

Challenges with Funding of Information Security Projects per Threat Perceptions: A  
Qualitative Case Study

Dissertation

Submitted to Northcentral University

Graduate Faculty of the School of Business and Technology Management  
in Partial Fulfillment of the  
Requirements for the Degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

JEFFERY J. MADISON

Prescott Valley, Arizona  
March 2016

ProQuest Number: 10256844

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



ProQuest 10256844

Published by ProQuest LLC (2017). Copyright of the Dissertation is held by the Author.

All rights reserved.

This work is protected against unauthorized copying under Title 17, United States Code  
Microform Edition © ProQuest LLC.

ProQuest LLC.  
789 East Eisenhower Parkway  
P.O. Box 1346  
Ann Arbor, MI 48106 – 1346

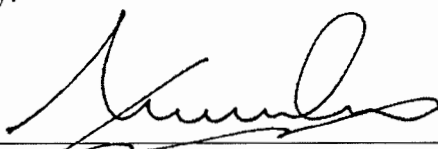
## Approval Page

Challenges with Funding of Information Security Projects per Threat Perceptions: A  
Qualitative Case Study

By

Jeffery J. Madison

Approved by:

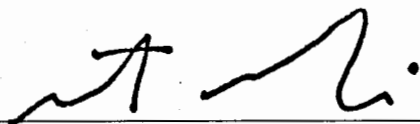


Chair: Dr. Nicholas Harkiolakis

02/06/2017

Date

Certified by:



Dean of School: Peter Bemski, Ph.D.

2/6/17

Date

### Abstract

This research study examined the reasons for the failure of information technology staff to properly protect the organization's data systems from cyber threats. Information technology staff have been assigned the responsibility of protecting the organization's information systems amid a growing number of both internal and external security threats. While the responsibilities have escalated, the funding to adequately protect the organization is not always being made available. The purpose of this qualitative case study was to identify the reasons behind the insufficient funding of information security projects in the private sector. Data collection was conducted by interviewing business leaders and Information Technology (IT) staff from small to medium sized businesses in the United States that are involved in information security decision making. The research methodology used for this study was qualitative. Qualitative research methodology provided an ideal approach to understanding organizational changes, especially changes involving complex stake-holder organizing, work place practices and organizational structure. This made qualitative research a choice method when trying to understand why information technology departments still receive insufficient funding. The following recommendations are being made as a result of this study: It is recommended that companies that want to avoid unnecessary exposure to cyber-attacks and risks take a more serious approach to approving IT security budget requests. It is recommended that organizations invest in a multifaceted cyber-threat defense strategy. This strategy needs to consist of: encryption technologies, security technologies, identification technologies and remediation technologies. The final recommendation is that companies work on creating a more cohesive technical infrastructure. Organizations need to have properly

trained staff working in their Information Security departments and those individuals must be given the financial resources necessary to keep the company secured against both internal and external cyber-security threats (Vuuren, 2016). It is recommended that future researchers monitor the advancements in new cyber-defense technologies and the increase or decrease in successful cyber-attacks. This will serve as a good gauge to determine if organizations are taking proactive steps to defend their organizations against cyber-threats.

## Acknowledgements

I would like to acknowledge everyone that has supported me and encouraged me on this strenuous journey to complete my Doctorate degree. My wife, Kimberly Madison, for encouraging me to continue and persevere through all the frustrations. My daughters, Jmeira and Kaelah. They have been a constant source of inspiration for me. I have been determined to show them that they can do anything they put their minds to do and that hard work does pay off in the end. I also would like to acknowledge all of the rest of my family and friends that offered a word of inspiration as I continued to complete my Doctorate. This includes my parents, in-laws, and family and friends.

## Table of Contents

Chapter 1: Introduction .....	7
Background .....	9
Statement of the Problem.....	11
Purpose of the Study .....	12
Research Questions .....	12
Nature of the Study .....	13
Significance of the Study .....	14
Definition of Key Terms .....	14
Summary .....	15
Chapter 2: Literature Review .....	17
Documentation .....	17
Information Security Challenges .....	17
Information Security Breaches .....	24
Information Security Risks .....	28
Information Technology Protection.....	32
Budgeting and Information Technology Security Projects.....	35
The Risk of Cloud Computing on Cyber Security.....	50
Platform as a Service (PaaS).....	51
Information Technology Governance .....	54
Summary .....	58
Chapter 3: Research Method.....	60
Research Methods and Design(s).....	61
Population .....	65
Sample.....	65
Materials/Instruments .....	66
Data Collection, Processing, and Analysis .....	70
Assumptions.....	71
Limitations .....	71
Delimitations.....	72
Ethical Assurances .....	73
Summary .....	74
Chapter 4: Findings.....	80
Results.....	81
Evaluation of Findings .....	89
Summary .....	90
Chapter 5: Implications, Recommendations, and Conclusions .....	93
Implications.....	95
Recommendations.....	97
Conclusions.....	97

References .....	99
Appendixes .....	106
Appendix A: Interview Guide.....	107
Appendix B: Informed Consent.....	110



## Chapter 1: Introduction

Organizations both public and private, large, and small are all being plagued by a similar problem. They are all struggling to keep their infrastructures secured from both internal and external threats (Pernebekova & Ahbergenovich, 2015). To some this may seem like a small task, but to the business owners, this could mean the difference between longevity and dissolution. One of the primary contributors to the management of internal and external information security threats is the lack of necessary funding to complete information security projects (Pernebekova & Ahbergenovich, 2015; Velmurugan & Mathiyalagan, 2015; Chen, Ramamurthy, & Wen, 2015). This lack of funding is a catalyst for both current and future vulnerabilities to continue to putting the organization at risk (Chen, Ramamurthy, & Wen, 2015).

All businesses rely on data in some way or another. When that data is compromised via an internal data leakage or an external hacking of the systems, there is a cost to it (Velmurugan & Mathiyalagan, 2015). There are the upfront costs such as: compensating customers for any losses they may have incurred as a result of the breach, patching systems that allowed the breach to occur, paying any fines that may result from the breach and many more (Boulesnane & Bouzidi, 2013). The cost of a security breach can be high and can have a negative impact on the business for a very long time (Velmurugan & Mathiyalagan, 2015; Pernebekova & Ahbergenovich, 2015; Boulesnane & Bouzidi, 2013).

Businesses desiring to minimize information security vulnerabilities must be willing to look at all of the individual pieces of technology that are allowed to access their network resources (Brand, Kruger-Van Renen, & Rudman, 2015). Each device that

the organization allows to access its network resources is a device that could be used to leak information (Brand et al., 2015). These devices include things like: laptops, tablets, smart phones, and users that work remotely from a home computer (Brand et al., 2015). Each of these various types of technologies require the organization to have the tools in place to manage them. These tools need to evolve as the technologies evolve (Brand et al., 2015).

In addition to having policies in place to manage the technologies, organizations need to have policies in place to govern the usage of those technologies (Brand et al., 2015). An alarming number of organizations fail to implement policies that govern the users of mobile technologies (Brand et al., 2015). This failure to implement an Acceptable Use policy and have the employees to sign off on it is a set up for a cyber disaster for the organization (Brand et al., 2015).

Organizational success and failure is directly linked to how well the organization implements and manages their technology (Brand et al., 2015). Many organizations implement new technology, but the failure often comes on the management of that technology. The source of the failure to manage new technologies is a lack of resources allocated to its management (Brand et al., 2015).

## **Background**

Companies throughout the world are relying on their information technology staff to keep them secured against both internal and external cyber-security threats (Ifinedo, 2014). Studies are revealing that more organizations have come to understand that malicious individuals want to steal their data and use it for destructive purposes (Gupta & Shakya, 2015). These purposes include things like: stealing client account numbers, stealing banking information, stealing patents, exposing confidential emails and company secrets and much more (Makarevic, 2016). An example of these types of problems can be seen in the attack that Sony Pictures Corporation suffered in September of 2011. In 2011 a hacker used a SQL injection attack against Sony's website allowing the hacker to steal the company's data (Broadhurst, Grabosky, Alazab, & Chon, 2014). That data that was stolen included: names and addresses of employees, employee phone numbers, and email addresses for thousands of Sony customers (Broadhurst et al., 2014). Sony Pictures was aware of the vulnerability, but failed to protect their organization against the threat (Broadhurst et al., 2014).

Other companies to suffer due to cyber-attacks include: Paypal, Gucci, and Home Depot (Broadhurst et al., 2014). The exploit at Gucci was the result of an ex IT staff member exploiting known vulnerabilities in the company's information systems. The former employee created a bogus administrator account while he worked for Gucci and once terminated, he used this account to log in and shut down the computer operations of the entire organization (Broadhurst et al., 2014). In addition to shutting down the servers, the former employee deleted server data, destroyed backup jobs and wiped out user email mailboxes (Broadhurst et al., 2014). The total cost of the exploit cost Gucci

approximately \$200,000 and landed the former employee in jail for 2 years (Broadhurst et al., 2014).

The exploit at Paypal lead to many of their customers be scammed out of monies ranging from \$50 to \$3,000 (Tham, 2013). Customer data was stolen via emails and spoofed webpages. After the exploit, Paypal strengthened their security systems to offer better protection for their customers (Tham, 2013). They also refunded all their customers who disputed charges on the credit cards that they had stored on their Paypal accounts (Tham, 2013).

The Home Depot Corporation suffered from a cyber-attack due to known software vulnerability in 2014 (Elgin, Riley, & Lawrence, 2014). Home Depot had the software available to prevent the attack, but failed to put the software in place (Elgin et al., 2014). This failure costed the company 62\$ million. The vulnerability put 56 million card holders at risk of having their information stolen (Elgin et al., 2014).

It is the duty of the information technology staff to keep the company's technological infrastructure secured. To maintain a high level of security, the technology staff needs access to the necessary resources to complete system critical projects (Chen, Ramamurthy, & Wen, 2015). The problem is that the resources are not always made available. This failure to provide adequate resources to complete information technology projects has cost many organizations large amounts of money could present a huge problem for the security of the organization's information technology systems (Makarevic, 2016).

## **Statement of the Problem**

As information security threats continue to skyrocket, business leaders need to adjust their responses to these threats with an elevated sense of urgency (Ifinedo, 2014). A key component used to determine which security technologies to invest in and implement is cost (Gupta & Shakya, 2015). The majority of information security projects come at a costs that start in the thousands of dollars and these costs are often a source of trepidation for controlling managers (Gupta & Shakya, 2015; Chen, Ramamurthy, & Wen, 2015).

When businesses look for an area of operations to cut cost from, the Information Technology department's budget becomes under consideration (Gupta & Shakya, 2015; Luftman et al., 2013). Business leaders often struggle with the decision to make these capital investments because they cannot easily measure the return they are receiving on their investment (Makarevic, 2016; Otieno & Biko, 2015; Gilbert, Pick, Alan, & Ward, 2012).

A large number of information system (IS) projects are considered to be failures with only 32 % proving to have successfully reached their objectives (Fulk, Kwun, & Alijani, 2013). The high failure rate is attributed to the managerial controls over the project funding and the limited resources allocated to the projects (Fulk et al, 2013). Failure to believe in or understand the validity of the requested information systems (IS) project is listed as one of the primary reasons for receiving limited funding (Dwivedi, Wastell, Laumer, Henriksen, Myers, Bunker, Srivastava, 2015).

The specific problem this research addresses is the lack of knowledge on how information technology managers perceive the reasons information security is

underfunded at small and med-sized private firms in the United States. (Pernebekova & Ahbergenovich, 2015; Velmurugan & Mathiyalagan, 2015; Chen, Ramamurthy, & Wen, 2015; Makarevic, 2016; Otieno & Biko, 2015; Peffers & Santos, 2013; Conboy, 2009; Cao, Mohan, Ramesh, & Sarkar, 2013; Gottron, 2013; Marshall, 2012).

### **Purpose of the Study**

The purpose of this qualitative case study was to identify the reasons behind the insufficient funding of information security projects based on the perceptions of information security decision makers at small and midsized private firms located in the U.S. This study also examined, based on the perceptions of the information technology managers, if the information security systems were adequately able to protect the organization from cyber-threats. Data collection was conducted using interviews of business leaders and Information Technology (IT) staff of small to medium sized businesses in the United States that are involved in information security decision making.

### **Research Questions**

As security violations continue to expose government, public, and private sector security vulnerabilities, it is important to recognize that more needs to be done to fix the problems. The following question has been designed to determine the effects that insufficient IT Project funding can have on an organization:

**RQ1:** What do information security decision makers at small and midsized private firms located in the U.S. believe about the insufficient funding of their information security projects?

**RQ2:** What do information security decision makers at small and midsized private firms located in the U.S. believe are the reasons behind the levels of funding dedicated to their

information security systems?

### **Nature of the Study**

The research methodology used for this study is qualitative. Qualitative research methodology provides an ideal approach to understanding organizational changes, especially changes involving complex stake-holder organizing, work place practices and organizational structure (Gentles, Charles, Ploeg, & McKibbin , 2015). This makes qualitative research a choice method when trying to understand why information technology departments still receive insufficient funding.

The qualitative research design being used in this research was case study. Case study focuses on what is to be studied and is distinguished from the other two design options by its analytical focus on a small number of cases (Gentles et al., 2015). Each case has been studied within its distinct context. The collected data for each case often comes in varying forms including: observations, interviews, documents, and etc. (Gentles et al., 2015).

There are several sources of information used throughout this study like past research findings, media reports, and interviews. Previous research has been extracted using the online database ProQuest. The search criteria included data from the past three years from select businesses located in the US. These businesses were small to medium sized businesses (50 to 250 employees) that have attracted media attention for their failed security measures. Media reports were collected by accessing the following databases: ABI/Inform (Business and Management), IEEE Computer Society Digital library, First Research, and Business Source Premier Databases. The primary source of information used were case studies and interviews.

### **Significance of the Study**

This study was significant because it challenged the concept of doing more with less funding in the area of information technology project management. Many organizations have suffered terrible losses due to insufficiently funded information technology departments (Elgin et al., 2014; Broardhurst et al., 2014; Tham, 2013). The losses have impacted the organizations directly and their customers. This study contributes to the field of information technology by highlighting the growing responsibility of information technology staff and the need to have adequate resources to fulfill those responsibilities. This study uses past research to highlight the growing trend in cyber-attacks. The past research was used to show how some of the cyber-attacks could have been possibly prevented if the proper resources would have been available. Failure to understand the significance of this problem has caused an organizations to become vulnerable to future cyber-security exploits. These exploits have been enough to completely put the organization out of business and permanently injure their customer base. These cyber-security exploits have the potential to cost lots of money to mitigate.

### **Definition of Key Terms**

The terms below appear throughout this research study.

**Data Security:** is defined as the measures taken to protect digital information from unauthorized access (Jafari, 2014).

**Network security:** is defined as the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, and destruction (Jafari, 2014).



**Network Infrastructure:** is defined as the hardware (routers, switches, servers and computers) that are interconnected throughout an organization (Gottron, 2013).

**Information Security Threats:** is defined as a person or thing likely to cause damage or danger to hardware and software programs or processes (Wall, 2013).

**Vulnerabilities:** is defined as a flaw or weakness hardware & software programs and processes that exposes a system to compromise (Wall, 2013).

**Information Security Project:** is defined as a project that is requested to address the information security needs of the organization to keep the organizations hardware, software and processes safe from threats (Wall, 2013).

**Information Security Risks:** is defined as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization (Wall, 2013).

### **Summary**

A key concern for information technology staff in most organizations is the protection of the company's computer systems from both internal and external threats (Wilding & Wheatley, 2015). To properly protect the organization's computer hardware and software systems, the ITS staff must request adequate funding. This adequate funding needs to be sufficient enough to install the systems necessary to keep the organization secured and to maintain those systems (Wall, 2013). This means that the funding needs to be setup to be used on a recurring basis.

Many organizations have suffered because they failed to utilize and support the systems necessary to keep both themselves and their customers safe from cyber-threats (Elgin et al., 2014). Case studies help prove that it is better for companies to be proactive

when funding information technology projects then trying to recover from an exploit (Elgin et al., 2014; Wall, 2013; Wilding & Wheatley, 2015). The reason this theory may prove true is that the impact of a cyber-attack can be felt by an organization well into the future depending on the severity of the exploit.

One of the unfortunate problems for the information security staff is that most of the tools required to keep the business safe from internal and external threats can be quite costly (Wilding & Wheatley, 2015). Compounding the issue of the cost of the projects is the lack of understanding that upper and middle management may have for how the systems work and the benefits they provide for the organization (Wall, 2013).

Information Technology (IT) leaders have the daunting task of proposing information security projects and then justifying the need for the project (Wilding & Wheatley, 2015). Depending on how well the IT leadership can sell the importance of the project can be a key determinant factor to whether the project gets tentative approval for funding (Wall, 2013).

## **Chapter 2: Literature Review**

### **Documentation**

The literature search strategy consisted of searching peer-reviewed journals and scholarly articles that were no older than three years old and found using ProQuest online database and EBSCOHost online database. The research criteria used for searching for articles included: Peer-reviewed, scholarly articles posted within the past three years. The reason for these search criteria is: scholarly articles are considered to be written by industry experts, which is important for this research. Peer-reviewed articles include research publications that have been evaluated and approved by other industry experts. The keywords that were used for during the search include: information technology theories, information technology budgets, information technology security problems, information technology security issues, organizations that have suffered from cyber-attacks, the problems with cloud storage, information technology training, professional and university information technology training, information security vulnerabilities, information technology management, and lack of budgetary theories. Lastly, a three-year time window was used because in the field of information technology things are changing daily and the three year time window span seemed to offer the best chances of locating the most current research available.

### **Information Security Challenges**

One of the top five challenges facing the business world today is the risk of suffering a cyber-attack (Fenz, Heurix, Neubauer, & Pechstein, 2014). This statistic is based on the intrinsic relationship with society and technology. It has been realized that any devices (smart phones, tablets, laptops, smart watches etc.) that are operated by a

commercially available software package and connected to the internet can be manipulated into performing in an undesirable fashion (Fenz et al., 2014). This problem is only expected to worsen in the years ahead (Wall, 2013). Many technology industry reports have summarized that nearly every industry, country and type of data has been involved in a data breach in one way or another (Fenz et al., 2014). Some knowingly and others unknowingly. Symantec Corporation released a publication in 2012 stating that hackers are now targeting smaller businesses, which were once thought to be of little interest to hackers (Fenz et al., 2014).

These escalating threats continue to present challenges for the information technology field. Specifically, to the area of information security. The purpose of the information security team of an organization is to protect the organization's assets, data and technology from both internal and external threats (Wall, 2013). One of the problems that hinder the ability of the information security team to protect the organization is a lack of Risk Management tools (Fenz et al., 2014).

The term "Risk Management" as it relates to information security dates back to 1975 and was coined when the USA National Bureau of Standards proposed Annual Loss Expectancy (ALE) as a metric for measuring computer related risks (FIPS, 1975). Annual Loss Expectancy is calculated by summing up the products of impact ( $I(O_i)$ ) and frequency ( $F_i$ ) of harmful outcomes (Fenz et al., 2014). The challenges of information security have only continued to escalate as the years progressed. In the 1980's the USA National Bureau of Standards sought to further refine the process or risk management by coming up with several key steps in the process of assessing the risk. These steps include: identification of the requirements (asset values, threats,

vulnerabilities, existing safeguards, etc.), analysis of threats, vulnerabilities and the scenario, risk measurement, acceptance test, and safeguard selection and implementation (Fenz et al., 2014).

