THE SUCCESS OF INFORMATION SECURITY PROJECTS: AN INVESTIGATION OF THE PROJECT MANAGEMENT PROCESS, PROJECT COST, PROJECT RISKS AND USER ACCEPTANCE

by

Ken Lee Chow

RONALD BENSON, Ph.D., Faculty Mentor and Chair

MARGARITA ROVIRA, Ph.D., Committee Member

DONNA DIMATTEO, Ph.D., Committee Member

Kurt Linberg, Ph.D., Dean, School of Business & Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

April 2008

UMI Number: 3297915

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

Abstract

The study was conducted in order to evaluate the relative role of project management, project cost, project risks, and end user acceptance in the success of information security projects. This research is a case study of a single company, utilizing a mixed methods research approach in the form of interviews and surveys. In particular, the researcher conducted a survey of 200 randomly selected employees of a company deploying IT security solutions. In addition, five employees from this company were interviewed. With this, the researcher makes an analysis out of the qualitative and quantitative data collected.

Dedication

This research is dedicated to my beloved sister who will always live in my heart.

Acknowledgments

I would like to thank Mr. Bill Tomlinson, who brought me into the IT security world. Mr. Tomlinson provided me with an opportunity to learn the methodology of Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), which became the foundation of my knowledge regarding IT security. Mr. Tomlinson was my mentor; his extensive experiences from the military further enhanced my knowledge in managing IT security.

I would also like to thank Dr. Shane Shook. Dr. Shook is an expert in the areas of IT risk management, privacy, and electronic discovery. Dr. Shook taught me the core of IT risk management, and especially, the demanding field of electronic discovery and computer forensics. Dr. Shook helped me see, from his perspective of IT security, the legal and expert witness service areas.

And special thanks to Mr. Scott Emery for his encouragement from the beginning of my research, proofreading my writing, and providing valuable feedback throughout this process.

I would like to take this opportunity to thank my mentor and committee chair, Dr. Ronald Benson for his encouragement, flexibility, and timely guidance. Without Dr. Benson's assistance, I could not have completed this difficult journey, and the research conducted for this study would not have been possible.

I would also like to thank my committee members: Dr. Margarita Rovira and Dr. Donna DiMatteo. Dr. Rovira's experiences in management provided me with great ideas regarding users’ acceptance and project management. Dr. Rovira’s feedback helped me to look at IT from a different, more enlightened, perspective.

Dr. DiMatteo’s expertise in psychology provided me with the critical knowledge to build the surveys and questionnaires. Dr. DiMatteo’s feedback really helped me fine tune my research.

Finally, I would like to thank those who took the time to participate by completing my surveys and questionnaires

TABLE OF CONTENTS

List of Tables

List of Figures

CHAPTER 1. INTRODUCTION

Information Technology (IT) security research is an assessment of the relationship between organization structure, culture, management, staff, and the organization's technical environment. This relationship can be compared to a driver who takes his/her car for a checkup, and at the same time has an evaluation performed to determine the driver's skill, the condition of the car, and the road conditions to ensure that there is a balance between all these variables.

IT is the application of modern technologies, such as computers, software technology, telecommunications, office systems, or any combination of these elements in the creation, management, processing, dissemination, and use of information. The other technologies utilized in information technology include the telephone, CD-ROM, video recorders, and other computer-based tools.

The Information Technology Association of America (ITAA) defines IT as the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware (Information, 2007). In the modern world, IT plays a vital role in the effective and efficient utilization of information. In fact, almost all transactions are carried out through IT as a medium. Different activities and process that relate to the use of information rely on the power of IT.

Indeed, IT is the prodigy of the modern world that paved the way for the information superhighway. Like a literal highway, security is significant to assure a safe flow of traffic; but in this case, the traffic is information. In this context, the issue of security as it relates to IT comes to fore. Since there is a free flow of information, IT security must be assured. In this way, one will be able to conduct business effectively and successfully.

IT security has been fraught with controversies and issues throughout the years. Problems regarding information technology security are documented by the Computer Emergency Response Team (CERT) surveys (Alberts & Dorofee, 2003) regarding security incidents and breaches. According to the survey, security attacks come from both the outside and inside of an organization. As such, there is a definite need to look at the security of IT.

In line with this, project management is deemed to be indispensable to the effective implementation of IT security projects. Project management is otherwise defined as the application of modern management techniques and systems to the execution of a project from start-to-finish, achieving predetermined objectives of scope, quality, time, and cost, to the equal satisfaction of those involved (Razalli, 2007). In other words, project management deals with the overall planning and coordination of a project (from inception-to-completion) aimed at meeting the client’s requirements and ensuring the project’s completion on time, within cost, and to required quality standards (Project Management, 2007).

With this in mind, this research aims to identify whether the utilization of a formal project management approach will lead to higher rates of success of IT security projects. This research will utilize the mixed method research which consists of qualitative and quantitative data analysis in the form of interviews and surveys.

More specifically, this paper will determine the relationship between IT security and project management. From there, this study will determine the way project management affects the effective implementation of IT security projects. It is also important to identify the various security issues and problems which occur on IT security projects. Moreover, this paper will examine the critical success factors of project management in the process of utilizing project management skills in order to address IT security. Lastly, this paper will resolve the role of end user acceptance/satisfaction levels in the capacity of project management to address the issues on security of IT.

Background of the Study

The emergence of IT has undoubtedly transformed not only the world of business, but the conduct of people's everyday activities as well. More importantly, the concept of IT has evolved along with the creation and development of a wide array of technologies. These technologies range from telecommunications to various computer-based tools.

The coming of the Internet technology has paved the way for the flourishing of IT. In particular, the Internet technology changed the conventional way of utilizing IT. The Internet presented mankind with unlimited opportunities, thereby increasing the rate of technological development. As a result, Internet technology became an important aspect of realizing the potential of IT.

In spite of the massive changes that occurred in the field of IT, the issue of security still surfaces as one of the major problems in IT. In fact, this problem did not subside, but, in fact, became more prevalent. Even with the presence of security vendors, IT security is still considered to be a major concern of people, especially in the business world.

Peter Neuman, principal scientist at SRI's Computer Science Lab, and author of "Computer-Related Risks" said, "Computers are tied to infrastructure and the core operations of business and have absolutely become a part of the fabric of how we function as a society. Yet comparatively few [in society] are aware of the risks imposed by distributed computing. That puts all of us in a more vulnerable position" (Neumann, 1994).

This study involves the interaction of IT security and project management. Background on these two topics follows.

Information Technology Security

It is known that IT has become an integral part of the way business is conducted today (Frame, 2002). According to Brian (1999), corporations allocate significant amounts of their budgets to safeguard their network infrastructure. Thus, the influx of security vendors is inevitable given the significance of safeguarding these investments. Security vendors all claim high comprehensiveness and reliability of their products including the assurance of confidentiality, integrity and security of the corporations' critical assets (Brian, 1999).

Information Technology Security Issues

The high visibility of security issues is apparent in several ways. A SANS™ Institute survey (The Sans 2005-2007, 2007) indicated that the IT security career field is one of the top pay areas in IT, and it also has the highest job demand. Traditional antivirus vendors, such as Symantec™ and McAfee®, have entered the arena of IT security solutions. Clearly, security is critical to IT's successful use.

IT security is highly needed because of the threats coming from viruses, phishing, and spyware (Brown, 2005).

Viruses are defined as a malicious program; the sole intent of which is to cause problems on a computer. Because of this, various antivirus programs are created in order to combat viruses. Among these programs are the McAfee and Norton™ Utilities (Glossary, 2007).

In the case of phishing, identity theft is the primary issue. Specifically, it is considered as a form of Internet fraud that aims to steal valuable information, such as credit cards, social security numbers, passwords, as well as user IDs. This is done through the creation of a fake Web site, which appears similar to a legitimate organization; the mock site is typically a reflection of a well-known financial institution, such as a bank or insurance company (Glossary, 2007).

Spyware deals with the class of software that monitors the actions of a computer user. In particular, this software can be divided into different categories, such as the software that may be installed legitimately to provide security or workplace monitoring, software with relatively benign purposes that may be associated with marketing data collection, and software that is maliciously installed, either as a general violation of a user's privacy or to collect information, to allow further attacks on their computer or online transactions (Victorian Electronic, 2005).

Without security, these kinds of threats can penetrate and potentially damage the information or compromise important data of an individual or organization. As a result, it can delay the conduct of business or even prevent it, thus significantly affecting the financial flow of businesses. In other words, threats derived from viruses, phishing, and spyware can result in financial setbacks. For example, Bielski (2005) asserts that the loss of government worker data and data leaks on the Bank of America in February and April 2005 resulted in a great loss of money.

The continuous emergence of new threats substantiates the inevitable need to utilize IT security. The nature of viruses, spyware, and phishing changes constantly, thereby preventing the company from settling on a certain security product. In fact, these security products need to be regularly updated in order to get rid of the new and emerging threats. Because of this, the fraudsters, malicious insiders, and hackers have become the top priority of some organizations and security vendors as well.

Additionally, the cost of IT security products is very high, such that the companies feel that they are being figuratively robbed by security companies. In one case, the spending of North American banks on IT security reached an estimated $1.8 billion in 2005, according to Celent Research (Bielski, 2005). Because of this, organizations, especially in the field of banking, have faced constant pressure to seek out better ways to secure data while continuing to deliver data and online services as most companies do, in an increasingly paperless way (Bielski, 2005). In some cases, companies are even seeking alternatives to expensive IT security products. They are now looking for some unconventional ways to protect valuable information.

User Preferences

The preferences of the user and customer, as well as their satisfaction level, are indispensable in the process of developing security products. In fact, the process of developing and then implementing security products lacks certain elements that pertain to customer preferences. In addition, developers fail to consider the compatibility of the solution to the employees (Andreas & Boone, 2002). Moreover, product developers do not usually take into consideration the organization's risk assessment (Alberts, 2003). David (2004) suggested that these problems also affect IT implementation because it becomes difficult when customer preferences are not met.

Information Technology Security Selection

The emergence of different security vendors allowed organizations to have a wide range of choices regarding a security product which is deemed suitable for the needs, demands, and nature of the company. Companies are able to choose among the security vendors whichever one they believe can best protect the information of the company.

For security selection for IT, the preferences of the user are still an inevitable consideration. According to Grance, Hash, Stevens, O'Neal, & Bartol (2003), frequent evaluation and selection of a variety of IT security services is a must in order to holistically improve IT security architecture, related to product development and implementation. This indicates that user preferences are a vital part of IT security selection among corporations, but it remains as a missing element with regard to security products (Grance et al., 2003).

Project Management

The role of the project management team is critical when it comes to addressing the missing elements of product development and implementation (David, Geoff, & Peter, 2004). Effective project management can carry on the development of IT security services namely, management services, operational services, and technical services (Grance et al., 2003).

Management services refer to the management of computer security program, including the risk within the organization. Operational services focuses on controls implementation and execution by people. Technical services refer to the security controls executed by a computer system. Thus, the project management team is left with the task to consider the customer preferences during the process of developing the products in order to complete the IT security services.

According to Stuckenbruck (1982), a project can be a single chance, time-limited, goal directed, a major undertaking, and requires the commitment of varied skills and resources. Project management is “a critical mechanism for capitalizing on entrepreneurial spirit and generating new products and services” (Gobeli, Gray, & Larson, 1991). The concept of project management, which actually came into being in the Post-World War II era (Frame, 2002), has only been recently given enough attention to produce systematic results for organizations. This was because new project management tools were needed in order to effectively implement projects.

There are three project management approaches: functional, project team, and matrix (Larson, 1987). The functional approach makes use of the functions of existing chains of command when completing a certain project that is divided into segments that have their own head of functional groups. The project team has semi-autonomous project teams that complete certain aspects of a project and are typically headed by a project manager. Finally, a matrix management approach imposes a project system within the functions of an organization where teams can have overlapping functions on other aspects of the project (Gobeli, 1991). These approaches can be used to develop IT security products, as this process involves project management.

Project management is essential for IT projects in order to reduce risks to the success of the project. Amongst many things, a project manager is responsible for identifying cost categories and expenditures, and the value of time in relation to a project. Thus, this makes project management an essential tool for IT projects. The high failure rate of IT projects has been recorded (David et al., 2004), and these failures may be attributable to project management (or lack thereof). The project manager, project teams, performance measurement systems and supporting management practices encompasses a successful project (Korin & Laura, 2004).

Statement of the Problem

This research proposes to evaluate the relative role of project management processes, project cost, project risks and end-users' acceptance in the success of IT security projects. This research is a case study of a single company and utilizes a mixed methods research approach in the form of interviews and surveys.

Significance of the Study

The significance of the study resides on the fact that security attacks and breaches do not come only from the outside, which is the stereotypical case, but also from the inside or within a corporation (Alberts & Dorofee, 2003). Thus, this indicates that security should cover both external and within the company information networks.

As mentioned earlier, a high failure rate of IT projects has been recorded and these failures may be due to the failure of project management (David et al., 2004). Korin & Laura (2004) argue that project managers, project teams, performance measurement systems and supporting management practices are all required for a successful project. Given the extent to which project management is given significant responsibilities on IT projects, the general question that this study will answer is whether project management increases the success of IT security projects. Although there is significant research on the importance of project management skills and IT projects, there are still many research problems and questions that remain unanswered in the area of IT security projects and the project team project management skills (David 2004).

This research is focused on the relationship between IT security team project management skill, the user's acceptance, and satisfaction level regarding the IT security project. From the research findings, organizations can identify how project management skills will help them to obtain a better end users' acceptance and satisfaction level.

Research Questions and Hypothesis

Fisher & Howell(2004) indicated that the failure rate of IT systems is almost 50 percent, but the failure should not be blamed on the system alone, but also on user acceptance of IT. Accordingly, IT acceptance models have gained significant attention. The user acceptance factor is a very significant part of creating information systems, and project management sometimes fails to consider this factor. This shortcoming of project management certainly affects the overall IT project outcome.

Based on the statement of the problem previously mentioned, these are the following research questions that shall be answered in this study:

1. Do project management processes improve the success rate of information security projects?

2. Does the cost of an information security project affect its successful implementation?

3. Do risks and perceived threats affect the success of information security projects?

4. Does the end user acceptance of information security solutions significantly affect the success of information security projects?

