Correlation between Information Security Budgets and Information Security Attacks within Higher Education

Dissertation Manuscript

Submitted to Northcentral University

School of Business

in Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy in Business Administration

by

Stephen Lyford

La Jolla, CA

October, 2019

Approval Page

Correlation between Information Security Budgets and Information Security Attacks within Higher Education

By

Stephen Lyford

Approved by the Doctoral Committee:

DocuSigned by: Garrett Smiley 458DFCD61B5A4C7...	Ph.D.	11/18/2019 | 16:40:14 MST
Dissertation Chair: Garrett Smiley	Degree Held	Date
DocuSigned by: 6A181F4E9401489D...	Ph.D.	11/18/2019 | 11:40:24 MST
Committee Member: Larry Hughes	Degree Held	Date
DocuSigned by: Leila Sopko 1F89B29081C9435...	Ph.D., MBA	11/18/2019 | 12:29:31 MST
Committee Member: Leila Sopko	Degree Held	Date

Abstract

Information security has become a vital aspect to every organization, and higher education is no exception; and the amount of an information technology (IT) security budget can play an important part of the success of IT security in an organization. With IT security attacks and breaches on the rise, the need for an effective IT security plan is crucial the success of an organization's IT department. The problem addressed in this study is that in many organizations it is found that developing and implementing an effective information security plan is challenging due to either inadequate budget funds, or unqualified staff; this creates a gap in security defense. This quantitative correlational study affects higher education institutions across the world, by indicating whether a relationship exists between the amount of an IT security budget and effectiveness of the IT security plan. Archival data were used to gather the appropriate information and then that information was analyzed to see if a relationship is present between IT security budgets and the effectiveness of an IT security plan in higher education institutions. The analysis of the data that was received from the research was used to find any correlation between the budgets and the effectiveness of an IT security plan. The findings of this study showed only one area that had a positive correlation present between the IT budget and the effectiveness of the IT security plan; this was with two-year colleges. The other two areas, four-year public schools and four-year private schools had no correlation present between the budget and the effectiveness of an IT security plan. This study helped shining the light on higher education institutions to establish effective and economical IT security plans to help benefit their organizations, students, faculty, staff, and board of directors.

Acknowledgements

I would like to thank my amazing wife, Stephanie, and my kids Owen, Elijah, and Amelia for all the support given while working through this milestone. Their patience and caring nature during the long hours and sleepless nights made the process of completing this dissertation and the all the work that led up to it that much easier; I never could have done this without any of you. I would also like to my dissertation chair, Dr. Garrett Smiley for all the great advice and direction he gave in order to complete this dissertation and make it the best possible. The rest of my dissertation committee, Dr. Larry Hughes, and Dr. Leila Spoko was also vital in making this possible, and I thank them very much for all the support and advice they gave throughout this process.

Table of Contents

Chapter 1: Introduction 8

Statement of the Problem 10
Purpose of the Study 11
Theoretical Framework 12
Nature of the Study 14
Research Questions 15
Hypotheses 16
Significance of the Study 17
Definitions of Key Terms 18
Summary 19

Chapter 2: Literature Review 21

Theoretical Framework 25
Information Technology 27
Cybersecurity 30
Cybersecurity within Industry 35
Information Security Plan. 38
Cybersecurity within Higher Education. 42
Breaches 44
Budgets 49
Industry Budgets. 51
Higher Education Budgets. 54
Information Technology Budgets. 56
Information Security Budgets. 58
Summary 61

Chapter 3: Research Method 64

Research Methodology and Design 66
Population and Sample 68
Materials/Instrumentation 72
Operational Definitions of Variables 72
Information Security Budget 72
Cyber-attacks. 73
Study Procedures 74
Data Collection and Analysis 75
Assumptions 76
Limitations 76
Delimitations 77
Ethical Assurances 78
Summary 79

Chapter 4: Findings 81

Validity and Reliability of the Data 82

Results 85
Research Question 1/Hypothesis $H1_0$ 89
Research Question 2/Hypothesis $H2_0$ 93
As stated previously, research question 2 is: 96
Research Question 3/Hypothesis $H3_0$ 97
Evaluation of the Findings 104
Research Question 1/Hypothesis $H1_0$ 104
Research Question 2/Hypothesis $H2_0$ 105
Research Question 3/Hypothesis $H3_0$ 106
Summary 108

Chapter 5: Implications, Recommendations, and Conclusions 110

Implications 113
Recommendations for Practice 116
Recommendations for Future Research 118
Conclusions 121

Appendix A: 133

List of Tables

Table 1. Chi-Square Table.... …….…….....85

Table 2. U.S. Demographic Data for Higher Education Table..... …….....86

Table 3. Correlational Two-year College Table……....90

Table 4. Correlational Public College Table .....……...94

Table 5. Correlational Private College Table 98

Table 6. Correlational Table of All Higher Education Institutions.....101

List of Figures

Figure 1. G*Power Figure ……...……....69

Figure 2. Two-year schools' scatterplot of attacks……...…….....91

Figure 3. Two-year schools' scatterplot of affected records…..…….....92

Figure 4. Public schools' scatterplot of attacks……...…….....95

Figure 5. Public schools' scatterplot of affected records…….....…….....96

Figure 6. Private schools' scatterplot of attacks…….....…….99

Figure 7. Private schools' scatterplot of affected records…….....99

Figure 8. All schools' scatterplot of attacks……...……102

Figure 9. All schools' scatterplot of affected records……..103

Figure 10. All schools' histogram of attacks……...104

Chapter 1: Introduction

Information security is becoming a highly discussed topic in most businesses and organizations worldwide, because keeping information safe has become a difficult task (Kim, 2014). Cyber-attacks within businesses have forced executives, boards of directors, and others within organizations to pay attention to information security and to ensure that a certain level of protection is made available (Imboden, 2014). These attacks range from breaches in email and credit card fraud to big data breaches that cost companies millions of dollars' worth of damages and the potential loss of customers in the process (Adler, 2015). With the advancement of hackers and hacking abilities, the need for information security policies within all organizations has become crucial to protect vital data (Gao, 2015). These security policies can include but are not limited to network monitoring, network hardware, access control lists, proper employee training, and network designs; it is the combination of all these different tools that help to build an effective information security plan, as seen in some of the standards in the Critical National Information Infrastructure (CNI) (Shamala, 2016). Information security policies now must be developed with the coordination of the chief information officers (CIO), chief financial officers (CFO), the Directors of Information Security, and many other directors and executive officers to ensure that the policies are developed correctly (Abdelwahed, 2017). Although some policies can be developed without the involvement of several executives, an information security policy is different because of the effect that it is has on the information technology (IT) budget. The tools needed and the training involved can be expensive in some circumstances (Subsermrsi, 2015). After a policy is implemented, the manner in which the plan is administered and maintained will also play an integral role in the effectiveness of the security policy; without proper employee education, training, and constant reevaluation of the ever-changing security needs, a security policy can

fail quickly (Maroria, 2013). In addition to how an information security policy is administered, the way management and senior staff support the security policy will also make a difference in its success; without the proper support and enforcement from management, the security policy will not be effective (Abdelwahled, 2017).

Without the proper money to carry out an information security policy, attacks and data loss are still going to occur; this emphasizes the importance of the budget process (Coman, 2016). One of the largest constraints to information security is the barrier of budgeted items within the information security realm, making it difficult to develop an effective information security policy (Kim, 2014). This will require, in many organizations, the setting of priorities in the information security budget or, if a security budget does not exist, the creation of an information security budget within the established information technology budget (Boon, 2015). Given that most organizations are trying to reduce and cut budgets as much as possible, finding more money for IT can be difficult; this raises the concern of whether adequate information security protection can be developed at a minimal cost (Radulescu, 2016). According to Berinato (2002), the majority of information security budgets have had a minimal increase in the budget despite an increase in the number of security attacks and the need for additional security measures. Information security comprises about five percent of the entire IT budget in some organizations; there are other organizations that set aside more budget money for information security, but five percent is normal for many businesses (Romanosky, 2016). Finding a compromise between budgeted money for information security and a proper security protection plan can be a hard task for any organization (Kayode, 2016). The budgeted amount will also vary depending on the organization type, with larger businesses having a much larger IT budget compared to small

or medium sized businesses; non-profit and educational organizations generally have a much smaller IT budget then even some small and medium sized businesses (Marchany, 2014).