Even in the 1980s it was realized that a formalized structure was needed to deal with the challenges of information security. Information security specialists need to know what they are protecting. Is it a hardware or software asset? Who has access to it? Does the access allow for internal (employees) access or both internal and external (contractors or vendors) access? How is the asset being secured? How is the access being controlled? What security measures does the organization have in place? How often are they evaluated? These are the types of questions that the information security team need to be asking themselves as they seek to control and safeguard the assets of the organization.

Information security specialists must also deal with challenges that come along with culture (Arutyunov, 2014). Cultural challenges include challenging accepted beliefs. These cultural beliefs come into play when they impact how a business handles its operations. These are the businesses that may put spiritual beliefs over practicality. It is okay to expect everyone to do the right thing, but statistics have proven that people exploit the opportunities to do wrong if they are given the chance (Arutyunov, 2014).

Another challenge that plagues the information security field is the lack of properly trained information security staff and employees (Sauls & Gudigantala, 2013). Maintaining a properly technologically secured environment takes a combination of high level information security personnel and properly trained regular employees (Sauls & Gudigantala, 2013). There was a time during history when businesses promoted staff to

positions based on tenure rather than qualifications (Sauls & Gudigantala, 2013). This means that a person with no real skills or abilities in a given area could be placed in a vital position and expected to learn the duties of that position as they go. While this method may be manageable in a more industrial setting, it does not work in the information security field.

As new information security threats continue to be revealed, it is important that organizations recognize the value in having highly trained staff available to deal with those threats (Sauls & Gudigantala, 2013). Information Security personnel need to be familiar with the assets they are entrusted to protect. This includes all hardware, software and processes (Sauls & Gudigantala, 2013). It is this understanding that help them understand the gravity of what they have been entrusted to do. The information security staff not only need to be familiar with the technology of the organization, but they also need to be familiar with the most current methods of threat remediation (Sauls & Gudigantala, 2013). This means that these individuals are expected to stay current on technological trends, threats, tools and techniques used to properly identify and stop all threats to the organization's assets.

With most commercial and government information systems connected to the internet, it is only a matter of time before they are attacked by a cyber-threat (El-Taj, 2015). The challenge for information technology professionals is to identify these threats quickly and prevent them from doing malicious things to the organization's information technology systems (El-Taj, 2015). One of the complicated decisions that must be made by the information technology staff and the organization's management team is which type of intrusion detection system do they want to put in place, if any (El-Taj, 2015).

There are different types of intrusion detection systems, with each setup for a particular purpose. The first is the active Intrusion Detection System (IDS) also known as the Intrusion Detection and Prevention System (IDPS) (El-Taj, 2015). This type of setup is designed to automatically block suspected attacks without any interaction of an operator (El-Taj, 2015). This system has the benefit of real-time corrective action in response to an attack (El-Taj, 2015). The challenge with this system is that it must be subscribed to an online service so that it can receive updates from the manufacturer that contain the latest threat definitions (El-Taj, 2015). This type of system is strictly reliant upon its threat definition database being current and accurate.

The next type of intrusion detection system is known as a Host Intrusion Detection System (HIDS) (El-Taj, 2015). Host Intrusion Detection Systems rely on the computer operating system to audit and monitor data and analyze the events being generated by programs (El-Taj, 2015). The challenge that comes along with type of system is its limited protection abilities. This type of protection can only monitor the local workstation and if the workstation's database becomes corrupted, then this type of system does not provide sufficient protection (El-Taj, 2015). This type of solution may work for personal use, but it does not provide adequate protection in a corporate environment (El-Taj, 2015).

There is a knowledge-based (Signature-based) Intrusion Detection System and this type of intrusion detection system references a database for the signatures of known threats (El-Taj, 2015). Each intrusion or threat leaves behind a digital footprint which gets cataloged in a central database and gets accessed by the intrusion detection system (El-Taj, 2015). Some of the challenges with this type of intrusion detection system is that

the Signature database must be constantly updated to provide optimal protection (El-Taj, 2015). When this of intrusion detection system does not know how to identify a threat, it typically ignores it and this allows the threat to continue to cause damage the organization's computer systems (El-Taj, 2015).

The last type of Intrusion Detection System is the Behavior-based (Anomaly-based) intrusion detection. Behavior-based intrusion detection learns normal patterns of system activity and uses this pattern to help it identify anomalies (El-Taj, 2015). The challenge with this type of intrusion detection system is that it has high rate of false alerts (El-Taj, 2015). This is because various programs can change their behaviors due to system updates or other program modifications (El-Taj, 2015).

In addition to having properly trained and highly skilled information security staff, businesses face the challenge of keeping their staff updated on various aspects of information security as well. This is a definitely a challenge for many organizations. They must decide things like: how much does the staff need to know? Do all of the employee's need the same level of information security training? How often do we train on information security? These types of questions and scenarios present a very real challenge in the area of information security.

Proper employee training is a challenge to organizations large and small, public and private (Sauls & Gudigantala, 2013). What organizations need to understand is that some risk could be reduced through proper training (Hedstrom et al., 2013). Statistics have proven that when employees are properly trained on information security risks that they are more likely to avoid the things that present risk for the organization (Fenz et al., 2014). Employees need to be trained on the importance of things like: Internet



Acceptable Use (as most threats seem to occur online), the importance of keeping their credentials secured. This means not sharing passwords with their peers, not writing passwords down and not storing passwords on systems that others can access without encrypting the file (Fenz et al., 2014).

When businesses understand that the information security team and the employees must work together to keep the business safe, the challenges begin to diminish. Information security is a team effort. The information security team watches out for the organization at a high level, but they cannot catch problem. This is why teamwork is so vital. The employee is more likely to be the first person to recognize a problem or abnormality in their daily duties. If they report the problems to the information security team right away, there is a good chance the team can locate, isolate and remediate the problems (Fenz et al., 2014).

Another challenge of the information security team is trust (PN, 2014). As the news and media continues to inundate the airwaves with stories of data breaches at some of the largest and most popular organizations in the world, it has left some doubting if they can really trust the technology to help them accomplish the goals of their organizations (PN, 2014). More businesses are coming around beginning to realize just how vital technology is to their operations. It is through technology that businesses have a web presence to conduct business all over the world. It is through technology that businesses can process payments in minutes which is a significant improvement over the days and weeks it used to take (PN, 2014). This same technology that has opened the proverbial global door for businesses is the same technology that has allowed for all of the cyber exploitation (PN, 2014).

The challenge to the information security staff has been to get both the upper management and middle management to trust that their investments in modern technologies are in the organization's best interest (PN, 2014). This means that the information security professional needs to be able to properly explain the necessity for the investment and highlight the risks that come along with delaying this investment. This is information that the media is not going to highlight. It is important that the information security team be able to demonstrate the effectiveness of the organization's current technology and emphasize how investing in the new technology would strengthen the company's defense against cyber-threats (PN, 2014). Information security teams face many challenges and each challenge needs to be addressed appropriately if they are to successfully keep the organization secured from cyber threats.

### **Information Security Breaches**

Hedstrom et al. (2013) goes in to great detail to addressing all of the facets of risks that companies are being inundated with. Otieno & Biko (2015) also go into great detail on how the growth in services organizations have gained access to by using the internet has also led to a heightened concern for security breaches. As organizations become more reliant upon internet and cloud based services they are putting their organizations in a position to suffer from a cyber-attack (Otieno & Biko, 2015). The driving factor pushing organizations to web and cloud based services has been identified as costs (Otieno & Biko 2015). Internet and cloud based services allow organizations to have access to resources including software and services that they could not normally afford or justify purchasing on their own due to the cost (Otieno & Biko 2015).

Many of the organizations that provide the online software and services attempt to

reassure their customers by implement various levels of security to help eliminate the risk of a security breach (Otieno & Biko 2015). Security of the information on the internet platforms continues to be a major concern for many businesses and in some instances the lack of security is overshadowing the benefits the services are providing (Otieno & Biko 2015). Businesses that conduct business using the various internet based platforms have a responsibility to their customers to do everything possible to keep them safe from the malicious cyber-attacks that continue to hinder businesses with a strong web presence (Otieno & Biko 2015).

With the continued rise in web based threats, companies are being subjected to an increasing number of compliance requirements from both their clients and government agencies. They must deal with all of these new requirements while trying to manage internal and external threats. Depending on the size of the operation, they may not have the appropriate staff to manage the information technology security of their environment (Hedstrom et al., 2013). Some may have systems in place, but they failed to keep them updated and have no real person monitoring them (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2012). While other organizations have the staffing in place to adequately address technological threats, but they are not given the resources necessary to do the job.

Large corporations throughout the world have been the victims of major cyber based threats in the past several years. These companies include: Sony Pictures, Google Inc., Home Depot, Target and Capital One (Wilding & Wheatley, 2015). All of these institutions had systems in place to detect threats, but they failed to have anyone monitoring the systems (Wilding & Wheatley, 2015). This failure to allocate needed resources to their information security staff led to these companies having their

vulnerabilities exposed to the world (Wilding & Wheatley, 2015).

One of the largest organizations to suffer a costly loss to hackers was Epsilon, the world's largest provider of marketing and handling services (Hausken, 2015). In 2011 Epsilon suffered damages ranging from \$225 million to \$4 billion dollars (Hausken, 2015). In this same year Citibank, Microsoft and the National Aeronautics and Space Administration (NASA) were also hacked (Hausken, 2015). Organizations that are targeted by hackers are chosen for a variety of reasons and one of those reasons could be an insufficient level of security for their networks (Wilding & Wheatley, 2015).

Sony Pictures had a system in place where they stored the passwords used to access their systems on those same systems in unencrypted folders marked passwords (Wilding & Wheatley, 2015). These passwords were on a system that was not being monitored and had no resources allocated to its monitoring (Wilding & Wheatley, 2015). This allowed hackers to access anything they wanted on Sony Pictures servers. This included things like: emails, financial information, unreleased movie information and much more. It is highly plausible that these leaks could have been prevented had the resources been put in place to monitor these systems.

The attack on Target is another example of a company that failed to have the proper resources allocated to their IT Dept. Target's compromise came as the result of their supervisory control and data acquisition system (SCADA) (Wilding & Wheatley, 2015). Target did have a system in place to detect threats, but no one to monitor this system and by the time the threat had been identified, millions of customers had their credit card information stolen (Wilding & Wheatley, 2015).

Of all of the companies that have suffered attacks, they all seemed to share the

same problem, they failed to put the tools in place to keep themselves safe (Wilding & Wheatley, 2015). They failed to allocate sufficient resources to their IT staff so they could do the jobs they were hired to do and that is keep the company's information technology systems up and running and safe(Wilding & Wheatley, 2015).

Other companies to suffer due to cyber-attacks include: Paypal, Gucci, and Home Depot (Broadhurst et al., 2014). The exploit at Gucci was the result of an ex IT staff member exploiting known vulnerabilities in the company's information systems. The former employee created a bogus administrator account while he worked for Gucci and once terminated, he used this account to log in and shut down the computer operations of the entire organization (Broadhurst et al., 2014). In addition to shutting down the servers, the former employee deleted server data, destroyed backup jobs and wiped out user email mailboxes (Broadhurst et al., 2014). The total cost of the exploit cost Gucci approximately \$200,000 and landed the former employee in jail for 2 years (Broadhurst et al., 2014).

The exploit at PayPal lead to many of their customers be scammed out of monies ranging from \$50 to \$3,000 (Tham, 2013). Customer data was stolen via emails and spoofed webpages. After the exploit, PayPal strengthened their security systems to offer better protection for their customers (Tham, 2013). They also refunded all their customers who disputed charges on the credit cards that they had stored on their Paypal accounts (Tham, 2013).

The Home Depot Corporation suffered from a cyber-attack due to known software vulnerability in 2014 (Elgin, Riley, & Lawrence, 2014). Home Depot had the software available to prevent the attack, but failed to put the software in place (Elgin et

al., 2014). This failure costed the company 62\$ million. The vulnerability put 56 million card holders at risk of having their information stolen (Elgin et al., 2014).

The US Navy suffered an information security breach that put over 130,000 Navy sailors at risk (Chief of Naval Personnel Public Affairs, 2016). Hewlett-Packard is a contractor for the US Navy and one of the laptops that the company uses for storing information for the contract was compromised on sometime during 2016. The compromise was brought to the Navy's attention on October 27, 2016. Analysis of the compromise revealed that the social security numbers and names of sailors were taken. The sailors were offered free credit monitoring for their trouble (Chief of Naval Personnel Public Affairs, 2016).

The last security breach to be analyzed in this research is the attack on the Democratic National Committee server by Russian hackers (Nance, 2016). In March of 2016 an unknown entity had hacked into the Democratic National Committee's server (Nance, 2016). The hackers were searching for information on presidential candidate Donald Trump. After locating the information they were looking for, the attackers spent months going through the server stealing data. The stolen data consisted of emails, donor bank account information, credit card information, and even donor social security numbers (Nance, 2016). The group responsible for the attack is called the Cyber Bears (Nance, 2016).

The attack was eventually halted after an IT security company called CrowdStrike had been hired by the DNC to determine the severity of the attack (Nance, 2016). The DNC reported that they are attacked regularly by different groups based on their political agendas. CrowdStrike used analytical tools to see where the breaches occurred, what was

compromised and how long the intruders had been in the DNC's servers. It was determined that the attack went back as far as April 2015 (Nance, 2016). CrowdStrike was able to work the DNC to neutralize the threat, though it took over a year before the threat was ever noticed (Nance, 2016).

### **Information Security Risk Management**

In order to quantify the benefits of making sound IT Project investments the organization needs to have the proper staff available to perform information security risk assessments (Fenz et al., 2014). These assessments need to be based on sound risk management strategies. ISO 27005 (ISO/IEC, 2013) breaks down information security risk management methodology into three categories: risk assessment, risk treatment and risk acceptance (Fenz et al., 2014). Each step is crucial to the proper identification and handling of risks. What systems are impacted? What is the most efficient way to mitigate the risk? How much risk is the company willing to accept? These are all key questions in a risk assessment plan.

If the results of the risk assessment are acceptable, then the risk treatment phase can be started (Fenz et al., 2014). If not, the organization will need to conduct another risk assessment to gather more detailed data on the system, potential threats and vulnerabilities (Fenz et al., 2014). In the risk treatment phase, the company puts the treatment plan into action (Fenz et al., 2014). This includes the implementation of various controls based on the risk assessment phase to reduce risk down to an acceptable level (Fenz et al., 2014).

There is another type of information technology risk management called EBIOS

(DCSSI, 2004). This method has five phases. These phases are: a context study to properly identify the environment, purpose and operation of the target system (Fenz et al., 2014). The next phase is the expression of the security needs (risk assessment) phase. During this phase there is an evaluation of the essential assets in terms of availability, integrity and confidentiality. Next a threat study is conducted to properly identify potential threats effecting the systems and the corresponding vulnerabilities which could be exploited by these threats. There is the identification of security objectives to formalize the risks by comparing the potential impact of potential threats to the security needs of the company and lastly there is the determination of security requirements to determine functional requirements which allow the accomplishment of the defined security objectives (Fenz et al., 2014).

Another method of information security risk management is the OCTAVE method (Alberts et al., 2003). The OCTAVE method is a three-phased methodology. The phases are: determination of important assets, already implemented security controls and the most critical assets as the creation of the threat profiles. The identification of infrastructural vulnerabilities and the identification of risks relevant to the critical assets and of possible controls to mitigate the risks to an acceptable level along with the creation of a protection strategy (Fenz et al., 2014).

CRAMM (the CCTA Risk Analysis and Management Method) is another method that focuses on three phases of information technology risk management with its origins in the UK (Fenz et al., 2014). The three phases of CRAMM are: asset identification and valuation: threat and vulnerability assessment; and countermeasure selection and recommendation (Fenz et al., 2014). The asset identification and valuation focuses on



cost. The cost to replace hardware and software (Fenz et al., 2014). The vulnerability assessment is used to assign a specific value to an asset based on its risk (Fenz et al., 2014). Lastly, the recommendation is used to implement a plan of action to reduce the risks to acceptable levels (Fenz et al., 2014).

The FAIR risk management methodology was introduced by an industry consortium striving for IT-standards and boundary less communication (Fenz et al., 2014). FAIR (Factor Analysis of Information Risk) is based on four stages to determine and articulate risks. These stages are: identification of assets and threats to them; identification of influencing variables and evaluation of loss event frequency; evaluation of probable loss magnitude; and derivation of risks (Fenz et al., 2014).

The FAIR-methodology relies on an existing Information Security Management System compliant with ISO 27001 (ISO/IEC, 2013) in order to provide sufficient risk management (Fenz et al., 2014). It's methods allow for the easy identification of risks. The simplicity of FAIR also presents its downside, as results depending on variables outside FAIR's considerations are consequently wrong, but not perceived to be erroneous or critical by the methodology itself (Fenz et al., 2014).

ISAMM, established by the Telindus group, uses quantitative risk management methods (qualitative methods are supported as well) to determine risks and express their monetary value (Fenz et al., 2014). ISAMM uses ALE (annual loss expectancy) to form a return of investment approach and economic justification for controls under considerations of the risk treatment plan. ISAMM provides tools that are capable of simulating and comparing the effect of implemented controls on the ALE, helping decision makers in their task of selecting cost-efficient controls (Fenz et al., 2014).

ISAMM risk assessment usually consists of four steps: scoping; identification of threats and compliance; validation of compliance and threats; and calculating and reporting (Fenz et al., 2014). This methodology was developed to offer full support for ISO 27001, allowing simple compliance with the standard. ISAMM methodologies sound promising, because it supports both statistical and quantitative methods and aids decision makers in answering tough questions through simulations on the return of investment of security controls (Fenz et al., 2014).

IT Risk Management training is just as important as the methodologies that are implemented to keep organizations safe (Ahmad & Maynard, 2014). Training needs to take many forms to properly prepare the individuals that will be entrusted with the tasks of information security and risk assessment. This training will need to come in the form of formal, information and technical training (Ahmad & Maynard, 2014). An assessment of formal training at the university level found that the training focused too much on the technical aspect of information security and risk management and not enough on the management side (Ahmad & Maynard, 2014).

Many researchers have identified significant problems regarding the lack of security awareness training in organizations. Successful implementation of security awareness training programs have been identified as a pivotal way to proactively address security vulnerabilities (Williams, Hardy, & Holgate, 2013). The primary reason given for failing to implement security awareness training programs was cost. The cost to pull the staff away from production and have them sit through training can be quite substantial (Williams et al., 2013), but it is still proven to be necessary.

While the technical training is important, the major decisions that are made

regarding risk management happen on the strategic management side (Ahmad & Maynard, 2014). This is why it is important that students entering the Information Technology field have a wide array of training and that the training covers the many facets of information technology and risk assessment (Fenz et al., 2014). When a review was done on universities in China and the USA, the lack of managerial training was further realized (Ahmad & Maynard, 2014). In both countries, the students were being trained to be great engineers without much emphasize on leadership (Ahmad & Maynard, 2014).