Accordingly, the study has the following hypotheses:

$H1_1$: The use of project management processes can significantly improve the success rates of information security projects.

$H1_0$: The use of project management processes cannot significantly improve the success rates of information security projects.

$H2_1$: The high cost of information security projects significantly affects information security project success.

$H2_0$: The high cost of information security projects does not affect information security project success.

$H3_1$: Perceived risk of information security threats significantly affects information security project success

$H3_0$: Perceived risk of information security threats does not significantly affect information security project success.

$H4_1$: The end user acceptance of information security solutions significantly affects the success of information security projects.

$H4_0$: The end user acceptance of information security solutions does not significantly affect the success of information security projects.

Research Purpose and Objectives

In an effort to improve the success rate of IT security projects, it is important to understand the real cause and effects of information technology security project failures. The purpose of this research is to study the relationship between IT security, project management skills, and the end-users' acceptance and satisfaction level with the IT security project.

The following objectives direct the research:

1. To determine whether the use of project management processes can improve the success rate of information security projects.

2. To identify whether the cost of information security projects affect its successful implementation.

3. To resolve whether the risk and perceived security threats affect the success of Information Security Projects.

4. To verify whether the end user acceptance of information security solutions affect the success of Information Security Projects.

Definition of Terms

Availability – when or how often an asset must be present or ready for use (Alberts, 2003).

Balanced Scorecard – the Balanced Scorecard is a carefully selected set of measures derived from an organization's strategy (Niven, 2002).

CERT – it is a center of Internet security expertise, located at the Software Engineering Institute (SEI), a federally funded research and development center operated by Carnegie Mellon University (Cert, 2007).

Confidentiality – the need to keep proprietary, sensitive, or personal information private and inaccessible to anyone who is not authorized to see it (Alberts, 2003).

Critical assets – critical assets are the information-related assets that are believed to be most important in meeting the missions of the organization (Alberts, 2003).

Integrity – the authenticity, accuracy, and completeness of an asset (Alberts, 2003).

Operationally Critical Threat, Asset, and Vulnerability Evaluation – a risk assessment methodology developed by Software Engineering Institute (SEI), also called OCTAVE Method (Alberts, 2003).

Qualitative – a research approach that the inquirer often makes knowledge claims based primarily on constructivist perspectives or advocacy/participatory perspectives or both (Creswell, 2003).

Quantitative – a research approach that the investigator primarily uses post positivist claims for developing knowledge, employs strategies of inquiry such as experiments and surveys, and collects data on predetermined instruments that yield statistical data (Creswell, 2003).

Risk assessment – a process to look at the security-related risks within a company, including internal and external sources of risk as well as electronic-based and people-based risks (Alberts, 2003).

SANS – the SysAdmin, Audit, Network, Security (SANS) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share the lessons they are learning and jointly find solutions to the challenges they face (SANS, 2007).

Script Kiddie – a technologically unsophisticated person who uses a “hacking kit” in order to break into the systems that may have vulnerabilities. Script kiddies rarely contribute new techniques, but simply use existing techniques, programs and scripts (Script Kiddie, 2007).

Six Sigma™ – an applied methodology for improving business and organizational performance (Gygi, DeCarlo, & Williams, 2005).

Vulnerabilities – the current technological weaknesses (technology vulnerabilities) in the key components of the computing infrastructure (Alberts, 2003).

Assumptions and Limitations

This research topic was selected to identify the relationship of the IT security team project management skill with the end-users’ satisfaction level of the outcome. The following assumptions are made:

1. Some individuals may not complete the survey, possibly creating bias in the collected data. Because of this, incomplete survey questionnaires will immediately be invalidated and will not be included in the analysis.

2. Individual participant survey will be confidential. In this way, the researcher will be able to ensure the full cooperation of the participants.

3. Participant industries will not be disclosed in this research. The tough competition in the market today brought about the strict security on any information disclosed by companies in the public.

The following limitations are important to consider:

1. Due to the confidentially nature of a targeted company, the information collected can be very limited.

2. The company may not elaborate on the information regarding the strategies which are being employed by the company in order to address security problems on information technology.

3. The security vendors being contracted were not disclosed.

4. The scope of this research is limited to the information technology department and/or a few others business units.

5. The participating company will limit the use of data that presents potential security concerns.

6. The survey will be limited to only one company, limiting the generalization of the results.

Research Methodology

The research design is exploratory and descriptive in nature. This research will utilize the mixed methods research approach, which will include qualitative and quantitative data analysis in the form of interviews and surveys. The descriptive method of research is appropriate to describe the nature of the existing situation in the business and IT world and the issues on security. Moreover, it explores the causes of particular phenomena or issues (London, 1997).

In order to answer the research questions, this research will be segmented into two phases. The first phase deals with the quantitative aspect of research. Survey questions will be asked regarding the relationship and effects between IT project management skills and the success rate of IT security project. The second phase consists of the qualitative aspect of research. Interviews will be conducted with project management experts and IT security experts to investigate significant factors that can affect the end-users' acceptance and satisfaction level.

Organization of the Remainder of the Study

First a discussion of the literature related to this research problem is discussed in Chapter 2. This research is based on various topics, such as IT end-users' acceptance model, project management best practices and quality assurance process, etc. Chapter 3 presents the research methodology to collect and analyze the requisite data. The three basic types of data sources are: (a) IT security team's skills profiles; (b) interviews; and (c) a survey that specifically focus in the human attributes, such as users' acceptance level and users' satisfaction level. Chapter 4 will show the results of the collected data and its analysis. Chapter 5 will interpret the results and suggests implications of the research and the conclusion.

CHAPTER 2. LITERATURE REVIEW

This chapter will set the foundation of the research study and establish relationships with the conceptual research framework of chapter 3. This chapter also explains the significance of different areas of literature that will be reviewed.

The first area of the literature review defines IT threats and the significance of IT security. The second area of the literature review tackles project management in general. It will also identify the effects and impacts of the project team’s skills profile, technology acceptance model, risk management model, and general users’ acceptance of IT security solutions and how these factors affect the success rate of IT security project.

Information Technology

Tansey (2002) defines information technology as the “systematic study of the industrial arts relating to the communication of instructive knowledge.” As such, this definition includes studying, printing, or, for that matter, smoke signals. However, according to Tansey the more acceptable definition describes IT as “the application of computers and telecommunications to the collection, processing, storage, and dissemination of voice, graphics, text, and numerical information.”

In the information economy, IT involves the combination of “cutting-edge technology,” ranging from laptops to fiber-optic and wireless communication, and their incorporation into the current structure of commerce. Consequently, business organizations invest large amounts of money in this technology because they perceive it as a productivity-enhancing mechanism. In fact, the idea of efficiency and productivity has gained popular support throughout the different sectors of the society (Diwan, Kudyba, & Mcginn, 2002).

On the part of businesses, IT is considered as a means to an end. In particular, this means that IT is the use of knowledge to make and implement commercial decisions. Efficient organizations would require established systems in order to allow them to make the best possible decisions in the situations they are likely to encounter. The table below is the list of the typical uses of computers in business (Tansey, 2002):

1. Storage and easy retrieval of information: databases
2. Analyzing information: spreadsheets, accounts packages
3. Internal communications (within business): networks
4. External communications (with other businesses and customers): e-mail, booking systems, etc.
5. Presentation of information: word processing and desktop publishing.
6. Computer-aided design (CAD)
7. Computer-aided manufacture (CAM): robots, process control
8. New and better products: video recorders, washing machines, etc.

The utilization of IT, especially in the realm of business and commerce, resulted in great changes in the way organizations conduct their business operations. The same is true with the way individuals carry out their day-to-day activities or affairs. As a matter of fact, it can be said that the integration of IT, to commerce in particular and society in general, can be considered as the highlight and turning point of the modern age of information.

According to Diwan, Kudyba and Mcginn (2002), the introduction of the various forms of IT has significantly altered the pace and character of production and consumption from the structure that prevailed only a few decades ago. The introduction of increased processing power of hardware, along with complementary software and telecommunications infrastructure, facilitated the enhanced ability to store, retrieve, analyze, and communicate data and information within organizations, between organizations and their partners and suppliers, and, finally, to the ultimate consumer.

Bill Gates provided this assessment on the information age:

> “Well, it really changes the nature of how you think about a computer. Twenty years ago, it was mostly for tracking large databases. And so your tax departments, banks, airlines would have one very, very expensive computer with lots of people taking care of it to manage centralized information. As the price came down, it became much more of a personal thing. Individuals could own their own computers, create documents, and look at different what-if scenarios through a spreadsheet. Now, with those computers being connected together, we have the most powerful communications medium of all time.” (Diwan et al., 2002)

Undeniably, the proliferation of IT throughout all sectors of the economy paved the way for the emergence of different terminologies like the “information age” and the “information economy.” These terminologies have become a common form of verbiage as evidenced by their propagation in various forms of publications, such as the textbooks, magazines, newspapers, non-print media, class-rooms, conference rooms, and throughout society in general. Nevertheless, in spite of the proliferation of the terms, the concept still remains to be a complex and dynamic phenomenon that may be difficult to fully and clearly comprehend (Diwan et al., 2002).

IT Significance

IT is deemed significant not only to organizations, but to individuals as well. Primarily, IT benefits the organization by serving as the medium for conducting the regular activities or operations of the company. On the other hand, it also benefits the individuals since the services and products developed by organizations are dedicated to the consumer or the individuals.

Recent innovations in various forms of IT have resulted in its vast utilization by both consumers and corporate enterprises (Diwan et al., 2002). Evidently, both of the key players in society, as well as the economy, benefited with the coming of IT. More profits are gained through the utilization of IT, and at the same time there is an easier conduct of activities in our everyday life. With this, IT has become even more demanding in the life of every individual and in the success of every organization. In other words, information technology is already interwoven with practically every activity of the society.

Meanwhile, the benefits of IT are specifically evident at the macroeconomic level. The IT revolution has triggered the development of various economies of different countries. In particular, the effects of IT revolution have occurred in three main stages. First, technological change raises productivity growth in the innovating sector. Secondly, falling prices encourage capital deepening. Lastly, there can be significant reorganization of production around the capital goods that embody the new technology (World Economic, 2001).

IT Threats

IT threats are far more complicated than threats in the physical world due to the fact that cyberspace is not easily monitored. It is easier to catch bank robbers than to arrest cyber hackers. The Glory (1997) study indicates that the chances of catching a bank robber who steals $85 per holdup is 80 percent, while the chances of catching a single cyber attack costing an average of $800,000 is only 2 percent.

This study provides certain information on the stress caused by IT threats and the difficulty of arresting cyber hackers. This information includes the actions taken by corporations regarding the issue of IT threats together with cooperation between government and business on addressing these threats. The study is significant to this research since it undertakes an investigation on cyberspace in general and, specifically, in solving the issue of IT threats that can be meaningful in this research.

Halachmi (1992) contends that IT influences new devices (i.e., computers) for handling, entering, retrieving, and manipulating data. Thus, IT threats primarily involve stealing and manipulating data as the hacker sees fit. Halachmi’s study provides details on the effects of IT threats on management practices within an organization. The study is relatively significant; as it points out the threats coming from inside the organization as IT is employed. Thus, Halachmi provides necessary information on the effect of threats within an organization.

In line with the influence of IT on devices that handle information, IT threats are carried on, as Halachmi (1992) indicates, with the development accompanied by IT. IT threats are computer-related fraud, computer forgery, damage to computer data or programs, unauthorized access to restricted data, unauthorized interception to restricted data, unauthorized reproduction of a protected computer program, and so on (Hannaford, 1995).

The aforementioned IT threats are all carried on by computer devices - the same devices that handle information. Thus, IT threats are essentially critical since information is intangible, yet one of the most valuable assets in any business. Hannaford (1995) also provides insight on how technology threats affect the integrity of IT. Today's reliance on IT is inevitable in every aspect of human activity, especially in businesses. Hannaford gives an account of the actions taken against IT threats, such as signing laws against cyber hackers in Canada. Hannaford's study is related to this research, as it can aid in gathering certain firsthand details on IT threats and security.

Andress (2003) presents the three most common type of attacks on IT. These are the Denial of Service (DoS), intrusion, and information theft. The DoS is aimed at depriving an organization of a resource it expects to be able to use. The different types of DoS are the butterfly overflows, SYN attack, and the teardrop attack. Intrusion, on the other hand, is the attack that targets and exploits the vulnerabilities of the specific server. Lastly, information theft is almost the same as intrusion, in that it tends to penetrate and destroy the information asset of the victim. In fact, information theft attacks are often the first step in an intrusion attack.

The different types of attackers can be categorized into hackers, crackers, script kiddies, malicious insiders, and industrial spies. These attackers have different motivations in carrying out the attacks. Some attack the system just for fun, while others have malicious intent. Also, the capability of the attackers varies. Some are extremely knowledgeable, while other attackers just run scripts which are written by others (Andress, 2003).

The prevalence of Internet threats has resulted in great damage to companies and individuals. This is especially seen in the financial losses or setbacks experienced by organizations and individuals.

The failure of companies to develop an effective IT security gravely affects the rate of success which can be acquired by organizations. The attacks mentioned above are only few of the possible threats brought about by the utilization of information technology (Andress, 2003).

IT Security

In response to IT threats, studies are also reviewed regarding the IT security and its significance. Since large enterprises rely on IT to operate, any access and threat to the infrastructure can significantly impact the company. Any downtime caused by cyber attacks may cost the company millions in revenue.

When discussing IT security, there are two questions that need to be addressed: What is IT security and what exactly is being secured?

According to Quinn (2002), IT security refers to the protection of information that can be otherwise abused by anyone who can access information technology systems. The study provides certain information regarding how IT security can be developed, which can help this research identify what IT security needs to address. Regarding what is being secured, Anhal, Daman, O'Brien, & Rathmell (2003) stated that IT security secures information within a company. In other words, security is about information assurance, which means that information within the organization is reliable, secure, and private.

Even with the introduction of the first computer, the need for security existed. This is because of the valuable information stored on the computer. Through this technology, the ways of processing data such as storing, retrieving, and analyzing it has become much easier. Because of this, information has become vulnerable to security issues.

