture at the project level and therefore make the organization stronger. At the very least it has the potential to produce team members that are more security conscience. As a professional PM, what do you think about this?

While I think the mandating of proper involvement comes with the best of intentions, I would picture that would lead to an broader perception of security involvement is red-tape. I think the grassroots or heightened awareness is a better route. Maybe it's something as simple as the PM asking is this important enough to protect – ok, let's bring in a resource to help protect it. Start bringing metrics together that show what is the cost of losing this work (whether intellectual property, re-work involved in breach) and get the project team to want to protect this project instead of mandating it with policies. Additionally, when you go more from the grass roots perspective, it becomes a much better collective knowledgebase with still a few "security experts" who are still beyond the collective norms.

2. As I understand it, in the environment you work in, you have multiple groups that deal with cyber/virtual security and physical security in various ways. Would it make sense to you as a project manager to combine both within your own project in order to mitigate most security risks and improve your security posture?

I would imagine that would help. I don't come from a strong security perspective, but now in my role I'm surrounded by it at work and also married to that. Because of this new knowledge of all these threats surrounding the work we do, I place a much bigger importance on it. I know that other PMs don't have it as the same level of importance as I now do, but that's only because they are unaware of these risks. Security is often an afterthought or something people need to work in later, or perceived as red-tape. If we were to work together and involve security from the beginning, I think that perception of difficulty could be overcome.

- This seems similar to how quality was viewed in the past (or in some cases still is). As an afterthought. For now it appears that the organization needs to provide the mandate, and the funding, to have PM's conduct more security management. Security

needs to be an integral part of project planning and execution. If a project has no need for an extensive security management plan, then so be it, however chances are that PM's will have to spend a few hours a week managing the security plan just like any other knowledge area. This leads back to what I have discovered in my research regarding information security governance (ISG). The idea that the CEO and the Board are just as responsible for, and concerned about information security as the guy or gal in the cubicle doing the day to day security work. It comes down to who is responsible. It seems in the past CISO's were not directly tied into the executive level at organizations (or didn't even exist), until bad things happened and governments started to regulate more. Do you have any input on this? Do you think security management is similar to where quality management was in the past? What is your perspective on the executive level in your organization as far as security is concerned?

I completely agree that it's like quality and the progress we've made with that (SixSigma). I think the public perception hasn't made information security (and to a much less degrees physical security) a valuable enough asset to get outraged towards it yet. The "bad things happening" haven't been a big deal enough that makes people realize that it's all our responsibilities yet. Example, we constantly hear where your data has once again been breached. We (as a society), doesn't really care about the follow-up of what's being done to stop this from happening, but rather just contact your bank or an identity protection service and put on the personal band-aid and continue on with life. PCI regulations are fairly new, and they are a very positive addition to mandating security practices into a diverse market. There certainly have been some industries that have successfully incorporated a security posture into their field (changes in airport security since 9/11/01), but with so much digital data being generated, many industries can't even fathom what could happen.

My perspective on executive level involvement with the security as a whole isn't too high, at least here at Purdue. At the moment, I think we are fairly immature with our risk & security management. The model you mention is a much more proactive stance than we have.

3. In general, do you consider security (cyber and physical) falling within the realm of risk management, or some other area of management (perhaps a separate and unique management knowledge area)?

I see security as part of risk management. While it's most commonly focused on standard items such as acceptable, scope, or resourcing, I think the loss of your intellectual property through other mechanisms other than losing a resource is just as much as a risk. I've never written this in a risk register, but one could conceive of a cyber-attack on the network infrastructure (since it's really just 3-5 locations around the world) that could bring many projects to a screeching halt.

- It seems that all professionals I've talked to agree with you that it is risk management. That is good information for me. Just to expand on this, what if you had some security management framework, including accepted standard templates, that you

could use to build a plan under risk management? You could add something to the risk register stating "see security management plan", and anyone could immediately reference the managed security risks based on your specific situation. I can imagine there will be some projects where the plan is quite minimal (in cases where the organization takes most of the security responsibility for example), and others that are very large and extensive. It all depends on the project scope etc. What do you think?

Certainly beneficial. I can picture it trying to establish what is needed to adequately incorporate security. What is trying to be secured? Similar to a risk register, what could be incorporated, cost of damage, long-term security maintenance…

4. Do you have any hard numbers on security expenditures, both in management and employee actions (money, effort), for projects you have managed in the past or are managing now? I am looking for some general percentage based numbers that will let me build a valid model (ex. 5% of budget spent directly on security measures, or 10 hours a week spent on security management tasks).
I don't have this type of information, very rarely do we quantify our expenses as security specific.

- Fair enough, this seems consistent with most people I talk to. If you do spend on security, how is security funded? Through operational expenses? Has there ever been a case where you had someone charge hours to security specific tasks on a contract or project, or employed someone exclusively for dealing with information security tasks? Would that even be necessary in your opinion? I do believe this would be a great metric to track at all levels of an organization.

Purdue IT finally started formalizing our Portfolio and it is a work in progress on improving how security tasks early on are charged back. Very often my team (the security experts) are involved in the very beginning of a project (reviewing contracts, cloud services security profiles) & closer to the end when it's closer to "go-live" (pen testing, vulnerability scanning…). We are now able to track our hours spent towards these other projects which aren't security focused at all. Down the road, once we mature the model a bit, it would be nice to look ahead and predict that certain IT resources will be involved at different times and plan for that. Right now, we're still closer to just getting a more realistic perspective of where time is going.

I appreciate your time and the opportunity to speak to you on this topic.

Thank You,

Robert

We have 5 or 6 people we "rescued" from startups, where they were being worked to death. They were attracted more by the security of a larger company willing to stand behind the project for more than 6 months, and we haven't really pressed people into overtime the way startups do. But we haven't offered any of them significant stock, so they probably wouldn't do it for very long if we tried to.

The interesting thing to me as that so many companies realize that their "normal" way of launching projects has low success rates, so they need to "break the mold" and do something different. I suspect a lot of this is also driven by the idea of potentially spinning off the project as another company, or selling it off. By separating it this way, it could continue to function with no huge staff shakeup.