It is important that students understand that Information Technology Risk Management programs cover more than just systems and processes, but they also cover the people who are using these systems on a daily basis (Ahmad & Maynard, 2014). This is why it is important that the students understand that the decisions are often not resolved based on mathematical equations alone. Some suggestions may make great technical sense, but unless there is buy in from management and sometimes staff, the project could be delayed or even denied (Ahmad & Maynard, 2014).

### **Information Technology Protection**

Some organizations have adopted an older technology in an effort to deter cyber criminals from interfering with their operations. The technology many have reverted is cryptography (Otieno & Biko 2015). Cryptography is ancient technique uses various algorithms to conceal the context of a message from outside parties (Otieno & Biko 2015). The components of the algorithms include security details such as digital signatures, secret security keys and even security challenge questions (Otieno & Biko 2015). Each component has to be successfully passed before the message can be

decrypted for the recipient.

There are two main techniques for cryptography which include: Symmetric and Asymmetric (Otieno & Biko 2015). Their primary differences are in the way they encrypt and decrypt messages (Otieno & Biko 2015). Symmetric encryption is a secure communication method that uses a single secret key to develop the encryption method and decrypts the message from the cipher (Otieno & Biko 2015). This method requires both the sender and the recipient to share secret keys and use similar methods of decoding the message in their secure communications (Otieno & Biko 2015). The primary purpose of this technique is to ensure high levels of privacy between the two parties. The benefits of this technique of encryption is that it reduces the ability of the information being compromised by a 3<sup>rd</sup> party because only two individuals have access to the decryption keys (Otieno & Biko 2015). This type of encryption starts to see vulnerabilities as the number of parties grows beyond two people. The more the encryption keys are shared the more vulnerable the encrypted message is to interception (Otieno & Biko 2015).

The next type of encryption is called Asymmetric encryption. Asymmetric encryption differentiates itself from symmetric encryption by using different keys for encrypting and decrypting a system message (Otieno & Biko 2015). The use of different keys in the creation of the cipher and the retrieving of the message reduces the probability that someone using either of them to outline any malicious objectives (Otieno & Biko 2015). One of the primary advantages of this type of encryption is the control that it gives to the message creator. A sender using asymmetric encryption can develop a key that is unique to them and use it to generate many messages and control who has the

ability to read them (Otieno & Biko 2015).

Asymmetric encryption requires the use of two keys, a public key and a private key (Otieno & Biko 2015). The sender has to have access to a directory that has the public keys of the recipients that they wish to exchange messages with (Otieno & Biko 2015). The recipients have a private key that goes with their public key and they use this key to decrypt the message (Otieno & Biko 2015). Any individual trying to intercept the message needs to have access to the private key and the private key is not something that is shared.

As organizations share more information over the internet and using cloud services, they need to understand the importance of cryptography (Otieno & Biko 2015). Any data in motion over networks (internal or external) is susceptible to interceptions from malicious outsiders (Otieno & Biko 2015). Encrypting data transmissions adds another layer of security to the organization's activities. Encryption takes data transmission security to a new level beyond mere password encryption (Otieno & Biko 2015).

Passwords are often thought of as a strong defense against individuals trying to intercept data transmissions (Otieno & Biko 2015). While passwords do provide a basic level of protection, they do not provide enough protection when sending confidential information to various parties (Otieno & Biko 2015). Some institutions have implemented the policy of strong passwords. A strong password is a password that has a minimum number of letters, both upper and lower case, numbers and special characters and the password cannot be the individual's name (Otieno & Biko 2015). While these type of passwords offer more protection than standard passwords, they still fail to provide

an adequate level of protection against transmission interceptions (Otieno & Biko 2015).

Password authentication key exchanges exist to prevent individuals from accessing whole systems, but the strength in cryptography is that it protects the information while it is in transit (Otieno & Biko 2015). Both technologies are necessary for the protection of the organizations information and both have their specific purposes. It is up to the organization to properly implement the technologies to maintain the integrity and security of their data (Otieno & Biko 2015).

### **Budgeting and Information Security Projects**

The rigorous duties of the information technology department cannot be completed without proper funding (Tsohou et al., 2012). The responsibilities of those tasked with network and infrastructure security are ongoing and ever changing (Hedstrom et al., 2013). This is because they are dealing with things like: software and hardware maintenance, protecting the organization from new cyber-based threats, replacing out dated hardware, protecting the organization from internal threats and much more (Tsohou et al., 2012)

These sentiments are echoed by Analyzing trajectories of information security awareness. Information technology departments are being overwhelmed by the increasing requirements to secure their company's infrastructures with a decreasing number of resources (Tsohou et al, 2012). This is being further complicated by more legislation that fails to tell companies how to implement the new requirements. The purpose of the legislation is clear, it is to reduce the possibility of businesses putting their customers and employees at risk, but failure to audit for compliance of implementation is

where legislation falls short.

Many companies are forced to choose between the risks of not complying with new information security legislation, which may require huge capital investments that they do not have, and investing their resources in other areas of the operation (Tsohou et al., 2012). This decision is often based on how the decision makers in the organization feel their investment may pay off for them.

There are many information security standards available for both public and private sector businesses to adopt. Some are federally enforced and others are optional or best practices. A few of these standards are: ISO/IEC 27001/27001, Sarbanes-Oxley and even Payment Card Industry (PCI) compliance standards. Sadly, less than 43% of surveyed company's felt they were budgeting properly for security threats, this is out of the 275 US companies that were surveyed (Tsohou et al., 2012). At the government level the statistics are more difficult to get due to the latency in which updated information is published. Despite the entity, most found themselves unprepared to address a threat.

Much research has been done to identify the problems associated with insufficient funding for information technology projects, but the one constant failing in research is the cost of a security breach. While (Williams et al., 2013) focuses on the security shortcomings of business leaders, their research is following the same patterns as other researcher work that has been done. Government offices, public and private sector businesses have many regulations to comply with, yet they are guilty of not taking the proper proactive steps to keep their environment secure.

When questioned about the various reasons why many updated security measures had not be implemented, the answer was consistently a lack of funding (Williams et al.,

2013). Research data was analyzed from the Information Security Governance (ISG) database to come up with this information. Studies continue to identify with no uncertainty that there is a problem, yet the problem continues to grow because the full cost of a violation remains a mystery. It is often times difficult for those on the information technology staff to convince those in management that their projects need immediate funding because the majority of IT projects are requested that way (Williams et al., 2013).

It is clear that violations are happening in public, private and government offices, but educational institutions are also at a great risks (Yoon, Hwang, & Kim, 2012). Research was conducted at several universities through the US to determine how secure the students perceived their environment to be. The survey was submitted anonymously and consisted of several thousand students to protect their identities. The survey revealed that many students admitted to engaging in practices that violate the school's rules because there is no perceived consequence (Yoon et al., 2012).

The same type of scenario was observed during the research conducted by (Ilvonen, 2013). Where there is no enforcement, the rules are typically broken. There is often no enforcement of security standards because the institutions like corporate organizations have not invested in technological projects that would keep both them and their student body safe from both internal and external cyber-threats (Ilvonen, 2013).

Some researchers (Halaweh, 2012) believe individual security mandates are increasing and that people come to a stage of self-regulation and the need for continuous security improvements are diminishing, but that remains to be proven (Halaweh, 2012). All indicators seemingly point to individuals with unchecked authority and privilege



exploiting those rights. Other theories used to assess information security failings are all reactive. Some researchers have attempted to use grounded theory (GT) to understand the why behind security disasters. These theorists seem to be overlooking the research that has indicated that a lack of oversight is often of the problem. GT's usefulness is only fully realized when the data collected is used to implement an effective change policy.

Every facet of the business environment in North America continues to struggle with the question of "how do we implement better security measures" (Noor & Ajis, 2013)? Business leaders struggle with the decision to release the resources for information technology projects that are required to properly secure their environments. It is this continual struggle and justification process that has organizations in North America in a state of vulnerability (Noor & Ajis, 2013).

When it comes to the US military, there is the expectation that high security standards are the norm, yet they suffer from the same problems as the rest of the free, technology driven world, the lack of sufficient funding to implement a properly secured infrastructure (Noor & Ajis, 2013). The lack of funding for those working in government institutions is often weighed down with political red tape which can take a significant amount of time to work through (Noor & Ajis, 2013). This type of situation leads to vulnerable systems and serves as a beacon for attackers or perpetrators. The attacks do not always occur from the outside either. Some of the attacks and infiltrators are those working for these government agencies. Those committing the infractions are those that know they are not being monitored and that the consequences for their actions should they be caught are trivial. A constant reminder that the costs of infractions are truly an unknown and security project requests deserve significant consideration.

There are those theorists that also believe training is the answer. Maybe if more companies had security awareness training programs that would help (Ilvonen, 2013). It is more than a lack of training that has created culture of individuals that thrive on hurting businesses. The motives of some individuals will never be known, while others are just out to be malicious.

When surveying 1000 companies in the US, it was realized that 73% of them had security awareness training programs (Ilvonen, 2013). What was also assessed during the analysis of the results is that the training information is rarely updated and that the training typically only happened when an individual was first hired. Insufficient training programs are often the result of a company failing to see the value in them (Ilvonen, 2013).

This meant that employees were not being required to acknowledge updated security standards and changes (Noor & Ajis, 2013). The problem is that management often times does not see the value in stopping production to have staff attain training for an hour (Pathari & Sonar, 2013). Yet, these employees present a source of great vulnerability for the company. The cost of stopping production is immediately realized, but the cost of a security threat is not always so obvious and neither are the benefits of investing in information security project (Ilvonen, 2013).

Employees are the both the greatest asset of any business, government, educational or military institution and they are also the biggest source of threats (Thomson & Niekerk, 2012). The higher the level of the employee, the higher they are on the threat list. It is because they have access to all of the company's critical information. Having a properly trained staff that is equipped with the resources they

need to do their jobs is a great benefit for any organization (Thomson & Niekerk, 2012). It is when individuals begin to feel unappreciated that they have the tendencies do things that could harm the company (data leaks, file deletions, etc.) (Thomson & Niekerk, 2012).

Properly equipped employees can foster an environment of comradery or one of rebellion (Ilvonen, 2013). The company needs to make sure these individuals don't go unchecked in their power. Those creating the rules must also be expected to abide by them (Sommestad, Hallberg, Lundholm & Bengtsson, 2014). 54% of breaches in firms are the result of a staff member not doing their jobs (Sommestad et al., 2014). This is an unacceptable statistic. This is behavior that could be prevented with the right auditing systems in place and a properly trained staff to monitor it. Security staff should be required to go through ongoing industry specific training so they are prepared to handle new information security scenarios as they arise (Sommestad et al., 2014).

There are also those entities that do take security more seriously, yet they are hampered by politics (Koong, Merhi, & Sun 2013). Homeland security is one of those agencies. It is unimaginable that such a powerful agency could be hampered by politics. Out of a survey of 24 federal agencies and their security standards, 75% were behind on security mandates (Koong et al., 2013). The staff knew what needed to be done and what changes needed to be implemented but were not given the resources that they required to implement them. The survey revealed that the agencies are not likely to be tested for compliance, so the department heads simply acknowledge the new standard. The reason given for failing to follow new legislative mandates was insufficiency budgeting. Another example of failing to fully understand the cost of a security breach.

### **Theoretical perspectives**

There are many applicable theories when it comes to information security and project budgeting. Understanding and applying relevant theory can be pivotal to the success of an organization (Jamali, Voghouei, & Md Nor, 2014). Some of the theories include: general deterrence theory, protection motivation theory, theory of reasoned action, theory of planned behavior, social control theory and the theory of moral decision making.

General Deterrence theory (GDT) is a conception in the legal system and criminology which proposes the use of punishment as a threat to deter people from offending (Hassan, Reza, & Farkhad, 2015). This theory places an extreme importance in the role of punishment and strict legal penalties for unacceptable behaviors (Hassan et al., 2015). GDT has been used to combat criminal justice, ethics and most recently cyber-loafing problems. Cyber-loafing is when employee's use of company-provided internet access and corporate email during work hours for non-work purposes (Hassan et al., 2015).

As the information technology staff at organizations struggle with implementing policies and procedures to keep the organization safe from threats, GDT often comes to mind. GDT suggests that the threat of sanctions can modify unacceptable employee behaviors by emphasizing the consequences of certain behaviors over the perceived benefits of partaking in those behaviors (Hassan et al., 2015).

There are three components that make up GDT. These components are: sanctions, detection, and enforcement (Urgrin & Michael, 2013). Sanctioning is the

primary factor of GDT (Hassan et al., 2015). The undeniable promise of consequences of a purported activity is believed to be a great deterrent in preventing individuals from engaging in cyber-slacking activities (Ugrin & Michael, 2013). The more severe the sanctions, but the more effective they are believed to be. GDT emphasizes the follow through of the threats that should be outlined in the organizations Acceptable Use Policy (AUP). The AUP is an agreement that should be signed by all employees that dictates what behaviors are allowed and not allowed when using the company's technological resources (Hassan et al., 2015).

(Ugrin & Michael, 2013) proposed that the effectiveness of the potential sanctions on cyber-loafing can be moderated by an increased likelihood of detection and evidence of past enforcement for less abusive behaviors (Ugrin & Michael, 2013). In other words, when the employees know that they are being watched and they are aware of other employees that have been busted for cyber-loafing, they are less likely to engage in those activities. It is important for the employees to understand that there is a strong chance that they will be caught if they engage in cyber-loafing (Hassan et al., 2015). This means when a person is caught engaging in cyber-loafing behaviors, the punishment must be imminent, this will increase the policy's effectiveness (Ugrin & Michael, 2013).

Protection Motivation Theory (PMT) posits that when someone is presented with a threat, he or she experiences cognitive processes of threat appraisal and coping appraisal (Menard, Gatlin, & Warkentin, 2014). After assessing the threat and its associated coping mechanisms, one decides to perform either adaptive or maladaptive behaviors (Menard et al., 2014). Adaptive responses are recommended responses that are intended to protect in the event of a threat and maladaptive responses occur when the

individual avoids performing what is considered a reasonable response (Menard et al., 2014).

PMT theory is used by many in the information technology arena to guide daily decisions. The implementation of PMT can be seen in activities such as deciding on the need for a daily system backup. The fear of data loss and system failure compels the system admins to make sure the company's data is backed up successfully (Menard et al., 2014). The fear of not being able to recover from a catastrophe is the motivation for the technology team.

In order for PMT to be implemented successfully, there must be a threat appraisal process. The threat appraisal process involves the following: threat susceptibility, threat severity, and the extrinsic or intrinsic benefits gained from participating in maladaptive behaviors (Menard et al., 2014). Threat susceptibility refers to the degree to which someone feels at risk to a particular threat (Menard et al., 2014). Threat severity refers to how severe a threat is perceived to be (Menard et al., 2014). Intrinsic benefits relate to the pleasure of non-compliance, whereas an extrinsic benefit may be obtaining something valuable that could not be feasibly obtained without committing the act (Menard et al., 2014).

Once the threat appraisal process has been completed, the next process of PMT is the coping appraisal process. The coping appraisal process involves the evaluation of the responsiveness, self-efficacy, and response costs (Menard et al., 2014). Response efficacy is the perceived effectiveness of the suggested adaptive behaviors whereas self-efficacy is the degree to which a person believes they are able to effectively perform the recommended adaptive behaviors (Menard et al., 2014). The response costs is the

visualized extrinsic or intrinsic personal costs of performing the suggested adaptive behaviors (Menard et al., 2014). Response costs are realized in things such as: money and personal extended efforts. Response and self-efficacy have positive effects on intention to perform adaptive behaviors, whereas response cost affects adaptive behavioral intention negatively (Menard et al., 2014).

When it comes to the issues of information system (IS) security research, PMT is highly applicable due to the tangible threat-response pairs evident in IS security (Menard et al., 2014). If the threat is identity theft, the response is to frequently change and maintain strong system passwords. If the threat is data loss, then the response is performing regular system backups and double checking those backups for successfulness. If the threat is a virus, the response is scanning with reputable antivirus software.

PMT should be used to keep IS/IT staff on guard against complacency. The fear of the worst possible scenarios impacting the technological infrastructure should be viewed as motivation to always safe the company's assets. This may mean looking at alternative solutions to securing the firm's resources. Creating avenues of redundancy help to ensure that the company can survive in the event of a hardware failure or climate related disaster (Menard et al., 2014).

The next theory is the theory of reasoned action. The theory of reasoned action deals with the motives of a particular individual and whether those motives were ethical or unethical (Lin, Tsai, Joe, & Chiu, 2013). An ethical issue often arises when one party in pursuit of their goals engages in activities and behaviors that affect the ability of another party to pursue their goals (Lin, Tsai, Joe, & Chiu, 2013). If the effect is helpful,

good, just or right, then the actions are praiseworthy (Lin, Tsai, Joe, & Chiu, 2013). If the actions on the other hand cause harm to the other party they could be considered unethical (Lin, Tsai, Joe, & Chiu, 2013).

The theory of reasoned action comes into play in the field of information security quite often. The concept applies to IT service providers and other IT industries. IT Service providers have access to a user's private information and they have an obligation to protect that information. When the IT service providers fail to do so, they put their customers in jeopardy of having their identities stolen (Lin, Tsai, Joe, & Chiu, 2013). The IT service providers have to weigh the cost of doing what is right against the costs of the potential harm the customers could feel.

This same behavior transcends IT markets and operations to impact the entire IT software, hardware, and service industry. It is very rare that a software manufacturer recalls a software programmed that the company knows is flawed (Lin, Tsai, Joe, & Chiu, 2013). The risk to the company outweighs the risk to the customer and unfortunately this is the standard thought process of businesses (Lin, Tsai, Joe, & Chiu, 2013).

The theory of reasoned behavior can even be used to analyze hackers and cyber-terrorists (Lin, Tsai, Joe, & Chiu, 2013). These individuals are making a conscious decision to perform an action that causes harm to more than just the company. Their activities hurt the company, shareholders, employees, and even the company's vendors. In turn, the company is now analyzed using this same theory. The company has to choose between doing enough to properly secure their technological infrastructure, which could cost a lot of money, or doing just enough to give the illusion that their organization is properly secured. This theory has a broad application and when properly used could be



beneficial in preventing harm to many companies and customers alike.

The next theory to be examined is the theory of planned behavior (TPB). TPB has been used to analyze manager's attitudes and participation in the budgeting process. TPB concludes that there are two constructs that influence behaviors. The first construct is an individual's attitude toward a specific behavior which refers to positive or negative feelings on specific behavior (Su & Ni, 2013). The other construct is subjective norms which refer to the individual perceived social pressure on specific behaviors (Su & Ni, 2013). These two constructs work together to influence behavior intention and then affect specific behaviors (Su & Ni, 2013).

As managers are required to take part in the budgetary process of their organizations, it has been noted that many are in engaging in budgetary slack. Budgetary slack refers to a behavior in a budget setting in which a manager proposes the goals that are beneficial for themselves and easy to achieve (Su & Ni, 2013). If a manager knows that larger projects are likely not to be approved, they may not propose them and instead budget for items that have a high risk of approval. This creates a positive environment and feeling the manager and encourages him/her to continue to create the budgetary slack.

TPB suggests that managers take the path of least resistance to accomplish their goals. One of the reasons for this noted behavior is the discomfort that comes along with rejection (Su & Ni, 2013). When it comes to preparing for information technology budget items, the information technology team has to prepare for possible rejection. Some have therefore opted for the path of least resistance and chosen to only budget for items that have a low probability of rejection (Su & Ni, 2013). It has been noted that this

method of budgeting creates an excess amount of stress on other managers as they prepare their own budget items.