Protecting a system was never an issue until the paradigm shifted to client/server technology, which paved the way for countless new security problems. Processor utilization was not a priority, but access to networks, systems, and files grew in importance. Access control became a priority since the sensitive information was being stored on public file servers. Among this sensitive information are the human resources and payroll files. Obviously, companies did not want this kind of information to be revealed to the public or to be made inaccurate. So, new technologies were developed, such as the granular access control, single sign-on, and data encryption. Moreover, various methods of circumventing and exploiting these new applications and security products quickly arose (Andress, 2003).

With this, one can see that the advancement of IT significantly influences the new devices for handling, manipulating, retrieving and entering data. The changes in IT should also be followed by a corresponding change in structure and management practices. And with the emergence of new technologies, issues of security as well as safety are highly influenced (Halachmi, 1992).

Certainly, security has been an important component of IT even from the beginning. More importantly, the importance of security has become even more demanding nowadays. Security has played a vital role in ensuring the success of various organizations and individuals. In other words, the present-day need for security in the field of IT can be equated to the triumph of the company or an individual. On the other hand, the inability of organizations to have an effective IT security is can cost a lot of damage or setbacks, and even failure of the company.

The Computer Security Institute in San Francisco revealed in their survey the extent of security issues and problems experienced by individuals and organizations. Below are the highlights of their 2002 survey entitled ‘Computer Crime and Security Survey’ (Andress, 2003).

According to Andress, “Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last 12 months. Seventy percent reported a variety of serious computer security breaches other than the most common ones of computer viruses, laptop theft, or employee “Net abuse”-for example, theft of proprietary information, financial fraud, and system penetration from outsiders, denial-of-service attacks, and sabotage of data or networks. Eighty percent acknowledged financial losses were due to computer breaches.

Forty-four percent were willing and/or able to quantify their financial losses. The losses from these 223 respondents totaled $455,848,000.

As in previous years, the most serious financial losses of 2002 occurred through theft of proprietary information (26 respondents reported $170,827,000) and financial fraud (25 respondents reported $115,753,000).

For the fifth year in a row, more respondents (74 percent) cited their Internet connection as a frequent point of attack than those who cited their internal systems as a frequent point of attack (33 percent). Thirty-four percent reported the intrusions to law enforcement. In 1996, only 16 percent acknowledged reporting intrusions to law enforcement.)”

The survey demonstrates that even with information technology security, one is still not assured of being safe from various IT threats. The recurrence of different forms of attacks is one of the looming problems of security on IT. This is evident in the rate of respondents who agree that computer security breaches are always detected on their systems. And among the variety of major computer security breaches are the computer viruses, laptop theft and employee net abuse.

IT Security Solutions

According to Andress (2003), security is not a single solution. Rather, it is a pervasive, ongoing process of reviewing and revising based on changes to the business and corporate environment. Moreover, security is considered as the culmination of the interaction between people, process, and technology. In other words, Andress implies that security is not a product but a process. It is not something that you can “get” in order to build an effective security infrastructure; it requires an analysis, as well as planning along with the development of policies and procedures. Also, it will need a little help from security products.

One way of addressing the security issues with respect to IT is through the security policy manual. Boyce (1996) states that the largest contributor to information loss is insufficient internal security policies. The case for organizations is that they do not have a well-coordinated information security policy most of the time. As a result, the issues of IT security are not always prioritized and, oftentimes, they are set aside. Companies became increasingly alarmed with IT security due to the rise of threats to information assets ranging from industrial espionage to malicious hackers. From then on, various companies began to re-evaluate their information security policies and decided to develop a detailed IT security manual.

More specifically, the proposed security manual of Boyce (1996) consists of several components. These components are perceived to be indispensable in ensuring the security of IT in the company. For instance, the primary component of the manual is the process of “instilling ownership” among employees. Specifically, the drafting committee included representatives from each department in the organization. Giving all departments a voice not only promotes consensus, but also instills a sense of ownership among employees.

The other components of the IT security manual include the duties of the employees in general and the IT department in particular, including physical security, fire and water (prevention, detection, and control procedures for fire and water damage) mediation, access control, asset control, software security, data security, access rights, distribution, viruses, encryption, monitoring phones, configuring networks, encrypting faxes and implementation.

Undeniably, the use of a policy manual for IT security is also beneficial in addressing the problems, as well as issues that arise from the security of information/data in an organization. Through the policy manual, organizations are able to implement effective rules and regulations regarding the security of IT in the company. More importantly, the manual serves as a guideline or a basis in making decisions that are related to the threat in IT security.

Andress (2003) agrees by confirming that it is the policies that form the foundation of an organization’s security infrastructure. It is through policies that organizations are able to define company approaches; employees are able to handle security; and the ability to address certain situations is established. Indeed, a security infrastructure is only realized through the strong policies being implemented by the company, which are reviewed on a regular basis.

IT Projects

To better understand IT security, IT projects needs to be explored. IT in this study pertains to its use in businesses. Tansey (2002) investigated the impact of IT in the modern world. The study gives general background on the history of IT projects. IT projects were primarily initiated as defense-related projects for the Army, which included developments in computer technology. Eventually, IT projects were established to make life easier for society. Thus, when IT was commercialized, it was defined as “the application of computers and telecommunications to the collection, processing, storage, and dissemination of voice, graphics, text, and numerical information" (Flowers, 1988).

Accordingly, IT projects are known as the projects using IT to gain competitive advantage. Tansey (2002) indicates that successful IT projects require careful planning not only on the technical side, but also from the human aspect, which basically pertains to project management. Thus, Tansey's study is relevant to this study as it tackles, in general, the effectiveness of IT projects. It is also important for providing details on successfully developing and implementing IT projects to acquire a competitive advantage, which can also cover IT security projects.

IT has certainly accumulated a lofty role in businesses; it is now included in the overall business planning, with IT projects essential in the overall operation of businesses, especially major corporations. A study by Bloomfield, Coombs, Knights, & Littler (2000) indicates the position of IT on businesses. Today's corporations have an IT Committee to plan and manage IT projects and other IT-related activities. IT projects, in this sense, become an integral part of business - including IT projects and, inevitably, IT security projects.

Corporations need to protect company information, which is what IT security projects are all about: protecting necessary information that, when abused, can threaten or destroy a business. Tansey (2002) provides the necessary information on how IT projects affect business and also the significance of IT projects on the overall operation of business. The study is important in this research since it can provide information on the importance of impact on IT projects.

IT Security Projects

IT security projects refer to projects that intend to protect information within an organization. Security projects are different from other IT projects due to their focus on information security. According to Charp (2003), IT security projects include the development and implementation of security applications, such as firewalls (81 percent), antivirus software (79 percent), or using virus protection access management and other security applications (71 percent). Unfortunately, IT security projects are only temporarily successful because new portal of threats are developed regularly.

Charp (2003) identifies the problems with IT security projects that include the continuous development of IT threats, such as computer viruses. IT security projects fail to address the need to secure employees' computer usage, which may open the organization's system to attacks. The problems of IT security projects are also explained in the organization behavior section that follows.

Organizational Behavior

Another focal point of project management is to understand the effects and impacts on employees or general users of IT security deployments. As Maris & Patrick (1999) state, "An effective information system (IS) consists of the right information technology application to help the right people perform the right process". Maris & Patrick further stated that the "human" element has become the most critical factor of any successful IT/IS environment. The study also indicates the role that the human aspect has on successful IT projects.

IT is not a one-man show; it requires the cooperation of human resources for a competitive advantage to be achieved. Thus, IT has certain impacts such as those on employee's culture and philosophy: Some employees may be reluctant to use or are intimidated by IT devices. This organizational behavior is tackled by Maris & Patrick (1999). The study is a significant contribution to this research since it tackles the human aspect of IT projects, which is the core of project management as project management involves the human aspect.

The study of the effects of any IT project on general users is important to the IT security project. The development of a research model of the relationship between IT, people, and business is becoming an essential element of IT security project deployment (Boynton, Zmud, & Jacobs, 1994).

Boynton et al. (1994) provides quantitative information on the effectiveness and impact of IT projects on employees. This also relates to organizational behavior, since the effectiveness of IT projects relies greatly on its impact on users. Employees or the users of IT solutions must be able to rate their experience positively - if not, the project is a failure.

Boynton et al.'s study provides information on the issue of IT project user compatibility and its importance to business success. The study is significantly related to this research, as it contains firsthand information on the connections between IT and organizational behavior. Organizational behavior is an important factor to consider in developing IT security projects since it is also aimed at protecting information from forces within the organization.

According to Watkins (1998), IT has definitive effects on users, especially on the organization as a whole, as it provides investigation regarding the effect of IT on people and organizations. Watkins further states that the initial effect of IT on organizations is the drive for structure transformation. This includes overall behavior of people within an organization to make way for IT. The study also suggests that structural transformation brought about by IT has a significant effect on the behavior of people within an organization. Thus, the study can aid this research in identifying the human element of IT security projects, and how project management can consider organizational issues on developing and implementing IT security projects.

Technology Acceptance Model (TAM)

One way of identifying the effectiveness of IT security projects is through the technology acceptance model, or TAM. As Gao (2005) asserts, the user's attitude and the actual usage of a technology are addressed in the TAM. In other words, the technology acceptance model is used to predict the user acceptance of a technology before they even get heavily involved with the technology. As a result, the model can be considered as a cost-effective tool in the process of screening the potential candidate systems or programs.

Basically, the technology acceptance model is embedded in the Theory of Reasoned Actions (TRA). More specifically, this theory is aligned with psychology research. This model states that the perceived ease of use and perceived usefulness of technology are predictors of user attitude toward using the technology, subsequent behavioral intentions, and actual usage. As such, this perceived ease of use significantly influences the perceived usefulness of technology (Gao, 2005).

Risk Management

A risk-management program includes the techniques and methodologies currently available to help identify IT threats and to effectively manage these threats through. Many executives believe that information technology risk management is critical to a company - but not all executives utilize risk-management programs to reduce their risks.

Risk management is about dealing with risks faced by people. Since the world is an unpredictable place, one needs to deal with risks and/or uncertainties. And as long as there is some uncertainty about the future, the world will continue to be a place where risk must be managed. And in modern times, there is a greater need for risk management because the world is perceived to have become a more risky environment.

Risk is predominantly present in health and safety, and in finance. People, especially the American society (in spite of being the wealthiest and richest in the world) are still considered to be the most seemingly risk-averse and are even more so within the context of finance, as many contend that the world has become more dangerous (Culp, 2001).

According to Culp (2001), it is change that often creates new risks. Since change is a constant phenomenon, one cannot really avoid risks. Development or progress is accompanied by risks. In fact, progress without risk is not just paradoxical, but also futile. In line with this, there are three common fallacies about risk. First, the perception that risk is always bad. Second, some risks are so bad that they must be eliminated at all costs. And third is the belief that “playing it safe” is the safest thing to do.

Risk Management in IT

In the case of IT, risk management is mostly directed to computer security. Through the risk management, it tends to understand the threats and vulnerabilities of automated information systems. In fact, it’s a lifeline for embattled physical security professionals as it demonstrates that it is possible to manage the security of information systems without a strong computer background (Johnson, 2005).

A study shows that 84 percent of executives agree that IT is a critical element to their business, but only 13 percent believe that their risk management program is aligned with its business objectives, and only 33 percent believe that IT related risks are well defined and understood by their companies (Louisa, 1998).

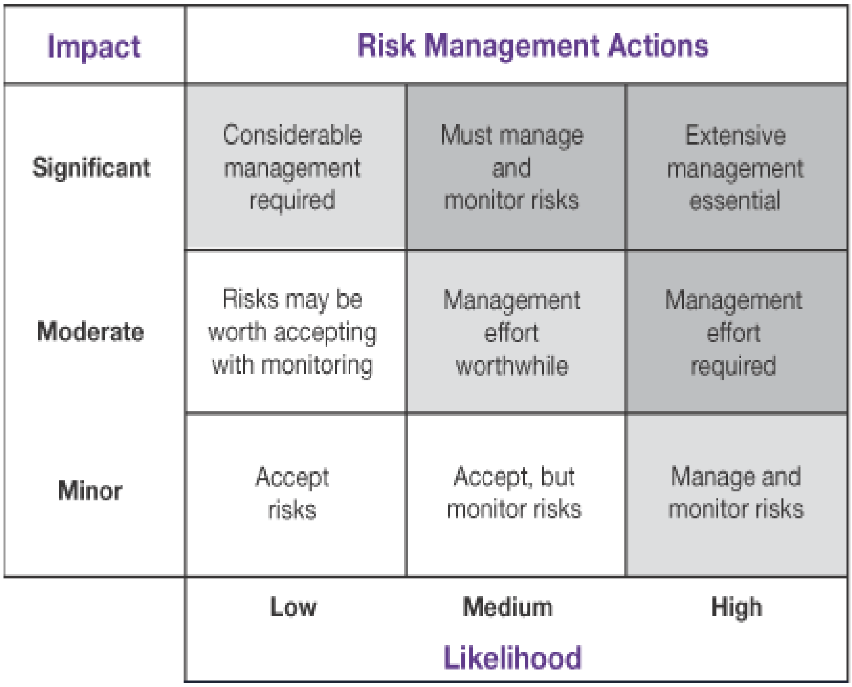
Louisa (1998) further provides information on the difficulty of managing IT risks, including IT security. Cyber hackers can hack complicated systems containing critical information, making IT security a critical part of IT risk management. This is significantly relevant to this study since it gives details on the implementation of IT and how risks, such as IT threats, can be handled.

Risk Management Model

In order to address various risks, there is a need for individuals to recognize that the risky changes are beneficial. With this, one begins to develop a framework for managing risks responsibly. And so, a healthy and responsible framework is the one that neither lends itself to over caution nor to carelessness. In addition, this framework tends to avoid the three basic fallacies: that risk is always bad; that some risks are so bad that they must be eliminated at all costs; and that playing it safe is the safest thing to do (Culp, 2001).

In managing risk at a technical level, one can use various tools and techniques. Among these are the risk maps modeling tools, framework on the precautionary approach, qualitative techniques, and Internet and organizational intranets. With this, the figure 1 below shows an example of a risk management model. In the model below, it enables the organizations to assess where a particular risk falls in terms of likelihood as well as impact. Also, it establishes the strategy and response of organizations to manage risk (Secretariat, 2001).