Statement of the Problem

The problem is that some organizations face challenges implementing an effective information security plan due to inadequate budget funds (Marchany, 2014). Some organizations cannot develop an information security policy without the proper IT budget in place (Imboden, 2014). This can create a gap in security defense. Whether a budget is developed to assist with proactive or reactive security measures, it has been found that without proper funding, a higher risk for an attack could exist (Kayode, 2016). Information security attacks have become more consistent and aggressive which warrants a security policy or protection plan in virtually every industry (Abdelwahed, 2017). Some of the larger organizations have adequate funds to build effective information security plans, while small and medium-sized companies, colleges, universities, and other entities are not able to spend that amount of money on security (Choong, 2017). The ability to determine the correlation between an effective security defense and the amount of money spent on that defense will allow organizations with smaller information security budgets to determine if a proper security policy is possible without using funds that are hard to come by or not available (Abdelwahed, 2017). Although there is published work that addresses information security budgets, articles that deal with information security budgets and their related effectiveness are very difficult to locate (Garg, 2015). Additional research may determine whether a correlation exists between information security budgets and information security effectiveness. The ability of an organization to build an effective information security policy without expending a large amount of money could determine whether an organization can

stay in business or not; a low cost and effective information security protection plan should be a viable option in any organization (Abdelwahed, 2017).

Purpose of the Study

The purpose of this quantitative study was to determine if there is a correlation between the budget and the effectiveness of an information security plan (Marchany, 2014). This was conducted using a correlational design, exploring the relationship between an information security plan and an information security budget. The ability for an organization to apply an effective and cost-saving information security policy can end up saving organizations in the long run; and for smaller organizations this can make or break their business (Adler, 2015). To conduct this study, data was gathered from public information showing the amount of money spent on information technology and which higher education entities have been attacked and/or breached in the past. The public information was gathered from public websites and databases such as www.air.org, itdashboard.gov, usaspending.gov, informationisbeautiful.net, www.statescoop.com, and www.dhs.gov, in order to collect archival information for analysis. Using the data gathered from this public information, statistical analysis was conducted using G*Power in order to try a find a correlation between the budget amount of information security and the actual protection provided. The specific information within the G*Power application used an effect size of 0.5, an Alpha value of 0.05, a Power value of 0.95 and used three groups. These groups represented the different types of higher education institutions studied: two-year or community colleges, four-year public schools, and private higher education institutions. Using this application, a sample size of 66

was found, giving a sample size of 22 per group to determine if a correlation exists between budgets and IT security effectiveness.

Theoretical Framework

The theoretical framework is known as the *blueprint* for a dissertation and a study in general (Grant, 2014). Given the nature of IT security attacks, the importance of the information security plan is becoming more vital; this requires an effective and efficient plan to be designed and put into place (Lee, 2014). One of the guiding theoretical frameworks used in this study was the theory of resourced-based view (RBV), which establishes that different information security investments are used to obtain security assets to protect investments (Weishaupl, 2015). This theory explores the use of tangible and intangible resources such as firewalls, security knowledge, and other areas used to protect and cover IT information (Weishaupl, 2015). This theory helps to guide the study given that the different types of investments covered in the RBV theory show the effects that additional resources can make in combating IT security attacks on different types of organizations (Weishaupl, 2015). The development of the information security plan is usually hindered in many arenas through the IT budget or the IT security budget; lower budgets do not allow for proper development and implementation of a security plan, allowing for more attacks to occur (Garg, 2015). The importance of properly investing in security resources can affect the protection against and prevention of attacks, which helped to guide the direction of this study, showing that proper investments must be made to protect an organization (Nagurney, 2017). The area of emphasis for this study was higher education as IT budgets within higher education can be lower and the number of IT staff tend to be smaller; this does not eliminate the fact that an effective IT security plan is needed (Subsermsri, 2015). The theory based on this information is that a relationship is present between the amount of money spent on an IT security plan through the

budget and the effectiveness of that plan (Weishaupl, 2015). The amount of money spent on the development and implementation of an information security plan and therefore the assets that are acquired through security investments, could include employing additional employees, purchasing new software, and purchasing additional hardware if needed; all of these could have an impact on the effectiveness of a security plan and how attacks are handled (Zavada, 2014). While other researchers have investigated similar theories in non-profit and corporate areas, like the study conducted at West Chester University, a theory testing the relationship at the higher education level has not been conducted thoroughly (Imboden, 2014). The idea of an effective IT security plan can be ambiguous and hard to determine, but this was examined and established by determining the number of attacks that occurred within an institution within a set amount of time (i.e. three months, six months, one year) and finding the threshold of what was deemed an effective security plan (Li, 2015). Budgets used for the IT security plan were deemed as IT security specifically and not general IT budget monies, therefore giving a more accurate account for the money spent through the budget to establish the IT security plan (Marchany, 2014). Several schools of thought exist on this topic, which range from everything from the correct allocation of funds within the budget to the fact that budgets make no difference in the IT security effectiveness (Boon, 2015). Other schools of thought believe a proper security protection plan is only possible if the proper IT security budget is in place in addition to a general IT budget (Filkins, 2016). One researcher found that a limited budget can decrease the effectiveness of an IT security plan, making it harder for an organization to defend itself form attackers (Romanosky, 2016). Still, existing literature and current articles lack the topic of how the IT budget of a higher education institution affects the success of the IT security plan (Marchany, 2014). This study related to other current articles and literature by tying in the existing studies of effects of budgets and IT

security within other industries and provided information for the effects within the higher education realm.

Nature of the Study

This study consisted of a correlational quantitative study based on the statistical data that was collected and analyzed to understand whether a correlation exists between information security budgets and information security effectiveness (Grant, 2014). Within the quantitative method of research there are different approaches that can be applicable; this study consisted of a ratio or interval type of research method, although there was a possibility of a mixed method research study being done (Jogulu, 2011). The reason this study used the ratio or interval type of research method was because the data was collected through publicly released information to analyze and categorize the data into proper areas to correlate with the study's objectives (Filkins, 2016). The use of proper research methods was very important as it properly analyzed the data collected and determined if the research questions and the hypothesis were valid or not (Friberg, 2013). The mixed method process is one in which more than one research method is used in order to properly collect and analyze the type of data that is gathered for the study (Jogulu, 2011). In addition to the methodology used to process the data in this study, the data had to be properly prepared, meaning that it had to be assessed to ensure the data was corrected and that all the data used in the study was valid in order to ensure legitimate results (Ifenedo, 2014). Data within the information technology field can be easily skewed or reported incorrectly; therefore, a proper process must be established to ensure that proper data is collected and used for the study (Yuksel, 2014). Using inaccurate or improper data can skew the results of the study and can even give the wrong results, making the entire research study inaccurate, null and void; this requires that all data in a study is checked for validity to ensure the most accurate study is completed (Ifenedo,

2014). After ensuring the validity of the data presented in this study, the data was then analyzed and presented in a manner which the reader was able to understand, thus helping to prove the research questions and hypothesis throughout the study (Filkins, 2016).

Research Questions

Research questions help to narrow the purpose or goal of a study into specific questions so the researcher can then address the questions within the study; in this study these questions addressed information security policies (Ellis, 2008). Defining an effective information security policy can be difficult, but by examining the number of successful attacks that have occurred within one year, the effectiveness can be determined. The ability to determine if there is a correlation between the amount of money spent on an information security and the effectiveness of the protection provided will help schools, colleges, non-profits, and other private institutions know that information security protection is possible. Any effective information security policy will be difficult to block 90-100% of attacks just because of the nature of security attacks, but an effective policy will be able to thwart majority of the attempts to steal data and information from an organization (Das, 2013).

Research Question 1. To what extent, if any, is there a relationship in two-year or community college higher education entities between information security funding and information security effectiveness?

Research Question 2. To what extent, if any, is there a relationship in four-year public college higher education entities between information security funding and information security effectiveness?

Research Question 3. To what extent, if any, is there a relationship in private college higher education entities between information security funding and information security effectiveness?

Hypotheses

Given that this study was quantitative, there was a null hypothesis and an alternative hypothesis.

$H1_0$. A positive correlation does exist when comparing the amount of money spent on information security protection within a two-year or community college organization and the number of successful attacks and/or breaches that organization has experienced.

$H1_a$. A significant correlation does not exist when comparing the amount of money spent on information security protection within a two-year or community college organization and the number of successful attacks and/or breaches that organization has experienced.

$H2_0$. A positive correlation does exist when comparing the amount of money spent on information security protection within a four-year public college organization and the number of successful attacks and/or breaches that organization has experienced.

$H2_a$. A significant correlation does not exist when comparing the amount of money spent on information security protection within a four-year public college organization and the number of successful attacks and/or breaches that organization has experienced.

$H3_0$. A positive correlation does exist when comparing the amount of money spent on information security protection within a private college organization and the number of successful attacks and/or breaches that organization has experienced.