The next theory for review is social control theory. Social control theory (SCT) falls in the category of deterrence theories. Deterrence theories suggests that an individual can be discouraged from offending either generally through the threat of punishment and knowledge of others experiences or specifically through their own experiences (Worrall, Els, Piquero, & Teneyck, 2014). SCT takes deterrence theory a step further by suggesting that culture can be used to control behaviors.

An organization's culture is used to create the kind of workplace dynamic that the shareholders believe to be indicative of the company's values (Worrall et al., 2014). SCT utilizes all facets of the corporate environment to control the environment. This means the company has the signed forms from each employee in which they acknowledge their awareness of the rules, but they also have social controls in place (Worrall et al., 2014). These controls come in form of publicized punishments for offenders and peers who help maintain a certain workplace standard (Worrall et al., 2014).

A poll was taken of students at a University in the US and the students were asked how they felt about their peers knowing they got in trouble and 98% of those surveyed acknowledged that they would be ashamed (Worrall et al., 2014). It did not matter what type of trouble it was, but it was that fact that the students perceived that their peers would in some look down upon them.

SCT plays on an individual's desires to fit in with their peers and their surroundings. SCT can be observed through the way people dress, the desire to achieve great levels of wealth, and even the types of automobiles they drive and the

extracurricular activities they engage in (Worrall et al., 2014).

The final theory to be reviewed is the theory of moral decision making. The purpose of this theory is to gain a better understanding of the ethical decision-making process by considering the moral competencies of the decision maker (Morales-sánchez & Cabello-medina, 2013). This theory acknowledges four key characteristics that an individual goes through prior to making any decision, good or bad. These four characteristics are called Rest's Four-Component Model (Rest 1986). Rest's model indicates that an individual facing a moral goes through the following stages: moral sensitivity, moral judgment, moral motivation and moral character (Morales-sánchez & Cabello-medina, 2013).

Each element of the Four-Component Model is taking into consideration on a subconscious level by all individuals struggling with making the right decision (Morales-sánchez & Cabello-medina, 2013). Moral sensitivity is defined as being aware of the problem or existence of a situation that could lead to questionable behaviors (Morales-sánchez & Cabello-medina, 2013). The individual has to have some knowledge that their actions could lead to a questionable outcome and this is where moral sensitivity comes in. It is the voluntary acknowledgement that a problem exists (Morales-sánchez & Cabello-medina, 2013).

Moral judgment is the stage in which the individual assesses the good or bad of an act (Morales-sánchez & Cabello-medina, 2013). Rest (1986) suggest that an individual must have the capacity to make a sound judgment about a course of action in determining if the action is morally justifiable or not. The ultimate purpose in this component is to be able to properly identify every possible action based on the decision made, irrespective of

any personal interest (Morales-sánchez & Cabello-medina, 2013).

The third component is moral motivation. Moral motivation is defined as the willingness to take the moral course of action by placing moral values above other values and taking personal responsibilities for moral outcomes (Morales-sánchez & Cabello-medina, 2013). Moral motivation make the individual have a moral intention or willingness to engage in a particular action (Morales-sánchez & Cabello-medina, 2013). It has been realized that moral intention precedes ethical behaviors (Morales-sánchez & Cabello-medina, 2013). The results of moral intention can be different from the result of moral judgment because in this stage of the process, many other variables are involved such as: the person's personal interest and the assessment of the damage that each action could cause (Morales-sánchez & Cabello-medina, 2013).

The fourth component is moral character. Moral character involves executing and implementing certain behaviors (Rest, 1986). The path from moral intention to moral action is not always a simple path because the individual has to work around various factors that hinder them. These factors include: impediments and difficulties, fatigue and frustration, temptations and challenges to take the right actions (Morales-sánchez & Cabello-medina, 2013).

In addition to these four components that contribute to the moral decision making theory, there are other components that contribute to it as well. These components include: ethical corporate culture, significant others (home life), obedience to authority figures, the structure of rewards and punishments, job context, conduct codes, policies and rules, leadership influence and organizational structure (Morales-sánchez & Cabello-medina, 2013). All of these elements play a significant role in moral decision making

theory. It is the expectation that this theory can be used to assist in predicting those individuals more prone to engaging in ethical/unethical behaviors (Morales-sánchez & Cabello-medina, 2013).

### **The Risk of Cloud Computing on Cyber Security**

If internal security problems were not already getting the best of organizations, they now have to worry about the security of cloud computing services. Cloud computing simply means storing information in remote location via the internet. Companies have to take another cost initiative and determine whether it is a justifiable risk. Cloud solutions often save companies money by allowing them to access goods and services that they may not be able to afford to purchase on their own (Bradley & Cooper, 2014).

There are three different variations of Cloud Computing: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) and businesses must decide which Cloud offering best suits their needs if they are going to embrace Cloud Computing (Bradley & Cooper, 2014). Each option is designed to fulfill a particular need and it is imperative that organizations understand how each option works.

Software as a Service (SaaS) is also known as “software-on-demand” (Bradley & Cooper, 2014). This is when businesses allow remote or cloud based servers do all of their “heavy lifting” which eliminates the need to have a physical server on site (Bradley & Cooper, 2014). When businesses engage in SaaS they reduce their in-house needs to an internet connection and a computer (Bradley & Cooper, 2014). These services often come with annual fees or startup costs that are significantly less expensive than

purchasing and maintaining a server onsite. The options for SaaS are almost limitless and include options such as: accounting, collaboration, Enterprise Resource Planning (ERP) and even Human Resource Management (HRM) (Bradley & Cooper, 2014). Pushing all of these services to the Cloud takes the worry off of the company to hire specialists to manage these systems (Bradley & Cooper, 2014).

### **Platform as a Service (PaaS)**

It is the next category of cloud computing. PaaS systems facilitate the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities, providing all of the facilities required to support the complete life cycle of the building and delivering of web applications and services entirely available through the internet (Bradley & Cooper, 2014). With PaaS, everything is done remotely and no computing is taking place on the host systems, but is done on the host server (Bradley & Cooper, 2014).

Currently, there are four different types of PaaS. These are: add-on development facilities, which are add-ons to existing SaaS's, stand-alone development environments, which provide a general development environment, application delivery-only environments, which only act as a hosting platform and open platform as a service, which allows the client or developer to use a variety of programming languages and database types (Bradley & Cooper, 2014). Examples of PaaS systems include: ORACLE RDMBS (object-relational database management system), which is provided by the Oracle Corporation and the Google App Engine (Bradley & Cooper, 2014).

The last category of Cloud Computing is Infrastructure as a Service (IaaS). IaaS is when an organization outsources the equipment used to support operations and can

include: storage, hardware servers and even networking components (Bradley & Cooper, 2014). IaaS is primarily used by organizations to manage customer relations (Bradley & Cooper, 2014). IaaS allows companies to test possible software and hardware solutions without incurring the costs of the hardware and software. Examples of IaaS services include: Windows Azure, a service provided by Microsoft that allows the development and management of Microsoft based applications (Bradley & Cooper, 2014).

Organizations have many considerations to make before pursuing the various Cloud Computing options. Where is the company's data actually stored (what country)? Who has control over or access to it? How secure is the connection to the information? Many companies have decided that outsourcing to India is the best way to go (Mukundan & Prakash, 2014). India has become the number 2 cloud services offering in the technological world. The number one is the US (Mukundan & Prakash, 2014). Yet, before companies commit to outsourcing over the oceans, they need to fully understand the cost of a security violation if something should occur.

As companies find more cost efficient solutions in the cloud they must also consider the culture of where they are now sending their business (Shaaban & Conrad, 2013). This greatly impacts the security of their information. Many countries do not have the same security standards as those businesses that operate in the US. These types of scenarios need to be fully discussed before sending information into the cyber world (Thompson & Lee, 2013). Companies need to constantly be asking themselves the following questions: Is outsourcing really a better solution? Are those companies that I am trusting with my company's information maintaining their systems? What are the costs associated with recovering my data should a problem occur?

Research has revealed that many companies spend more money trying to resolve a security breach than putting the resources in place to prevent one (Thompson & Lee, 2013). This is an alarming fact, often referred to as a game of risk. While all businesses take risks in one way or another, it is important to understand the short and long term potential consequences of those risks. Choosing cloud based storage and services is an option that is filled with risks. Businesses need to be selective in deciding which of their operations they are willing to send to the cloud. This process should begin by determining, first is cloud computing right for their organization. If so, what type of information should be stored in the cloud? Some companies have taken to storing financial information in the cloud (Ionescu & Tudoran, 2013). Cloud services offer a cost savings that are often hard to match internally, yet they come with risks. What is the cost of those financial records falling into the wrong hands?

Security perception and reality need to stay in alignment (Bahl & Wali, 2014). Risks are a part of doing business, but the types of risks the company takes on are under their control. Oftentimes the decisions of business leaders today fall on the Information Technology team to resolve (Järveläinen, 2012). This is just one more cost that often gets overlooked. Security decisions are being are often made by those who are least qualified. Which leads to security vulnerabilities. These vulnerabilities transcend countries to wreak havoc for businesses.

All of the research continues to point to a common problem with awareness. Business leaders, military staff, higher education and many more industries suffer from a failure to understand the cost of security violations. It is this failure to appreciate the costs that are included in security violations that demands that more research be done.



## **Information Technology Governance**

IT governance has been defined as a structure of relationships and processes to control an enterprise in order to achieve the enterprise's goals of by adding value while balancing the risk versus return over IT and its processes (Ali & Green, 2012). Effective information technology governance ensures alignment between the information technology (IT) department's needs and the business goals (Ali & Green, 2012). It has been established that organizations with ineffective IT suffer due to poor performance of IT resources that stem from inaccurate information quality, inefficient operating costs, runaway IT projects and even the demise of its information technology department (Ali & Green, 2012). In 2003 study conducted by Gartner (The Ten CIO Management Priorities for 2003), more than 80% of Chief Information Officers (CIOs) admitted that it was vital that their organizations improve IT governance (Ali & Green, 2012). A survey conducted by (Weill & Ross, 2004) revealed that organizations with effective IT Governance initiatives in place were 25% more profitable than those with insufficient IT Governance procedures in place given similar strategic objectives (Ali & Green, 2012).

If a corporation is to maximize its performance then it is crucial that they have effective IT governance (Ali & Green, 2012). Effective IT governance requires a set of controlling or governance mechanisms be put in place. These mechanisms include an IT steering committee and an IT organizational structure that encourages behaviors that align with the organization's mission, strategy, values, norms and culture (Ali & Green, 2012). Businesses must be constantly reviewing which IT governance strategies are most cost effective for their operation and which strategies are pivotal to the longevity of their

operations (Ali & Green, 2012).

IT governance is not a cookie cutter situation, but varies from industry to industry as the governance needs to comply with industry standards (Ali & Green, 2012).

Organizations with ineffective IT governance tend to suffer more than organizations without effective IT governance. The areas of operations most impacted include: inefficient operating costs, runaway IT project costs (e.g. being over budget and under specification), loss of competitiveness and the solvency of the organization itself could even be at risk (Ali & Green, 2012).

To achieve effective IT governance an organization needs to implement well-designed, well understood and transparent governance mechanisms (Ali & Green, 2012). Proper IT governance is seemingly impossible without the cooperative efforts of the IT steering committee, the involvement of senior IT management, and the corporate management team (Ali & Green, 2012). Effective IT governance is critical to every facet of the operations of the organization because every facet of the organization is dependent on the information technology team in some capacity (Ali & Green, 2012).

Information or data is of the primary assets of an organization (Barbosa, Rodello, & de Pádua, 2014). This is especially proven to be true in the financial industry. In the global context of rapid changes and fast communication, not only is information a primary asset, but it is also a strategic asset as it is an important contributor to the success of the economy (Barbosa et al., 2014). It is imperative that businesses understand the growing importance of IT and consider it a treasure in enhancing their competitive position by adding value to their operations (Barbosa et al., 2014).

Just as information is an asset to an organization, information technology must be

viewed the same way (Ali & Green, 2012). It is crucial for growth, innovation, mergers, and acquisitions (Barbosa et al., 2014). In order for an organization to truly derive any benefits from their IT operations, it is imperative that those in charge have some basic level of understanding in what they do (Barbosa et al., 2014). The failure to understand the vitality of the IT operations of an organization can prove to be a fatal flaw in any organization (Bahl & Wali, 2014). The significance of IT governance has a direct correlation to project funding and project success (Barbosa et al., 2014).

A key position in IT governance is the senior IT Director, Manager, or Chief Information Officer (Bahl & Wali, 2014; Barbosa et al., 2014; Ali & Green, 2012). These individuals must manage the IT activities as well as make sure their activities are directly in line with the objectives of the organization (Barbosa et al., 2014). One of the continued areas of concern in the area of IT governance is expenses. The costs of managing an IT department (which includes staffing and completing projects) has continued grow and have surpassed more than half of the working capital of large companies (Economics & Statistics Administration, 2003). Despite the growth of managing the information technology needs of an organization, it is still a critical part of the company's operations (Barbosa et al., 2014).

Within the organization, it is important that the IT governance work in tangent with Corporate Governance (CG) (Barbosa et al., 2014). Corporate Governance is the system by which organizations are directed and controlled and dates back to the mid-1990s (Barbosa et al., 2014). Corporate Governance is the system by which companies are directed, monitored and stimulated, and it involves relationships among owners, boards of directors, and control institutions (Barbosa et al., 2014). This is why it is

important that the IT Governance initiatives are line with the Corporate Governance initiatives. Both IT Governance and Corporate Governance serve as a controlling mechanism for monitoring the actions, policies, and decisions of corporations (Barbosa et al., 2014).

Wilkin & Chenhall (2010) have described IT Governance as policies, structures, and processes of management that involve IT functions. IT Governance is comprehensive and focused on transforming and directing the IT resources toward current and future business needs (Barbosa et al., 2014; Wilkin & Chenhall, 2010).

An important facet of IG is the ability to audit the processes and controls that have been put in place (Hosban, 2015). Governance was first position to be an agency problem where power between the owners of a corporation was less than that of its managers, who, though not owners, had near-perfect information about the organization and its operations (Hosban, 2015). Governance served to reduce the sometimes conflicting goals between the managers and the shareholders, where the shareholders are often concerned about maximizing profit and managers with the sustainability of the operation (Hosban, 2015).

Neutral auditors of Governance help ensure that all facets of the operations of the organization are operating in the best interest of the company and help to uncover fraudulent activities at all levels (Hosban, 2015). This type of auditing is internal auditing and is often performed by someone trained to know what to look for as signs of fraud (Hosban, 2015).

One of the primary reasons for IT Governance is that businesses are constantly striving to couple their operational and IT processes in order to cut costs and increase

efficiency, though these two do not often work well together (Croteau, Bergeron, & Dubsky, 2013). As more businesses desire to have interorganizational relationships, the need for quality IT Governance escalates (Croteau et al., 2013). The business world is starting to accept the fact that information technology is the primary driving force to most new business ventures (Croteau et al., 2013). These new ventures including individual organizational growth and working with new business partners. IT Governance should increase value, manage risks, maintain accountability and measure program performance and growth (Croteau et al., 2013).

Weill (2004) states that governance is about systematically determining who makes each type of decision (a right decision), who has input to a decision (an input right) and how these people (or groups) are held accountable for their roles. Effective IT Governance draws on corporate governance principles to manage and use IT to achieve organizational performance goals (Croteau et al., 2013).

## **Summary**

In the field of information technology there is a problem that the information technology staff struggles with. This problem is the continual lack of funding to complete information technology projects that are necessary to keep the organization secured from both internal and external threats. Throughout the literature review section different works have been analyzed and different theories reviewed to highlight the problem. The literature review begins with (Fenz et al., 2014) identifying that one of the top five problems facing organizations today is the risk of a cyber-attack. (Wilding & Wheatley, 2015) further identified the problem by identifying several large organizations

in North America that have suffered tremendously due to cyber-attacks.

Several methods were identified for addressing information security risk management techniques. These methods included EBIOS (DCSSI, 2004), OCTAVE (Alberts et al., 2003), CRAMM, FAIR, and ISAMM (Fenz et al., 2014). It is believed that by implementing one or a variety of these strategies that organizations could reduce their risks for cyber-attacks (Fenz et al., 2014).

During the analyzing of information security standards, several industry standards were highlighted to emphasize their effectiveness in maintaining a secured network infrastructure. These standards include: ISO/IEC 27001/27001, Sarbanes-Oxley, and Payment Card Industry (PCI) standards (Tsohou et al., 2012). In addition to information technology industry standards several theories were analyzed. These theories include: General Deterrence Theory (GDT) (Hassan et al., 2015), Protection Motivation Theory (PMT) (Menard et al., 2014), Theory of Reasoned Behavior (TRB) (Lin et al., 2013), The Theory of Planned Behavior (TPB) (Su & Ni, 2013), Social Control Theory (SCT) (Worrall et al., 2014) and the final theory was Lack of Budgetary Theory (Cheng et al., 2014). The literature review also examined the topic of cloud computing. Cloud computing and storage has offered many organizations a less expensive way to address some of their computing and storage needs (Mukundan & Prakash, 2014). In addition to opening up opportunities for organizations, the cloud has also brought threats to information security, not just for the organization, but for the organization's suppliers, customers and employees (Bahl & Wali, 2014). It is the expectation that further research aides in bringing more attention to this dilemma and get IT/IS staff the funding they need to keep their organizations secured.

### **Chapter 3: Research Method**

As information security threats continue to skyrocket, business leaders need to adjust their responses to these threats with an elevated sense of urgency (Ifinedo, 2014). A key component used to determine which security technologies to invest in and implement is cost (Gupta & Shakya, 2015). The majority of information security projects come at a costs that start in the thousands of dollars and these costs are often a source of trepidation for controlling managers (Gupta & Shakya, 2015; Chen, Ramamurthy, & Wen, 2015).

When businesses look for an area of operations to cut cost from, the Information Technology department's budget becomes under consideration (Gupta & Shakya, 2015; Luftman et al., 2013). Business leaders often struggle with the decision to make these capital investments because they cannot easily measure the return they are receiving on their investment (Makarevic, 2016; Otieno & Biko, 2015; Gilbert, Pick, Alan, & Ward, 2012).

A large number of information system (IS) projects are considered to be failures with only 32 % proving to have successfully reached their objectives (Fulk, Kwun, & Alijani, 2013). The high failure rate is attributed to the managerial controls over the project funding and the limited resources allocated to the projects (Fulk et al, 2013). Failure to believe in or understand the validity of the requested information systems (IS) project is listed as one of the primary reasons for receiving limited funding (Dwivedi, Wastell, Laumer, Henriksen, Myers, Bunker, Srivastava, 2015).

The specific problem this research addressed is the insufficient funding of information security projects (Pernebekova & Ahbergenovich, 2015; Velmurugan &

Mathiyalagan, 2015; Chen, Ramamurthy, & Wen, 2015; Makarevic, 2016; Otieno & Biko, 2015; Peffers & Santos, 2013; Conboy, 2009; Cao, Mohan, Ramesh, & Sarkar, 2013; Gottron, 2013; Marshall, 2012).

The purpose of this qualitative case study was to identify the reasons behind the insufficient funding of information security projects based on the perceptions of information security decision makers at small and midsize firms located in the U.S.