On Mon, Mar 9, 2015 at 12:22 PM, Robert Bott <rbott@purdue.edu> wrote:

That is quite the complicated answer, but very good answer for me to use. I have been reading a lot about and talking to people about large companies treating new ideas just like startups, with the same processes and semi-separate from the rest of the organization. That seems to be the model that works for these times. I wonder if they also provide the employees who work on these internal startups the same stock options and opportunities to own a piece of the pie, just like real" startups. I can't think of anything that would motivate an individual to work hard for this kind of opportunity. Incentives matter …

From: <REDACTED> [mailto: <REDACTED>]
Sent: Monday, March 09, 2015 1:04 PM
To: Robert Bott
Subject: Re: Research Question Responses

I'm fine with the consent form as long you don't publish my name or company. :-)

Company wide, we're very functional: Sales, Marketing, Engineering, Support. There are also cross-cutting concerns (Accounting, Operations, ...)

Within engineering, we're project focussed for the most part, but there are 3 or 4 of us that answer directly to the the VP of engineering instead of the project manager. Sort of "staff level engineer" that float between projects as needed, although we all have different titles. The rest of the engineers stay on the particular project they were hired in on, unless that project ends, or a new project starts up and siphons people off their old project.

The actual project I'm on has been treated very differently. We're acting like a startup within the company. We have our own product manager, or own executive officer, our own marketing team, etc. The only place we plug into the rest of the company is in accounting, where we use the same backend systems, and a bit of IT.

So there's a complicated answer for you.

On Mon, Mar 9, 2015 at 8:02 AM, Robert Bott <rbott@purdue.edu> wrote:

<REDACTED>,

I wanted to make sure you are OK with the consent form. You don't have to print it out if you do not want, I simply wanted to know if you had any questions or concerns.

Also, I had another small follow up for you. How would you best describe the organizational structure of your company? Functional, Matrix or Projectized (see PMBOK p. 22)?

Thanks,

Robert

From: <REDACTED> [mailto: <REDACTED>]
Sent: Tuesday, February 24, 2015 5:03 PM
To: Robert Bott
Subject: Re: Research Question Responses

information/assets - high. Unless there's some unkown bug associated with VPN that hasn't become publicly known.

our product - high. Unless there's some inherent bug in Amazon's VPC implementation that hasn't become publicly known.

On Sun, Feb 22, 2015 at 4:04 PM, Robert Bott <rbott@purdue.edu> wrote:

<REDACTED>,

I have one more general question for you.

How effective do you believe your security controls are in keeping your information/assets secure during development. Also, how do you rate the security of your product? Perhaps a simple scale of low, medium and high would suffice, though you may of course elaborate.

Thanks,

Robert

From: <REDACTED> [mailto: <REDACTED>]
Sent: Wednesday, February 11, 2015 1:01 PM
To: Robert Bott
Subject: Re: Research Question Responses

IT owns Stash (the physical servers) and the overall administration of those servers. We have no person designated as IT within our group. We answer to the VP of engineering, IT answers to the CEO.

But we have a "group", and I have administrative privileges within the group to set who can access our Stash Repos, and to create / delete repositories within our group. Other project managers have there own group.

On Wed, Feb 11, 2015 at 11:56 AM, Robert Bott <rbott@purdue.edu> wrote:

Which level of IT owns the security on Stash? Is it just your team, or is it higher level IT?

Yep, I won't mention anything in the paper, I simply need your general impressions articulated. The details are good for me to understand what you are doing. It seems like a well-oiled machine.

From: <REDACTED> [mailto: <REDACTED>]
Sent: Wednesday, February 11, 2015 12:53 PM
To: Robert Bott
Subject: Re: Research Question Responses

When I was at Nokia, a competitor had paid a local private eye to dumpster-dive us looking for what we were up to. Crazy but true.

Our proprietary code is stored in Stash (a git-based system). So people are constantly pushing branches to Stash. IT owns the security of Stash. We are doing continuous integration and deployement... Bamboo takes whatever is merged onto the "develop" branch and builds it, then pushes is to our integration environment in AWS. Every tuesday, we merge what's on develop to "master" branch, which gets pushed to our staging environment. (Each AWS environment is it's own virtual private cloud, with it's own domain name, databases, etc.) We run our internal team communication team (it's called <REDACTED>... similar to HipChat or Slack) on staging all day, and on Thursday we roll what's in staging to our production environment, which is where our customers connect.

<REDACTED> is open source in github (look for <REDACTED>). We're also offering it as a new hosted service for companies to use. (Because Slack and HipChat are so popular). It could be the product we pivot to if it becomes super successful.

On Wed, Feb 11, 2015 at 11:43 AM, Robert Bott <rbott@purdue.edu> wrote:

Project assets as far as information, which you seem to have good policies and practices to protect. It seems to me you ARE doing project security management and you have a strong security posture overall. Remembering to erase whiteboards, as trivial as that might sound, is a practice that is part of information security management, although not over electrons of course.

I am guessing when you all write new code locally (which is an asset), it is stored on your local machines and then certain builds transferred securely to repositories. I am guessing your IT folks handle all the details of keeping this secure on local desktops and servers. If not, this would be an issue your local managers would have to deal with. Maybe there is a special need at your HSV location that requires extra attention security wise, maybe not. Who better to know the environment the project operates in than the project manager and his/her team? Managing this possible security concern might be as simple as getting corporate IT to run down to your location, assess and implement controls. I would suggest that the point is that someone is thinking about these risks, in this particular scenario. Would you not agree?

This is really good stuff and something well worth mentioning in my work. I don't mean to suggest that there is always a need for specific management of security at the lowest level, just that in some cases it will benefit everyone and should be considered. It all comes at a cost though, so I am trying to gather information on the relationship between cost and effectiveness.

Robert

From: <REDACTED> [mailto: <REDACTED>]
Sent: Wednesday, February 11, 2015 11:56 AM
To: Robert Bott
Subject: Re: Research Question Responses

"...do you think that project managers who assist in managing security could produce safer project assets..."

So in my current case, the "project assets" needs definition. I'm not sure if you're thinking of things like a project plan (staffing, budget, design documents, etc.) or are you talking about the end product itself?

In my case, it's really interesting. All of our documents (requirements, design, lessons learned, test plans) are captured on an internal wiki. This wiki is editable by the entire team. There are sections that a product manager is responsible for (the guy defining the requirements) and parts that are owned by the project manager (the guy managing the engineering team). We're a distributed company, so of course we support VPN access to our network. But the security of our company network is totally in the hands of IT.

For our whiteboard notes, and especially for our hardware lab (which is a big open area), we don't allow visitors to have cameras. And (because we have training classes for our open source project, with international visitors come to) we're good about erasing white boards before outside visitors are given a tour.