A Risk Management Model



Impact	Risk Management Actions		
Significant	Considerable management required	Must manage and monitor risks	Extensive management essential
Moderate	Risks may be worth accepting with monitoring	Management effort worthwhile	Management effort required
Minor	Accept risks	Accept, but monitor risks	Manage and monitor risks
	Low	Medium	High
	Likelihood		

Figure 1. A Risk Management Model.
From *Treasury Board of Canada*, 2001. Retrieved August 21, 2007, from http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/rmf-cgr01-1_e.asp

Project Management

This study’s concept of project management is defined by Reiss (1995) as follows: “Project management is a collection of loosely connected techniques, some of which are useful in bringing projects to a successful conclusion.”

More importantly, project management serves as a way of reducing risks, capturing the total cost of the project, enhancing quality and managing the time elements and resource constraints, and increasing the likelihood of meeting target dates. In addition, project management also enables the managers to focus on other critical success factors of the company such as the vendor capability (Crandall & Murray, 2006).

In the modern world, the new project management is suitable in most all fields of industry. Project management is utilized by various individuals in different fields who struggle to manage projects in a chaotic world. From conventional projects in construction or the defense industry or pursuing Information Age projects in such areas as information systems, finance, research and development, marketing, pharmaceuticals, or insurance, various individuals have discovered the conventional wisdom present in project management. Undeniably, project management has surpassed the capacities found in mastering schedule techniques such as the Program (or Project) Evaluation and Review Technique (PERT), budgeting techniques such S-curves, or even the resource allocation techniques like the resource histograms (Frame, 2002).

Accordingly, project management encompasses planning and implementation. Reiss (1995) also states that project management is the management of change. IT security projects are required to address changes in cyberspace that threaten an organization’s IT systems but, most importantly, changes that are more evident on the system users. Thus, implementation of IT security projects becomes difficult due to the attitude of employees toward change.

According to Frame (2002), project management is critical in IT projects, which is why project managers undergo professional advancements, such as passing the Project Management Institute (PMI) certification process. Project management in IT security projects is not usually employed because it is only a branch of an overall IT project (Frame, 2002). In this sense, certified Project Management Professionals (PMPs) may not even be hired to manage IT security projects.

The Frame (2002) study investigates the necessity of professional project managers, which can aid this study in identifying the need for project management in IT security projects. Frame also discusses the importance of Capability Maturity Model Integration (CMMI), a tool that assesses the quality of IT operations. This helps project managers review the adequacy of an organization’s process.

Risk Assessment Project Effectiveness Metric and Quality Assurance

To understand the effectiveness of given IT security deployment project, it is beneficial to study how effectiveness is measured, as it is a primary element on the overall success of a project. According to Niven (2002), a measurable metric is needed to “score” the project. The Balanced Scorecard can be an effective model to capture, describe, and translate intangible assets into real values that are understandable by all the stakeholders of the security project. At the same time, the Balanced Scorecard will generate a “report card” at each milestone and at the end of the security deployment project.

With a measurable metric, the project team and the stakeholders can more easily communicate using a common language - a common language that generates effective communication needed for the success of any project. Niven’s (2002) study is significant for understanding how IT projects are rated in order to identify the role of project management in an IT security project’s success.

Accordingly, another critical element of an IT security project is a quality assurance standard. One of the industrial standards for quality assurance is Six Sigma^{SM}. The five phases of Six Sigma are Define, Measure, Analyze, Improve, and Control (George, Rowlands, Price, & Maxey, 2005). The Six Sigma is the global standard of quality business practices (Gygi, 2005). The Six Sigma concept can possibly be integrated into security project phases in conjunction with a Balanced Scorecard to ensure a successful outcome of any IT security project.

Six Sigma is a management concept that started in the 1980s. It was first used by Motorola$^{®}$ in order to improve the quality of the work. This is done through statistical measurement and benchmarking (Donnelly, 2006). However, others have argued that Six Sigma was already practiced even as early as early as 1798, and it was only in the 1980s that it became popular and widely recognized.

Six Sigma is a business concept that answers customers demand for high quality and defect-free business processes. Customer satisfaction and its improvement should be the highest priorities of any business. In other words, Six Sigma is about abandoning the uncertainty of goals and forecasts" (Pande, Neuman, & Cavanagh, 2000). It is a high performance data driven approach for analyzing the root causes of business processes and problems and then solving them. "The real challenge with Six Sigma is not the statistics; it is getting to the point where one can meaningfully measure a business's current performance against dynamic customer requirements while developing the internal abilities to respond to changing market place conditions" (Haubner, 2004).

Today, this management approach is more commonly associated with the drive for improved productivity and profits. In fact, world-class organizations and companies are mostly employing the Six Sigma management concept. Indeed, Six Sigma proves to be the most popular quality improvement methodology in history (Eckes, 2001). For instance, the IT organization of the Raytheon Aircraft saved almost $500,000 from a single project back in 2002. In addition, the Textron Company also utilized this approach and saved $5 million within six months. Moreover, at the Fidelity Wide Processing, the targeted cost reduction is expected at $6 –to-$8 million (Mayor, 2004).

Literature Review Summary

Related literature provides necessary information on IT and specifically, on IT projects with focus on IT security projects, IT implementation and its effect on organizations and, lastly, the role of IT projects in business. Addressing the threats to IT proves to be an essential element in business planning since information theft can irreparably damage a company. Common threats are usually computer generated or done within the boundary of cyberspace which, by its very nature, is unidentifiable. This makes IT theft far more problematic than the usual theft.

In response to the threat, IT security projects were established with the primary intention of protecting information from both outside and within the organization. Thus, IT security projects are a significant part of business planning, as they solve the issue of information theft that drastically affects any organization. The literature reviewed can provide necessary information on the subject of IT threats and security.

The reviewed literature also helps shape this research on project management and its connection with IT security projects. Risk management, organizational behavior, and performance measure are also discussed. Studies indicate that IT security projects are contained in the risk management of organizations since IT threats are considered risks that a company must manage as it employs IT. In other words, the literature on risk management provides information on how risks are managed, including IT threats, which must be considered in any IT security project.

It is undisputed that IT affects people and, most importantly, the people within organizations - or in a much clearer sense, the users. The literature reviewed also indicates that the human factor is essential with respect to IT projects, as people are the ones who rate the projects. This indicates how important organizational behavior is for IT projects. Moreover, this implies that organizational behavior is a considerable factor in project management since it deals with people. This also proves that IT security projects need project management, inherent in the fact that organizational behavior will affect IT projects.

Finally, the literature reviewed also includes information on studies that measure IT effectiveness, providing information that this research needs in identifying the success of IT security projects. Moreover, this is also connected with the methodology that will be used in this research.

Through the review of related literature, the researcher was able to determine the position of project management in IT security projects. Consequently, there are hardly any studies that pertain to the relationship between the project management and IT security. As such, this study would be beneficial in enlightening society, especially the organizations, regarding the effects of project management on IT security projects.

CHAPTER 3. METHODOLOGY

The methods of data collection are growing, and they increasingly involve active participation and sensitivity to the participants in the study (Creswell, 2003). “Qualitative research uses multiple methods that are interactive and humanistic” (Creswell, 2003, p.56). Quantitative research will provide hard data to confirm and categorize the collected data.

This research will be a case study of a single company and will utilize mixed methods: quantitative and qualitative. Surveys will be sent to the employees of the company for the quantitative portion of the study. Interviews will be conducted also for the selected IT employees within the company for the qualitative portion of the study. The IT employees will be purposely selected by determining their background on the area of IT.

Before the actual conduct of the survey and the interview, the researcher will conduct a pilot study in order to determine the validity as well as reliability of the chosen data gathering tools. More specifically, the pilot study will consist of several respondents. For the interview, one (1) manager will be utilized as a participant of the pilot study. In the case of the survey, there will be twenty (20) employees which will be needed to participate.

Before the survey was conducted, the researcher informed the respondents that the filling up of the questionnaire is voluntary. In short, they are not obliged to answer the different items in the survey questionnaire if they believed that it is not relevant to them and to the study.

Primarily, the research methodology will be presented in three parts. First, the dependent variable is discussed. Second, the research methodology for the quantitative measures of the variables is presented. This is also followed by the qualitative aspects of the research. Lastly, a discussion is held regarding the integration of these two approaches in order to achieve the final analysis.

Dependent Variable

The dependent variable for the two phases of the study is the effectiveness of IT security solutions as viewed by the participants. Hard data on actual security breaches will also be included when it is not confidential in nature and therefore not available for the study.

The data for the dependent variable will be collected through the qualitative and quantitative methods, which are the survey and the interview respectively. In this way, the researcher will be able to gather directly the views from the participants of the study regarding the effectiveness of IT security solutions. It is deemed that the answers of the participants will significantly affect the condition or the value of the dependent variable.

Quantitative Variables

Quantitative surveys can certainly expose measurable facts for the researcher and reliability, validity, and generalization of the results can be enhanced by obtaining uninfluenced answers from respondents (Creswell, 2003).

Sample and Population: Quantitative

The study shall administer a survey on a company deploying IT security solutions with an approximate population of 1000-3000 employees. The survey shall determine the effectiveness of IT solutions within the company. The sample size that can represent the population of the organization will be two hundred (200) respondents. This is based on the sample size calculator of the survey system (Creative Research Systems, 2003).

Design of the Study: Quantitative

Prior research has indicated that the respondent’s demographic profile generally affects their answers to surveys (Brockhaus, 1986), thus demographic variables are included to identify specifically the influences of personal issues on their answers. The demographic variables used in this study are age, gender and the number of years of service in the company. The backgrounds of the participants are perceived to play a vital role in shaping the trends of the results of the study. Other independent variables relate to “knowledge on information technology” and the “confidence on information technology solutions” variables. These can indicate whether some respondent’s answers are affected by their preconceived ideas of IT and are listed below.

1. General view on information technology. This indicates the basic view of the respondents on information technology, whether or not they favor it.

2. IT threats. This indicates the view of respondents on IT threats especially on its effect on the organization’s operation.

3. IT security. This indicates the view on the general IT security concept, whether or not they perceive it as a solution to IT threats.

4. IT security projects. This indicates the view on the company’s IT security project planning, development, and implementation.

Instrumentation: Quantitative

The survey questionnaire can be found in Appendix A. It will be administered to a sample size of 200 employees. Respondents will be randomly selected in order to ensure the impartial selection of the participants of the study. In this way also, the researcher can assure the validity of the outcome of the survey.

The survey questionnaire will consist of two parts. The first part of the survey questionnaire would delve into the demographic profile of the respondents. Participants' characteristics such as age, gender and the number of years in the company will be asked. The personal profile of the respondents is necessary information for the study because it influences the kind of response given by the participants. In other words, the outcome of the survey can be partially explained through the demographic profile of the respondents.

The second part of the survey includes participant identification of the different issues that significantly affects the success of information security projects. With this, it will tackle project management processes, project risks and user acceptance.

Data Collection: Quantitative

Surveys will be sent to IT employees in the company for the quantitative portion of the study. Interviews will be conducted from selected managers and other IT employees within the company for the qualitative portion of the study. A selected portion of the company shall be subject to answer the survey while the respondents are randomly chosen, which means that everyone in the selected population has an equal chance of being selected.

Data Analysis: Quantitative

Statistical tools will be used to process the control and predictor variable data derived from the survey and their relationship to the dependent variables. The predictor variable data is collected using a five-point Likert scale. Before processing it, the responses will be quantified using the weighted mean. The weighted mean was computed as Figure 2:

Weighted Mean Computing

$$x = \frac{f_1x_1 + f_2x_2 + f_3x_3 + f_4x_4 + f_5x_5}{x_t}$$

where: f – weight given to each response

x – number of responses

x_t – total number of responses

Figure 2. Weighted Mean Computing.

Table 1 will show the equivalent weights for the responses:

Table 1. Equivalent Weights for the Responses

Range	Interpretation
4.50 – 5.00	Strongly
3.50 – 4.49	Agree
2.50 – 3.49	Undecided
1.50 – 2.49	Disagree
0.00 – 1.49	Strongly Disagree

Qualitative Variables

Currently, most security assessments are more directed toward qualitative approach, such as Operationally Critical Threat, Asset, Vulnerability and Evaluation (OCTAVE). OCTAVE stated that an organization should take the ownership of its security and it should involve everyone within the organization to ensure minimization of IT related risks (Alberts, 2003).

Description of Methodology: Qualitative

The qualitative data analysis will consist of personal interviews. More specifically, the interviews shall generate the qualitative data regarding the connection between project management and its security project success. The general sample size for the interview will be five IT employees within the company. The survey will be conducted first and will be followed by the interview.

Overall, there will be five IT employees who will be interviewed. This number is deemed to represent the principles and advocacies of the company since the employees who will be interviewed are those familiar enough with the processes of the company in relation to the security in information management. And so, unlike in survey, the interviews will stress the quality of the responses given by the participants.

Design of the Study: Qualitative

First, the qualitative research involves a critical assessment of literature regarding the subject of IT security and project management in the business area, and also the critical assessment of the interview results. A primary activity of this research is to accumulate the necessary information on the background of the study and the concepts that can support the quantitative information. Secondly, interviews shall be conducted that shall also yield significant information regarding the topic.

Sample and Population: Qualitative

Five IT employees within the company, who are knowledgeable on information technology, shall be interviewed regarding possible outcomes of the project management on IT security projects. The participants who will be interviewed will be purposely selected to ensure that the participants have enough knowledge on the subject of the study, vis-à-vis the activities of the company. The researcher will choose participants who are directly involved with the company's IT operations. . There are no particular job positions or titles which will be the basis of choosing the participants although participants will likely be a network officer, IT specialist, information security officer, computer analyst or manager.

The interview shall consist of semi-structured questionnaire. Questionnaire and interview methods are both valid and reliable instruments for conducting this research (Saunders, 2003). A semi-structured questionnaire (see APPENDIX B) shall be employed in order to control the information given by the interviewee. The Input-Process-Output model shall be the instrument on presenting the data. The Input-Process-Output model represents the survey (input), data analysis (process), and the conclusion (output).