The following questions were designed to determine the effects that insufficient IT Project funding can have on an organization based on the interpretations of information security decision makers:

**RQ1:** What do information security decision makers at small and midsize private firms located in the U.S. believe about the insufficient funding of their information security projects?

**RQ2:** What do information security decision makers at small and midsize private firms located in the U.S. believe are the reasons behind the levels of funding dedicated to their information security systems?

This chapter covered the research methods and design used for this research paper, the research method and research design and the data collection method. The population, sample size, limitations, delimitations, data analysis methods, and ethical assurances measures that were taken to ensure that the research was done ethically are also discussed in this chapter.

### **Research Methods and Design**

The research methodology used for this study was qualitative. Qualitative research methodology provided an ideal approach to understanding organizational



changes, especially changes involving complex stake-holder organizing, work place practices and organizational structure (Garcia & Gluesing, 2013). This made qualitative research a choice method when trying to understand why information technology departments still receive insufficient funding. Qualitative research methods are not superior to other research methods and each research method has its appropriate uses. Researchers use qualitative researchers to observe subjects in their natural settings and interact with them on their terms (Abusabha & Woelfel, 2003). The use of qualitative research can provide insights into understanding how workplace practices are evolving in day-to-day interactions as well as how they relate to contextual influences at multiple levels (Garcia & Gluesing, 2013). The use of qualitative methodology allows for the subject's perspective of the behavior or the phenomenon under study while quantitative is concerned with the discovery of facts. Quantitative research is designed as a detailed plan of operation with predetermined hypotheses (Abusabha & Woelfel, 2003). Conceptually qualitative methodology assumes a dynamic and subjective reality while quantitative assumes a fixed and measurable reality.

There are several research designs available to choose from when using qualitative research methods. These design options include: grounded theory, phenomenology and case studies among others (Gentles, Charles, Ploeg, & McKibbin, 2015). Grounded theory is a flexible method used for developing substantive theory that traditionally emphasizes understanding of social processes (Gentles et al., 2015). Phenomenology is a qualitative approach in which researchers aim to develop new understandings of the human lived experience, often relying on first person accounts generally obtained through participant interviews (Gentles et al., 2015).

The qualitative research method being used in this research was case study. Case study focuses on what is to be studied and is distinguished from the other two design options by its analytical focus on a small number of cases (Gentles et al., 2015). Each case was studied within its distinct context. The collected data for each case came in varying forms including: observations, interviews, documents, and etc. (Gentles et al., 2015).

Case study explores real-life, contemporary bounded system over time and often involves multiple sources (Priya, 2014). Case studies produce a case description and case themes and present an in-depth understanding. As opposed to group designs, case study research designs follow an inductive approach, where researchers formulate general principles based on results from particular sets of results and data. A case study may be descriptive, explanatory, or exploratory (Priya, 2014). This research used exploratory case study. In single case research, multiple experiments may be conducted over time, exploring various aspects and effects of particular interventions (Priya, 2014), use statistics and a rich, qualitative narrative of the circumstances under which the experiment took place to describe the “how” of the results (Yin, 2015).

There were several sources of information used throughout this study like past research findings, media reports, and interviews. Media reports were collected by accessing the following databases: ABI/Inform (Business and Management), IEEE Computer Society Digital library, First Research, and Business Source Premier Databases. The primary sources of information were interviews. Interview protocols were developed and validated via a pilot testing program.

The interviews were conducted electronically using computer-mediated

communications (Onwuegbuzie, Leech, & Collins, 2010). Virtual interviewing is where an internet connection is used to study either synchronously or asynchronously a situation or phenomenon (Onwuegbuzie et al., 2010). Asynchronous methods include those interviews that can be conducted at various times such as email and websites such as [www.surveymonkey.com](http://www.surveymonkey.com) (Onwuegbuzie et al., 2010). Synchronous methods include those that are time sensitive, including blogs and instant messaging (Onwuegbuzie et al., 2010).

The selection process for individuals consisted of contacting individuals via email and telephone. The individuals that responded and agreed to take part in the study were given directions on how and when the study would place. The participants answered interview questions via telephone conference line. Each candidate was required to complete an assessment of their qualifications before completing the interview. The results were stored in a database by the researcher for comparison and analysis. The individuals were allowed up to two weeks to complete the interview.

Validity was achieved in this research by triangulating the evidence from the past research findings, media reports and interviews. The interviews consisted of phone interviews. The research looked for similarities in responses from interview participants and compared it against previous research and what is discovered in media reports. To aide in preventing bias, it is always better to use multiple sources rather than a single a source of evidence (Yin, 2015).

To aid in establishing validity, this research also focused on credibility, dependability, transferability, and trustworthiness of the research information. The credibility criterion involved establishing that the results of qualitative research were

credible or believable from the perspective of the participant in the research. The trustworthiness of the research was contingent upon having credible, dependable, transferable and confirmable data (Sinkovics, Penz, & Ghauri, 2008). An effective way to ensure the data is transferable is to use a computer assisted qualitative data analysis software (CAQDAS) (Sinkovics et al., 2008).

### **Population**

The population of the study included approximately 340,000 (U.S. Bureau of Labor Statistics, 2015) people that serve in one of the following capacities: Information Technology managers, Information Technology Directors, and other information technology personnel from small and midsize firms that are familiar with the project approval and budgeting process. The population consisted of men and women of varying ages with at least five years of experience in managing information technology projects. The study sought out individuals with a minimum of a Bachelor's degree in the Information Technology field. These individuals were located in various states within the contiguous United States and working in the private sector.

### **Sample**

Sampling is defined as the act, process, or technique of selecting a representative part of a population for the purposes of determining parameters or characteristics of the whole population (Gentles et al., 2015). This research was conducted using purposive sampling. Purposive sampling required selecting information rich cases that allowed for in depth study (Suri, 2011). Information rich cases are those cases from which a great deal can be learned about issues of central importance to the purpose of the inquiry (Suri, 2011). Studying information-rich cases leads to insights and in-depth understanding

rather than empirical generalizations (Patton, 2002). Purposeful sampling required access to key individuals in the field of study that can help in identifying information rich cases (Suri, 2011).

The sample for this research consisted of 8 individuals with IT budgeting responsibilities working in the private sector in the U.S. It was important to have a sample that was large enough to represent the target population, but not so large and extensive that it became unmanageable (Yin, 2015). These individuals were chosen because of their industry knowledge and their organizational responsibility to keep the business's technological infrastructure secured from both internal and external threats. Some of the individuals were located by posting an ad on the CLS User group listserv with a notification to participate in research regarding problems with IT budgeting request. Other individuals were direct referrals from other candidates. The researcher requested access to post in the CLS User group and received approval to do so.

The specific steps taken to reach the required sample were: A post was made in a user group called the "CLS User Group" introducing the call for participation in the research study. The CLS User Group is a Google User group consisting of Information Technology leaders located in the US and working in the private sector at small to midsized organizations. This group is used to collaborate on a wide range of technological issues. This is a private group and anyone desiring to view the feeds in this group must request permission. This post asked for individuals to email the principal investigator if they were interested in taking part in a study regarding insufficient information technology project funding. The initial post remained active for one week. As potential interviewees responded to the post, they were required to answer a

prescreening questionnaire located in the Interview Protocol. The screening questions were used to determine if the potential interviewee was qualified to take part in the study. The initial responses to the ad were slow. To compensate, the principal investigator solicited referrals via the candidates that responded. The referred candidates were put through the same screening criteria as the candidates that responded to the ad located in the CLS User group posting. This strategy allowed the researcher to reach its targeted sample size of 8 participants. Each of 8 participants were required to complete the prescreening questionnaire successfully before being offered the opportunity to participate in the actual research study. Any potential participants that did not meet the qualifications to take part in the study were thanked for their time and informed that they do not meet the minimum criteria for this study.

### **Materials/Instruments**

Data collection is critical to research (Rimando, Brace, Namageyo-Funa, Parr, Sealy, Davis, & Christiana, 2015). When implemented correctly, data collection enhances the quality of research as data collection is the first phase of the research process (Rimando et al., 2015). The data collection method for this case study consisted primarily of interviews which used open-ended questions given to the participants. Information was also collected from previous case studies. The interview questions are listed at the end of the study. Information was also collected from various online databases such as: ProQuest and EBSCOHost.

The interview protocol has six key stages that were implemented into this study (Rabionet, 2011). These stages are as follows. Stage 1 included selecting the kind of interview. This study was conducted using semi-structured interviews. Stage 2

involved establishing the ethical guidelines of the study. This stage of the interview protocol was used to cover the purpose of the study, the potential consequences of the study, to give the informed consent document, highlight the confidentiality of the results and answer any questions (Rabionet, 2011). Stage 3 is where the interview protocol was drafted. In this stage two important concepts were realized. The first concept was the introduction of the study topic to the interviewee. The next step, which was the most important was the development of the interview questions (Rabionet, 2011). The successful completion of this stage required the in depth analysis of known problems as highlighted by other researchers. The research questions and probes were all based on problems that have been identified from existing literature (Schultze, 2014; Pernebekova & Ahbergenovich, 2015; Broadhurst et al., 2014; Makarevic, 2016; Gupta & Shakya, 2015; Tham, 2013; Elgin et al., 2014; Otieno & Biko, 2015; Fulk et al., 2013; Chen et al., 2015; Conboy, 2009; Cao, Mohan, Ramesh, & Sarkar, 2013; Gottron, 2013; Marshall, 2012).

Dr. Nicholas Harkiolakis also served as an expert in providing feedback for the design and development of the interview questions. Stage 4 included conducting and recording the interviews. After applicants have been identified and demonstrated their ability to take part in the study, the interviews were scheduled and recorded for future transcription.

Stage 5 of the interview protocol consisted of analyzing and summarizing the results (Rabionet, 2011). It is in this stage that the information was transcribed and entered into Nvivo for processing and analysis. Stage 6, which is the final stage consisted of reporting the findings (Rabionet, 2011). All transcribed interviews will be

shared with the interviewees and other researchers upon request to ensure the integrity and trustworthiness of the information.

The interview began with an opening question to determine the participant's eligibility to take part in the study (Turner, 2010). In addition to determining if the interviewee is eligible to participate in the study, the open questions was also used to gauge whether the interviewee was still interested in taking part in the study (Creswell, 2007).

All subsequent interview questions were designed to meet the following criteria: to be open ended to elicit as much detailed feedback as possible, all questions were written in a neutral manner to avoid attempting to sway the interviewee's answers, all questions are asked regarding a specific point in time (their current employer), and great care has been taken to ensure all questions had been worded clearly to minimize the risk of confusion (McNamara, 2009). The first couple of interviews served as the pilot testing phase of the interview protocol. The pilot test revealed that some of the interview questions were not broad enough to solicit the required feedback needed for the success of this research. Those research questions were modified to prevent the interviewees from giving answers that provided no substance.

The interview consisted of 8 interview questions with four additional probing questions. The interviewer collected preliminary tracking information about the participants. The interviews were concluded by offering the interviewee the opportunity to share any additional information they believed was relevant or could be beneficial to the research. Once they had concluded their additional input, they were thanked for their time and the interview was ended (Turner, 2010).



Interview Question 1. How familiar are you with the information technology project approval process? One of the primary reasons for information technology bottlenecks and failures is that individuals do not understand the importance of the project being requested (Schultze, 2014). Even those working in the information technology departments are sometimes not familiar with all of the various facets of the projects being requested (Schultze, 2014). This question was used to help gain insight into RQ2.

Interview Question 2. What is your role in submitting information technology projects for approval? (Schultze, 2014) Highlights the importance of having a project plan. This plan consists of having the proper people assigned to perform the proper roles in the project process (Schultze, 2014). This information should be documented in the project plan to ensure the appropriate individuals are qualified to do the project duties that have been assigned to them. This question was used to help gain insight into both RQ1 and RQ2.

Interview Question 3. Has your organization ever suffered from a cyber-attack? Many organizations have suffered from cyber-based attacks for failing to implement the proper controls to prevent what are often known vulnerabilities (Pernebekova & Ahbergenovich, 2015). These are often well known organizations and include: Home Depot, Sony Pictures, Target, Citi Bank and many more (Broadhurst et al., 2014). These companies were made aware of their weaknesses and failed to invest in the resources to keep their organizations secured (Makarevic, 2016). This question was used to support RQ2.

Interview Question 4. What percent of IT projects are approved in a timely

manner? Business leaders have to make decisions on a regular basis regarding project approval including which projects to fund and which ones to put off until a future date (Gupta & Shakya, 2015). These decisions are often based on the difference between actual costs and perceived costs (Tham, 2013). The actual cost of putting off an IT project is unknown and because these projects are often costly, decision makers often feel comfortable taking their time about approving them (Tham, 2013). The perception of many company leaders is that IT Projects are too costly and will not yield a sufficient benefit to justify their costs (Broadhurst et al., 2014). This question was used to support RQ1 and RQ2.

Interview Question 5. Do you believe your organization's information security systems can provide adequate protection? Many organizational leaders believe that their current information security infrastructure is sufficient to prevent a cyber-attack (Elgin et al., 2014). This was the case for Home Depot. The Home Depot company had purchased the software to provide the additional layer of protection the company needed, but they failed to have it installed (Elgin et al., 2014). This vulnerability put 56 million Home Depot card holders at risks of having their credit card and financial information stolen by hackers (Elgin et al., 2014). This question was used to support RQ2.

Interview Question 6. Do you believe the levels of funding set aside for IT security projects is too low? When organizations look for an area of operations to cut cost from, the Information Technology department's budget is always on the chopping block (Gupta & Shakya, 2015). It is an unfortunate reality that many organizational leaders do not understand what their Information Technology departments do for their organizations and as such, they consider the IT department to be overhead (Otieno &

Biko, 2015). It is this lack of understanding that creates an atmosphere of fear of investing heavily into the Information Technology departments of many organizations (Fulk et al., 2013). This question was used to support RQ1.

Interview Question 7. How does your organization's leadership understand the importance of their information technology department? A lack of understanding of the functions of the Information Technology department is one of the primary reasons for the Information Technology often not having the resources to complete projects (Fulk et al., 2013). The Information Technology department of many organizations is located in an isolated area of the company and often not thought about until there is a system failure (Chen et al., 2015). This is the time when the Information Technology department demonstrates their worth to the organization, but given the right resources, the Information technology department could be more proactive to prevent problems verses reactive to resolve them (Conboy, 2009; Cao, Mohan, Ramesh, & Sarkar, 2013; Gottron, 2013; Marshall, 2012). This question was used to support RQ1 and RQ2.

### **Data Collection, Processing, and Analysis**

This is a qualitative study and the primary method of data collection used was interviews. To ensure the integrity of the information, triangulation was used. Triangulation was used by comparing information from case studies, media reports and interviews.

Prior to conducting the interviews, which were all conducted via a toll free conference line, the interviewees were all asked to sign an Informed Consent document and return it to the principal investigator. The Informed Consent outlined what the participant was consenting to and included a separate signature line consenting to the

recording of the conversations. Three of the candidates did not consent to having their conversations recorded. They were reassured that their conversations were not being recorded and that all answers given would be kept in strict confidentiality.

Each interview was used to create a transcript that was then used to enter information into Nvivo. A copy of the transcript was emailed to the interviewees that requested it to ensure the integrity of the information they had provided. The information that was entered into Nvivo was coded based on the participant's initials. Removing the interviewee's names added another layer of security to the interview process. All data is stored on an encrypted flash drive which is being kept in a fireproof safe at the researcher's home. The researcher only accesses the data from a password protected laptop to help further ensure the privacy of the data.

The data analysis method that was used in this research was clustering. Cluster analysis can be helpful in identifying patterns where numerous cases are studied (Macia, 2015). Cluster analysis is an exploratory tool meant to support the analysis of qualitative data (Macia, 2015). Cluster analysis techniques aid the classification of multivariable data by grouping the variables into classes (Macia, 2015).

In using clustering for this research three steps were taken. The first step was the manipulation of the data to make it suitable for inputting into a qualitative research software program. NVivo word frequency queries was used to identify common themes. Next a cluster analysis was done. The cluster analysis was used to identify common themes in the data that may not be easily discernable. Then a matrix coding query was executed to identify theme and concept frequency.

One of the goals of this study was to reach data saturation within the 8

participants selected to take part in the interview process. Data saturation is reached when there is enough information to duplicate the study when the ability to obtain additional new information has been achieved, and when further coding is no longer feasible (Fusch & Ness, 2015). The inability to reach data saturation will have a negative impact on the validity of the research (Fusch & Ness, 2015). While no official rules exist to determine when a study has reached saturation, this research continued until the principal investigator was satisfied with the ability to replicate the results of the outcome without using new coding or research information (Fusch & Ness, 2015).

All interviewees that consented to having their calls recorded were recorded using a toll free conference line paid for by the researcher. All of the interview information was collected by the principal investigator. The research data was analyzed using Nvivo. Nvivo is a software program that is used in qualitative and mixed method research to organize, analyze and find insights in unstructured data such as: interviews, open-ended survey responses, articles, social media, and web content (<http://www.qsrinternational.com/what-is-nvivo>). This required the researcher to repeatedly listen to the recorded interviews and reread the questionnaires completed during the telephone conversations to ensure that no vital information was missed that could be used to strengthen the research.

### **Assumptions**

The primary assumption was that there would be a consistency in responses from the study participants in which they acknowledge that funding to complete critical projects is not always readily available. It was further assumed that the participant criteria that was outlined for this study would yield participants that were qualified to

speak on the study topic.

It was assumed that the population being polled for this research had been working in the field for a long enough period of time that they would be able to offer valid input. It was further assumed that the design of the research study would adequately allow the researcher to achieve the expected outcome. It was assumed that the research methodology was appropriate and that the research questions were adequate to support the research. It was assumed that the researcher would be unbiased with the results of the study (Yin, 2014). It was assumed that all in depth analysis would be done ethically to avoid skewing the results in favor of the researcher.

### **Limitations**

Price & Murnan, (2004) propose that a limitation of a study design or instrument is the systematic bias that the researcher did not or could not control and which has the potential to inappropriately affect the results. There were many aspects of this study that were beyond the control of the researcher and that contributed to the limitations of this study. These limitations included the amount of time interviewees were willing to invest in this study and the ability to locate willing participants that were willing are to commit to this study. To address these limitations, the researcher worked with each participant's schedule of availability. This included allowing the participants to dictate the interview schedule and being respectful of the interviewee's time by starting the interview process on time and allowing the candidates ample opportunities to answer all questions thoroughly.

Another limitation to the study was the use of the Nvivo program. This program presented a learning curve for the researcher. It was overcome by the use instructional

YouTube videos that offered step by step instructions on how to get the results the researcher was looking for. To add credibility and trustworthiness to qualitative research the study must be transparent (Yin, 2015). To add credibility and trustworthiness to this study, all case studies have been properly cited and all interviewee answers have been used verbatim. The contents of the interviewees will be made available upon request in their coded form.

### **Delimitations**

The delimitations of this study were set to prevent the study from getting beyond the control of the researcher. The researcher chose to use the interview process to reach a pool of participants that would expectantly have real world experience in answering questions regarding the efficiency of the information technology project and budgeting process. The number of participants was set to a maximum of eight by the researcher. This number allows the researcher to have reasonable sampling of the population for the benefit of this study (Yin, 2014).