$H3_a$. A significant correlation does not exist when comparing the amount of money spent on information security protection within a private college organization and the number of successful attacks and/or breaches that organization has experienced.

Significance of the Study

The significance of this study may be obtained from different perspectives such as education and businesses. Higher education institutions may benefit because information security is becoming vital to virtually every industry. Certain organizations lack employees with the expertise needed to make security decisions; therefore, they rely on studies like this to make educated decisions (Shahpasand, 2015). The aim of this particular study is to understand how the higher education field is affected by lower IT budgets; oftentimes, inexperienced employees lead to IT implementations. The study explores how budgets can affect the efficiency of information security in higher education (Garg, 2015). This study may reveal to higher education that with, skilled employees and proper training a suitable infrastructure and security plan can be implemented in the IT department (Garg, 2015). Expelling the notion and the mantra that higher education and academics in general have poor IT security could also begin to be alleviated through this study, in finding that a low-budget IT security plan can be possible (Choong, 2017). Indicating whether there is a relationship between an IT security budget and an effective IT security plan can also significantly prepare higher education administrators and legislators for whether or not an effective IT security budget is possible within the budget available to higher education institutions (Marchany,

2014). While exploring if a relationship exists between the IT security budget and the effectiveness of the IT security plan, a set of IT security standards is likely to be established to help all higher education institutions in developing and implementing their IT security plans in the future (Abdelwahed, 2017).

Definitions of Key Terms

The key terms in this study surround the topic of information security budgets and how they affect IT security attacks within higher education. Information security policies have become a necessity in almost every realm of business; and these policies have required the allocation of budget money and the cooperation of several different aspects of an organization (Subsermrsi, 2015). By understanding the terminology of these aspects of information technology better, a more general understanding of this study and this topic can be accomplished.

Budget. An estimate of income and expenditure for a set period of time or the amount of money needed for a specific purpose (Nagurney, 2017).

Cyber-attacks. An attempt by hackers to focus an attack or destroy a computer network or system (Gao, 2015).

Higher Education. Education beyond high school, especially at a college or university (Marchany, 2014).

Information Security. A set of processes, procedures, personnel and technology charged with protecting an organization's information assets (Shamala, 2015).

Information Security Policy. A set of rules governing an Information System that provides an established level of protection (Abdelwahed, 2017).

Summary

The number of cyber-attacks continues to increase along with the costs, which causes organizations, businesses, and higher education institutions to lose money and valuable information (Romanosky, 2016). The problem found is that a lack of funding in IT budgets may limit the effectiveness of an information security plan thus making the organization susceptible to cyber-attacks (Abdelwahled, 2017). The purpose of this study was to understand the relationship between the IT budget and the corresponding effectiveness of the IT security plan within higher education institutions. This study was conducted through comparing existing literature and current articles surrounding IT budgets and IT security effectiveness and gathering information from other publicly released information regarding higher education institutions. The nature of how this information was gathered was through publicly released websites and databases about higher education institutions showing budgetary costs, the number of attacks the entity had encountered over the past year, and some common best practices in order to determine how an effective security plan could be established.

Using the hypotheses and research questions will help higher education institutions to determine how IT security plans can be developed. Through research, the learner can determine whether a relationship exists between the amount spent in an IT budget and the effectiveness of the IT security plan; higher education institutions can determine the best practices to develop and maintain an efficient IT security plan. An effective security plan can enable organizations to fight off cyber-attacks, helping to protect valuable information and saving organizations millions of dollars annually (Imboden, 2014). Throughout the next

chapter the effects and importance of an effective information security policy are discussed to gain a better perspective on the topic.

This chapter has introduced the topic of this study which deals with the current state of information security attacks and the security policies that are now needed in virtually every aspect of industry. Within this topic a purpose was given to this paper to determine if a correlation between an information security budget and the effectiveness of an information security plan exists (Marchany, 2014). This correlational quantitative study used a resourced-based view theory, which indicates that different security investments are used to obtain different assets to protect an organization's investments (Weishaupl, 2015). The study was conducted by using a ratio or interval type of research methodology, gathered through publicly released information through public databases or public websites (Filkins, 2016). The results of the study are important because they reveal the impact that a budget amount can have on the effectiveness of an information security plan, specifically in the higher education field (Garg, 2015). Through different themes such as information security budgets, information security policies, cyber-attacks, breaches, and attacks, a need for this study should be made apparent. The literature review presented in the next chapter highlights articles related to the research topic.

Chapter 2: Literature Review

This quantitative study has the purpose of exploring information security budgets and determining if there is any correlation between budgets and information security effectiveness; this is done in the area of higher education where budgets can be more limited (Marchany, 2014). According to Peralta (2017), a literature review is "a systematic, explicit, and reproducible method of identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers" (p.630). The following literature review consists of examining budgets in the rest of industry and then also in higher education to find the difference between these two areas; although all budgets have similarities, there can be differences. The budget information covered risk management among other things because, when developing information security budgets, risk management is crucial, asking one of the most important questions; how much is enough, in order to determine the effectiveness of an information security budget (Radulescu, 2016). The importance of a separate information security budget was also emphasized in this chapter, showing the advantages that such a budget can have for an organization; which many times includes some type of employee awareness and training in order to ensure proper information security is understood throughout the whole organization. An information security budget can save money for an organization, their system, and their brand in the long run because of the impact and the negative associations with cybersecurity attacks when they occur (Adler, 2015). The examination of budgets is followed by reviewing the literature within information technology, focusing on information security plans since they, as well as cyberwarfare and cyber-terrorism, have become so prominent in all aspects of the world today.

Information security has become a vital strategic goal for every responsible and safety-conscious organization that wants to follow current technology trends and keep their

organization secure (Prislan, 2016). It is also crucial to acknowledge a paradigm shift in the field of information security: while this field used to be reserved for experts and individual professionals, it has now moved to integrating people from other areas of an organization, requiring virtually all employees and management to become involved in ensuring that information stays secure and protected (Syuntyurenko, 2015). This has resulted in almost every organization employing some type of information security plan in order to protect their assets and their customers. Ahmad (2014) found that over 60% of organizations were employing some type of information security countermeasures, including but not limited to anti-virus software, firewalls, anti-spyware, virtual private networks (VPNs), patch management, encryption of data, and intrusion detection. As shown in several articles now, this type of deployment of information security plans requires every new employee to come into an organization with an understanding of what information security is and how to properly practice it, which is something that is found in most educational programs in today's higher education system (Kim, 2014). The need for information security is also examined in this chapter, hence the reason for a separate information security budget in many cases. Prislan (2016) stated that the major barrier to proper information security management is the lack of financial means for an effective information infrastructure. The importance of an information security plan or policy is also discussed in this chapter of literature review, exploring what makes an information security plan effective in an organization. An information security policy helps to provide an organization with a set of expectations that the organization must keep regarding information security and consequences for when these expectations are not met within the organization (Imboden, 2014).

An area that is lacking in recent articles is the focus of a higher education institution's budget and how it corresponds to information security; in order to fill this gap, this is the

primary focus of this study. The focus of a higher education institution's budget and how it corresponds to information security is an area lacking in recent articles. The primary focus of this study is an attempt to fill this gap. This is one area to consider when dealing with information security; another area in regards to information security studies deals with the data that is returned in the studies. Studies conducted regarding information security are generally limited in their results because of low responses gathered through questionnaires; this is often due to security issues that would be revealed within organizations (Sung, 2014). When considering this study of information security plans and the budgets that accompany them, other aspects need to be observed; an important fact to understand when dealing with information security and budgets is that no matter how much money is designated in a budget, no organization is ever 100% protected from cyber-attacks or information security breaches as found in several articles throughout this literature review (Nagurney, 2017). This type of information shows the unpredictability of information security and the difficulty of ensuring a secure network even given a large amount of resources. This study was conducted to see if the amount of money spent does correlate to the amount of protection that is available for a system. Before reviewing what different articles and literature were present for budgets and information security, the theoretical framework for this study was explored to gain a better understanding of the study.

In order to complete this literature review, several different search engines, databases, and search terms had to be used; while some were used more heavily than others, all were equally important in finding the articles needed to conduct this study. Some of the databases that were used more heavily than others included ProQuest Central, ProQuest Computing, Google Scholar, and SAGE journals. In addition to these databases, some articles were also found using databases like Academic Search Complete, IEEE Xplore Digital Library,

EBSCOhost, and SAGE Knowledge. All of these databases included a large number of articles that were both peer-reviewed and up to date which was needed in order to conduct a study of this caliber. Search engines and databases can only get someone so far in a study like this; the keywords used to conduct the searches have a tremendous amount of power in finding the relevant articles needed.