Instrumentation: Qualitative

Clerical tools shall be used as instruments in this research. The basic topic that shall be discussed is IT. Accordingly, IT's issue on security shall discuss with management. Then, they shall be asked about the effectiveness and shortcomings of IT security project solutions. The other branch is the discussion on the viability of project management, including its relation to IT security projects, and its possible outcome when employed within IT security projects, and its possible relation or effect to the success of IT security projects. Figure 3 shows the structure of the interview that shall be conducted:

Interview Structure

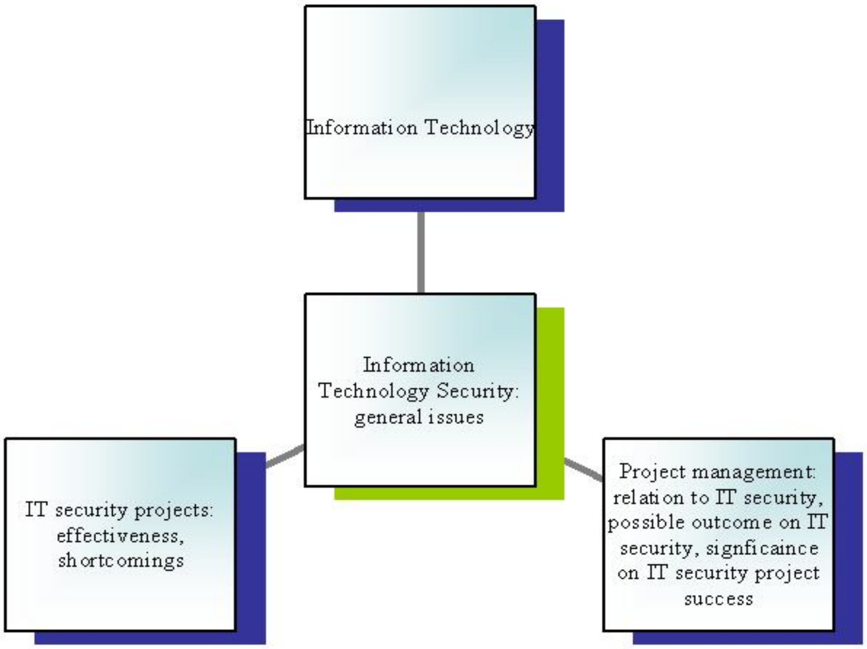

Information Technology
Information Technology Security: general issues
IT security projects: effectiveness, shortcomings
Project management: relation to IT security, possible outcome on IT security, signficaince on IT security project success

Figure 3. Interview Structure.

Data Collection: Qualitative

As mentioned earlier, interviews will be conducted to collect qualitative data for the study. The researcher will personally conduct the interview among the selected employees of various companies. The respondents are not randomly selected to yield particularly knowledgeable individuals.

Data Analysis: Qualitative

Content analysis shall be the method of analysis for the interview. This includes the identification of common answers of the interviewee and then critically examining the comparisons and contrast of views. Since the design is a case study, all the analysis of both quantitative and qualitative data shall be presented to prove that there are no biases in the analysis.

Secondary Qualitative Data

Aside from the interviews, other qualitative data will be derived from the literature review. The information collected through the review of related literature is deemed indispensable in the study because it can consolidate the data acquired through the interviews, as well as surveys.

Quantitative and Qualitative Integration

The quantitative and qualitative data will be utilized to evaluate the hypothesis. The diagram in Figure 4 summarizes how the data shall be analyzed in the case study.

Integration of Quantitative and Qualitative Aspects of Study

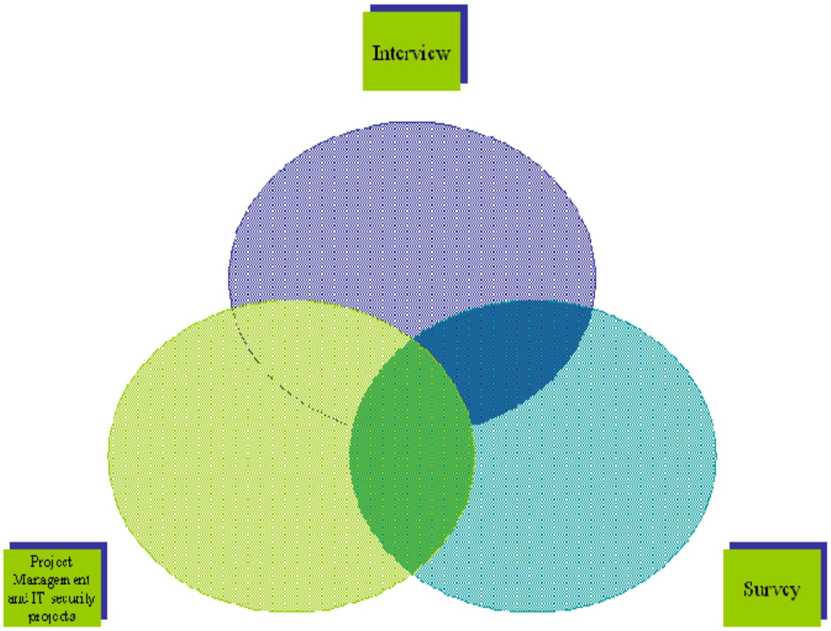


Figure 4. Integration of Quantitative and Qualitative Aspects of Study

Table 2 below shows the correspondence between hypothesis and the data collection instruments.

Table 2. Hypothesis and Data Collection Correspondence

	H1	H2	H3	H4
Survey Q1				⌖
Survey Q2				⌖
Survey Q3				⌖
Survey Q4			⌖	
Survey Q5			⌖	
Survey Q6		⌖		
Survey Q7		⌖		
Survey Q8				⌖
Survey Q9	⌖			
Survey Q10	⌖			
Interview Q1	⌖			
Interview Q2				⌖
Interview Q3			⌖	
Interview Q4			⌖	
Interview Q5		⌖		
Interview Q6		⌖		
Interview Q7	⌖			
Interview Q8	⌖			

Ethical Considerations of the Study

The ethical consideration of the study would be the confidentiality of the identity of the respondents involved in the survey, as well as in the interview. In particular, the identity of the respondents was not disclosed in the paper in order not to compromise the value of the information they provided.

The data collected from the respondents is indispensable in the study. As such, the researcher greatly observes the condition of confidentiality among the respondents. It is in this way that the researcher can expect full cooperation on the part of the respondents.

Research Methodology Summary

Generally, the research methodology of the study entails quantitative and qualitative approaches. Nonetheless, the study will have a dependent variable which will be the basis for collection of quantitative and qualitative data. This dependent variable is the effectiveness of IT security solutions as viewed by the participants of the study. On one hand, the quantitative approach of the research methodology deals with the conduction of the survey. In particular, the survey will be conducted within a company with an approximate population of 1000-3000 employees that is deploying IT security solutions. There will be two hundred employees which will be utilized as the respondents of the study. With this, various questions will be asked, ranging from the demographic profile of the respondents to questions that relate to IT security and its implementation.

More specifically, the respondents will be randomly selected from the IT employees of the company. The results of the survey will be analyzed using the weighted mean through the aid of the Likert scale. In this way, the raw data collected through the survey will be processed into meaningful information. On the other hand, the qualitative approach of the research deals with the conduct of interview. Specifically, the personal interviews will be carried out on five (5) employees who are purposely selected. The participants of the survey will be IT employees of the company as well.

The interview will be a semi-structured questionnaire. The Input-Process-Output model shall be the instrument for presenting the data. The topic of the questions in the interview will focus on the issues of security on information. From this topic, it will branch out to several sub-topics on IT. Furthermore, the Input-Process-Output model represents the survey (input), data analysis (process), and the conclusion (output).

With this, there will be an integration of the two approaches (quantitative and qualitative) in order to come up with the final analysis of the study. The result of the survey and the interview will be collectively analyzed in relation to the dependent variable which is the effectiveness of IT security solutions.

CHAPTER 4. FINDINGS AND ANALYSIS

Research Problem

The purpose of this paper is to evaluate the relative role of project management, project cost, project risks and end/user acceptance in the success of information security project. It will be determined whether factors like the project management processes, project cost, project risks and end user acceptance can significantly affect the success of information security projects.

The design of the study utilized mixed methods of a quantitative survey, and qualitative interviews.

Pilot Study

A pilot study was conducted in order to determine the validity and reliability of the survey and interview research instruments. The interview was tested using one manager and the questionnaire was tested using twenty (20) respondents.

Survey Questionnaire

The survey questionnaire consisted of two parts: the demographic profile of the respondents and the statements regarding the security on IT and project management. The effectiveness of the questionnaire was tested on twenty respondents. The pilot study did not require the respondents to answer all questions in the questionnaire; they were free to respond only to questions that believe were relevant to the study.

There were only thirteen questions in the pilot survey, of which three were demographic. On the demographic profile, the option to not disclose their personal profile information, such as their age, sex, and number of years in the company, was chosen by a large portion of the respondents during the pilot study. Since only a few respondents answered the demographic questions, the researcher removed it from the actual survey questionnaire.

The second part of the survey consists of questions regarding the security of IT and the different issues related to project management. There are ten questions asked which include the aspect of security as a source of competitive advantage for the company, IT implementation in their own organization, sufficiency of the IT security, company security threats, risk management on IT security, high cost of IT security products, IT security alternatives, IT security improvement, project management potentials, and the high success rate of IT security project when integrated with project management system.

In all the answers of the respondents on the second part of the survey, it can be observed that a large portion of them would usually choose the ‘undecided’ category as their answer to statements given to them. The high rate of answers under the ‘undecided’ category means that the researcher will have difficulty arriving at significant results for the study. This is because of the nature of the undecided category as not yielding any significant position on the part of the respondents.

Because of this, it was decided that the researcher would eliminate the ‘undecided’ category. In short, the Likert Scale would only now consist of a four-point scale instead of being a five-point scale. Usually, researchers use a four-point Likert scale rather than the five-point scale in a population which can be characterized as highly inclined to prefer the undecided 'category' (Sclove, 2001).

Interview

The original interview consisted of nine questions to guide the researcher in asking the participant interviews. Out of these nine questions, only one of them needed to be removed because it was deemed to be a basic assumption regarding IT.

The first question was intended to serve as a foundation of the interview. In other words, it checks the relevance of the subject of the study on the knowledge of the respondent. The first question prepares the respondent for the succeeding questions of the interview because it tends to evaluate the extent of information that the respondent has on the topic of the study.

The succeeding questions were easily facilitated by the researcher except for fifth question, which, based on this, was merged with the sixth question. In this way, a more meaningful answer can be derived.

Thus, the questions that were included in the data collection are: 1) the consideration for information technology security as one of the sources of competitive advantage, 2) the assessment of the implementation of information technology security in one's organization, 3) the sufficiency of the company's security to address the threats, 4) issues and problems that are related to security, the risks involved in managing information technology security, 5) the alternative ways of achieving effective information technology security without its high costs, 6) the ability of project management to improve the information technology security of the company, 7) the most critical elements of a successful project, and 8) the ability of project management to increase the success rate of the company.

Overall, it was deemed that the interview questions were effective in prompting answers to the problems and issues posed in this research. The resulting eight questions were found to be relevant and valid. Through these questions, the researcher has verified its usefulness in collecting indispensable information for the study.

Pilot Study Conclusion

The desired results were achieved in the pilot study. With this, it could be safely concluded that the survey and interview instruments, as altered, are suitable, as well as effective, in addressing the problems of the study. As such, the conduct of the actual survey questionnaire and interviews were conducted with confidence in the instruments.

Data Collection Process

Through the mixed method research approach, the researcher gathered qualitative and quantitative data using a survey and personal interviews. The respondents of the survey and interview came from one company that deploys IT security solutions. The sample size for the survey respondents is two hundred (200) employees, of which 140 surveys (i.e., 70%) questionnaires were returned or. The data collected from the survey was analyzed through the use of the Likert Scale Rating and the weighted mean (See Table 1 for the formula and interpretation). On the planned interview sample size of 5, only 4 could be conducted. The personal profile of the interviewees will not be disclosed in order to protect the confidentiality of their identity.

Does the Use of Project Management Processes Improve the Success Rate of Information Security Projects?

Different approaches and techniques have been utilized in the process of implementing information security projects. In the first problem of the study, it determines whether the use of project management system can improve the success rate of information security projects. As such, the hypothesis for this problem is stated as follows:

> H_1: The use of project management processes can significantly improve the success rates of information security projects.
>
> H_0: The use of project management processes cannot significantly improve the success rates of information security projects.

To test the hypothesis, the survey and interview results are examined. Table 3 presents the findings of the survey for the research problem on the effective implementation of IT security projects in the context of project management. Through the weighted mean and the Likert rating scale, the researcher was able to weigh the answers of the respondents.

Table 3. Information Security Projects and the Project Management System

Statement	5	4	2	1	Weighted Mean	Interpretation
Through the project management system, the company can improve its security on information technology.	24%	63%	11%	1%	3.08	Strongly Agree
Project management, when integrated with the IT security projects, can improve the success rate of company.	29%	46%	22%	3%	2.98	Agree

The first statement on the survey states that through the project management system, the company can improve its security on IT. The respondents strongly agreed with the statement (3.08). This implies that IT security can be enhanced with the utilization of the project management.

The respondents also agreed that project management, when integrated with the IT security projects, can improve the success rate of the company (2.98). Project management does not only aid in the improvement of IT security projects, but it also improves the overall effectiveness of implementation.

Even in the interview, all of the respondents agreed, “project management can increase the success rate of the IT security of the company.” One respondent emphasized, “the project management system has already increased the success rates of the company.”

Indeed, the organization being studied can attest to the potential of project management. It is also claimed, “no executive level support would be possible or resource commitment, without a well thought out plan that includes business drivers and a managed expectation of successful outcomes with a clear return on investment.”

There are significant success factors involved in using project management to address IT security. The interviewees were asked to identify the critical elements of a successful project. Among the elements of a successful project include the plan development and execution, scope management, time management, quality management, cost management, communication, risk management and procurement.

The first interviewee claimed that “the most important elements of a successful project are the plan development and execution, communication and risk management.” The second respondent asserted the importance of “plan development and execution, scope management and quality management.” Moreover, the other respondents also prioritized aspect of “plan development and execution.” The other elements which are perceived by the respondents to be important are “quality management, risk management, time management and communication.”

With this, the researcher shall reject the null hypothesis and accept the alternative hypothesis. This means that the researcher shall embrace the hypothesis that the use of project management processes can significantly improve the success rates of information security projects. It rejects the hypothesis that the use of project management cannot significantly improve the success rates of IT projects.