The criteria for participants for the interview process was: individuals with a minimum of five years managing information technology projects, been with their present employer for a minimum of five years, have some formal education in either business or information technology, and have gone through the process of soliciting funding for information technology projects. It was believed that individuals meeting these criteria would be in the best position to answer the interview questions.

### **Ethical Assurances**

To ensure no ethics were violated, this study complied with the rules that Northcentral University has put in place. This meant that no research was conducted

prior to Institutional Review Board (IRB) approval. This study was not sent to the IRB until the mentor had approved that it was ready. All participants were asked to sign off on an informed consent document (Appendix B), which outlined the purposes for which this research was conducted and it explained how their answers would be used. The Informed Consent Form was very detailed in that it: described the purpose of the research study, detailed the expectations for the participants, highlighted the fact that this study was voluntary and came with an anticipated time obligation, gave participants the option to ignore certain questions if they felt uncomfortable answering them, or cease participation in the study at any time without penalty.

All participant information is being held in the strictest confidence and only information relevant to the study will be requested (Yin, 2014). In addition, the initial communication with the potential participants included the: researcher's name, cell phone number, name of the institution (NCU), the title of the study, the confirmation of privacy and concealment with no risk for the participants as well as a probable time assurance for the interview.

Additionally, to ensure that high ethical values are maintained, raw data will be provided upon request by other researchers so they can make an independent interpretation of the findings (Yin, 2011). The data gathered from the research has been organized systematically into tables increasing the simplicity of reviewing it.

### **Summary**

In summary, threats to information security systems have continued to escalate and it is essential that organizations stay technologically prepared to respond to those threats (Ifinedo, 2014). Those responsible for protecting the organization's technological



infrastructure are constantly charged with making decision on how to best protect them (Gupta & Shakya, 2015). This is done by selecting which projects will be funded and which ones will be put on the back burner until a future date (Ifinedo, 2014).

It has been documented that many business leaders struggle with allocating the necessary resources to information technology projects because it is not always easy to see the return on their investment (Makarevic, 2016; Otieno & Biko, 2015; Gilbert, Pick, Alan, & Ward, 2012). It is this mindset that has translated into a low success rate for information system projects with just 32% of IS projects proving to have successfully accomplished their objectives (Fulk, Kwun, & Alijani, 2013).

The purpose of this qualitative case study was to identify the reasons behind the insufficient funding of information systems projects in the private sector. The data collection process was conducted using the interview method conducted via questionnaires and surveys. The participants were selected from small to medium sized businesses located in the United States and have an active role in the IS project request and budgeting approval process.

This research relied on several mediums for information. This includes: previous research, media reports, and interviews. Previous research was extracted using the online database ProQuest. The search criteria included data from the past three years from select businesses located in the US. These businesses were small to medium sized businesses (50 to 250 employees) that have attracted media attention for their failed security measures. Media reports were collected by accessing the following databases: ABI/Inform (Business and Management), IEEE Computer Society Digital library, First Research, and Business Source Premier Databases. The primary source of information

came from the interview process.

The significance of this study is that it challenges the concept of the information technology team being required to do more with the same or fewer resources. Many organizations have suffered terrible losses due to insufficiently funded information technology departments (Elgin et al., 2014; Broardhurst et al., 2014; Tham, 2013). These losses have had direct impacts on the organizations, their employees and even their customers and suppliers (Elgin et al., 2014; Broardhurst et al., 2014; Tham, 2013). This study contributes to the field of information technology by highlighting the growing responsibility of information technology staff and the need to have adequate resources to fulfill those responsibilities.

## **Chapter 4: Findings**

The purpose of this qualitative case study was to identify the reasons behind the insufficient funding of information security projects based on the perceptions of information security decision makers at small and mid-sized firms located in the U.S. The qualitative research design used was case study. The case study involved researching current and previous research works that dealt with IT budgeting, information security and project management. This study also used interviews to sample real world input in the problems of Information Technology projects not receiving sufficient funding.

This chapter begins with restating the questions being used to guide this qualitative research study. The results of the case study appear under a different heading. This chapter concludes with an evaluation of the findings and summary of the pivotal points

### **Results**

The results section of this research consist of a combination of data gathered from case studies and semi-structured interviews. The interviews were presented using a predeveloped interview protocol. Five of the interviewees consented to having their interviews recorded and three did not. The researcher took notes during all of the interviews for all eight participants. The interviews ranged in time between 40-65 minutes, depending on how much information the interviewees wanted to share. All of the interviewees had their interviews coded using their initials to disguise their identities. All of the information from the interviews was saved and secured via a password known only to the researcher. For backup purposes, that same file was also saved to an

encrypted flash drive and stored in a fireproof safe. All of the data is being stored for a period of seven years then permanently destroyed.

The interview included eight information technology and systems professionals that have direct knowledge of the information technology budgeting process. The interviewees presented their opinions about the reasons for the insufficient levels of funding for information technology projects. These individuals were initially solicited through a Google user group called the “CLS User Group”. These individuals all came from different backgrounds with varying IT experiences. This user group consists of information technology professionals located in the United States. The interviews were conducted via Uberconference. Uberconference is a hosted conference line service that allows the participants to interact with each other as well as record the conversations.

The participants of this study included five males and three females ranging in ages between 37 and 56 years of age. Their titles included the following: Enterprise IT Consultant, IT Manager, Director of Technology, Senior Systems Engineer, Director of Engineering Services, Chief Information Officer, Senior Project Engineer and an IT Director. All of the interviewees had a minimum of a Bachelor’s degree and a minimum of 5 years of experience in dealing with IT Project request and budgeting. All of the interviewees were assigned unique codes to protect their identities. The interviewee demographic table is below.

Table 1						
Demographics						
Participant ID	Age	Gender	Education	Title	Years in field	

JM	38	Male	Masters	Enterprise IT Consultant	7
LM	37	Female	Bachelors	IT Manager	9
MG	50	Male	Masters	Director of Technology	17
MTZ	50	Male	Bachelors	Senior Systems Engineer	20
MTE	46	Male	Bachelors	Director of Engineering Services	19
NO	56	Female	Masters	Chief Information Officer	32
RS	40	Male	Bachelors	Senior Project Engineer	20
RW	56	Female	Bachelors	IT Director	11

### **Thematics Analysis of Research Question 1**

Research Question 1: What do information security decision makers at small and mid-sized private firms located in the U.S. believe about the insufficient funding of their projects? This research question was the catalyst for interview questions Q1, Q2, Q4, Q6, and Q7. Case studies have highlighted that fact that many individuals working in the Information Security arena do not feel that they received adequate support to complete the necessary projects required to keep the organization safe from both internal and external cyber-threats (Makarevic, 2016). Many organizational leaders tend to fixate on the amount of resources being requested for Information Technology projects instead of the good that the project can do for the organization (Chen et al., 2015). It is this way of thinking that continues to be a source of concern for IT security staff (Otieno & Biko, 2015).

Research has reported that only 32% of IT projects are successful (Fulk et al., 2013). This means that 68% of IT projects are failing for various reasons. IT managers attribute that failure to too much managerial oversight and too few resources to make available to complete the projects in a timely manner (Fulk et al., 2013). Information Technology leaders do not feel like valued members of the company in many

organizations because they are the first departments to have their budgets rejected or reallocated based on the needs of the organization (Elgin et al., 2014).

Information technology leaders believe it is impossible to properly protect the technological infrastructure of an organization without being given the financial resources to get the job done (Wilding & Wheatley, 2015). The IT management team understands a concept that others in the organization's leadership struggle with and that concept is that IT security cost money (Wilding & Wheatley, 2015). Cyber-threats are one of the top five risk facing organizations today (Fenz et al., 2014). Companies need to be prepared to deal with these threats in proactive manner versus a reattactive one (Sauls & Gudigantala).

This research was able to detect a pattern of data breaches that continues to impact both public and private sector organizations. Companies like: Paypal, Sony Pictures, and Home Depot Inc. each failed to properly invest in their information security infrastructures and this failure to invest properly made these companies vulnerable to cyber-attacks (Broadhurst et al., 2014; Tham, 2013).

The exploit at Paypal lead to many of their customers be scammed out of monies ranging from \$50 to \$3,000 (Tham, 2013). Customer data was stolen via emails and spoofed webpages. After the exploit, Paypal strengthened their security systems to offer better protection for their customers (Tham, 2013).

Sony Pictures Corporation suffered in September of 2011. In 2011 a hacker used a SQL injection attack against Sony's website allowing the hacker to steal the company's data (Broadhurst et al., 2014). That data that was stolen included: names and addresses of employees, employee phone numbers, and email addresses for thousands of Sony

customers (Broadhurst et al., 2014). Sony Pictures was aware of the vulnerability, but failed to protect their organization against the threat (Broadhurst et al., 2014).

Home Depot Corporation suffered from a cyber-attack due to known software vulnerability in 2014 (Elgin et al., 2014). Home Depot had the software available to prevent the attack, but failed to put the software in place and this failure costed the company 62\$ million. The vulnerability put 56 million card holders at risk of having their information compromised (Elgin et al., 2014).

The US Navy sailors were put in a position of vulnerability because Hewlett-Packard, a Navy contractor, had one of the laptops compromised that they used for doing Naval projects (Chief of Naval Personnel Public Affairs, 2016). Hewlett-Packard had failed to put the proper security measures in place to protect the sailor's sensitive information. This failure allowed the names and social security numbers of the sailors to be hacked. The US Navy gave each sailor free credit monitoring for this imposition (Chief of Naval Personnel Public Affairs, 2016).

The Democratic National Committee was also compromised during 2016, actually they were compromised in 2015 and it was not discovered until April of 2016 (Nance, 2016). ). The hackers were searching for information on presidential candidate Donald Trump on the DNC's servers. After locating the information they were looking for, the attackers spent months going through the server stealing data. The stolen data consisted of emails, donor bank account information, credit card information, and even donor social security numbers (Nance, 2016). The group responsible for the attack is called the Cyber Bears (Nance, 2016).

The attack was eventually halted after an IT security company called CrowdStrike

had been hired by the DNC to determine the severity of the attack (Nance, 2016). The DNC reported that they are attacked regularly by different groups based on their political agendas. CrowdStrike used analytical tools to see where the breaches occurred, what was compromised and how long the intruders had been in the DNC's servers. It was determined that the attack went back as far as April 2015 (Nance, 2016). CrowdStrike was able to work the DNC to neutralize the threat, though it took over a year before the threat was ever noticed (Nance, 2016).

All of these incidents made a strong correlation the information obtained from interviews conducted by the researchers. The participants answered each question based on the experiences at their current places of employment and many of their organizations have suffered similarly to those previously listed for failing to invest in their information technology infrastructure.

**Q1. How familiar are you with the information technology project approval process?**

Each of the eight interviewees were required to answer this question prior to proceeding with the rest of the interview. The purpose of this specific question was to make sure that each participant qualified to take part in this study. To qualify, each participant had to have direct, hands on experience with some phase of the information technology budget submission and or approval process. Each of our participants met that criteria. 63% of the interviewees reported that they work either as a team or independently to submit IT projects for approval. The remaining 37% served on a board that either approves or denies the IT project requests.

**Q2. What is your role in submitting information technology projects for approval?**



Question 2 was designed to specifically learn just what each participant does in project submission process. The question was used to further gauge the participant's level of understanding in the IT Project submission process. MTE's role was to design the project, create the bill of materials and explain the necessity of the project to upper management when required. JM's role was in project submission was more extensive than some of the others.

"I have served in the capacity of project coordinator and SME for speaking on the need for the rollout of the project. As project coordinator, I was responsible for researching, validation and coordination of demos from vendors in regards to the specific product we thought desirable to the organization. I then had to prepare all of the information for management. This included cost analysis, product alternatives and projected timelines for project completion pending approval"

Participate NO (these are the participants initials) had a very unique role in that the candidate had to submit their project request to a panel of 12 non-technical people. "The budgeting process requires me to submit my projects to the budget management team. This is one of the rare positions that I have held that I have had to go before an actual panel and justify my budget requests in person. The thing that makes this difficult is that I am often trying to explain technical things to non-technical people, but as the CIO, it is my job to make sure the company understands our technical needs, so I spend quite a bit of time preparing IT Project budgets for submission to the panel".

All of eight of the interviewees had demonstrated that they have had unique experiences when it comes to submitting information technology projects for approval.

None of the participants were able to approve their own projects or budgets. Each was accountable to a higher level of management that required the candidates to justify the need and the cost for the projects they were requesting approval for.

**Q4. What percent of IT projects are approved in a timely manner?**

When each participant was asked to give their opinion on whether IT projects are approved in a timely manner, their answers varied. The two probes in this question appropriately aided in identifying the variances in the answers given. JM felt like 60% of IT Projects are approved in a timely manner. The amount of the project played a direct impact on whether the project was approved and how fast it was approved. Ultimately, JM determined that the levels of funding set aside for IT Projects was too low. JM has witnessed the company setting a low IT Project budget, then later further removing funds from that budget to use those funds in other areas of the organization deemed more important by the company's leadership. Two of the interviewees believed that IT Projects in their organizations get approved at the 90% rate. Both MG and LM attribute this high rate of approval to better planning. They happen to work for organizations that allow them to submit budget items in advance so the companies can prepare the capital expenses.

Two other interviewees believed their organizations approved IT Projects at the 75% rate. Once again, the size of the investment was a huge factor in determining which projects would get approved. MTE and RS have both noted significant improvements in the way their organizations handle IT Project approval. MTE noted that project request based on the aged of equipment are approved at the 30% level and projects that directly impact day to day operations are approved at higher levels.

MTZ believed based on his experience with the organization that IT Projects are approved at the 10% level. This low approval rating is attributed to the lack of understanding by upper management of why IT does and how important their projects are. MTZ further mentioned that there are no ITS staff on the budgeting boards and when the ITS staff mention how other organizations have been compromised by cyber-attacks, the leadership downplays it. Interviewee RW stated that IT Projects for their organization get approved at 40%. This approval level was not impacted by the size of the project and the company sets very little resources aside for IT Projects. The company is on the small side and does not see the value in investing huge amounts of capital in IT Security projects. Those resources are often allocated for marketing and sales.

**Q6. Do you believe the levels of funding set aside for IT security projects is too low?**

88% of the interviewees stated that the funding set aside for IT security projects is too low. 12% stated that the funding levels set aside were not too low, but the approval process was too convoluted. IT security projects are defined as any IT Project that is being requested that has a direct impact on information security. The things that fell into this category included: firewall upgrades, maintenance and replacement, antivirus subscriptions, upgrades and maintenance, tools to monitor and control file access, tools to control Virtual Private Network (VPN) access, tools to control access to secured files and even tools to filter incoming and outgoing emails. There are other areas that are also considered areas of Information security did not make the list above.

The consensus for the number one reason behind the low levels of funding was a failure of management to understand the importance of properly funding the IT Security projects. RW noted that the IT staff is often pushed to a corner of the office and treated

like they do not exist until a problem arises. JM noted that their organization had no one monitoring their IT staff, which led to a huge security vulnerability. The vulnerability had the organization down for four days.

**Q7. How does your organization's leadership understand the importance of their information technology department?**

All of the interviewees formed a consensus when answering interview question 7. They all agreed that the leadership within their various organizations do not understand the importance of their information technology departments. Some mentioned that their organizations are too big and the leadership does not take the time to learn what they do. MTZ mentioned that there are no members from the Information Technology department on any of the leadership committees. The participant stated this lack of meaningful participation in the leadership of the organization demonstrates just how undervalued the Information Technology department is. RW mentioned that their organization only realizes the value of the Information Technology department when things are not working. Things like email, internet access, and access to shared network files. As long as management can get to the things they need, they take very little interest in anything else going in IT department.

Participant NO mentioned that while the leadership does not show that they understand the importance of the IT department, they do know where and how to call when there is a problem. However, ultimately, there is seems to be a greater concern with the budget than with dealing with issues of cyber-security. MTE stated that things

could be better if the leadership would take a more proactive approach to addressing problems instead of a reactive one.

### **Thematic Analysis of Research Question 2**

Research Question 2: What do information security decision makers at small and midsized private firms located in the U.S. believe are the reasons behind the levels of funding dedicated to their information security systems. The second research question was used to help hone in on specific reasons being attributed to Information Technology project and budget approval or denial as viewed by Information Security decisions makers. This research question was used to develop Q3, Q5, and Q8 for the interviewees.

Information security decision makers believe the reasons for their lack of funding have to do with organizational leadership not understanding what the IT department really does (Williams et al., 2013). The news inundates society on a regular basis with information about cyber-attacks, infiltrations and security breaches. These types of news stories have the ability to desensitize organizational leadership because they begin to think the problems cannot happen at their place of business (Ahmad & Maynard, 2014).

Information security decision makers understand that until management understands the seriousness of cyber-security threats that their project funding continues to be in jeopardy (Fenz et al., 2014).

### **Q3. Has your organization ever suffered from a cyber-attack?**

Of the participants that took part in the interview, 50% of them admitted that their organizations have suffered from some sort of cyber-attack. Participant JM's organization suffered from a spam email attack. The attack was initiated when an

employee clicked on a phishing email. The attack was trying to send out massive amounts of email from the company's email server, which caused the email server to fail. The company had systems in place to detect the attack but not to stop it. Those responsible for keeping the servers patched and protected had not been doing their jobs. The company lost four days of productivity and countless thousands of dollars behind the attack.

Candidate MTZ's organization suffered from a brute force attack on their firewall. The vulnerability was known to the IT team and made known to the CFO, which was also over the IT department. This attack stemmed from a port being left open on the firewall that the CFO was using to work remotely. The IT staff had offered the CFO other options, but the individual was uninterested in learning a new technology. This brute force attack costs the organization over \$8,000 in labor and software to defend against the attack. The CFO was not penalized by the organization for failing to do their part to keep the company safe.

The other cyber-attacks mentioned were minor and did not real damage to the organizations. All of the candidates mentioned that the most seen attacks are email phishing attacks. Attackers use email attacks because they have proven to be a good way to get unaware individuals to click on them, which grants them access into the network.

**Q5. Do you believe your organization's information security systems can provide adequate protection?**

While many of the participants saw the problems with their organizations, some also saw hope. 63% of those interviewed believed that their organization's information security systems can provide adequate protection, but that improvement was needed. The other 37% stated that they did not believe that their organization's information security

systems could provide adequate protection. The reasons listed included: outdated systems, lack of resources to maintain systems and no end user training. No end user training was repeated by both NO and MG. The candidates mentioned how even with patched systems, they still need to be able to train the end users on how to avoid clicking on phishing emails and other areas of cyber-security. When asked why there was no end user training the answer was the same by both candidates, the company did not have the time or resources to devote to it.

**Q8. Would you like to add any other information on the reasons behind the insufficient funding of information security projects in the private sector?**

The question was designed to give the participants the opportunity to give their input on other areas that have a direct impact on Information Security. The answers varied greatly. NO believed that companies as a whole need to spend more time and resources on information security systems. The candidate went on to emphasize how the extra effort upfront could save the company time and money in the long run. The example the candidate gave is that their organization does not have the funding for a full-time IT Security professional. The company is also unwilling to bring in a consultant to assist with the areas of information security. This means that those duties fall on staff that may not be fully qualified to handle those responsibilities.