When exploring the subject of information technology, the following terms were used: information technology, IT, industry IT, industry information technology, higher education information technology, and higher education IT. When exploring the subject of information security, the following keywords were used: information security, cybersecurity, IT security, industry security, and higher education IT security. The additional subject of information security plans used keywords such as information security plan, IT security plan, IS plan, and information security policy. Then while examining security attacks and breaches, several different keywords had to be used, including: cyber-attack, cyber-terrorism, cyber-warfare, security breach, IT breach, IT security breach, IT security attack, and IT attack. All of these keywords helped with the first part of the literature review, examining information technology, IT security, and attacks; but there was still the matter of budgets, for which several different terms were used. The different keywords used to find the articles on budgets included budget, IT budget, information security budget, IT security budget, higher education budget, college budget, university budget, industry budget, business budget, information technology budget, information security plan budget, and information security policy budget. Together these keywords were used in different combinations to arrive at the articles that were used to conduct this literature review and, while some combinations could have helped to produce better results, the amount of literature found on this topic was found to be abundant.

Theoretical Framework

The theoretical framework is known as the *blueprint* for a dissertation and a study in general (Grant, 2014). One of the guiding theoretical frameworks used in this study is the theory of resource-based view (RBV), which establishes that different information security investments are used to obtain security assets to protect investments (Weishaupl, 2015). The resource-based view originated as a management strategy in business literature and has been used in the information technology area since early 2000 (Baharadwaj, 2000). Although this framework has been used in information technology since early 2000 as well, the application of this theory was not applied to information security until late 2005-2007 when it was used to measure the capability of IT services that can be applied to a business system, similar to the function the theory is being used for in this study (Tang, 2007). This theory helped to guide this study given that the different types of investments covered in the RBV theory show the effects that additional resources can make on combating IT security breaches and attacks on different types of organizations (Weishaupl, 2015). Even though this theory has been used across many different venues, other studies have been conducted in which the RBV theory is used for information security and the measure of how different tools acquired to help with information security can help benefit the security of a system (Diamantopoulou, 2017). Studies in this area include examining how secure a system can get depending on the what resources are available, looking at both hardware and software resources as well as processes that are put into place as a resource to help make a system work better and become more secure and stable; this demonstrates the nature in which this theory was used in this study as well (Diamantopoulou, 2017). The RBV theory is not only used with information security but also in the field of information technology as well, measuring the overall performance of an

IT system based on the resources that have been put into place in a given company or firm (Baharadwaj, 2000).

Different studies regarding information technology and information security demonstrate the relevance of this study, showing that the way in which information security plans are established and developed as well as what tools are put into place will affect the overall security of a system (Sindhuja, 2014). The development of the information security plan is usually hindered in many areas through the IT budget or the IT security budget; lower budgets do not allow for proper development and implementation of a security plan, allowing for more attacks to occur (Garg, 2015). This requires not only that proper processes are put into place in developing an information security plan, but also that the components of an information security plan be put into action in the correct sequence to ensure it is the most secure option possible for an organization (Hryszkiewicz, 2015). The area of emphasis for this study was higher education as IT budgets within higher education can be lower and the number of IT staff tend to be smaller; this does not eliminate the fact that an effective IT security plan is needed (Subsermsri, 2015). The theory based on this information is that there is a relationship between the amount of money spent on an IT security plan through the budget and the effectiveness of that plan (Weishaupl, 2015). Since different size businesses and institutions have different size budgets to utilize for information security, the goal of this study was to discover if there is a way in which a lower budget can establish a secure and effective information security plan (Zavada, 2014). Research has shown that an effective information security plan is possible; however, these articles do not indicate the amount of budget money that was used to achieve this goal (Ahmad, 2014). The idea of an effective IT security plan can be ambiguous and hard to determine, but this was examined and established by determining the number of attacks that can occur within an institution within a set amount

of time (i.e. three months, six months, one year) and finding the threshold of what is deemed an effective security plan (Li, 2015). Recent articles have shown significant findings in relation to information security budgets or information technology budgets, but they do not correlate the relationship between the amount of the budget and the overall effectiveness of the information security plan (Marchany, 2014). In a similar method, research is lacking in dealing with higher education information security and the budget amounts within higher education (Kim, 2014).

Information Technology

Information technology has changed over the years, as it has developed from being an administrative tool helping optimize office processes; to now being a strategic instrument in any given forum, business, industry, higher education, and non-profit organization (Georgescu, 2105). Given the fact that IT is entangled in every facet of an organization, information security has become a problem for not only businesses but also other non-business organizations, nations, and individuals (Mubarak, 2016). Information technology is quickly being seen as the key to warfare; in recent times, studies show this is mostly related to cyberwarfare (Raha, 2015). Cyberwarfare has been referred to as the new dimension in national conflicts, where cyber terrorists could cripple a nation and bring it to its knees without the use of a single weapon or violence of any kind (Raha, 2015). Because of these new capabilities of information technology, many authors are recommending that for the sake of the country certain critical infrastructures have either a fully-manual option or a locked-out network solution to keep them safe from possible cyberwarfare (Rege, 2014). These new cyber-capabilities are now much harder to gather information about and to divulge information from; therefore, they have been creating uncertainty and mistrust throughout almost every facet of society (Cavelty, 2014). When considering modern terrorism, cyber-

terrorism is a wise choice given the anonymity and the potential for massive damage. Studies show that the growing dependence on information technology has given terrorists the opportunity to exploit different vulnerabilities to approach targets such as national defense systems and other defense systems (Yayla, 2014). By definition, cyber-terrorism involves an attack that results in violence against persons or property or, at the very least, causes harm or creates fear (Georgescu, 2015). All these different threats have culminated in one of the newest types of crime growing in popularity: cybercrime (Kayode, 2016).

Cybercrime is when a criminal activity, anything illegal, is carried out using an information technology infrastructure; this can include but is not limited to illegal access, illegal interception, data interference, system interference, misuse of devices, forgery, fraud, and many others (Kayode, 2016). With the advances in information technology cyber terrorists have taken new information technology and used it to carry out attacks on different organizations, people, and nations, most often without being detected (Yayla, 2014). Although literature indicates that cyber-criminals have utilized the advances of information technology to add to their toolkit, their goals are more personal or self-motivated, meaning that they haven't brought the internet crashing down even given these advances in information technology (Kenney, 2015). Cybercrimes have now reached a worldwide cost of over $110 billion and these crimes have affected 566 million victims annually, averaging out to around 1.5 million victims a day throughout the world (Maheux, 2014). Although literature reviewed for this study showed the criminal side of cyberspace, it is evident in other studies how information technology can be used in other ways, negatively and positively; examples can include cyberbullying, shared research and discoveries, and many other possibilities (Zezulka, 2016). These additional information security threats continue to grow and include different areas of cyberspace; such as hacking, cracking, cyber-terrorism, cyber-grooming,

cyber-pornography, cyber-stalking, phishing, piracy, malware attacks and many more in today's rich cyber world (Kayode, 2016). Given the nature of recent cybercrimes, all IT departments need to be prepared in case of an attack or any other type of event that could occur and result in damage to IT infrastructure or loss of data (El-Temtamy, 2016).

A large amount of literature exists on the topic of information technology, including topics such as best-practice standards, guidelines, technical whitepapers, and the implementation of security controls (Ahmad, 2014). In today's society, information technology helps organizations achieve their goals and has become critical to an organization's success (Hosban, 2015). But the definition of information technology has changed over the years; studies have shown that with information technology becoming so integral in businesses the focus has shifted from the physical computing system to the more important assets of data and information (Mushtaque, 2015). This everchanging definition and use of information technology is great for IT professionals, but as seen in several articles, with the subject of information security now at the forefront of all organizations throughout the world, these skills and this subject matter must be passed on to all employees and individuals. This can be very difficult at times since not all people are ready or willing to keep up with the ever-changing subject of information technology (Wong, 2015). Over the last couple of decades research has shown that IT departments should be prepared with a well-established and tested disaster recovery plan in case something should occur; in relation to disaster recovery the only thing that has changed over time is that cyber-attacks are now one of the things that could cause a disaster in certain circumstances (El-Temtamy, 2016). These concepts are crucial to understand the remainder of this study; and now this section will explore cybersecurity, including cybersecurity in higher education, cybersecurity in industry

and information security plans. That section is then followed by exploring breaches and attacks in order to gain a better understanding of the different threats in cybersecurity.