The result of the survey implies the ability of project management to improve the IT security of the company, thereby contributing also to their success rates. Similarly, the interview reveals that while there are limitations to the project management system, it is still a significant feature of the company's IT security project.

Does the Cost of Information Security Projects Affect its Successful Implementation?

The second problem of the study deals with the cost of information security projects. One of the security issues involving the IT projects is its high cost. As such, it is highly indispensable to determine whether the project cost can affect the successful implementation of the IT security projects.

The hypothesis for the project cost problem is given below:

> H_1: The high cost of information security projects significantly affects information security project success.
>
> H_0: The high cost of information security projects does not affect information security project success.

Table 4 shows the result of the survey regarding IT security project costs. On the first statement, the respondents strongly agreed that IT security comes with a high cost (3.25). It has always been the claim that the security on IT projects is expensive, and this has been affirmed by the respondents. Nonetheless, the respondents also agree that there are alternative ways of achieving effective IT security without its high cost (2.73). The respondents are still optimistic in spite of the rising cost of IT security. It is believed that through alternative methods, the company will be able to avoid the high cost of IT security costs.

Table 4. Information Security Projects and Project Cost

Statement	5	4	2	1	Weighted Mean	Interpretation
The IT security of the company comes with a high cost	38%	52%	7%	2%	3.25	Strongly Agree
There are alternative ways of achieving effective IT security without its high cost/price.	13%	56%	26%	5%	2.73	Agree

In the interview, the high cost of IT security is emphasized by the respondents. Because of the high cost of the security, it compromises the company's ability to deliver effective IT security projects. Other issues on IT security include the data leakage or disclosure, the inability to address the new and emerging threats and, the use of the wrong method or approach

One of the respondents asserted that IT security is not "cheap." The respondent reported, "It can run over their original budget of direct cost as well as employee time." As such, "the spending for security initiatives should be tied to asset valuation and risk appetite."

In other words, the high cost of IT security should be justified based on the gains which can be acquired by the company. The companies should see to it that the security should be able to address the problems and issues on IT projects. This includes the ability "to address errors and omissions which can contribute to data leakage or disclosure. Otherwise, this high cost would only contribute to the failure of the company."

A respondent also claimed, "There are really no alternative ways of achieving effective IT security without its high cost." However, the other interviewees disagree with this claim, saying, "There are still ways to have an effective information technology security without its high cost." One respondent pointed out "achieving low-cost IT security also depends on whether or not the company can find a knowledgeable and ethical lead."

Further, it is believed by a respondent that, "Information technology governance and security governance have to find their way into a risk management program. Risk assessment facilitates the companies' prioritization effort. How much money is spent to remediate a risk will depend on how great executive management perceives the prevailing threats to be and how much it potentially stands to lose. Once these determinations are made and an acceptable level of risk is provided, remediation and IT security investment has the potential to produce the so-called acceptable return on risk. This means that remediation has been optimized to the appropriate risk level set by senior management. Cost can then be offset by return on investment and risk minimization as a result of the new control."

With the different survey and interview questions pertaining to the research problem on the project cost, the alternative hypothesis shall be accepted and the null hypothesis shall be rejected. Indeed, the high cost of information security projects significantly affects information security project success. The dominance of security projects that are expensive plays a great role in the ability of the company's security project to become successful.

Does the Risk and Perceived Security Threats Affect the Success of Information Security Projects?

Another research problem in this paper is the perceived risk of information security threats that can affect the success of information security projects. The presence of risks and threats to IT projects is determined in relation to the extent of influence that it can give to the achievement of the project's success. The hypothesis for this problem is declared as follows:

> H_1: Perceived risk of information security threats significantly affects information security project success.
>
> H_0: Perceived risk of information security threats does not significantly affect information security project success.

In the survey results, there is a strong agreement on the part of the respondents regarding the statements given about the perceived risks and threats on IT security projects. Table 5 presents the detailed findings on the security risks and threats survey.

Table 5. Information Security Projects, Security Risk, and Threats

Statement	5	4	2	1	Weighted Mean	Interpretation
The threats acquired by the company can bring potential damage to its operation and eventually its success.	45%	45%	6%	4%	3.28	Strongly Agree
There are great risks involved when it comes to managing the issues and problems of security in information technology.	32%	59%	7%	2%	3.17	Strongly Agree

One of the statements in the survey states that the threats to IT security can bring potential damage to the company. This statement is strongly agreed upon by the respondents (3.28). Particularly, these threats can highly affect the conduct of operations of the company and, eventually, its success. The respondents strongly agreed with second statement also, confirming that there are great risks involved when it comes to managing the issues and problems of security in IT (3.17).

In the interview, it has been claimed, “information technology security is considered as one of the sources of competitive advantage in the company.” Security is the "element that needs to be considered in all types of assurance/audit engagements." It is also necessary in "the conduct of business processes such as financial transaction or even information movement. Through the security on IT, it contributes to the credibility of the company, which is significant especially on the part of the customers."

In a nutshell, "security provides the business with the ability to conduct business online, to conduct business globally and to maintain consumer confidence. Not considering security in any of these areas would place the organization at great risk." Undoubtedly, "consumers are critical when it comes in the conduct of digital business. The average consumer is very in tune with what is at stake and that they are less willing to compromise with a company that has a low level of security."

While the respondents of the interview all understand the importance of security, they also admit that their company's "information technology security is not sufficient to address the various threats, issues and problems that are related to security." More specifically, only 1 out of the 4 interviewed respondents consider their IT security to be adequate.

One interviewee cited the need to "identify the significant security risk and vulnerability in IT projects." Primarily, the significant risk involved in managing IT security is "the use of wrong method or approach." Nonetheless, "even though the risks are well-measured by the company, it cannot stop the new and emerging threats. For instance, the risk considered in last year's planning cycle is not anymore the same with the current period."

Overall, on the problem of security project risks and threats, the alternative hypothesis is accepted thus, rejecting the null hypothesis. Perceived risk of information security threats significantly affects information security project success. In other words, security threats can be a potential factor in project failure.

Does the User Acceptance of Information Security Solutions Affect the Success of Information Security Projects?

The last problem stated in this research deals with the way the end user acceptance or satisfaction level can affect the success of information security projects. It is believed that the level of acceptance on the projects by its ultimate or end users can influence the success rate of the projects. The hypothesis for this problem is declared as follows:

> H_1: The end user acceptance of information security solutions significantly affects the success of information security projects.
>
> H_0: The end user acceptance of information security solutions does not affect the success of information security projects.

Table 6 shows the result of the survey towards the user acceptance level on information security solutions. The survey questions which are included on this problem evaluate the perception of the respondents regarding the information security solutions, which in turn can affect success of information security projects.

Table 6. Information Security Projects and User Acceptance

Statement	5	4	2	1	Weighted Mean	Interpretation
Security is a source of competitive advantage for various organizations.	42%	43%	6%	9%	3.08	Strongly Agree
There are still many aspects of IT security of the company that needs to be improved.	30%	55%	13%	3%	3.07	Strongly Agree
There is an effective implementation of IT security in the company where I work.	26%	50%	21%	3%	2.96	Agree
The IT security of the company is sufficient to address the threats, issues and other problems that are related to security.	23%	51%	21%	5%	2.85	Agree

Primarily, the survey respondents strongly agreed that the security on the company's IT projects is a source of competitive advantage (3.08). This is true not only for their organization, but with other organizations as well. By asserting the position of IT security, one can go into its deeper facets. In addition, the respondents strongly agreed on the statement that there are still many aspects of IT security of the company that needs to be improved (3.07).

With respect to the implementation process, the respondents agreed that there is an effective implementation of IT security in the company (2.96). The general agreement on the effectiveness of IT security is strengthened by the respondents' agreement on the sufficiency of their IT security to address the threats, issues and other problems that are related to security (2.85).

In the second and fourth statements in Table 6, it is revealed that although the employees perceive that there is an effective implementation of IT security in their company, they also believe that there are still many aspects of the project that needs to be improved. In other words, one can say that at present, the company's IT security is still able to address its basic needs. However, its sustainability is still highly critical because of the need for more improvement.

Moreover, the emphasis on the fourth statement is the effective implementation of the IT security projects. The employees perceive that with the current state of their IT security, it can still be improved. It is deemed that although effectiveness is observed, there is still a huge for the project to be consolidated.

In the interview, there is an observed optimism in the answers from the respondents regarding the implementation of IT security in the company. When the respondents were asked regarding the implementation of IT security by the organization, they said, "It is utilized effectively through the use of the project management system. Their processes or activities included in the implementation of IT security are the predetermined metrics which are determined in a planning council or with senior management commitment."

Aside from the predetermined metrics, "surveys and interview or random discussion with IT and Business Management about their perception of information security and how well they think the process is currently working and how they believe it can be improved. Lessons learned at the end of projects also provide very good sources of information. And finally, security and audit assessments will be and are important elements of this assessment element of the security lifecycle."

Because of the perceived insufficiency of IT security, project management is deemed to play a role in improving the company security on IT. All of the respondents agreed with the potential of project management to improve the current state of company IT security. However, one of the respondents argued that "the contribution of project management in improving IT security is up to certain extent only." This is because of the belief of the respondent that "security is not necessarily a project with finite timelines. The implementation of technology, processes, or policies always benefits from a structured deployment plan in the form of a project. But the true measure of success is derived from how well security is sustained in the long term."

The respondents believe that the current IT security of the company is not sufficient to address the various threats, issues and problems that are related to security. As such, the integration of project management would be indispensable.

With this, the results of the interview and the survey point out to the need for the alternative hypothesis to be accepted, and the null to be rejected. The alternative hypothesis states that the end user acceptance of information security solutions significantly affects the success of information security projects.

Findings and Analysis Summary

This chapter has presented and analyzed the findings of the study. Basically, the data are collected through the survey and interview instruments. The data is analyzed using the Likert rating scale and the weighted mean. In addition, an analysis of secondary information is also conducted in relation to the findings from the primary sources of data, which are the survey and interview.

The information collected and analyzed aims to answer the research problem of the study. Mainly, this paper has evaluated the relative role of project management, project cost, project risks and end/user acceptance in the success of information security project. With this, it determined whether the factors like the project management processes, project cost, project risks and end user acceptance can significantly affect the success of information security projects.

In the actual survey and interview, the return rate is not one hundred percent (100%). Out of the possible 200 survey respondents, only 140 of them turned it in. On the interview, only 4 out of the 5 target interviewees were interviewed. The demographic profile of the respondents of survey and interview was not determined because a majority of them preferred not to disclose their personal information from the pilot study.

The first problem of the study delves into the way project management affects the effective implementation of information technology security projects. Based on the results of the survey and the interviews, this paper shall reject the null hypothesis and accept the alternative hypothesis. This means that the researcher shall embrace the hypothesis that project management can significantly improve the success rates of IT projects. It also rejects the hypothesis that project management cannot significantly improve the success rates of IT projects. The application of project management in the IT security of the company can aid the organization in achieving greater rates of success because it serves as an indispensable instrument in the effective implementation of IT security projects.

Indeed, there are significant success factors involved in using project management to address IT security. Among the important elements included in the critical success factors of project management are plan development and execution, communication, risk management, scope management, quality management and time management.

The second problem of the study deals with the aspect of the cost of IT security projects and how it affects successful implementation. Because of the prevailing high cost of security projects, it is found out that it can hinder the ability of the company to deliver a successful IT security project. As such, the alternative hypothesis is accepted, wherein it states that the high cost of information security projects significantly impact information security project success.

Moreover, the third problem of the study is focused on the risk and perceived security threats that can affect the success of information security projects. In the result of the survey and interview, it shows that there is a general agreement that the risk and threats can be detrimental to the process of achieving success in the security projects of the company. Therefore in the hypothesis, there is a need to reject the null in order to accept the alternative hypothesis, which states that the perceived risk of information security threats significantly affects information security project success.

Finally, the last problem of the study is the way end user acceptance or satisfaction levels affect the capacity of project management to address the issues of IT security. The findings suggest that the alternative hypothesis should be accepted and the null should be rejected. The alternative hypothesis states that the end user acceptance/satisfaction level significantly affects the capacity of project management to address the issues on security of IT. Undeniably, the way the end users react will have a great impact on the outcome of the project management utilization on IT security.

Overall, this study was able to determine that there is a significant role played by project management processes, project costs, projects risks and end/user acceptance in the success of information security projects. The findings of the study reveal the perception of the employees that the utilization of a formal project management approach will significantly lead to more successful IT security projects. There are critical success factors of the project management system which are indispensable in the effective implementation of IT security projects. However, the prevalence of expensive security projects can mar its effective implementation. The same is true with the perceived risks and threats which can affect the success of security projects. But on a lighter note, the end users are highly satisfied with the project management system. They have acknowledged the large role of the project management system in the success that their organization is achieving now.

CHAPTER 5. SUMMARY, CONCLUSION AND SUGGESTIONS FOR FURTHER RESEARCH

This chapter provides the summary and conclusion for the study. It will summarize the points, claims and arguments made in the research. The findings will be discussed based on the problems posed in the study. After summarizing, the researcher can conclude or make generalizations about the whole paper.

To review the problem, this chapter evaluates the relative role of project management, project cost, project risks and end/user acceptance in the success of information security projects. With this, it determined whether factors like the project management processes, project cost, project risks and end user acceptance can significantly affect the success of information security projects.

The review of related literature served as the foundation of the research. The implications of the literature search were confirmed by the primary data collected through the surveys and the interviews.

Summary

IT security projects refer to projects that intend to protect information within an organization. Basically, security projects are different from other IT projects due to their focus on information security. In the paper, the process of evaluating the success of information security projects is done in the light of various factors, such as the project management processes, project cost, project risks and the end/acceptance.

Project Management

Project management is perceived to be an important factor in ensuring the success of the information security projects. In this chaotic world, the use of project management is highly available in almost any field. Thus, it can serve as a catalyst in ensuring the success of managing various projects. This is also true in the case of the company being studied in this research. Part of the success of the information security project is attributed to utilization of the project management system.

Indeed, this is emphasized in the survey and interview results wherein the respondents were in strong agreement regarding the positive role of project management in their company, especially in managing security projects. It is highly believed that the use of project management can significantly improve the success rate of information security projects.