RW mentioned that the organization's leadership has a lack of what is going on in the industry. This means they are unfamiliar with new threats and new technologies to address those threats. Leadership does not always demonstrate confidence in the IT staff and this creates a problem when they are submitting IT security projects for approval. MTE also mentioned their leadership does not believe that their organization is

susceptible to real world threats. It is this lack of corporate cohesiveness that creates stress for the IT staff and information security concerns for the organizations.

### **Evaluation of Findings**

The failure to invest properly in IT infrastructure has been detrimental to many companies. Paypal, Sony Pictures, and Home Depot Inc. each failed to properly invest in their information security infrastructures and this failure to cost these companies millions of dollars and created unnecessary hardships for their staff and customers (Broadhurst et al., 2014; Tham, 2013). The staff suffer because they companies lose sales and could end up downsizing their staff and the customers suffer because their sensitive information is now in the hands of attackers.

Paypal's lack of security lead to many of their customers be scammed out of monies ranging from \$50 to \$3,000 (Tham, 2013). Attackers used spoofing programs to manipulate Paypal's customers into providing them with their information. Paypal did eventually incorporate a better protection profile for their customers, but for some it was too little too late because their information had already been compromised (Tham, 2013).

Sony Pictures Corporation sufferings in September of 2011 were the result of SQL injection attack (Broadhurst et al., 2014). This attack made the staff vulnerable because their names, addresses, phone numbers, and email addresses were compromised (Broadhurst et al., 2014). Sony Pictures was aware of the vulnerability, but failed to protect their organization against the threat (Broadhurst et al., 2014). These types of failures are avoidable with the proper investments and support from organizational management.



Home Depot Corporation sufferings were from a cyber-attack due to known software vulnerability in 2014 (Elgin et al., 2014). Home Depot had the software available to prevent the attack, but failed to put the software in place and this failure costed the company 62\$ million. This attack highlights the importance of having properly trained IT staff and management working together. Properly trained IT staff can advocate for the security of the organization even when the road to project approval is difficult. The vulnerability put 56 million card holders at risk of having their information compromised (Elgin et al., 2014).

The US Navy sailors were put in a position of vulnerability because Hewlett-Packard, a Navy contractor, had one of the laptops compromised that they used for doing Naval projects (Chief of Naval Personnel Public Affairs, 2016). Hewlett-Packard could have implemented any number of security or encryption programs that would have rendered that laptop useless in the event of a compromise. Instead, Hewlett-Packard's failure implement proper security measures has put over 134,000 US Navy sailor's sensitive information at risk. The US Navy gave each sailor free credit monitoring for this imposition (Chief of Naval Personnel Public Affairs, 2016).

The Democratic National Committee's server attack during the 2016 Presidential election highlighted the importance of implementing appropriate information security practices (Nance, 2016). Their servers were attacked by hackers searching for information on presidential candidate Donald Trump on the DNC's servers. The attackers found what they were looking for and much more. They were able to compromise data consisting of emails, donor bank account information, credit card information, and even donor social security numbers (Nance, 2016). The group

responsible for the attack is called the Cyber Bears (Nance, 2016).

The attack was eventually neutralized after an IT security company called CrowdStrike was hired by the DNC to determine the severity of the attack (Nance, 2016). The DNC reported that they are attacked regularly by different groups based on their political agendas. The DNC knowing they were a regular hack target, failed to implement any kind of preventative security controls to keep their information secured. CrowdStrike used analytical tools to isolate the breach, but it was too late because the attackers had been sitting on the DNC's server for approximately one year without notice (Nance, 2016).

After interviewing the eight candidates for this study, it is evident that there are some very strong feelings pertaining to the funding of information security projects in small to mid-sized businesses in the U.S. The participants continuously emphasized a disconnect between those responsible for security the organization's technical infrastructure and those who must approve the budgets. This disconnect has led to project budgets being delayed and even denied which has hurt many of the organizations. Many of the organizations have suffered from cyber-attacks because they failed to fund the necessary projects to keep their systems secured (Pernebekova & Ahbergenovich, 2015). The IT staff understands that information security is not a problem that only impacts large, public organizations, but it impacts all organizations (Brand et al., 2015).

The IT staff of many organizations have the uphill battle of struggling to get organizational leadership to understand what they do and why funding their projects is so important (Brand et al., 2015). Companies that continue to fail to invest in their information security infrastructure are setting themselves up to experience the kind of

attacks that have impacted some of the larger known companies like: Paypal, Home Depot, and even Gucci (Broadhurst et al., 2014). Information Security decision makers are ready for their budgets to be approved and treated with dignity instead of as an afterthought, due to an exploitation of the company's systems.

Information Security decision makers believe the reasons behind the insufficient funding of information security projects is multifaceted. Many business leaders do not understand what their IT departments do (Gupta & Shakya, 2015). This lack of understanding has had a direct impact on project funding (Ifinedo, 2014). The IT department in many companies is still viewed as overhead and not a necessity, which creates a burden on the IT staff who are seeking project funding (Gupta & Shakya, 2015; Luftman et al., 2013). Small to mid-sized companies believe they can "get away" with not having fully staffed IT departments because they do not believe they are vulnerable to attacks (Makarevic, 2016). These problems are just some of the reasons information security decision makers have attributed to their insufficient levels of project funding.

The eight participants that took part in this study all worked in different industries within the private sector. Each offered their opinions based on their years of experience in the Information Technology field and experience on their current jobs. All of the participants were at a manager level on their current jobs and played a direct role in either submitting IT projects for approval or approving the projects. Their feedback tended to coincide heavily with the information gathered during the literature review.

## **Summary**

The study of eight individuals that play a direct role in the IT budgeting process have been evaluated and found synchronous with the data that obtained during the

literature review. The findings obtained during the literature review highlighted a disconnect between organizational leadership and those working in the IT departments. The eight participants that took part in the interview emphasized that organizational leadership fail to understand the importance of what the IT department does and those that had leadership that understood still failed to receive adequate funding to complete necessary Information Technology projects with any regularity.

The primary reasons identified during the interview process for receiving insufficient funding included: management being discouraged by the cost of the projects, management having no one on the budget approval committee with an IT background to help them understand the project request, and management not understanding the value of preventative maintenance when it comes to technology. This echoes the problems identified during the literature review (Gupta & Shakya, 2015; Fulk et al., 2013; Pernebekova & Ahbergenovich, 2015; Velmurugan & Mathiyalagan, 2015). This problem was identified at both small and medium sized organizations.

## **Chapter 5: Implications, Recommendations, and Conclusion**

Information security threats and concerns are on the rise and it is up to organizations to address these threats with a high sense of urgency (Ifinedo, 2014). One of the problems that organizations have to deal with when determining how to prepare for dealing with the elevated cyber-threat levels is cost (Gupta & Shakya, 2015). The majority of IS projects come at a high cost (Gupta & Shakya, 2015; Chen, Ramamurthy, & Wen, 2015).

Compounding the funding issues for IS staff requesting funding for new IS projects is that only 32% of new IS projects are successful (Fulk et al., 2013). The items contributing to this low success rate include: too much managerial oversight and limited resources (Fulk et al., 2013). The limited resources means that the IT/IS staff may not have gotten all of the resources they requested to actually complete the job.

The specific problem this research addressed is the lack of knowledge on how information technology managers perceive the reasons information security projects are underfunded at small and med-sized private firms in the United States. (Pernebekova & Ahbergenovich, 2015; Velmurugan & Mathiyalagan, 2015; Chen et al., 2015; Makarevic, 2016; Otieno & Biko, 2015; Peffers & Santos, 2013; Conboy, 2009; Cao, Mohan, Ramesh, & Sarkar, 2013; Gottron, 2013; Marshall, 2012).

The purpose of this qualitative case study is to identify the reasons behind the insufficient funding of information security projects based on the perceptions of information security decision makers at small and midsized private firms located in the U.S. This study also assess, based on the perceptions of the information technology

managers, if the information security systems are adequately able to protect the organization from cyber-threats.

The research methodology that was used for this study was qualitative. Qualitative research methodology provides an ideal approach to understanding organizational changes, especially changes involving complex stake-holder organizing, work place practices and organizational structure (Gentles, Charles, Ploeg, & McKibbin , 2015). The qualitative research design being used in this research is case study. Case study focuses on what is to be studied (Gentles et al., 2015).

Price & Murnan, (2004) propose that a limitation of a study design or instrument is the systematic bias that the researcher did not or could not control and which has the potential to inappropriately affect the results. There are many aspects to this study that were beyond the control of the researcher that could have contributed to the limitations of this study. These limitations include things like the amount of time and willingness of the participants to commit to this study. Other potential limitations to this study could have been: too few participants or the participants being unwilling to answer all of the questions honestly, which could have skewed the results.

To ensure no ethics were violated, this study complied with the rules that Northcentral University has put in place. This means that no research was conducted prior to Institutional Review Board (IRB) approval. This study was not sent to the IRB until the mentor had approved that it was ready. All participants were asked to sign off on an informed consent document (Appendix B), which outlined the purposes for which this research was conducted and it explained how their answers would be used.

The Informed Consent Form was very detailed in that it: described the purpose of the research study, detailed the expectations for the participants, highlighted the fact that this study is voluntary and comes with an anticipated time obligation, gave participants the option to ignore certain questions if they feel uncomfortable answering them, or cease participation in the study at any time without penalty.

Chapter 5 includes the implications, recommendations and the conclusion. This chapter also includes a summary of the key points in the conclusion.

### **Implications**

A qualitative study was conducted to explore information technology decision makers perceptions of the problems with insufficient funding of information technology projects in small and mid-sized organizations located in the US. The implications for organizations are that they need to have leadership that understands what their IT staff does, the IT staff must be seen as an ally and not overhead. Organizations must be willing to provide the necessary resources for the IT staff so that they can do their jobs and keep the companies protected from any vulnerabilities that could occur from having an unsecured network. Failure to provide the IT staff with the necessary tools will lead to more companies suffering from cyber-attacks.

### **Research Question No.1**

The first research question explored what information security decision makers perceived about the insufficient funding of information security projects in small to mid-sized organizations located in the US. The findings suggested that there needs to be more collaboration and understanding between the IT departments and members of the organization's leadership teams. The themes identified in this research revealed that many

organizations are still unwilling to make investments into things that they do not understand or deem important. This problem parallels to the information found during the literature review (Wall, 2013).

There are important implications of these findings. Organizations need to have diverse leadership committees if they are to avoid the pitfalls of cyber-risks. The diversity needed is one where members of all critical departments are properly represented. This would mean that members of the IT staff would have a chance to speak at budget meeting, which would allow them the opportunity to emphasize the importance of properly investing in and approving IT project request.

Other implications include the need for security awareness training for staff at all levels an annual basis. This training would help ensure that the staff is doing their parts in keeping the organization safe from cyber-threats. The training should cover the latest threats and the how to take the necessary steps to avoid those threats. Threats like email phishing scams and avoiding clicking on random web pop ups should be covered thoroughly.

The last implication needs to be having the appropriate staff available to manage, monitor and maintain all networking equipment that is being used to protect the organization's technical infrastructure. Organizations need to recognize the value of having qualified staff onsite to quickly identify and resolve problems. These individuals should be highly skilled and proven and not staff that have been promoted due to tenure. Trained IT staff is one of the primary defenses against threats.

## **Research Question No.2**



The second research question explored the perceived reasons for the insufficient funding of information security projects as viewed by information security managers and decision makers. The findings highlight the need for greater working relationships between the IT department the budget approval committees within organizations. The IT staff must get better at emphasizing the importance of their request and the corporate leadership must get better at understanding the justifications being given. It takes teamwork to keep the organization secured from cyber-attacks.

### **Recommendations**

It is recommended that companies that want to avoid unnecessary exposure to cyber-attacks and risks take a more serious approach to approving IT security budget requests. To get to this point, leadership needs to understand the impact a malicious attack could have on their organization (Ahmad & Maynard). This means that leadership needs to know what is happening in their industries pertaining to cyber-threats and how well their organizations can defend against that threat (Otieno & Biko, 2015). This is the type of information that requires leadership to work with their IT security staff. The IT security staff is responsible for knowing what is going on the industry and ensuring the company is safe from both internal and external cyber-threats (Hedstrom et al., 2013).

It is important that organizational leadership understand that IT Projects cannot be completed without proper funding (Tsohou et al., 2012). IT security projects need to be viewed as insurance to keep the company's technological infrastructure secure (Tsohou et al., 2012). It is important for the decision makers to look at more than the dollars being requested for the project, but to look at what the project is proposing to do for the organization. An analysis of what it would cost if the company inoperable for week due

to a cyber-attack would help the leadership see how important it is to properly fund IT security projects. Findings from this study revealed that companies are still suffering from cyber-attacks that could have been avoided if the proper investments had been made to secure their infrastructures. In addition to the recommendation to properly fund information security projects, it is also recommended that all staff be put through annual security awareness training. Staff have the ability to create problems for the company when they are not aware of the risks of their actions. Properly training them would help to minimize the chances of them being victimized by an email phishing attack or by clicking on a malicious web pop up.

It is recommended that organizations invest in a multifaceted cyber-threat defense strategy. This strategy needs to consist of: encryption technologies, security technologies, identification technologies and remediation technologies. The encryption technologies would protect data as it is being transmitted and while sitting at rest on the companies servers.

Many manufacturers offer encryption programs that encrypt data to prevent compromise. One of those products is called Sophos. Sophos offers client side and server managed disk encryption solutions that encrypt the hard drives of laptops, computers, and servers.

Security technologies that could benefit companies include: managed firewall solutions, desktop and server antivirus and antimalware protection. Having a managed firewall solution would allow organizations to catch potential cyber-threats more quickly. There are many firewall manufacturers that incorporate tools like: Intrusion Protection Service and Intrusion Prevention Service. These tools are used to detect and block

potential threats. When these tools are combined with an effective managed antivirus and antimalware solution, the organization has a better chance of defending themselves against threats. It is recommended that all organizations invest in these technologies and that they keep their subscriptions to these technologies current so they can continue to get firmware upgrades so the devices are ready to defend the organization against the most current threats.

The final recommendation is that companies work on creating a more cohesive technical infrastructure. The IT staff should not be hidden in the lower levels of the organization with no thought or oversight. They are providing services that keep the company operating on many levels. The IT staff must be treated like a valued member of the organization and trusted to do the jobs they were hired to do.

## **Conclusion**

As cyber-security threats continue to escalate, so must the response levels by organizations. Organizations need to have properly trained staff working in their Information Security departments and those individuals must be given the financial resources necessary to keep the company secured against both internal and external cyber-security threats (Vuuren, 2016). Cyber-threats plague companies all over the world and cost companies countless sums of money trying to recover from them (Otieno & Biko, 2015).

Organizations can take a huge risk when they deny funding to information security projects. Information security projects are those vital projects that protect the organization's technological infrastructure from both internal and external threats. Too

many organizations have suffered because they have failed to properly support their IT staff and fund necessary security projects. The problems that plagued companies like: Paypal, Home Depot, Gucci, Sony Pictures could have been avoided with the proper support and investments (Elgin et al., 2014; Tham, 2013; Broadhurst et al., 2014).

The latest victims include the US Navy, which was notified by Hewlett-Packard on October 27, 2016 that one of their laptops used to support the naval contract had been compromised (Chief of Naval Personnel Public Affairs, 2016). This breach compromised the personal information for 134,000 navy sailors. The US Navy now has to investigate a problem that could have been prevented if Hewlett-Packard had implemented the proper security measures required to keep that data secured against both internal and external data security threats.

The last victim is the 2016 US Election (Nance, 2016). It was reported that beginning in March and April of 2016 that unknown entity hacked into the Democratic National Committee's (DNC) computer system. The perpetrators were looking for information on Donald Trump and after finding what they were looking forward, they also stole emails, voicemails and other information (Nance, 2016). It is reported that the perpetrators were on the DNC's servers for several months before their presence was ever noticed. By the time the DNC noticed the infiltration and shut down their servers, it was too little too late, the damage had already been and their security had already been compromised (Nance, 2016).

Examples like these and many others provide the ground work for implementing and supporting better information technology security practices. When companies fail to implement the proper security measures they put both themselves and their customers at

risk for cyber-attacks. The risk for cyber-attacks can be diminished with the proper technological investments such as: encryption technology, security technology, and threat identification and remediation technologies. A managed firewall solution with IDS and IPS could have prevented the attack on the DNC's server. Many manufactures make them such as: Cisco, Fortinet, Juniper, and Palo Alto. Having encrypted hard drives could have prevented the US Navy from needing to offer free credit reporting to the sailors that had their information compromised due to a security breach at Hewlett-Packard. Properly trained and empowered staff could have prevented the attacks at Paypal, Home Depot and Sony pictures.

These are prime examples of why organizations cannot afford to not fund information security projects. Information security projects are implemented to give the organization the advantage in the war against cyber-terrorists and cyber-threats. Each of the organizations that had their security compromise could have had the compromise prevented if they had invested in their information infrastructure proactively.

## References

- Abusabha, R., & Woelfel, M. L. (2003). Qualitative vs quantitative methods: Two opposites that make a perfect match. *American Dietetic Association. Journal of the American Dietetic Association*, 103(5), 566-9.
- Adler, J., Demicco, M., & Neiditz, J. (2015). Critical privacy and data security risk management issues for the franchisor. *Franchise Law Journal*, 35(1), 79-92.
- Ahmad, A., & Maynard, S. (2014). Teaching information security management: Reflections and experiences. *Information Management & Computer Security*, 22(5), 513.
- Al Hosban, A. A. (2015). The role of regulations and ethics auditing to cope with information technology governance from point view internal auditors. *International Journal of Economics and Finance*, 7(1), 167-176.
- Ali, S., & Green, P. (2012). Effective information technology (IT) governance mechanisms: An IT outsourcing perspective. *Information Systems Frontiers*, 14(2), 179-193. doi:<http://dx.doi.org/10.1007/s10796-009-9183-y>
- Arutyunov, V. V. (2014). On the modern problems and challenges of information security international scientific-practical conference. *Scientific and Technical Information Processing*, 41(3), 159-163. doi:<http://dx.doi.org/10.3103/S0147688214030022>.
- Boulesnane, S., & Laïd Bouzidi. (2013). The mediating role of information technology in the decision-making context. *Journal of Enterprise Information Management*, 26(4), 387-399. doi:<http://dx.doi.org/10.1108/JEIM-01-2012-0001>.
- Barbosa, S. C. B., Rodello, I. A., & de Pádua, Silvia Inês Dallavalle. (2014). Performance measurement of information technology governance in brazilian financial institutions. *Journal of Information Systems and Technology Management : JISTEM*, 11(2), 397-414.
- Bradley, Don B., I., II, & Cooper, J. (2014). Cloud computing's selection and effect on small business. *The Entrepreneurial Executive*, 19, 87-94.
- Brand, J. C., Kruger-Van Renen, W., & Rudman, R. (2015). Proposed practices to mitigate significant mobility security risks. *The International Business & Economics Research Journal (Online)*, 14(1), 199.
- Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber-crime: An analysis of the nature of groups engaged in cyber-crime. *International Journal of Cyber Criminology*, 8(1), 1-20.