Cybersecurity

Information security continues to be a popular topic of discussion at business functions and in research reports because of the number of attacks in recent years (Prislan, 2016). This is slightly due to the implementation and use of information technology throughout industry, as seen in many articles (Sindhuja, 2014). The increase of an organization's dependence on information technology has resulted in a proportional increase in the impact felt when an organization's information security is compromised (Sindhuja, 2014). This is also due to the risks involved; information security has attracted the attention of companies, and organizations of all sizes because of the large number of changes in the type and structure of information technology that can cause risks (Shamala, 2015). These risks are what drive information security within an organization; and while information security is often referred to as protecting the organization and the data of the company, customers are also protected using proper information security so that breaches don't cost customers additional information and monetary loss (Choong, 2017). Given this information, literature shows that spending on information security has increased significantly over the last several years with some companies spending as much on information technology as they do on offices, warehouses, and factories, thus making the need for effective IT governance programs paramount (Hoban, 2015). Filkins (2016) revealed that because of government initiatives and increased legislation, worldwide spending on information security had reached $75.4 billion in 2015. This includes government involvement as well; with the recent cybersecurity attacks, some countries are issuing regulations to organizations in order to ensure that a certain level of information security is taking place (Sadovnikova, 2015). In addition to these regulations,

federal efforts to promote the sharing of cyber threat information between private sectors and government entities have increased in order to form a better defense against attacks and cyber terrorists (Zheng, 2015).

Because cyber threats have become a widespread global problem, many believe that every country and every organization should have a shared interest and motivation to work together to develop a more comprehensive information security defense (Miron, 2014). Okuku (2015) discussed how the Kenyan government took this idea of aiding in information security and developed and published their information security plan; making them the only African nation to have a published information security policy. In addition, in South Africa they are also deploying an information security awareness program; within this program, topics such as online activities, cybercrime, social networks, password and hardware security, malware, cyberbullying, cyber-identity management, and others are all covered (Okuku, 2015). For the rest of us in order to fully understand and protect again information security attacks, organizations will have to take more than just the government's recommendations into consideration; literature shows that many different aspects have to be considered when working with information security (Mubarak, 2016).

Proper cybersecurity or information security is needed to enhance the confidentiality, integrity, and availability of data and to maintain the original design and efficiency of the network system (Mubarak, 2016). The problem found in many articles is that much of the current research focuses on the technical side of information security and doesn't consider some of the other aspects that help to make information security plans successful (Sung, 2014). Many functions of information security protect against viruses; which is done by focusing on the discovery of technical perspectives like certain methods, algorithms, and protocols within information technology (Sung, 2014). While this focus on cybersecurity is

very important, very few researchers focus on some of the other aspects that are needed within a sound information security plan (Mubarak, 2016).

In order to address the high number of information security attacks, organizations have to adopt a new view on information security; while it can be difficult for management and employees to change their perspective, adopting this new view is necessary in order to successfully fight off cyber-attacks (Taylor, 2014). Organizations have become well aware that all the different aspects dealing with security, like physical and social engineering, are just as critical to the mission of the organization as the technical aspects of security (Shamala, 2015). Implementing a successful information security approach within an organization includes technical systems as well as non-technical systems; for instance, the costs of proper information security will have to include proper training for employees to ensure their success with the plan (Alavi, 2016). Training for employees can be a crucial part in the development and implementation of an effective information security plan; while many authors have written articles on training employees, very few have incorporated this concept into studies on information security plans (Alavi, 2016).

In addition to concerns about the different types of security systems, organizations also face the problem of dealing with mobile devices in today's society (Das, 2016). While smartphones and mobile devices have gained in popularity, they have shown to be a terrible security risk, as they are still seen as a social device and can therefore spread malware and viruses, worms, and trojans onto personal and professional networks; proper security must be developed both on the personal level and the professional level (Das, 2016). Though this process is needed in order to have information security, many organizations today struggle with how to adopt and secure mobile devices; these devices can prove to be a great asset to the organization because they can make the employee more productive, but the organization

must also remember that the owner of the mobile device also has the right to have their own personal data present on the device; this can be a tough area for organizations to handle (Markelj, 2016). Numerous studies have been conducted about proper information security plans that include policies for use of mobile devices (Markejl, 2016). The real challenge for most organizations is ensuring that personal data and professional data on the device can be secure yet remain separate. (Markejl, 2016). One of the common problems in dealing with mobile devices is that users have a tendency to believe that they are not in danger or that information security problems exist only on personal computers or servers and not on mobile devices; this mentality leaves users exposed to attacks on mobile devices constantly (Markelj, 2016). Another security risk that mobile devices bring into organizations is that they connect to multiple types of wireless systems as their owner travels around, whether it is home WiFi or free café WiFi or the local McDonalds' free WiFi; whatever the case may be, by connecting to these different wireless internet networks, the mobile device has a better likelihood of being attacked and then the data on the device can be exposed, including work data (Harris, 2014). Das (2016) revealed that the majority of smartphone and mobile device users are heavily influenced by the level of trust they have in determining their level of information security; this leads to giving more access and sharing more information than needed causing security issues.

Although smartphones and mobile devices are developing into a serious security risk within an organization, the root of most of the information security issues is the risk of a network breach. Given that almost all information is transported across a network at some point the risk that the information can be comprised always exists (Sembiring, 2015). The need to prevent security breaches should lead to a greater focus on employee security training, revealed that employees who have violated the organization's information security policy

were responsible for more than half of all information security breaches (Sommestad, 2015). Because of violations like these and because of further threat to security, some organizations have begun monitoring their employees for various reasons; these employees may be monitored for ethical reasons, or to ensure they are working, and to help ensure the organization's information security (Michelberger, 2016). This process can be accomplished in several different ways, such as through keyboard loggers or software that runs on the computer, but the most common is the use of different types of descriptive logs. These logs contain more than just the user's log- in information; there is detailed information that has been documented so that any act that causes an information security breach can then be tracked and prevented in the future (Michelberger, 2016). Certain studies have also found that when employees lack resources, like time, budgets, equipment, software, information, and authority then the risk of unethical behavior increases; this could also account for employees not abiding by a given information security plan (Kaptein, 2015). This demonstrates the importance of incorporating a sound technical and ethical training program into an information security policy and explains also the importance of a security plan in general (Kaptein, 2015). The literature shows that while developing the right information security plan can be difficult, it is not impossible. (Kaptein, 2015). Certain studies have shown that students currently coming out of information technology or information security education programs are ethically aware but are looser on their ethical standards and more willing to allow certain unethical things to occur; this has even been seen to carry over to the personal side of individual computer use (Manly, 2015). Certain other studies have shown that in 1998 over 23% of business workers acknowledged entering into unethical behavior, and that about 40% admitted to having pirated software on their personal computer; this reinforces the importance of including ethical training and reinforcement in the workplace (Tahat, 2014).

Proper information security training or awareness can help to prevent some of these unethical acts, and a proper information security plan can even help to deter and catch any employees that are trying to carry out these acts from within the organization; for these reasons alone, the establishment of a proper information security awareness program is very helpful for an organization (Kim, 2014). Information security can be difficult in that there must be a balance maintained between establishing an effective information security plan and allowing for productive employees; finding the proper security tools and controls without affecting the ability of the employee to do their job can be the hardest part of information security; many times, strict controls can lead to loss of employee effectiveness and then refusal to abide by an information security plan developed (Chen, 2016). While other research exists in this area of cybersecurity and information security, this chapter will continue looking at the literature review while focusing in more confined areas related to this study, looking at cybersecurity within industry, information security plans, and cybersecurity within higher education.

Cybersecurity within Industry. Information security has become a priority in virtually every aspect of industry, including the financial realm, business, real estate, and even non-profit organizations (Ifinedo, 2014). Despite the belief that information technology and information security are the same thing, literature shows there is a difference between these two terms. Information security goes far beyond information technology in today's industry; it is present in every manifestation of the organization and helps to determine an organization's success in many cases (Kwecka, 2016). Literature in relation to cybersecurity within industry varies in many different areas, one being who is in control of developing a proper information security plan and developing an information security budget (Weishaupl, 2015). The Chief Information Security Officer (CISO) has the responsibility of allocating the information technology/information security budget and also justifying it to the Chief

Financial Officer (CFO) (Weishaupl, 2015). Whether a plan is developed by the CFO or a team of other individuals, the importance is the development of an effective information security plan within industry (Kim, 2014). As found in certain studies, one of the aspects that makes dealing with information security so difficult is taking into consideration that the investment of an organization in information security is only part of the equation for fighting information security issues; the investment that a hacker takes also comes into play in determining the overall effectiveness of information security (Gao, 2015). A more common approach in attempting to combat information security issues is to gain a better understanding of hacker behavior and thinking from a hacker's perspective; this can help professionals combat hackers to a better degree (Gao, 2015).