For sensitive paper documents, we have burn bins. Like every contractor in town, we rely on an outside contractor to collect and destroy the trash placed in these. (Which I think is a bit ridiculous, but I guess you can trust them as much as you'd trust a low-level hourly janitorial staff member to do it.)

So that covers "project assets" assuming you mean guidance documents. Now for our cloud service, we have all of our backend source code (which is proprietary) running in AWS. For some of our services, Amazon is (or soon will be) a competitor. So there's a huge amount of trust that they won't snatch and grab our source code. AWS is a huge part of Amazon's revenue... it's actually what puts them in the black... so it's in their best interest to not violate trust.

- <REDACTED>

On Wed, Feb 11, 2015 at 8:09 AM, Robert Bott <rbott@purdue.edu> wrote:

<REDACTED>,

To clarify:

Question 3:

In this case, information security regarding valuable information your project managers need and use daily to complete their projects. Anything that is a trade secret or critical for an organization that is being managed/created/used by a project. For example, if I were building a new weapons system, I would want to keep any information secure throughout the project life cycle (and beyond of course, but I am focused on project life cycles).

There are many reports of Chinese cyber warriors stealing information on the F35 and other platforms. If this information was stolen during the program's life cycle, then one can assume that the final product is less secure (historical evidence exists of this). We do not know what they know, so in potential future battles, the F35 might be countered to a point of being ineffective.

Project security management is not a fully defined concept. There is little literature on this idea. Basically, it is pushing some of the responsibility of security management, under risk management, to the project manager. This includes all security, though I am focused on information security for my thesis to manage the scope. Think of it in terms of quality management, just for security.

So my question was meant to be viewed in this context. Looking back at all of your experiences in contracting and private industry, do you think that project managers who assist in managing security could produce safer project assets during the life cycle and safe products at completion? If we push more responsibility in security to the "lowest level" of management, i.e. PM's, could this increase the security posture of these projects and the organization as a whole?

Sorry for being so long winded. I felt like I owed you a good explanation.

Robert

From: <REDACTED> [mailto: <REDACTED>]
Sent: Tuesday, February 10, 2015 3:45 PM
To: Robert B
Subject: Research Question Responses

OK... so here goes.

· Do you think project managers who manage security, including information security, for their project above and beyond what the organization mandates (assuming vulnerabilities have been considered and a threat assessment made) add to the security posture of the organization? Do you have any examples from past or current projects where you or others have done this, or similar management?

Yes. Our company provides both hardware and software products, as well as maintains a widely used open source software project. More recently we've added cloud-based services to our offerings. The mandates that exist are very different based on what a team is doing. Hardware products have all manner of government and industry mandated requirements. Our open source project, on the other hand, is guided more by community peer review than anything else, and the emphasis is more on end-user privacy (a common theme in open-source software).

Our cloud-based services are relatively new, so there isn't much precedence in the company to lean on. The project manager and system architect are responsible for ensuring that industry best-practices are followed, and (for international customers) regional law is being followed.

Security breeches in either our hardware devices (which are often connected to the internet) and our cloud based services would be economically devastating.

· Would you consider information security management a part of risk management?

Yes. But a formal risk assessment plan seems to be a relic of the past. I think the general trend is "fail at security at your own peril". It's as much of a concern as gaining sufficient market share to be successful. If you look at in the context of acquiring / retaining customers, it's as important as what features you provide, your marketing campaign, etc. You can do everything right, but a security failure can damage your brand irreparably.

· Do you think that project security management, in particular looking at information security, could lead to more secure project assets and products?

I suppose so. But you might want to define what you mean by information security and information security management. Are you talking about customer credit card numbers and other private information of a customer? Our employee contact list? Securing our email server?

Our business and accounting systems (including things like email servers, Salesforce, our accounting systems, etc.) are managed by our IT department. The security built into our products and services, on the other hand, are the concern of the engineering teams that design them. The projects I've worked on delineate the security concerns just as we do any "feature" of our system. For example, we have specific tasks defined to design how authentication is handled, how customer logs are handled, how and where encryption is applied, etc. It's impossible, in my opinion, to break out security from the overall design of the system. Just as we design the system to be scalable, or support a certain required throughput, we also design in security.

· How does your organization handle information security, in particular for projects? How are you organized, who is responsible for what tasks? In general, what technology do you use (does not have to be specific), how do you deal with human factors (ex. training) and what policies and practices are there in your organization regarding information security?

Refer to previous response for a lot of this. As I said, the project manager and system architect are responsible for the engineering team's product design, which includes security. Additionally:

> We use public key certificates to secure access to cloud APIs. (All of our APIs are encrypted, whether over HTTPS, websockets, or media frames using DTLS)

> We only expose servers that provide public APIs to the Internet. Our backend cloud servers run in a VPC which otherwise only see traffic to/from other servers within the VPC.

> We use Amazon security groups to further restrict ports, and access from the VPC back to our corporate network.

· Do you have any hard numbers of budget expenditures for information security and its effectiveness (ROI perhaps)? Any percentage numbers of information security expenditures per budget for projects would help. (If you do and it is propriety/secret information you don't have to divulge it of course - this is understandably the most difficult information to obtain)

The only thing that would appear outside of our normal engineering budget is we periodically hire external security consultants to do white hat attempts to breech our system. We provide them with a diagram of our architecture (major functional components, where public APIs are exposed, the technologies used to communicate among our backend servers, etc), which is more than we'd expect a random hacker to know. Essentially we give them as much information from an attacker viewpoint as only a current or former employee would have. I don't know the budget for this. We do it when there's significant architectural change to merit it.

Hope this helps! I'd prefer you keep my name / company name out of the paper.

- <REDACTED>

From: <REDACTED> [mailto: <REDACTED>]
Sent: Monday, February 23, 2015 9:17 AM
To: Robert Bott
Subject: RE: Thesis Research

1) Do you think project managers who manage information security for their projects above and beyond what the organization mandates add to the security posture of the organization? Do you have any examples from past or current projects where you or others have done this?
    a. I think if agile teams or projects had more of a thought or leaning towards security that this would create a better product, but it's a matter of time and resources. On no project I'm currently working on do we have any security experts at the team or project level. As you stated below, security and vulnerability assessments are normally conducted by an independent group of staff and usually after a product is at least into a systems

integration environment or just prior to putting it into production. I agree, that if you had a security minded person testing at the development level for security issues, you'd catch a lot more. Also, if teams were looking at their coding (as developers) with more a mind to current security vulnerabilities, they code would be safer. I think one way to do this is to do more periodic training in security vulnerabilities.

   b. I think another reason why a lot of government or company development teams don't focus on security, is that they assume that the network or firewalls in place will protect the software. Instead of "hardening everywhere" they simply assume that the outer castle wall will stop the attack, and thus don't plan to defend anywhere else.