- Cao, L., Mohan, K., Ramesh, B., & Sarkar, S. (2013). Adapting funding processes for agile IT projects: An empirical investigation. *European Journal of Information Systems*, 22(2), 191-205. doi:<http://dx.doi.org/10.1057/ejis.2012.9>
- Chief of Naval Personnel Public Affairs. (2016). Security Breach Notification of Sailors' PII. Retrieved December 11, 2016
- Chen, Y., Ramamurthy, K. & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems*, 55(3), 11-19.
- Conboy K (2009) Agility from first principles: reconstructing the concept of agility in information systems development. *Information Systems Research* 20 (3), 329-354.
- Creswell, J. (2007). Qualitative inquiry and research design: *Choosing among Five Approaches* (2).
- Croteau, A., Bergeron, F., & Dubsky, J. (2013). Contractual and consensual profiles for an interorganizational governance of information technology. *International Business Research*, 6(9), 30-43.
- Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 4(2), 92-100.
- Dwivedi, Y. K., Wastell, D., Laumer, S., Henriksen, H. Z., Myers, M. D., Bunker, D. Srivastava, S. C. (2015). Research on information systems failures and successes: Status update and future directions. *Information Systems Frontiers*, 17(1), 143-157. doi:<http://dx.doi.org/10.1007/s10796-014-9500-y>
- Economics & Statistics Administration. (2003). Digital economy 2003. Washington, DC: US Department of Commerce
- Elgin, B., Riley, M., & Lawrence, D. (2014). Home depot hacked after months of security warnings. *Business Week*, , 1.
- El-Taj, H. (2015). Intrusion detection and prevention systems (IDPS) state of art: IDPS challenges. *International Journal of Computer Science and Information Security*, 13(9), 28-35.
- Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, 22(5), 410.
- FIPS (1975), *PUB 65: Guideline for Automatic Data Processing Risk Analysis* , National Bureau of Standards US Department of Commerce, Gaithersburg

- Fujiura, G. T. (2015). Perspectives on the publication of qualitative research. *Intellectual and Developmental Disabilities*, 53(5), 323-328.
- Fulk, H. K., Kwun, O., & Alijani, G. S. (2013). Scapegoating humans, scapegoating technologies: examining another side of information system project control. *Academy of Information and Management Sciences Journal*, 16(2), 31-48.
- Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, 20(9), 1408-1416.
- Garcia, D., & Gluesing, J. C. (2013). Qualitative research methods in international organizational change research. *Journal of Organizational Change Management*, 26(2), 423-444. doi:http://dx.doi.org/10.1108/09534811311328416
- Gentles, S. J., Charles, C., Ploeg, J., & McKibbin, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*, 20(11), 1772-1789.
- Gilbert, A. H., Pick, J., Roger Alan, & Ward, S. G. (2012). Does "IT doesn't matter" matter?: A study of innovation and information systems issues. *The Review of Business Information Systems (Online)*, 16(4), 177.
- Gottron, F. (2013). Science and technology issues in the 113th Congress\*. *Current Politics and Economics of the United States, Canada and Mexico*, 15(1), 1-51.
- Gupta, A., & Shakya, S. (2015). Information system audit; A study for security and challenges in nepal. *International Journal of Computer Science and Information Security*, 13(11), 1-4.
- Halaweh, M. (2012). Integration of grounded theory and case study: An exemplary application from e-commerce security perception research. *JITTA : Journal of Information Technology Theory and Application*, 13(1), 31-50.
- Hassan, H. M., Reza, D. M., & Farkhad, M. A. (2015). An experimental study of influential elements on cyberloafing from general deterrence theory perspective: Case study: Tehran subway organization. *International Business Research*, 8(3), 91-98.
- Hausken, K. (2015). A strategic analysis of information sharing among cyber hackers. *Journal of Information Systems and Technology Management : JISTEM*, 12(2), 245-270.
- Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals. *Information Management & Computer Security*, 21(4), 266-287. doi:http://dx.doi.org/10.1108/IMCS-08-2012-0043



- Ilvonen, I. (2013). Information security assessment of SMEs as coursework - learning information security management by doing. *Journal of Information Systems Education*, 24(1), 53-61.
- Ifinedo, P. (2014). The effects of national culture on the assessment of information security threats and controls in financial services industry. *International Journal of Electronic Business Management*, 12(2), 75-89.
- Jafari, S. M. B. (2014). Strategic cost-cutting in information technology: Toward a framework for enhancing the business value of IT. *Iranian Journal of Management Studies*, 7(1), 21-39.
- Jamali, M. A., Voghouei, H., & Md Nor, N. G. (2014). Information technology and survival of firms: A review of economic literature. *Netnomics : Economic Research and Electronic Networking*, 15(2), 107-119. doi:<http://dx.doi.org/10.1007/s11066-014-9089-9>
- Kuo-Chih Cheng, Tsung-Cheng, C., & Nien-Su Shih. (2014). The influence of budgetary participation by R&D managers on product innovation performances: The effect of trust, job satisfaction and information asymmetry. *Asia Pacific Management Review*, 19(2), 133.
- Lin, C., Tsai, Y., Joe, S., & Chiu, C. (2013). Modeling IT product recall intention based on the theory of reasoned action and information asymmetry: A qualitative aspect. *Quality and Quantity*, 47(2), 753-759. doi:<http://dx.doi.org/10.1007/s11135-011-9542-x>
- Luftman, J., Zadeh, H. S., Derksen, B., Santana, M., Rigoni, E. H., & Huang, Z. (. (2013). Key information technology and management issues 2012-2013: An international study. *Journal of Information Technology*, 28(4), 354-366. doi:<http://dx.doi.org/10.1057/jit.2013.22>
- Macia, L. (2015). Using clustering as a tool: Mixed methods in qualitative data analysis. *The Qualitative Report*, 20(7), 1083-1094.
- Makarevic, N. (2016). Perceptions towards IT security in online banking: Croatian clients vs. clients of bosnia and herzegovina. *International Journal of Finance & Banking Studies*, 5(1), 1-13.
- Marshall, J. P. (2012). Information technology and the experience of disorder. *Cultural Studies Review*, 18(3), 281-309.
- McNamara, C. (2009). General guidelines for conducting interviews. Retrieved January 11, 2010, from <http://managementhelp.org/evaluatn/intrview.htm>
- Menard, P., Gatlin, R., & Warkentin, M. (2014). Threat protection and convenience:

- antecedents of cloud-based data backup. *The Journal of Computer Information Systems*, 55(1), 83-91.
- Morales-sánchez, R., & Cabello-medina, C. (2013). The role of four universal moral competencies in ethical decision-making. *Journal of Business Ethics*, 116(4), 717-734. doi:<http://dx.doi.org/10.1007/s10551-013-1817-9>
- Nance, M. W. (2016). The plot to hack America: How Putin's cyberspies and WikiLeaks tried to steal the 2016 election.
- National employment and wage data from the Occupational Employment Statistics survey by occupation, May 2015. Retrieved from <http://www.bls.gov/news.release/ocwage.t01.htm>
- Noor, I. J., & Ajis, A. (2013). Organizational climate and individual factors effects on information security compliance behaviour. *International Journal of Business and Social Science*, 4(10)
- Onwuegbuzie, A. J., Leech, N. L., & Collins, K. M. T. (2010). Innovative data collection strategies in qualitative research. *The Qualitative Report*, 15(3), 696-726.
- Otieno, O. C., & Biko, M. S. (2015). Security and cryptography on world wide web. *International Journal of Computer Science and Information Security*, 13(9), 136-141.
- Pathari, V., & Sonar, R. M. (2013). Deriving an information security assurance indicator at the organizational level. *Information Management & Computer Security*, 21(5), 401-419. doi:<http://dx.doi.org/10.1108/IMCS-02-2013-0011>
- Patton, M. Q. (2002). Qualitative research and evaluation methods (3)
- Peffer, K., & Santos, B. L. D. (2013). Research opportunities in information technology funding and system justification. *European Journal of Information Systems*, 22(2), 131-138. doi:<http://dx.doi.org/10.1057/ejis.2012.60>
- Pernebekova, A. P., & Ahbergenovich, B. A. (2015). Information security and the theory of unfaithful information. *Journal of Information Security*, 6(4), 265-272.
- PN, S. (2014). Impact of information security initiatives on supply chain performance. *Information Management & Computer Security*, 22(5), 450.
- Price, J. H., & Murnan, J. (2004). Research limitations and the necessity of reporting them. *American Journal of Health Education*, 35(2), 66-67.
- Priya, A. (2014). Revisiting case study method of social research examining its cardinal attributes and its potential for generating authoritative knowledge. *IOSR Journal of Humanities and Social Science IOSRJHSS*, 40-44.

- Rabionet, S. E. (2011). How I learned to design and conduct semi-structured interviews: An ongoing and continuous journey. *The Qualitative Report*, 16(2), 563-566.
- Rest, J. R. (1986). *Moral development: Advances in research and theory*. New York: Praeger.
- Riege, A. M. (2003). Validity and reliability tests in case study research: A literature review with "hands-on" applications for each research phase. *Qualitative Market Research*, 6(2), 75-86.
- Rimando, M., Brace, A., Namageyo-Funa, A., Parr, T. L., Sealy, D., Davis, T. L., Christiana, R. W. (2015). Data collection challenges and recommendations for early career researchers. *The Qualitative Report*, 20(12), 2025-2036.
- Sales, N. A. (2013). Regulating cyber-security. *Northwestern University Law Review*, 107(4), 1503-1568
- Sauls, J., & Gudigantala, N. (2013). Preparing information systems (IS) graduates to meet the challenges of global IT security: Some suggestions. *Journal of Information Systems Education*, 24(1), 71-73.
- Schultze, U. (2014). IT project governance at worthington health-care system. *Journal of Information Technology Teaching Cases*, 4(1), 1-10.
- Sinkovics, R. R., Penz, E., & Ghauri, P. N. (2008). Enhancing the trustworthiness of qualitative research in international business. *Management International Review*, 48(6), 689-713.
- Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance. *Information Management & Computer Security*, 22(1), 42-75. doi:<http://dx.doi.org/10.1108/IMCS-08-2012-0045>
- Su, C., & Ni, F. (2013). Budgetary participation and slack on the theory of planned behavior. *International Journal of Organizational Innovation (Online)*, 5(4), 91-99
- Suduc, A., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. *Informatica Economica*, 14(1), 43-48.
- Suri, H. (2011). Purposeful sampling in qualitative research synthesis. *Qualitative Research Journal*, 11(2), 63-75.
- Tham, I. (2013). More PayPal users fall victim to hackers. *The Straits Times*
- Thomson, K., & van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management &*

- Computer Security*, 20(1), 39-46. doi:<http://dx.doi.org/10.1108/09685221211219191>
- Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology & People*, 25(3), 327-352. doi:<http://dx.doi.org/10.1108/09593841211254358>
- Turner, Daniel W. (2010). Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report*, 15(3), 754-760.
- Ugrin, J., & Michael, P. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior*, 29, 812-820.  
doi:<http://dx.doi.org.proxy1.ncu.edu/10.1016/j.chb.2012.11.005>
- Velmurugan, J. S., & Mathiyalagan, P. (2015). SOCIAL NETWORKING THREATS AND SECURITY ISSUES: AN ENQUIRY. *International Journal of Management Research and Reviews*, 5(4), 270-274.
- Vuuren, I. E. V. (2016). IT security trust model - securing the human perimeter. *International Journal of Social Science and Humanity*, 6(11), 852-858.  
doi:<http://dx.doi.org/10.18178/ijssh.2016.V6.761>
- Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, 26(2), 107-124.  
doi:<http://dx.doi.org/10.1057/sj.2012.1>
- Wilding, R., & Wheatley, M. (2015). Q&A. how can I secure my digital supply chain? *Technology Innovation Management Review*, 5(4), 40-43.
- Wilkin, C., & Chenhall, R. (2010). A review of IT Governance: A taxonomy to inform accounting information system. *Journal of Information System*, 24(2), 107-146.
- Williams, S. P., Hardy, C. A., & Holgate, J. A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electronic Markets*, 23(4), 341-354.  
doi:<http://dx.doi.org/10.1007/s12525-013-0137-3>
- Worrall, J. L., Els, N., Piquero, A. R., & Teneyck, M. (2014). The moderating effects of informal social control in the sanctions-compliance nexus. *American Journal of Criminal Justice : AJCJ*, 39(2), 341-357. doi:<http://dx.doi.org/10.1007/s12103-013-9211-9>
- Yin, R. (2009). Case Study Research: Design and Method (4).
- Yin, R. (2011). Applications of Case Study Research (3).
- Yin, R. (2015). Qualitative research from start to finish.

Yoon, C., Hwang, J., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, 23(4), 407-415.

## Appendixes

**Appendix A: Interview Guide**  
 Challenges with Funding of Information Security Projects per Threat Perceptions: A  
 Qualitative Case Study

**Interviewer:** Jeffery Madison

**Date:** \_\_\_\_\_

**1. Introduction**

**To Interviewee:**

*“Have you read the information I sent in e-mail? Have you signed the Form to participate in this study?”*

*“The purpose of this qualitative case study is to identify the reasons behind the insufficient funding of information security projects in the private sector. The study seeks to get real world input from professionals like yourself that are involved in the project submission, budget requesting and budget approval process”.*

*“Do you wish to ask any question regarding the study or this procedure before we proceed?”*

**2. Exploring Interviewee Perceptions on the Study Topic**

**To Interviewee:** *“The purpose of this interview is to get real world feedback on the process in which IT projects either get approved or not approved. In addition, this interview will allow the interviewee to provide unsolicited feedback on the IT project approval process.”*

**Part A (Participant Demographics)**

The purpose of collecting this information is to validate participants and ensure they qualify to participate in this study. Also to investigate potential influences of the participant profile/demographics to the interview questions and by extension to the research questions.

**A1. Interviewee Identifier:** \_\_\_\_\_

**A2. Job Title:** \_\_\_\_\_

**A3. Department:** \_\_\_\_\_

**A4. Gender:** \_\_\_\_\_

**A5. Age:** \_\_\_\_\_

**A6. Years with the organization:** \_\_\_\_\_

**A7. Years in current position:** \_\_\_\_\_

**A8. Years in the field:** \_\_\_\_\_

**A9. Highest level of education completed:** \_\_\_\_\_

**A10.** *Area of expertise:* \_\_\_\_\_

Part B: Interview Questions that refer to Challenges with Funding of Information  
Security Projects per Threat Perceptions: A  
Qualitative Case Study

The interviewer will ask the interviewee to answer the following interview questions by freely expressing their beliefs, opinions, and feelings associated with the Challenges with Funding of Information Security Projects per Threat Perceptions: A Qualitative Case Study. The interviewees will be asked to elaborate on their responses when appropriate. The interviewer will follow normal in-depth interview procedures.

**Screening question:** *Do you believe your information security projects receive sufficient funding?*

*If no, thank you for your participation.*

**Q1.** *How familiar are you with the information technology project approval process?*

Justification: The purpose of this question is to gauge the interviewee's knowledge base with the company's policies.

**Q2.** *What is your role in submitting information technology projects for approval?*

Justification: This will help the interviewer assess the knowledge base and involvement level of the interviewee.

**Q3.** *Has your organization ever suffered from a cyber-attack?*

Justification: To see if the company is approving valid projects required to keep the infrastructure secured.

**Probe:** *If yes, what was the nature of the attack?*

**Probe:** *How could have been prevented?*

**Q4.** *What percent of IT projects are approved in a timely manner?*

Justification: To gauge the interviewee's perception on the progression of IT project approval.

**Probe:** *Has the size of the investment played a role in how fast the IT project has been approved?*

**Probe:** *Do you believe the levels of funding set aside for IT projects is too low?*

**Q5.** *Do you believe your organization's information security systems can provide adequate protection?*

Justification: To gauge the assessment of organization's leadership views on information technology projects.



***Probe:*** *If not, what else do you believe is required to ensure adequate protection for the organization's information systems?*

***Q6.*** *Do you believe the levels of funding set aside for IT security projects is too low?*

Justification: To gauge if the organization is properly planning for IT project funding.

***Probe:*** *If yes, what do you believe are the reasons behind the low levels of funding?*

***Q7.*** *How does your organization's leadership understand the importance of their information technology department?*

Justification: To gauge if they lack of understanding has an impact on budget approvals.

***Q8.*** *Would you like to add any other information on the reasons behind the insufficient funding of information security projects in the private sector?*

## Appendix B. Informed Consent

### **Introduction:**

My name is Jeffery Madison. I am a doctoral student at Northcentral University. I am conducting a research study on the insufficient funding of IT projects. I am completing this research as part of my doctoral degree. I invite you to participate.

### **Activities:**

If you participate in this research, you will be asked to:

1. Answer interview questions via telephone or Skype. The interview should take less than 30 minutes.

### **Eligibility:**

You are eligible to participate in this research if you:

1. Have gone through the process for requesting IT project funding.
2. Have over 5 years of experience in IT project requesting.
3. Have over 5 years of experience in with your current organization.
4. Have a minimum of a Bachelor's degree in Computer related field or Business.
5. Work for an organization located in the US.

You are not eligible to participate in this research if you:

1. Do not work for an organization located in the US.
2. Do not have a minimum of 5 years of experience in IT project funding.
3. Do not have a formal education in either Information Technology or Business.
4. Have not gone through the process of requesting IT project funding.

I hope to include 8 people in this research.

### **Risks:**

There are no known risks in this study.

To decrease the impact of risks, you can: (examples - skip any question, and/or, stop participation at any time, etc.).

### **Benefits:**

If you decide to participate, there are no direct benefits to you.

The potential benefits to others are: better access to resources for completing IT project request.

**Confidentiality:**

The information you provide will be kept confidential to the extent allowable by law. Some steps I will take to keep your identity confidential are: I will use a number to identify you, and I will keep your name separate from your answers.

The people who will have access to your information are: myself, my dissertation chair, and my dissertation committee. The Institutional Review Board may also review my research and view your information.

I will secure your information with these steps: locking it in a filing cabinet, locking the computer file with a password, and/or, using encryption on my computer, and transporting it in a locked case.

I will keep your data for 7 years. Then, I will delete electronic data and destroy paper data.

**Contact Information:**

If you have questions for me, you can contact me at: [j.madison2420@email.ncu.edu](mailto:j.madison2420@email.ncu.edu) or 414-759-5745.

My dissertation chair's name is Dr. Nicholas Harkiolakis. He works at Northcentral University and is supervising me on the research. You can contact him at: [nharkiolakis@ncu.edu](mailto:nharkiolakis@ncu.edu).

If you have questions about your rights in the research, or if a problem has occurred, or if you are injured during your participation, please contact the Institutional Review Board at: [irb@ncu.edu](mailto:irb@ncu.edu) or 1-888-327-2877 ext 8014.

**Voluntary Participation:**

Your participation is voluntary. If you decide not to participate, or if you stop participation after you start, there will be no penalty to you. You will not lose any benefit to which you are otherwise entitled.

**Termination of Participation:**

I may stop your participation, even if you did not ask me to, if: there is any indication that the interview is causing you undue stress or frustration.

If you decide to stop participation, you may do so by: sending me an email stating that you are no longer interested in participating in the study. If so, I will not use the information I gathered from you.

**New Findings:**

Sometimes during a study we learn new information. This information may come from our research or from other researchers. If new information might relate to your willingness to participate, I will give you that information as soon as possible.

**Signature:**

A signature indicates your understanding of this consent form. You will be given a copy of the form for your information.

---

Participant Signature

Printed Name

Date

---

Researcher Signature

Printed Name

Date