Another aspect of dealing with information security risks is having the proper staff, with the proper knowledge to deal with the problems that arise; this includes ensuring that during the hiring process the candidates applying have the necessary skill sets to handle the security of the organizations (Shamala, 2015). Maintaining the proper staff for an organization can be difficult at times, but if the organization allows for internal and external training, the staff that is currently employed can evolve into very productive information security professionals (Shamala, 2015). Organizations today must implement multiple information security strategies in order to ensure the effectiveness of security measures and to maintain security policies within the organization (Ahmad, 2014). Literature shows that in order to overcome the issues of poor information security within an organization, the organization is in need of the development of strong information security policy templates that an organization can easily adopt (Imboden, 2014). Different articles have shown that certain governing bodies such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have put standards into place to aid

organizations in the development of proper information security plans; with over 20 different published standards being in place and more on the way, this does help businesses and organizations in the proper development of an effective information security plan (Brand, 2015). This is beneficial given that different subjects need to be added to information security plans today; studies have shown that in virtually every aspect of PC-centric computing the information security behaviors and practices have been adapted over to the smartphone, showing the importance of adding smart devices to an information security plan (Das, 2016).

Literature has shown that mobile devices must be included in any type of information security throughout an organization in order to adequately protect data that is shared through different platforms (Markelj, 2016). As discussed in the previous section, one of the factors that has to be faced when working with information security is dealing with users and employees to ensure the plan is developed correctly (Alayi, 2016). One of the best uses of an information security budget; is the development and execution of a comprehensive information security awareness program among the users throughout the organization (Kim, 2014). Information security awareness can be defined as an employee's knowledge of information security and the company's information security awareness program (Shamala, 2015). One of the critical issues to face in information security is controlling access to systems, given that most breaches occur by human interaction with a system (Dreyfuss, 2016). Another challenge noted throughout the literature is having the development of an information security plan meet the needs of the users as well as the organization (Michelberger, 2016). One study found that usually only two components affected the largest number of information security policy violations: one being the human element and their awareness of the policy and the second being the policy itself and the clarity with which the policy is explained in the work environment (Al-Mukahal, 2015). This explains why information security policies are

often found by users within an organization to be ambiguous, hard to comply with, and hard to fit with other business policies and processes (Michelberger, 2016). Other studies have found that the type of employee and where he or she is working will also play into the security risk they may present; anxious employees are more likely to violate security policy rather than an employee that is more comfortable with their work environment and their duties (Al-Mukahal, 2015). Despite that many organizations have developed and put into effect information security plans; and given the different types of security incidents have plagued organizations in the past, proper information security is often found to be confusing and complicated, making the process difficult (Shahpasand, 2015). Given the importance of the information security plan, whether it is in industry, higher education, or a non-profit organization, it is crucial to evaluate the literature in that area as well.

Information Security Plan. As previously mentioned, the role of an information security plan is to handle the prevention of security breaches; to address the risk of information security breaches, an organization must implement an information security strategy that includes the development, institutionalization, assessment, and improvement of an information security plan (Ahmad, 2014). An information security plan or policy could also be defined as the "art of deciding how to best utilize what appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defend organizations' information infrastructure against internal and external threats by offering confidentiality, integrity and availability at the expense of least efforts and costs while to be effective" (Ahmad, 2014, p. 358). Several articles, show that information security plans are mostly driven by technology that is available rather than by strategic business objectives, making the plan more effective in protecting data and information (Ahmad, 2014). Many articles express different ways to ensure a successful

information security plan, an effective information security plan that ensures the security of information systems through IT rules, and procedures to enable the correct use of IT resources throughout the entire company (Hryszkiewicz, 2015). Other authors believe that the implementation of a proper information security plan requires a combination of security policies and procedures, a conscious and educated staff, and financial and technical resources that are designed to support the IT team in their efforts (Abdelwahed, 2017).

When exploring organizations of different sizes, one study found four common similarities in a working information security plan; they included having an information security champion (someone to own the information security plan), creating a simple policy that employees can understand, training and talking with employees to ensure they understand the plan, and developing and deploying organization-specific material to put out around the company to remind employees about the program and keep it on their minds (Imboden, 2014). Taylor (2014) found that in the information security plan developed for Texas Southern University they included a technical aspect of the plan and a behavioral aspect of the plan; this allowed for the technical aspect to protect against all the technical areas and the behavioral approaches to help with the social engineering and threats of that nature. While studies show that there are many different components that need to be included in an effective information security plan, it has been found that there is no widespread agreement on exactly what is needed in an information security plan and how to classify different information security plans (Ahmad, 2014). Imboden (2014) found that 30% of organizations develop their information security plans using a template that was found online and that 44% used more than one source to develop their information security plan. Other articles mention that a proper information security plan takes the cooperation and coordination of people, processes, and technology and involve different considerations; such as technical, formal and informal

controls, and information systems (Sindhuja, 2014). In addition, some studies have found that a proper information security plan requires both a technical side that deals with the tools and proper technical protection of data and devices as well as a human side that ensures that all those involved and affected by the information security plan are ready for the plan and willing to use it properly (Kim, 2014). In other cases, it has been found that even the country an individual or organization resides in can make a difference in the overall effectiveness of the information security plan, as certain countries handle information security differently and more efficiently than others do, making their plan more successful (Kim, 2014). Literature also shows many areas that can make an information security policy a success and several that can make it a failure; according to Imboden's study, several organizations found that their significant issues surrounding an effective information security plan were lack of time and lack of knowledge (Imboden, 2014).

Additional studies show that many organizations are having a hard time developing an effective information security plan given the fact that they are still trying to recover from and fix the problems that have plagued them in the past, in addition to being proactive for threats in the future (Prislan, 2016). This poses the common discussion point of whether to consider a proactive information security plan versus a reactive information security plan; the proactive strategy would, in general, lead to fewer breaches, but the reactive strategy can in several instances be more cost-effective (Kayode, 2016). In addition to what makes information security plans successful and what makes them fail, literature also explores the different levels of staff that need to be involved in an information security plan (Imboden, 2014). According to a survey in 2014, leaders found that an effective information security plan has to meet three conditions: employing capable staff in charge of information security, adopting detailed information security strategies, and analyzing the importance of information resources while

assessing the efficiency of security measures (Prislan, 2016). The implementation and success of an information security plan is difficult, and an organization has to meet many different standards to ensure a plan is a success: information security standards should be met, the plan should be communicated, and cooperation and coordination should take place across all levels (Abdelwahed, 2017). Additionally, studies have found that conducting an audit into the way information security is handled and how security incidents are dealt with after a successful breach will help to improve an information security plan by showing where gaps or holes may be present (Dragoi, 2015). Mobile devices and different platform computers are an example of why different articles show that many different departments have to be involved in developing an effective information security plan; some of these departments include the IT department, the security department, the information security department, the human resources department, and others depending on the organization (Markelj, 2016). Going beyond these departments, certain studies show the different general aspects that need to be covered or assessed in an information security plan; these include ensuring physical security, establishing a base security plan, providing virus, malware, and spyware protection, providing network security, ensuring IT continuity, and managing data and backups (Lee, 2014). In some instances, authors state this may be difficult; in many organizations, the formation of an information security policy is a challenge due to the fact that management lacks the understanding and need for security within IT (Imboden, 2014).

While it is vitally important, physical security is often overlooked when developing a proper information security plan (Lee, 2014). And as stated by many authors, employees make a big difference in the success of an information security plan. However, the decision making when dealing with mobile devices is much better left to the organization where the devices are being used, rather than the individual users as they do not consider information

security a necessity most of the time (Markelj, 2016). Even after an information security plan is established, authors point out that information security plans don't just apply to desktop computers and servers; other devices need security plans just as importantly if not more (Markeli, 2016). Mobile device users are much more careless with security on their mobile devices causing more chance of a successful attack (Markelj, 2016). According to Das (2016) in a study of security behaviors of smartphone users, it was found that employees' compliance with the information security policy is influenced by the benefits of the program and their overall security awareness. Whatever type of information security plan is established within an organization, it is important to include proper training of all individuals who will be given security access; this ensures that everyone understands the details of the security plan and that the plan is carried out to the best of their ability (Gharibi, 2016). But some organizations find it helps to have individuals on their information security implementation team that are responsible for ensuring the end users within the organization can connect to the information security policy; this can include training sessions, tips and tricks for users to follow, or other techniques to ensure users follow the policies and procedures of the information security plan (Kim, S., 2014). Then there are also several studies that indicate the importance of continuously updating and re-evaluating the information security plan in order to ensure it is always effective; given the nature of information technology and information security and the constant state of change, the updating of the information security plan is a necessity (Gharibi, 2016).