2) Would you consider information security management a part of risk management?
   a. I would. If I can mitigate the information security risk, then my overall risk profile decreases.

3) Do you think that project security management, in particular looking at information security, could lead to more secure project assets and products? What is your opinion?
   a. I think that projects looking at information security would lead to more security systems, but I think it's a matter of enforcements. Continuous Integration processes and DevOps tools have to be built in early so that these security, static code analysis, and other vulnerability finding applications/tools can be leveraged within the development process early (as a recommendation…at the nightly build after everyone commits). These security scans and issues that the tools find have to also be addressed within each team and sprint. Running the tool but not taking any action on the SQL injection or other issues you find does not do you any good. You've got to plan to have the team members and funding to have these tools, keep them running, and also address security concerns.

4) How does your organization handle information security, in particular for projects? How are you organized, who is responsible for what tasks? In general, what technology do you use (does not have to be specific), how do you deal with human factors (ex. training) and what policies and practices are there in your organization?
   a. In general we've got an Architecture & Engineering team that addresses the larger program/system issues & planning. Also, we have an ISSM and ISSO who is supposed to worry about our security concerns…but this is really only at the permissions/access level for system access. There is not anyone within the projects or systems who is worried about information security. There are teams within our client who do white hat hacking and other security attacks of the system…but these are normally post Production.

b. Within our development environment we use automated testing tools (Selenium for example) and some static code analysis tools and other CI tools that we bolt onto our builds and check ins (SonarQ for example). The training for information security is generic and mainly address PII and not handing someone your ID card and pin number.

5) Do you have any hard numbers of budget expenditures for information security and its effectiveness (ROI perhaps)? Any percentage numbers of information security expenditures per budget for projects would help. (If you do and it is propriety/secret information you don't have to divulge it of course - this is understandably the most difficult information to obtain)
   a. I don't have any information on that for our client. It's so removed from our development teams that I never hear this discussed.

Respectfully,

<REDACTED>
ACE Agile Development, <REDACTED>
SEACATS Agile Development, <REDACTED>
<REDACTED>

Robert,

Please let me know if I missed anything between both of your e-mails. I answered your additional questions in relation to the original 3 and 4, and left your new questions in blue font color as they were not numbered.

3) Do you think that project security management, in particular looking at information security, could lead to more secure project assets and products?

Yes. Managers need to ensure the products they delivering have security as part of the internal control and acceptance criteria. For example, it is not enough to produce a web application which meets all of the customer's requested functional features. Application developers should also have information security built in as part of their routine development lifecycle. The application team should routinely scan both their static code and compiled code for security and quality issues. There are numerous open source and commercial tools to assist with both (e.g., PMD, HP WebInspect / Fortify). Similar to the applications, the entire technology stack itself should be treated similarly (e.g., Nessus scans, AppDetective). Depending on the industry, there are further requirements which need to be taken into consideration such as HIPPA, Section 508 Compliance, etc. Furthermore, the overall Risk Management process should be looking at far more than just information security as other risks can have ripple effects. In the event there is an unplanned resource issue (i.e., risk was not properly identified and became an issue) then one of the items/areas which may suffer is the overall quality or security of the product – this falls under the triple constraint concept.

4) How does your organization handle information security, in particular for projects?

We adhere to FISMA requirements which have guided implementations through a combination of mandated standards (i.e., Federal Information Processing Standards), NIST Special Publications, and FISCAM specified controls when dealing with financial information. Every project is managed differently and while some projects managers may not go above and beyond, others will not only be required to take the additional steps but will be closely monitored for resolution. A common example is when a critical vulnerability is published and government agencies are required to report on their respective compliance state with the resolution (e.g., heartbleed vulnerability). During these times it is not an option for a project manager to accept the as-is security posture, and while they may not get additional funding or resources for the resolution, the outcome is still the same – they are required to resolve the issue. Taking into consideration the triple constraint, this may result in delayed project completion, or reduced quality in the final delivered product.

Further questions:

Are you familiar with the 20 Critical Security Controls published and maintained by the Council on Cyber Security (and championed by SANS)? If so, what is your opinion on these controls and the means by which they are supposed to be implemented. Also, how do you think they relate to the NIST 800-53rev4 and the ISO 27002 standards (as related to information security)?

The Top 20 CSC has a greater focus on metrics and validation approaches which other requirements such as NIST 800-53 do not include. The Top 20 CSC include specific metrics such as "*How long does it take to detect new devices added to the organization's network (time in minutes)?*", whereas NIST 800-53a does not have such specific metrics to assess/determine level of efficiency the NIST 800-53 controls.

For example: NIST 800-53 rev4, controls for High watermark systems have CM-8 (3) and SI-4 (4)(5) will cover most of CSC 1, however if you were to examine the test procedures for the NIST controls per 800-53a rev1, the tester or auditor only needs to ensure the basic elements of the control are place and not necessarily the true effectiveness (e.g., time in minutes to detect/alert/isolate unauthorized network assets). CSC 1-6 speaks to the implementation of a NAC solution to monitor unauthorized systems and to move the system to a specific virtual LAN in the event of an attack. Unfortunately, IR-4(2) is not required per NIST for High systems, although if successfully implemented would address a NAC-like approach.

How would you best describe the organizational structure of your company? Functional, Matrix or Projectized (see PMBOK p. 22)?

The vast majority of the organization is functional, with few instances of matrix.

<REDACTED>

From: Robert Bott [mailto:rbott@purdue.edu]
Sent: Monday, March 09, 2015 9:00 AM
To: <REDACTED>
Subject: RE: Assistance/Input Requested

<REDACTED>

I had another small follow up for you, on top of the others I sent you a few days back. Hopefully, these will be the last!

How would you best describe the organizational structure of your company? Functional, Matrix or Projectized (see PMBOK p. 22)?