While there are critical success factors of project management which can contribute to the overall growth of the company, there are also dangers perceived in the poor project management. Evans (1998) associates the dangers of project management to risk management. Indeed, the aspect of risk management is integrated in the critical success factors of project management. As a matter of fact, this element is considered by the interview respondents to be one of the most critical success factors of project management.

Through proper project management, companies can avoid various problems in the conduct of a project, such as IT security. By establishing appropriate supervision, insisting on a management protocol, and establishing a method of recovery should things go wrong, managers can protect their companies (Evans, 1998). The aspect of supervision is necessary to monitor the progress of a project. Close monitoring will enable the company to check for errors or flaws immediately. There should be a strict observance of the protocol also to avoid unnecessary hassles or setbacks. Finally, the recovery aspect is deemed important for successful project management. There should be a contingency plan in cases of the failure of completion of the job or delays.

Project Cost

The common problems in information security projects are found on the technical aspect most of the time. But aside from the technical problems of IT security, its high cost can also be a problem for various companies. The perceived “neglect” on data security cannot be all time considered as neglect because some companies may not really afford to have an effective security because of its high cost. Hence, there is a need for companies to find the cheapest possible IT security vendors that can offer them with highest form of security.

As mentioned above, the respondents of the survey and interview strongly agree regarding the high cost of IT security. However, one must also take note of the gains that can be achieved with having a high-level IT security. This can serve as a catalyst to success for companies. But then, as one of the respondents mentioned, the cost of security on the company’s IT should not overweigh its potential benefit. Otherwise, the purpose of adopting IT security is defeated.

Project Risks

When the security of IT projects fails to address the need to secure employee's computer usage, it can lead to the vulnerability of the organization's system. This is because it opens the system of the company to various attacks. In addition, the effectiveness of IT security projects is always a constant struggle. Its successes are always temporary because new portal of threats develop regularly.

Since data is stored electronically, there is a greater need for higher security in order to guard it effectively. Undoubtedly, the vulnerability of corporate information subjects the company to greater risks. And in any organizations, security should be the emphasis in the company's move to safeguard its information. Sometimes, the major flaw of other organizations is that they do not put greater emphasis on security thereby neglecting to address the company's goal of securing its most previous information.

Andress (2003) states that cyber hackers are just one type of the attackers on IT. Other types of attackers include crackers, script kiddies, malicious insiders and industrial espionage. These different types of attackers have also different motivation and capacity in attacking one's system. It can range from light attacks, to malicious ones and to extremely serious attacks.

The other known threats to IT security are theft of proprietary information, sabotage of data or networks, telecom eavesdropping, system penetration by outsider, insider abuse of Net access, financial fraud, denial of service, spoofing, unauthorized insider access, telecom fraud and active wiretapping. The denial of service or DoS, intrusion and information theft is the most common types of attack on information technology. Based on the study of Andress (2003), these threats can have a great financial impact on the company when incurred.

User Acceptance

It is likewise asserted that user acceptance plays an important role in the success of information security projects. The level of acceptance of the users on the project can determine its effectiveness. The users are the ultimate measurement of the performance of the project. Thus, a positive response implies that the project is perceived to be useful or beneficial.

In this paper, the respondents who belong to one company asserted their agreement regarding the effectiveness of their security project. But in spite of this agreement, they are still critical about the threats and other issues that surround the project. They believe that there is still a room for improvement. And with this insufficiency of IT security to address various threats, issues and problems, they look into the potential of a project management system in improving their project.

Conclusion

Overall, this paper has successfully evaluated the employees' perception on the role of project management processes within one organization, project cost, project risks and end/user acceptance in the success of information security projects. It has determined that the variables such as the project cost, user acceptance, project management and project risks are important factors that play a significant role in determining the success of information security projects. This is because they significantly affect the implementation of successful security projects. This has been observed in the case of the company being studied in this research.

Based on the findings, one can see the importance of securing or protecting one's system. There is valuable information in a company that needs to be protected in order to ensure its success. When an IT security system is ineffective, it can cost a lot of damage or even failure, and not only for a certain project, but for the whole company. Among the different problems and issues of IT security are laptop theft, viruses, employee net abuse, cyber hackers and many more.

While there can be no single solution that can address all the issues and problems of IT security, the project management system is a significant tool in helping the company implement an effective IT security projects. There is really no solution in the management of IT security projects. This is because the effective security management cannot be addressed through a single solution, which is by means of the different products. But it is best addressed by looking at the solution as a process.

Since project management is viewed as the management of change, it can be said that this technique is highly suitable in managing IT security projects. Basically, it is mentioned earlier that the success of IT security projects are always temporary because new portal of threats develop regularly. As such, the constant changes that occur are deemed to be best addressed through the project management system.

The benefits of project management system especially in IT security projects can be measured in various ways. For instance, it can be measured through benchmarking, by determining the satisfaction acquired by the customers, project cycle time, project profitability and many more.

Recommendation

With this, it is recommended that future research should delve into the aspect of project management as related to the success rates of IT security projects. Further studies on the role of the project management systems can yield significant findings on its great role as a catalyst for the success of IT security projects.

In this paper, project management is only one of the components studied alongside with project costs, project risks and user acceptance. As such, it is deemed that there may be factors or aspects of project management that are not included in the study. Since the concept of project management is not the only focus of the study, the researcher cannot incorporate all the information that pertains to project management.

During the conduct of the study, it became clear to the researcher that the concept of project management alone is a very significant factor in making the IT security projects successful. As such, it would be very beneficial to conduct research that would focus solely on the nature and the different properties of project management and relate it with the process of security projects in IT.

Indeed, future research on this topic can also give emphasis on a single component of the IT security project. This means that aside from project management, one can also focus on the other components of IT security project. For instance, one can concentrate on the role of user acceptance level in the achievement of success of the IT security projects. There are also emerging issues and problems in the implementation of

IT security projects that need to be addressed. The ever-modernizing conduct of business seems to be inevitable, thus influencing the development of IT security.

Undeniably, this research is very limited in the sense that it is focused on one company alone. To a certain extent, the findings of the study cannot be generalized to all organizations of different industries. The results show the perceptions of the employees of a single organization alone. It is therefore suggested that with a greater number of resources, such as time and financial supports, it would be better to conduct the study on a larger scale. This means that one would not only include a single organization but instead, a combination of various organizations. In this way, the findings can be generalized.

While this study is limited to a single organization alone, the findings are still indispensable. It has paved the way for a greater understanding of the critical components of IT security projects. For instance, the major concepts that have been evaluated in this paper are project management systems, project costs, project risks and user acceptance. The importance of these concepts in the success of IT security projects is manifested by presenting the case of a single organization. Finally, by focusing on the case of one organization, the paper was able to point out that effective security projects are not only based on the external factors but as well as in the internal.

Another important recommendation for the study is an evaluation of the way security projects affect the performance of workers. It has always been an issue that security projects often mar or get in the way of the work of the employees. Hence, by studying its role on the employees' work, one can look for solutions as to how security projects can be more of help on the part of the employees.

It other words, this suggested study implies that because of the tightness of security, it often compromises the effectiveness of the employees. It tends to result in inconvenience or uneasiness for the workers of the company. As a result, the output of the employees is affected. On the other hand, one can also look into other ways in which security projects affect and continue to shape the lives of workers at their workplaces. In fact, one can also examine the positive side of the IT security projects.

Regarding the people component of the implementation of IT security projects, it is recommended to examine the behavior and attitude of the workers towards the project. On the discussion about project risks, it is already mentioned that the resistance of employees can affect the success rate of the project. By concentrating on attitudinal problems, one can elaborate more on the aspect of employee resistance.

Furthermore, the concept of IT governance also plays an important role in the success rate of IT security projects. The different mechanisms and processes of IT governance are critical factors on the security projects' effective implementation. Indeed, there are only few studies pertaining to IT governance. While it is perceived as a vital component, it is nonetheless often overlooked.

Finally, the sustainability of security projects is also an issue that needs to be addressed. In spite of the high cost of projects, its sustainability is still not achieved. Indeed, the rapid pace of technological development and information explosion are among the factors that prevent the sustainability of majority of IT security projects. With this, it is necessary to examine the long-term performance of the project. This can be integrated with the concept of security life cycle.

Through these recommendations, the researcher believes that it can further the findings of this paper. Undoubtedly, this research can serve as a foundation for future research. Through this research and the recommendations given, the author hopes that it can trigger the minds of researchers and students, especially in the field IT.

REFERENCES

Alberts, C., & Dorofee, A. (2003). *Managing information security risks - The OCTAVE approach*. Upper Saddle River, NJ: Pearson Education, Inc.

Andreas, N. A., & Boone, L. W. (2002). The impact of information technology and cultural differences on organizational behavior in the financial services industry. *Journal of Intellectual Capital, 3*(3), 248.

Andress, A. (2003). *Surviving Security: How to Integrate People, Process, and Technology*. Boca Raton, FL: Auerbach.

Anhal, A., Daman, S., O'brien, K., & Rathmell, A. (2003). *Engaging the board: corporate governance and information assurance*. Santa Monica, CA: Rand.

Bielski, L. (2005). Security Breaches Hitting Home: Phishing, Information Leaks Keep Security Concerns At Red Alert. *Aba Banking Journal, 9*(7), 7-15.

Bloomfield, B. P., Coombs, R., Knights, D., & Littler, D. (2000). *Information technology and organizations: Strategies, networks, and integration*. Oxford, UK: Oxford University Press.

Boyce, B. (1996). A manual security solution. *Security Management, 40*(11), 67-75.

Boynton, Andrew C., Zmud, Robert W., & Jacobs, Gerry C. (1994). The influence of IT management practice on IT use in large organizations. *Mis Quarterly, 18*(3), 299.

Brian, J. K. (1999). Preserve, protect, and defend. *The Journal of Business Strategy, 20*(5), 22.

Brockhaus, R. H. (1986). *The psychology of the entrepreneur*. Cambridge, MA: Ballinger.

Brown, B. (2005, March). Paper maker documents key IT security issues. *Network World*.

CERT. (2007). Retrieved May 21, 2007, from Carnegie Mellon University Web site: http://www.cert.org/

Charp, S. (2003). Security and privacy of information. *The Journal, 31*(2), 8.

Crandall, R., & Murray, M. (2006). IT offshore outsourcing requires a project management approach. *Sam Advanced Management Journal, 71*(1), 4.

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks, CA: Sage Publications, Inc.

Culp, C. L. (2001). *The Risk management process: Business strategy and tactics*. New York: Wiley.

David, B., Geoff, S., & Peter, E. D. L. (2004). Management of risks in information technology projects. *Industrial Management + Data Systems, 104*(3/4), 286.

Diwan, R., Kudyba, S., & Mcginn, D. (2002). *Information technology, corporate productivity and the new economy*. Westport, CT: Quorum Books.

Donnelly, S. B. (2006, July 10). Lean and mean. *Time Magazine, 168*, 2.

Eckes, G. (2001). *The six sigma revolution: How general electric and others turned process into profits*. New York: Wiley.

Fisher, S. L., & Howell, A. W. (2004). Beyond user acceptance: An examination of employee reactions to information technology systems. *Human Resource Management, 43*(2-3), 243-258.

Flowers, S. (1988). *Success in information processing*. London: John Murray.

Frame, D. (2002). *The new project management: Tools for an age of rapid change, complexity, and other business realities*. San Francisco: Jossey-Bass.

Gao, Y. (2005). Applying the Technology Acceptance Model (TAM) to educational hypermedia: A field study. *Journal of Educational Multimedia and Hypermedia, 14*(3), 237-247.

George, M. L., Rowlands, D., Price, M., & Maxey, J. (2005). *The lean six sigma pocket toolbook*. New York: McGraw-Hill.

Glory, K. (1997). Information security. *Management Accounting, 79*(6), 18-24.

Glossary. (2007). Retrieved Jan 8, 2007, from Internet Corporation for Assigned Names and Numbers Web site: http://www.icann.org/general/glossary.htm#P

Glossary. (2007). Retrieved May 22, 2007, from Addr.com Web Hosting Web site: http://www.addr.com/help/show.cgi?glossary.htm

Gobeli, D. H., Gray, C. F., & Larson, E. W. (1991). Application of project management by small businesses to develop new products and services. *Journal of Small Business Management, 29*(2), 30.

Grance, T., Hash, J., Stevens, M., O'Neal, K., & Bartol, N. (2003). Guide to information technology security services. *Special Publication*, 800-835.

Gygi, C., DeCarlo, N., & Williams, B. (2005). Six Sigma for Dummies. Hoboken, NJ: Wiley Publishing, Inc.

Halachmi, A. (1992). The brave new world of information technology. *Public Personnel Management, 21*(4), 533.

Hannaford, C. S. (1995). Can computer security really make a difference? *Managerial Auditing Journal, 10*(5), 10.

Haubner, K. (2004). *Six Sigma*. Retrieved May 22, 2007, from Six Sigma IT Concepts Web site: http://www.sixsigma.de/english/index.htm

Information Technology. (2007). Retrieved May 22, 2007, from Information Technology Association of America Web site: http://en.wikipedia.org/wiki/ Information_technology

Johnson, R. (2005). Risk management for computer security: Protecting your network and information assets. *Security Management, 49*(11), 128.

Korin, K., & Laura, J. T. (2004). Project success: A cultural framework. *Project Management Journal, 32*(1), 30.

Larson, E. (1987, Summer). Matrix Management: Contradictions and Insights. *California Management Review*, 126-138.

London, M. (1997). *Job Feedback: Giving, Seeking, and Using Feedback for Performance Improvement*. Mahwah, NJ: Lawrence Erlbaum Associates.

Louisa, W. (1998). The risky business of managing IT risks. *Management Review, 87*(5), 6.

Ma, Q., & Liu, L. (2004). The Technology Acceptance Model: A Meta-Analysis of Empirical Findings. *Journal of Organizational and End User Computing, 16*(1), 59-72.

Ma, Q., & Ma, L. L. (2004). The Technology Acceptance Model: A Meta-Analysis of Empirical Findings. *Journal of Organizational and End User Computing, 16*(1), 59-72.

Maris, G. M., & Patrick, K. C. (1999). The influence of human factors and specialist involvement on information systems success. *Human Relations, 52*(1), 123.