Cybersecurity within Higher Education. Higher education institutions and non-profit organizations have a need now more than ever to pay attention to information security because issues are continuing to grow, largely due to online presence and lack of information security protection (Imboden, 2014). These institutions have also shown in different studies

that their need for information security, disaster recovery, and every other aspect of information technology is crucial in order to properly protect and sustain a healthy network (El-Temtamy, 2016). Studies have indicated that the problems that apply to industry and businesses also apply to higher education but can be amplified at times because of lower budget amounts (Imboden, 2014). Smaller IT security budgets can negatively impact the capabilities of an institution to protect against security attacks, leaving their staff to deploy and rely on freeware or open source products; this can create risk and produce maintenance overhead, not to mention a need for specialized skills that are required to run the software, all of which would be included in a contract with a commercial vendor (Marchany, 2014). The way in which information security budget money is spent is important, especially given the lower amount of budget money that is received in higher education and the number of attacks that are increasing on higher education institutions (Dreyfuss, 2016). Literature shows that the massive increase in information exchange has led to the need for higher education institutions to re-evaluate the way in which information security is handled and to redevelop proper information security policies and procedures (Abdelwahed 2017). Studies have also shown that many hackers are now drawn to attacking higher education because they have a limited budget and an open-access philosophy; therefore, they don't invest enough in their security (Dreyfuss, 2016). In addition to these added attacks, higher education is also faced with the same challenges as industry, including working with mobile devices and introducing new technologies (Kim, 2014). Many articles have been written displaying different models in developing an efficient and cost-effective information security plan, but almost all of these articles have been developed with strictly businesses in mind and not higher education or non-profit institutions (Shahpasand, 2015). Previous literature shows that attention to the mobile revolution is necessary to close the gap in information security between academics and

industry (Das, 2016). This is just one area; articles are now showing that industry is relying on higher education institutions for issues such as information security training of students and basic computer knowledge where in the past some of this was expected of the employer (Al-Mukahal, 2015). Given the fact that most college and higher education students are familiar with online classes, email, social networks, smartphones, tablets, and computers and use information technology for their education anyway, the job of introducing students to a proper understanding of information security and how to protect themselves and their employer is very important (Kim, 2014). Higher education institutions now have the responsibility of training students on information security awareness, which includes relaying to students the importance of protecting their company's data and the negative effects of a breach, if one were to occur (Kim, 2014). Although there are many articles that discuss attacks and breaches within higher education, information security plans, and IT budgets, there is virtually no literature on the effectiveness of a higher education institution's information security plan in relation to the amount of its budget (Marchany, 2014). Now that the different aspects of cybersecurity have been discussed in regard to this study, examining beaches and security attacks will be examined in order to gain a better understanding of the effects of being attacked.

Breaches

Breaches and information security attacks that allow unauthorized access to an organization's vital data underscore the importance of developing information security plans.; the protection of unauthorized access to this information is where the importance of information security comes in, and the development of information security plans (Mushtaque, 2015). When an information security breach occurs, the role of the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO) is extremely

important for the organization because they must respond quickly to any incidents that occur in order to assess and avoid further damage and reassure stakeholders and customers that the incident is under control and their data is safe after the breach has occurred (Zafar, 2016). Another trend that has been seen in certain studies is that different types of breaches have different impacts for instance, a breach that involves privacy violations has a significant impact on the organization, whereas a breach that has a data violation does not tend to have a significant impact on the organization (Zafar, 2016). Information security attacks and breaches can also be known as cyber events; these cyber events can be broken down into four different categories: data breaches, security incidents, privacy violations, and phishing/skimming incidents. Of all of these, data breaches seem to be the most common (Romanosky, 2016).

Prislan (2016) found that cybercrime is becoming more organized and focused on big-data environment in the pursuit of more useful information to be used for illegal or unethical gain. Part of cybercrime's organization is the result of social ties that cyber-criminal networks have grown and which continue to play an important role in the expansion of cyber-criminal activities throughout the world (Leukfeldt, 2015). An example of these social ties includes cybercafés that have developed into cybercrime cafes; articles have shown that in some predominant university towns, popular cybercafés have turned into these cybercrime cafes, allowing for additional social ties and coordination between cyber-criminals (Kayode, 2016). This has led to the number of information security attacks over the last decade having grown exponentially and continuing to increase, showing the importance of a proper information security plan (Prislan, 2016). This increase in the number of attacks over the last several decades could be caused by several different things, but literature has shown that user error is still the leading cause of breaches within an organization (Flores, 2014). It is known

through virtually all organizations that employees represent the weakest link when it comes to information security (Michelberger, 2016).

Mangelsdorf (2017) revealed that between 50% and 80% of all cyber-attacks within an organization are aided or abetted by someone on the inside; this is usually done unintentionally, through phishing attempts like in emails, and other form collecting websites. This can be done in numerous ways within an organization, but one common way is through password sharing; Al-Mukahal (2015) revealed that it was when the users shared their passwords that over 15% of those users suffered from some sort of breach within the next 12 months. Another common way that security attacks occur is by manipulating a computer by users installing malware on their computers, thereby revealing passwords, personal data, and even more information (Flores, 2014). Security breaches today have been accomplished by cyber terrorists using information technology techniques like those previously mentioned, along with other techniques like social engineering. One form of social engineering, simply talking to an individual and posing as someone else to retrieve personal information, has become highly effective (Leukfeldt, 2015). Another common practice in social engineering is persuading young people to give their debit or credit card information, including the PIN number, under the ruse of being part of a social media club or school; this practice results in stolen identities which can take months, and sometimes even years, to resolve (Leukfeldt, 2015). Training and information regarding these types of attempts to gather information should be covered in an organization's information security plan; then it is up to the employees to follow that security plan (Al-Mukahal, 2015). According to Al-Mukahal (2015), there is a strong relationship between the number of attacks in an organization and the number of employees that violate the information security policy. Proper prevention and monitoring can help deter some costs, which is why in every organization part of the

information security team's duty is to determine when a breach or attack has occurred, using tools like logs to monitor incoming and outgoing traffic and other tools; observing these areas and catching an attack as early as possible can help to lessen the effects of the cyber-attack (Adler, 2015). Studies show that on average a successful attack on an organization can go more than 200 days before it is discovered, causing more data and monetary loss (Mangelsdorf, 2017). One of the reasons this is so important to businesses and higher education institutions is because of the monetary and data loss that can occur when an attack is successful (Romanosky, 2016).

Information security attacks can incur major loss for business and schools alike, whether it be tangible costs, such as loss of business, increased maintenance, and repair of failed systems, or intangible costs, like loss of customer trust, reputation, and competitiveness (Gao, 2015). In studies where questionnaires were used, several showed that organizations would not want to have their reputation damaged through a cybersecurity breach or to lose the trust of the customer (Kayode, 2016). Other studies have shown that when developing information security plans, a customer's experience should also be considered, indicating that if a breach occurs and a customer's personal information is stolen that it could affect them for several months, causing the company to lose that customer for a while and sometimes even forever (Adler, 2015). Many articles have been published discussing the amount of money that these attacks have cost organizations, exploring some of the different costs that may occur, like those mentioned previously (Choong, 2017). Studies have found that one of the highest costs of a data breach is in the expense of contacting the possible victims, which can lead to additional direct and indirect costs for the organization (Adler, 2015). Certain articles have described tangible/direct costs to include such items as the repair cost of hardware that is damaged during a cyber-attack, software damage after a cyber-attack, software solutions and

updates after an attack, software and hardware maintenance, and the average costs of research and information gathering (Kayode, 2016). In the same way certain intangible costs have also been laid out in articles including items such as the resources required to respond quickly after a cyber-attack, the rate of data loss after an attack, the average customer inconvenience, the potential damage to reputation, and the rate of business interruption during and after the attack (Kayode, 2016). In certain instances, in the event of a security attack, an organization is likely to lose an amount exceeding the amount of their information security budget (Romanosky, 2016). Although literature can easily be found regarding the loss an organization can occur, articles are not always as easily found in other areas of security attacks (Choong, 2017).