Thanks,

Robert

From: <REDACTED>. [mailto: <REDACTED>]
Sent: Wednesday, February 25, 2015 5:38 PM
To: Robert Bott; <REDACTED>
Subject: RE: Assistance/Input Requested

Robert,

Thank you that answers my questions and concerns. What is your timeframe for being able to utilize our responses? The below can be considered an interim response in the event you need something soon, but ultimately would like to re-read my own answers and make repeated changes to an unhealthy extent (e.g., question 5) before you consider them as a final set of answers. Also, please let me know if you need anything else to increase validity.

Subject 1
Certifications:

- Project Management Professional (PMP)
- Certified Information Systems Security Professional (CISSP)
- Certified Authorization Professional (CAP)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Ethical Hacker (CEH)
- Certified Hacking Forensic Investigator (CHFI)
- Certified Penetration Tester (CPT)
- Contracting Officer's Technical Representative (COTR)
- Certified Scrum Master
- Certified Scrum Product Owner
- Information Technology Library Infrastructure (ITIL): Service Offerings & Agreements
- Information Technology Library Infrastructure (ITIL): Service Design
- Information Technology Library Infrastructure (ITIL): Foundations version 3

Note: The potential responses to these questions will inherently vary depending on the person being interviewed. I will be answering from my personal perspective and do not officially represent the U.S. federal government.

1) Do you think project managers who manage information security for their projects above and beyond what the organization mandates add to the security posture of the organization?

This depends on a few factors, such as the cost of the measure to implement, the cost of the measure once implemented, and the overall risk appetite of the organization.

For example, if an organization requires users to maintain an 8 character password which is changed only once a year, then in most cases the cost to change the requirements to 14 character passwords to be changed every 90 days, then the organization most likely observe an increased call volume to the help desk for forgotten passwords. The cost to implement is low, and the cost to maintain is high.

On the other hand, there are potential situations where an organization may not require their technical teams to encrypt data at rest or use a Public Key Infrastructure to protect data in transit. These two types of common data protection measures can be implemented with minimal costs and little to no increase in post-implementation support.

Do you have any examples from past or current projects where you or others have done this?

Yes. Several years ago I worked as a contractor for a federal client. The task we were given was to improve the overall FISMA score. At the time, there was a process which would allow for the system's score to show a level of compliance with security controls, even though the controls were not in place. This is due to the fact that the scoring process accepted properly documented and authorized exceptions to required security controls (i.e., Risk Acceptance). There was an approved exception to using TN3270 (IBM Mainframe client connection). The organization utilized certificates to establish secure connections (SSL at the time) on other information systems. We utilized their existing certificate issuance and management process and had the TN3270 sessions invoked through pre-established SSL connections. This was transparent to the users, did not improve their FISMA score, but greatly improved the security for their data in transit.

2) Would you consider information security management a part of risk management?

Both information security management and risk management are included in most major information technology lifecycle frameworks (e.g., National Institute of Standards and Technology Special Publication 800-37, ISO/IEC 16085:2006). The Office of Management and Budget Circular A-130, Appendix III requires adequate security to be implemented for federal information systems, at a degree commensurate with the risk and magnitude of harm if the system's confidentiality, availability, or integrity were compromised. In short, there are costs associated with implementing security controls, and that cost should be weighed against the resulting impact of the risk.

3) Do you think that project security management, in particular looking at information security, could lead to more secure project assets and products?

Yes.

What is your opinion?

The organization should adopt an existing and mature lifecycle framework which is best aligned to the organizations legal and business needs in relation to information security.

4) How does your organization handle information security, in particular for projects?

We adhere to FISMA requirements which have guided implementations through a combination of mandated standards (i.e., Federal Information Processing Standards), NIST Special Publications, and FISCAM specified controls when dealing with financial information.

How are you organized, who is responsible for what tasks? (Reference redacted email content (NIST, 2005))

"There are formal designations identified within FISMA and FISCAM, which map to several key roles, each with differing responsibility. Please refer NIST Special Publication 800-65 for more information on the following roles, to include additional roles not mentioned herein.

Senior Agency Officials
Senior agency officials provide information security for the information and information systems that support the operations and assets under their control, under the direction of the head of the agency. Delegating to the agency Chief Information Officer (CIO) the authority to ensure compliance with agency security requirements

Chief Information Officer
The Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act) requires agencies to appoint CIOs. The agency CIO is the senior IT advisor to the Investment Review Board and the head of the agency. Develops and maintains risk-based information security policies, procedures, and control techniques. Ensures IT training for agency staff and oversees IT security personnel. Designates a senior agency information security officer to carry out CIO directives as required by FISMA.

Senior Agency Information Security Officer
As mandated by FISMA, the senior agency information security officer is appointed by the CIO and manages information security throughout the agency. The senior agency information security officer is responsible for coordinating program requirements throughout the agency with designated points of contact and project managers.

System Owner

The system owner handles the day-to-day management of the IT investment. The system owner responsibilities include the following:

- Maintaining active senior-level involvement throughout the development of the system;
- Participating in project review activities and reviewing project deliverables;
- Coordinating activities with senior management;
- Obtaining and managing the budget throughout the project's life cycle against a project manager's delivered, locked baseline;
- Holding review and approval authority to ensure that developed products incorporate security and meet user requirements;

- Ensuring system has an up-to-date security plan, has a contingency plan, and receives full C&A;
- Providing baseline assessment performance measures to evaluate the security of the delivered IT initiative; and,
- Developing and maintaining system-specific POA&Ms.

Information System Security Officer
The Information System Security Officer is a direct report to the System Owner and assists in carrying out the responsibilities. However, the System Owner retains the accountability for the information system's security posture. There may be multiple Information System Security Officers for each information system, however there is only one assigned System Owner." (p. 19 – 22)

In general, what technology do you use (does not have to be specific), how do you deal with human factors (ex. training) and what policies and practices are there in your organization?

Microsoft Windows for most desktops, and iOS/Android for most smartphones. We utilize common commercial products to enforce configuration and security policies on all devices. We also use common commercial solutions for web servers (e.g., Apache, IIS, WebSEAL), application servers (e.g., WebSphere, WebLogic, Tomcat) and databases (e.g., Oracle, SQL, DB2, Datacom). The policies and practices in place are largely governed and derived through federal mandates from the Office of Management and Budget (e.g., OMB A-130 and OMB A-123), and Homeland Security Presidential Directives (e.g., HSPD-12). Note: Specific details on versions, and which products are used to secure these systems are intentionally excluded.