Mayor, T. (2004). *Six Sigma comes to IT targeting perfection*. Retrieved May 22, 2007, from CIO Business Technology Leadership Web site: http://www.cio.com.au/index.php/id;1718145589

Neumann, P. G. (1994). Technology, laws, and society. *Association for Computing Machinery, 37*(138), 3.

Niven, P. R. (2002). *Balanced Scorecard*. Hoboken, NJ: John Wiley & sons.

Pande, P. S., Neuman, R. P., & Cavanagh, R. R. (2000). *The Six Sigma Way: How GE, Motorola, and Other Top Companies are Honing Their Performance*. New York: McGraw-Hill.

Project management definition. (2007). Retrieved April 11, 2007, from Visitask Web site: http://www.visitask.com/project-management-g.asp

Razalli, Fadilah B. (2007). *Roles, skills and personal characteristics of project management in construction industry*. Retrieved March 11, 2007, from University of Teknologi Malaysia Web site: http://www.efka.utm.my/thesis/IMAGES/4MASTER/2007/2JSB-P/fadilahrazallima051022d07ttt.pdf

Reiss, G. (1995). *Project management demystified: Today's tools and techniques.* London: E&FN Spon.

Sample size calculator. (2007). Retrieved July 2, 2007, from The survey system Web site: http://www.surveysystem.com/sscalc.htm

The SANS 2005-2007 information security salary & career advancement survey. (2007). Retrieved March 11, 2007, from The SANS Institute Web site: http://www.sans.org/salary2005/

SANS. (2007). Retrieved April 2, 2007, from Sysadmin, Audit, Network, Security Institute Web site: http://www.sans.org/

Saunders, M. (2006). *Research methods for business students*. Upper Saddle River, NJ: Prentice Hall.

Script Kiddie. (2007). Retrieved March 1, 2007, from Wikipedia Web site: http://en.wikipedia.org/wiki/Script_kiddie

Stuckenbruck, L. C. (1982). *The implementation of project management: The professional's handbook*. Reading, MA: Addison-Wesley.

Tansey, S. T. (2002). *Business, information technology and society*. New York: Routledge.

Victorian electronic democracy, final report. (2005). Retrieved May 22, 2007, from Parliament of Victoria Web site: http://www.parliament.vic.gov.au/SARC/E-emocracy/Final_Report/Glossary.htm

Watkins, J. (1998). *Information technology, organizations and people: Transformations in the UK retail financial services sector*. London: Routledge.

World economic outlook: a survey by the staff of the International Monetary Fund. (2001). Retrieved March 12, 2007, from International Monetary Fund Web site: http://www.imf.org/external/pubs/ft/weo/2001/02/pdf/front.pdf

APPENDIX A. SURVEY QUESTIONNARIE

Part A: Demographic Profile

Direction: Put an “x” mark to your corresponding answer. Answer all items.

1. Age

[ ] 25 years old and below

[ ] 26-35 years old

[ ] 36-45 years old

[ ] 45 years old and above

[ ] Not to disclose

2. Gender

[ ] Male

[ ] Female

[ ] Not to disclose

3. Number of Years in the Company

[ ] 1 year and below

[ ] 2 – 3 years

[ ] 4 – 5 years

[ ] 6 years and above

[ ] Not to disclose

Part B: Information technology Security and Project Management

Direction: Please check the box of your corresponding answers.

1. Strongly disagree
2. Disagree
3. Undecided
4. Agree
5. Strongly agree

Statements	5	4	3	2	1
1. Security is a source of competitive advantage for various organizations.					
2. There is an effective implementation of IT security in the company where I work.					
3. The IT security of the company is sufficient to address the threats, issues and other problems that are related to security.					
4. The threats acquired by the company can bring potential damage to its operation and eventually its success.					

Statements	5	4	3	2	1
5. There are great risks involved when it comes to managing the issues and problems of security in information technology.					
6. The IT security of the company comes with a high cost					
7. There are alternative ways of achieving effective IT security without its high cost/price.					
8. There are still many aspects of IT security of the company that needs to be improved.					
9. Through the project management system, the company can improve its security on information technology.					

Statements	5	4	3	2	1
10. Project management, when integrated with the IT security projects, can improve the success rate of company.					

APPENDIX B. INTERVIEW QUESTIONS

1. Do you consider security on the aspect of information technology as one of the sources of competitive advantage of your company? Explain.

2. How will you assess the implementation of your organization on IT security?

3. Do you consider the company's IT security as sufficient to address various threats, issues and problems that are related to security? (Yes/No)

4. What are the risks involved in managing IT security?

5. What can you say about the price or the cost of IT security projects?

6. Is there any alternative ways of achieving effective IT security without its high costs?

7. Can the project management system improve the company security on information technology? (Yes/No)

8. Which three of the following you believe is most critical element of a successful project? 1.) Plan development and execution 2.) Scope management 3.) Time management 4.) Cost management 5.) Quality management 6.) Human resource management 7.) Communication 8.) Risk management 9.) Procurement

9. Can Project Management also increase the success rate of the company? (Yes/No)

APPENDIX C. SURVEY RAW DATA

1. Age

#	Answer	Response	%
1	25 years old and below	5	4%
2	26-35 years old	47	34%
3	36-45 years old	48	35%
4	45 years old and above	35	25%
5	Not to disclose	3	2%
	Total	138	100%

2. Gender

#	Answer	Response	%
1	Male	117	84%
2	Female	19	14%
3	Not to Disclose	3	2%
	Total	139	100%

3. Number of Years in the Company

#	Answer	Response	%
1	1 year and below	43	31%
2	2 - 3 years	36	26%
3	4 - 5 years	12	9%
4	6 years and above	42	30%
5	Not to Disclose	6	4%
	Total	139	100%

4. Security is a source of competitive advantage for various organizations.

#	Answer	Response	%
1	Strongly disagree	12	9%
2	Disagree	8	6%
4	Agree	57	43%
5	Strongly agree	55	42%
	Total	132	100%

5. There is an effective implementation of IT security in the company where I work.

#	Answer	Response	%
1	Strongly disagree	4	3%
2	Disagree	27	21%
4	Agree	64	50%
5	Strongly agree	34	26%
	Total	129	100%

6. The IT security of the company is sufficient to address the threats, issues and other problems that are related to security.

#	Answer	Response	%
1	Strongly disagree	7	5%
2	Disagree	28	21%
4	Agree	67	51%
5	Strongly agree	30	23%
	Total	132	100%

7. The threats acquired by the company can bring potential damage to its operation and eventually its success.

#	Answer	Response	%
1	Strongly disagree	5	4%
2	Disagree	8	6%
4	Agree	59	45%
5	Strongly agree	60	45%
	Total	132	100%

8. There are greater risks involved when it comes to managing the issues and problems of security in information technology.

#	Answer	Response	%
1	Strongly disagree	3	2%
2	Disagree	9	7%
4	Agree	76	59%
5	Strongly agree	41	32%
	Total	129	100%

9. The IT security of the company comes with a high cost.

#	Answer	Response	%
1	Strongly disagree	4	3%
2	Disagree	28	22%
4	Agree	60	46%
5	Strongly agree	38	29%
	Total	130	100%

10. There are alternative ways of achieving effective IT security without its high cost/price.

#	Answer	Response	%
1	Strongly disagree	6	5%
2	Disagree	32	26%
4	Agree	70	56%
5	Strongly agree	16	13%
	Total	124	100%

11. There are still many aspects of IT security of the company that needs to be improved.

#	Answer	Response	%
1	Strongly disagree	4	3%
2	Disagree	17	13%
4	Agree	72	55%
5	Strongly agree	39	30%
	Total	132	100%

12. Through the project management system, the company can improve its security on information technology.

#	Answer	Response	%
1	Strongly disagree	2	1%
2	Disagree	15	11%
4	Agree	85	63%
5	Strongly agree	32	24%
	Total	134	100%

13. Project management, when integrated with the IT security projects, can improve the success rate of company.

#	Answer	Response	%
1	Strongly disagree	3	2%
2	Disagree	10	7%
4	Agree	72	52%
5	Strongly agree	53	38%
	Total	138	100%

APPENDIX D. INTERVIEW RESULTS

Participant 1

1. Do you consider security on the aspect of information technology as one of the sources of competitive advantage of your company? Explain.

   Yes. Security provides a business with the ability to conduct business online, to conduct business globally, and to maintain consumer confidence. Not considering security in any of these areas would place the organization at great risk. The average consumer is very in tune with what is at stake and they are less willing to compromise when it comes to conducting digital business with a company or with a company on the other side of the glove for that matter.

2. How will you assess the implementation of your organization on IT security?

   Predetermined metrics determined in a planning council or with senior managements commitment. Surveys and interview or random discussion with IT and Business Management about their perception of information security and how well they think the process is currently working and how they believe it can be improved. Lessons learned at the end of projects also provide very good sources of information. And finally security and audit assessments will be and are important elements of this assessment element of the security lifecycle.

3. Do you consider the company's IT security as sufficient to address various threats, issues and problems that are related to security? (Yes/No)

   No

4. What are the risks involved in managing IT security?

   The risk that your measures and well thought out control will not stop new, emerging threats that were not considered in last year's planning cycle.

   The risk that the people component will not buy into the whole concept of security and through errors and omissions contribute to data leakage or disclosure.

5. What can you say about the price or the cost of IT security projects?

   See #6

6. Is there any alternative ways of achieving effective IT security without its high costs?

   I think so. IT Governance and security governance have to find their way into a risk management program. Spending for security initiatives should be tied to asset valuation and risk appetite. Risk assessment facilitates the companies' prioritization effort. How much money is spent to remediate a risk will depend on how great executive management perceives the prevailing threats to be and how much it potentially stands to lose. Once these determinations are made and an acceptable level of risk is provided, remediation and IT Security investment has the potential to produce what I call an acceptable return on risk. Meaning remediation has been optimized to the appropriate risk level set by senior management. Cost can then be offset by return on investment and risk minimization as a result of the new control.

7. Can the project management system improve the company security on information technology? (Yes/No)

   To a certain extent. I would say that implementation of technology, processes, or policies always benefits from a structured deployment plan in the form of a project. But the true measure of success is derived from how well security is sustained in the long term. Security is a process most of the time and not necessarily a project with finite timelines.

8. Which three of the following you believe is most critical element of a successful project? 1.) Plan development and execution 2.) Scope management 3.) Time management 4.) Cost management 5.) Quality management 6.) Human resource management 7.) Communication 8.) Risk management 9.) Procurement

   Plan development and execution
   Communication
   Risk management

9. Can Project Management also increase the success rate of the company? (Yes/No)

   It already does. No executive level support would be possible or resource commitment, without a well thought out plan that includes business drivers and a managed expectation of successful outcomes with a clear return on investment.

Participant 2

1. Do you consider security on the aspect of information technology as one of the sources of competitive advantage of your company? Explain.

   Yes. We do financial transactions, as well as information movement, as part of some of our business processes/business, making security of those essential.

2. How will you assess the implementation of your organization on IT security?

   Please clarify? Are you looking for a specific process? High level - list threats, list remediation taken, assess/test remediation, did it work/not work?

3. Do you consider the company's IT security as sufficient to address various threats, issues and problems that are related to security? (Yes/No)

   No

4. What are the risks involved in managing IT security?

   Technical? Hardware? Software?
   Policies?
   Procedures?
   Staffing?

5. What can you say about the price or the cost of IT security projects?

   Most run over original budget (time and cost).

6. Is there any alternative ways of achieving effective IT security without its high costs?

   Depends on whether or not you can find a knowledgeable, ethical project lead.

7. Can the project management system improve the company security on information technology? (Yes/No)

   Absolutely.

8. Which three of the following you believe is most critical element of a successful project? 1.) Plan development and execution 2.) Scope management 3.) Time management 4.) Cost management 5.) Quality management 6.) Human resource management 7.) Communication 8.) Risk management 9.) Procurement

   Isn't 2 part of 1? If not, I'll go with: 1, 2, and 5.
   Plan development and execution
   Scope management

Quality management

9. Can Project Management also increase the success rate of the company? (Yes/No)

   Absolutely!

Participant 3

1. Do you consider security on the aspect of information technology as one of the sources of competitive advantage of your company? Explain.

   Yes. Will have creditability to customers

2. How will you assess the implementation of your organization on IT security?

   Use Project Management

3. Do you consider the company's IT security as sufficient to address various threats, issues and problems that are related to security? (Yes/No)

   No

4. What are the risks involved in managing IT security?

   Using wrong method or approach in the first place.

5. What can you say about the price or the cost of IT security projects?

   It's worth it.

6. Is there any alternative ways of achieving effective IT security without its high costs?

   Not really

7. Can the project management system improve the company security on information technology? (Yes/No)

   Yes

8. Which three of the following you believe is most critical element of a successful project? 1.) Plan development and execution 2.) Scope management 3.) Time management 4.) Cost management 5.) Quality management 6.) Human resource management 7.) Communication 8.) Risk management 9.) Procurement

   1,5,8

9. Can Project Management also increase the success rate of the company? (Yes/No)

   Yes

Participant 4

1. Do you consider security on the aspect of information technology as one of the sources of competitive advantage of your company? Explain.

   Yes, security is an element that needs to be considered in all types of assurance/audit engagements.

2. How will you assess the implementation of your organization on IT security?

   N/A

3. Do you consider the company's IT security as sufficient to address various threats, issues and problems that are related to security? (Yes/No)

   Yes

4. What are the risks involved in managing IT security?

   Can only answer from an IT consultant perspective. There, a major risk would be not identifying a significant security risk or vulnerability.

5. What can you say about the price or the cost of IT security projects?

   They aren't cheap. As a consultant, there is a trend to either perform work in-house or engage in a joint effort w/ the consultants to minimize costs.

6. Is there any alternative ways of achieving effective IT security without its high costs?

   Internalize, train, have guidelines for security configurations, security software procurement, etc.

7. Can the project management system improve the company security on information technology? (Yes/No)

   Yes

8. Which three of the following you believe is most critical element of a successful project? 1.) Plan development and execution 2.) Scope management 3.) Time management 4.) Cost management 5.) Quality management 6.) Human resource management 7.) Communication 8.) Risk management 9.) Procurement

   1.) Plan development and execution
   3.) Time management

7.) Communication

9. Can Project Management also increase the success rate of the company? (Yes/No)

Yes