Training is provided to federal employees through a combination of computer based training and classroom. Contractors are expected to arrive with the necessary skills and experiences to fulfil their contracted duties. However, there are exceptions made depending on the circumstance (e.g., training provided for a new product to be supported by an existing contract team).

5) Do you have any hard numbers of budget expenditures for information security and its effectiveness (ROI perhaps)?

There would not be a Return on Investment for most of our expenditures in relation to implementing information security. Furthermore, security is typically implemented at a cost to meet a legal requirement in the federal government opposed to experience a financial return/gain. This is typically true for commercial organizations, with exception of measures protecting trade secrets; of which is still difficult to estimate the ROI.

Instead, there are times where implementing commercial solutions for increasing security or meeting a federal mandate may also result in an ongoing cost savings which at times could map to a perpetual ROI. For example, 35% of our current Help Desk calls are password reset (i.e., users forgetting passwords). We are in the process of implementing Single Sign-On utilizing two-factor authentication through PIV cards. This will result in a significant reduction in call volume as the cards utilize shorter character count PINs, that are easier to remember. In addition, there is also a method for a user to reset their own PIN by utilizing a fingerprint scanner. The result will enable the government to renegotiate the existing Help Desk contract at a lower price due to a significant reduction in the overall manpower necessary to provide their respective support services.

> Measuring effectiveness can depend on the unit within the organization. For example, a robust cybersecurity program with highly engineered systems will likely have a reduced active threat count and greater threat counter and resolution time compared to a less advanced engineered program.

Any percentage numbers of information security expenditures per budget for projects would help.

> I am not aware of any specific amount of required funding dedicated to information security (e.g., 15% of overall project), but will check with our budget teams.

<REDACTED>

From: Robert Bott [mailto:rbott@purdue.edu]
Sent: Wednesday, February 25, 2015 3:43 PM
To: <REDACTED>
Subject: RE: Assistance/Input Requested

Sir,

I can leave out your PII from my thesis for publication. The only thing I ask to publish is your job title and any certifications you have in order to increase validity. I do not intend to mention the name of your employer (other than "high tech company", "or government agency" – very general) or your PII.

An example would be "Subject 1 : PMP etc." in the list of professionals I reference. Then I will use "Subject 1" as your reference when I refer to the information you might provide me. I will publish the email conversations in Appendices and redact your PII and company or agency name. I hope this answers your question. If you have any other concerns, please let me know.

Respectfully,

Robert Bott

From: <REDACTED> [mailto: <REDACTED>]
Sent: Friday, March 06, 2015 10:06 AM
To: Robert Bott
Subject: Re: Assistance/Input Requested

Robert,

I would definitely like my PII and company name removed. My Title is Information Systems Security Manager. I hold the following certifications

- Information Technology Library Infrastructure Foundations (ITIL)
- Certified Information System Security Professional (CISSP)
- ICAgile Certified Professional (ICP)
- Certified Scrum Master (CSM)

Please feel free to ask as many questions as you would like. In addition to the responses <REDACTED> provided, here are some additional points to your questions from my perspective.

1) **Do you think project managers who manage information security for their projects above and beyond what the organization mandates add to the security posture of the organization? Do you have any examples from past or current projects where you or others have done this?**

I see Project Managers as the face of the Project. They have to lead by example and strive to meet or exceed the minimum organization's security requirements. Since they are in a position to interface between stakeholders, business and engineers, I see their value as trend setters.

As an example, I, along with my colleagues are also Team Leads that interface with business, stakeholders, and engineers that implement the solution. We have witnessed the organization setting minimum requirements for implementing IT security, such as implementing a database with shared database administration account. As we dug deep into the security posture, we discovered several deficiencies in the security of the databases. One of the things that we did as change agents, was to help the customer realize the weaknesses, and presented ideas on how to drastically improve it. In summary, we went above the bare minimum, and implemented encrypted databases, individual admin account for better auditing of administration responsibilities, enabling role-based single sign-on using PIV cards to name a few.

Project managers definitely have to go above and beyond to improve the security posture of the organization beyond the minimum requirements as they are considered change agents.

2) **Would you consider information security management a part of risk management?**

Absolutely. One of the key parts of the FISMA Score card is the risk factor which is derived from the NIST SP 800-37. One of the most common issues we face is protecting data in transit. In the digital age, almost all transactions are done electronically and that data must be protected. Security Managers often struggle to implement the protection of data in transit as this can be costly to implement. A perfect balance of cost and security posture has to be maintained. The most common implementations are to enable SSL encrypted communication channels secured by PKI certificates from valid CA Authority.

3) **Do you think that project security management, in particular looking at information security, could lead to more secure project assets and products? What is your opinion?**

Absolutely. In addition, I feel that an industry standard approach should be used such as CMMI or ISO to ensure correct processes and controls are implemented.

4) **How does your organization handle information security, in particular for projects? How are you organized, who is responsible for what tasks? In general, what technology do you use (does not have to be specific), how do you deal with human factors (ex. training) and what policies and practices are there in your organization?**

Same answer as <REDACTED>

5) **Do you have any hard numbers of budget expenditures for information security and its effectiveness (ROI perhaps)? Any percentage numbers of information security expenditures per budget for projects would help. (If you do and it is propriety/secret information you don't have to divulge it of course - this is understandably the most difficult information to obtain)**

In addition to <REDACTED> answer, I would like to add that the best Return On Investment is the peace of mind that one can provide to protect the assets of their Organization. Again the balance is to make information secure yet still usable by consumers. Some of the previous companies I have worked for used as much as 35% - 45% of their expenditures on security. This is of course dependent on the information that needs to be protected and the value of the business.
--

<REDACTED>

Appendix B Model Data

The following figures represents all data collected from each individuals run used for this paper. It contains all detailed results for each model run.

Total Attacks	Organizational Attacks	Successful Organizational Attacks	Organizational Defenses	Project Attacks	Successful Project Attacks	Project Defenses	Total Cost of CSCs to Project (% of budget)
1065	999	66	933	66	66	0	0
1063	1000	63	937	63	63	0	0
1045	1000	45	955	45	45	0	0
1049	1000	49	951	49	49	0	0
1046	1000	46	954	46	46	0	0
1043	1000	43	957	43	43	0	0
1043	1000	43	957	43	43	0	0
1048	1000	48	952	48	48	0	0
1045	1000	45	955	45	45	0	0
1045	1000	45	955	45	45	0	0
1049	**1000**	**49**	**951**	**49**	**49**	**0**	**0**

Figure B.2 – No Project CSCs

Total Attacks	Organizational Attacks	Successful Organizational Attacks	Organizational Defenses	Project Attacks	Successful Project Attacks	Project Defenses	Total Cost of CSCs to Project (% of budget)
1049	999	50	949	50	43	7	2
1060	1000	60	940	60	50	10	2
1043	1000	43	957	43	35	8	2
1052	1000	52	948	52	44	8	2
1044	1000	44	956	44	34	10	2
1048	1000	48	952	48	37	11	2
1044	1000	44	956	44	38	6	2
1057	1000	57	943	57	52	5	2
1040	1000	40	960	40	34	6	2
1052	1000	52	948	52	44	8	2
1049	**1000**	**49**	**951**	**49**	**41**	**8**	**2**

Figure B.3 – One Project CSC

Total Attacks	Organizational Attacks	Successful Organizational Attacks	Organizational Defenses	Project Attacks	Successful Project Attacks	Project Defenses	Total Cost of CSCs to Project (% of budget)
1035	999	36	963	36	20	16	4
1041	1000	41	959	41	25	16	4
1049	1000	49	951	49	37	12	4
1046	1000	46	954	46	30	16	4
1053	1000	53	947	53	28	25	4
1051	1000	51	949	51	30	21	4
1041	1000	41	959	41	25	16	4
1060	1000	60	940	60	37	23	4
1043	1000	43	957	43	29	14	4
1053	1000	53	947	53	31	22	4
1047	**1000**	**47**	**953**	**47**	**29**	**18**	**4**

Figure B.4 – Two Project CSCs

Total Attacks	Organizational Attacks	Successful Organizational Attacks	Organizational Defenses	Project Attacks	Successful Project Attacks	Project Defenses	Total Cost of CSCs to Project (% of budget)
1043	999	44	955	44	19	25	6
1045	1000	45	955	45	16	29	6
1038	1000	38	962	38	17	21	6
1050	1000	50	950	50	24	26	6
1053	1000	53	947	53	20	33	6
1043	1000	43	957	43	17	26	6
1044	1000	44	956	44	21	23	6
1043	1000	43	957	43	15	28	6
1054	1000	54	946	54	24	30	6
1048	1000	48	952	48	24	24	6
1046	**1000**	**46**	**954**	**46**	**20**	**27**	**6**

Figure B.5 – Three Project CSCs

Total Attacks	Organizational Attacks	Successful Organizational Attacks	Organizational Defenses	Project Attacks	Successful Project Attacks	Project Defenses	Total Cost of CSCs to Project (% of budget)
1048	999	49	950	49	10	39	8
1063	1000	63	937	63	18	45	8
1046	1000	46	954	46	16	30	8
1058	1000	58	942	58	11	47	8
1043	1000	43	957	43	10	33	8
1060	1000	60	940	60	12	48	8
1049	1000	49	951	49	9	40	8
1045	1000	45	955	45	8	37	8
1050	1000	50	950	50	14	36	8
1048	1000	48	952	48	12	36	8
1051	**1000**	**51**	**949**	**51**	**12**	**39**	**8**

Figure B.6 – Four Project CSCs

Total Attacks	Organizational Attacks	Successful Organizational Attacks	Organizational Defenses	Project Attacks	Successful Project Attacks	Project Defenses	Total Cost of CSCs to Project (% of budget)
1046	999	47	952	47	5	42	10
1035	1000	35	965	35	2	33	10
1065	1000	65	935	65	2	63	10
1052	1000	52	948	52	2	50	10
1071	1000	71	929	71	4	67	10
1051	1000	51	949	51	1	50	10
1041	1000	41	959	41	2	39	10
1051	1000	51	949	51	3	48	10
1049	1000	49	951	49	0	49	10
1046	1000	46	954	46	1	45	10
1051	**1000**	**51**	**949**	**51**	**2**	**49**	**10**

Figure B.7 – Five Project CSCs

Total Attacks	Organizational Attacks	Successful Organizational Attacks	Organizational Defenses	Project Attacks	Successful Project Attacks	Project Defenses	Total Cost of CSCs to Project (% of budget)
1039	999	40	959	40	3	37	12
1040	1000	40	960	40	3	37	12
1032	1000	32	968	32	3	29	12
1027	1000	27	973	27	1	26	12
1018	1000	18	982	18	0	18	12
1011	1000	11	989	11	1	10	12
1008	1000	8	992	8	0	8	12
1012	1000	12	988	12	1	11	12
1010	1000	10	990	10	0	10	12
1012	1000	12	988	12	1	11	12
1021	**1000**	**21**	**979**	**21**	**1**	**20**	**12**

Figure B.8 – Five Project CSCs with CSC 18

Appendix C CSC Selection Analysis

Critical Security Controls (CSCs) selected for model implementation. The information in this appendix was used to help design and implement the model. It consists of a description and analysis of the viability of selected CSCs for purposes of the model as well as potential costs and effectiveness metrics. Most of the following information referenced from (Council on Cyber Security, n.d.) and (Pruitt, 2013).

Critical Security Control #3: **Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**

Researcher Comments: Could be useful to model a lower level project with the need to manage their own configurations due to a business need. For example, the organizational level configuration standards are not strict, robust or effective enough for the specific demands of the project.

Description:

Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Type of control:

Policies, Practices & Procedures

Implementation method and estimated costs:

Implementation (partial):

- Establish and ensure the use of standard secure configurations for operating systems
- Implement automated patching for applications and operating systems
- Limit administrative privileges to a very few knowledgeable people
- Follow strict configuration management
- Purchase securely configured systems from manufacturers when possible

Estimated costs:

The costs are associated with the time expenditure of labor and the costs of purchasing well configured systems, as well as any tools used to manage configurations.

Model Abstract Cost: Percentage of total Budget (variable)

Effectiveness metrics:

- Time taken to detect and report unauthorized configuration changes to administrators
- Time taken to block/quarantine unauthorized configuration changes
- Ability to physically locate system

Related attacks:

- Attackers exploit weak default configurations of systems that are more geared to ease of use than security

Critical Security Control #7: **Wireless Access Control**

Comments: Might be useful to model given that a project could be at a separate location and/or isolated from higher organizational wireless infrastructure. There might be specific situations where the PM needs to pay special attention to the access points supporting his/her project.

Description:

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

Type of control:

Technology; Policies, Practices & Procedures

Implementation method and estimated costs:

Implementation (partial):

- Ensure each wireless device connected to the network matches and authorized configuration and security profile and it is associated with an individual and has a business need
- Configure network scanning tools to detect wireless access points connected to the wired network and ensure all wireless points are on approved lists
- Use wireless intrusion detection systems (WIDS) to detect rogue wireless devices
- Ensure all wireless traffic uses the latest encryption and authentication protocols
- **Disable all wireless services (peer-to-peer or bluetooth) unless a specific business need exists**

Estimated costs:

The costs are associated with the time expenditure of labor to deploy tools, configure access points and administer/supervise scans. Also the cost of deployed tools must be factored in.

Model Abstract Cost: Percentage of total Budget (variable)

Effectiveness metrics:

- Are systems capable of detecting unauthorized wireless devices or access points?
- How long does it take to generate alerts of unauthorized access?
- How long does it take to block access of unauthorized devices?
- Are additional alerts generated after the initial?
- Is the system able to determine the physical location of the unauthorized device or access point?

Related attacks:

- Attackers exploit wireless access points to gain entry into a target organization's internal network, and exploit wireless client systems to steal sensitive information.

Critical Security Control #9: **Security Skills Assessment and Appropriate Training to Fill Gaps**

Comments: This should be modeled given that projects are unique and each has its own vulnerabilities. PM's must ensure their team members are properly trained and educated and have a security mindset. This is above and beyond what the organization dictates.

Description:

For all functional roles in the organization (prioritizing those mission---critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Type of control:

Human Factors

Implementation method and estimated costs:

Implementation (partial):

- Perform a gap analysis to judge security awareness and training level of employees and build a baseline
- Perform training to fill the gap and expand security awareness/skills. Use an active and frequently updated online training program that focuses on the major problems in security
- Validate training through periodic testing of skills and training levels

Estimated costs:

The costs are associated with the time expenditure of labor to training employees and the loss of productivity of the trainees. Also, any initial costs to set up online training either in-house or through contracts must be considered as well as the continued validation efforts.

Model Abstract Cost: Percentage of total Budget (variable)

Effectiveness metrics:

- Participation rate of online training
- Average scores of online training tests and periodic tests based on the baseline
- Individual scores for mission-critical personnel

Related attacks:

- Attackers exploit users and system administrators via social engineering scams that work because of a lack of security skills and awareness
- Attackers trick a user with an administrator-level account into opening a phishing style e-mail with an attachment or surfing to the attacker's content on an Internet website, allowing the attacker's malicious code or exploit to run on the victim machine with full administrator privileges

Critical Security Control #15: **Controlled Access Based on Need to Know**

Comments: Good to model since this ties in day to day management of the need to know for team members. A plan must exist and must be managed that allows and retracts rights to certain information as well as account types.

Description:

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Type of control:

Technology; Policies, Practices & Procedures

Implementation method and estimated costs:

Implementation (partial):

- Locate all sensitive information and encrypt communications of it over less trusted networks
- Enforce audit logging of non-public information access
- **Segment the networks based on trust levels**

Estimated costs:

The labor costs for setting up and managing the segmented networks as well as the tools needed to encrypt information and log events.

Model Abstract Cost: Percentage of total Budget (variable)

Effectiveness metrics:

- Can the system detect all attempts to access data that a user does not have permissions to access?
- Time taken to send an alert when non-privileged users attempt to access privileged information

Related attacks:

- Attackers gain access to sensitive documents in an organization that does not properly identify and protect sensitive information or separate it from non-sensitive information
- Attackers compromise systems and alter important data, potentially jeopardizing organizational effectiveness via polluted information
- Attackers use malicious code to gain and maintain control of target machines, capture sensitive data, and then spread it to other systems, sometimes wielding code that disables or dodges signature-based anti-virus tools

Critical Security Control #17: **Data Protection**

Comments: Might be good to model since specific situations might require better encryption standards for the projects. Also, specific processes to access the data will differ based on the project vs. the organizational level day to day operations.

Description:

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Type of control:

Technology; Policies, Practices & Procedures

Implementation method and estimated costs:

Implementation (partial):

- Employ state-of-the-art encryption for data in transit and rest on all systems handling sensitive information
- Review cloud provider security practices for data protection
- Employ tools to monitor network traffic and servers for sensitive information
- Perform regular review of encryption algorithms and key lengths

Estimated costs:

The labor costs for managing the policies that are implemented and the continued review of them, as well as the use of tools. The costs for any tools used.

Model Abstract Cost: Percentage of total Budget (variable)

Effectiveness metrics:

- Does the system report on any violation of the set policies regarding encryption and data transfer on the network?
- Does the system store cryptographic key material properly?
- Does the system report on data exfiltration attempts?

- Does the system generate appropriate reports and send them to administrators or security personnel within accepted timeframes?

Related attacks:

- Attackers use malicious code to gain and maintain control of target machines, capture sensitive data, and then spread it to other systems, sometimes wielding code that disables or dodges signature-based anti-virus tools
- Attackers gain access to sensitive documents in an organization that does not properly identify and protect sensitive information or separate it from non-sensitive information
- Attackers compromise systems and alter important data, potentially jeopardizing organizational effectiveness via polluted information
- Attackers gain access to internal enterprise systems and gather and exfiltrate sensitive information without detection by the victim organization

Critical Security Control #18: **Incident Response and Management**

Comments: As far as the model, implementing this CSC might also demonstrate that over time, a project that has its own incident response and management plan will become a harder target vs. the other projects and the organization. The security posture of the project that implements this CSC will be higher than other projects.

Description:

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Type of control:

Human Factors; Policies, Practices & Procedures

Implementation method and estimated costs:

Implementation (partial):

- Ensure that there are written incident response plans that include roles and responsibilities of personnel
- Assign job descriptions and duties for handling incidents
- Define management personnel who will take change and handle the incident
- Devise standards for administrators to report anomalies and incidents to the response team
- Conduct regular incident scenario sessions (training) to ensure incident personnel understand the latest threats and their roles in an incident

Estimated costs:

The labor costs for creating and managing the incident plans as well as the required designation and training of personnel.

Model Abstract Cost: Percentage of total Budget (variable)

Effectiveness metrics:

- None listed

Related attacks:

Attackers operate undiscovered in organizations without effective incident - response capabilities, and when the attackers are discovered, the organizations often cannot properly contain the attack, eradicate the attacker's presence, or recover to a secure production state