There has been little literature that focuses on the aftermaths of a breach and the effect and impact on the consumer (Choong, 2017). Examples of data breaches that have occurred and include loss in both profits and reputations are businesses that were targeted directly and lost millions of customer records, like Target, Neiman Marcus, AT&T, J.P. Morgan, and Home Depot, which are just a few (Kearns, 2015). Instances like the attack on JP Morgan Chase show that even with an extremely large IT budget of $250 million, the failure to implement a two-step authentication process throughout their organization led to a breach in their IT system, showing that even the best-prepared system is still vulnerable (Nagurney, 2017). What studies have also found is that of the cyber-attacks and breaches that have occurred it is common for reports to mainly feature stories about stolen credit cards and other monetary effects for celebrities and companies, while what is overlooked are certain cyber-attacks that focus on critical infrastructure; these can vary from pipeline explosions, steel mill meltdowns, and other incidents that are overlooked because it does not directly involve money (Mangelsdorf, 2017). When these breaches have occurred, it was found that there was a

significant negative impact on the organization's market value or reputation the day the attack occurred, but then the effect of that attack decreased over just a few days (Zafar, 2016). An example of this would be when a bank that utilizes online banking has a customer's funds and information transferred or stolen electronically because they failed to perform their information security plan efficiently; under new civil liabilities, the bank would then be responsible for the customer's money (Nawafleh, 2016). The losses from cyber-attacks and breaches that have occurred over the last several years have also created different business opportunities as well; for instance, cyber-insurance has now been developed and is becoming exceedingly popular, continuing to increase by more than ten percent in premiums every year since 2013 (Adler, 2015). Although monetary loss is a great reason for information security protection, there are other equally important reasons; the fact that cyber-terrorists have expanded their skillset and their targets to include more than just companies, businesses, and schools, and that cyber-terrorists are using information technology to influence and sway governments and nations shows that information security is important on every front to protect our future (Raha, 2015). The fact that the internet has no single entity, that no government, company, governing body, or individual owns it or is in charge of it, results in the fact that cyber-space has no borders and makes prosecuting cyber-terrorists more difficult and making proper information security critical (Yayla, 2014). Now that security breaches and cybersecurity have been reviewed, the next section of this chapter will explore what literature shows about budgets.

Budgets

The budget process can play just as an important role in developing an information security plan as the planning and technology itself (Santos, 2017). Literature has shown that information security budgets are on a rise and that the budget money is generally spent on

improving in-house skills, updating and securing applications, intelligence and analytics, and data security (Filkins, 2016). While IT and information security is ever changing, certain articles found that some IT budgets are based significantly on the previous year's budget and to a lesser extent on the regulations and forecasts of the anticipated needs and possible threats (Rowe, 2006). Even if certain policies and procedures have been approved by management and in other areas, these still have to go through the budget process to ensure that there is funding available to purchase the necessary items (Santos, 2017). But whatever the process may be, there are still proper channels that must be followed during the budget process and after the budget is finished. Part of the budgeting process as shown in different articles is that once the budget is established, it must be communicated to proper personnel within the organization to ensure that it is carried out efficiently (Ferrerira, 2015).

IT budgets could be a little different given the nature of the work done in the IT department; either way, people with the proper knowledge and skills in IT are needed to make the proper budget requests (Santos, 2017). In many organizations it falls on the IT committee to request the proper budget money for the technology and services needed to carry out the proposed IT projects and plans; this includes submitting the justification of such budgetary needs (Santos, 2017). With the rising costs of information technology and information security, this has led to some organizations trying different techniques including the use of open-source software and free tools in order to cut costs where possible and make the budget meet the needs of the organization (Subsermsri, 2015). Studies have shown that the options for cutting budget costs are growing using options like open-source and even cloud-based options; with cloud options being more readily available and cost-effective, it does give an organization different options for their IT budget (Kalliosaari, 2016). Cloud computing can be defined as a model for enabling ubiquitous, convenient, on-demand network access to a

shared pool of configurable computer resources; this definition is according to The National Institute of Standards and Technology (NIST) (Ghazizadeh, 2014). Although this can be a great money saver, using cloud-based or shared-based software should be done with caution, as there are certain studies indicating that internet or cloud-based applications can face a lot of information security issues because they can be tied to fraudulent data collection and then cause the organization even further trouble (Vijayakumar, 2015). Cloud, along with any other web-based or online based software solutions, must deal with the information security aspect of password protection, given that most, if not all, logins will be conducted through the web and that more people will have access to it as well (Sung, 2014).

Information technology budgets have been found to be more difficult than other budgets because of the timing and the quickness with which information technology changes; a budget that is generally set once a year may have built-in costs that are not adequate for new tools and technology that will come out within that year (Misra, 2014). With IT budgets, there is also the problem of planning for something that has either never been done or that no one has any extensive experience working with, which could cause problems (Misra, 2014). IT budgets and even some information security budgets could fall into the same situation as what was known as the agile software development budget, which was established when software development started to get its own budget in the first several years, and costs exceeded the budget tremendously (Misra, 2014). In order to better understand the effects that budgets can have on information security, this section will explore different aspects of budgets, exploring higher education budgets, industry budgets, information technology budgets, and information security budgets.

Industry Budgets. Budget issues can have a significant impact on IT and in developing IT governance throughout public sector parts of industry (Santos, 2017). Given

the needs of an IT department, the budgeting process can be difficult and crucial in order to create a secure environment (Nagurney, 2017). Nagurney (2017) found that in industry many times budget constraints can delay the adoption and implementation of certain security measures or tools, causing subsequent cyber-attacks and heavy losses (Nagurney, 2017). In this study, it was also found that most times the budget is spent to resolve past issues and not to work on investing in future protection (Nagurney, 2017). A sufficient budget is one of the factors necessary for successful IT auditing, IT implementation, IT security, and many other IT functions (Wongpinunwatana, 2014). The use of a transparent budget can help especially when dealing with auditors and with checks and balances within an organizational system, although there is still the issue of most budgets being built to be reactive and not proactive (Subsermsri, 2015). This can lead to certain barriers that could cause issues within an IT department and within an organization. In Garg's article examining the barriers of implementing IT, he states that many organizations report certain barriers that are common among industries including implementation costs, limited budget, resources for IT implementation, and lack of IT leadership (Garg, 2015). This should have an effect on how budgets are adjusted for IT departments and in particular information security, allowing for businesses to adjust their budgets as needed to meet the security needs of the organization (Nagurney, 2017). Whatever the size of an IT budget, building in the proper amount for security and also for the proper training and awareness program for the organization can be the difference between a successful information security plan and a failure (Weishaupl, 2015).

Within a successful information security awareness program and information security plan is the truth that technology cannot provide all the security answers for an organization; awareness training and personal responsibility are crucial, both of which must be ongoing and not just a one-time incident (Gharibi, 2016). A common misconception among employees

and everyday users is that information security is the responsibility of the IT department and the CIO, that it is not the responsibility of the average user, and that digital data is not important (Zaveri, 2015). According to Taylor (2014), it is now time that we stop looking at information security as a technical problem and start considering it a social problem, because it has become so widespread that it is essentially needing to be addressed outside of the workplace, the IT department, or any other technical area and should be considered everywhere. PricewaterhouseCoopers reported in 2015 that medium and large companies raised their information security budget in light of security incidents; but small companies reduced their costs by 20%, partly due to overwhelming IT budget needs (Nagurney, 2017). As mentioned in this article the size of the business is going to make a difference in almost every aspect of information technology and information security (Imboden, 2014). Most small enterprises and businesses have a limited or smaller IT budget compared to larger companies, which can limit their protection and capabilities (Boon, 2015). The size of the company is not the only deciding factor in how the budget is developed and how information security is handled; for-profit and non-profit organizations, this can vary drastically in their processes (Boon, 2015). Several different studies have been carried out exploring the size of an organization's information security budget relative to the size of the overall organization; while this is very useful information, virtually no studies were conducted on the higher education side of this topic (Shamala, 2015). Information security budgets have to be carefully developed in non-profit organizations because the money and resources that are set aside for the information security budget is money that cannot be spent on developing and growing the organization (Imboden, 2014). In many instances, the budget process within industry will vary drastically compared to higher education, so it is important that both are examined (Radulescu, 2016).

Higher Education Budgets. Literature shows repeatedly that higher education generally operates their IT department and their budgets at a lower amount than that of industry, adding to the difficulties that higher education experiences (Liu, 2016). In higher education, it is found that inadequate budgets for tools, staff members, and services can create a significant gap in the institution's information security defense capabilities (Marchany, 2014). Marchany (2014) revealed that 43% of higher education institutions believe they cannot pay premium salaries needed to keep higher skilled information technology workers, leaving higher education at a disadvantage in their IT department. The amount an institution spends on their information security can vary greatly, but as long as the budget amount meets the needs of the higher education institution, then a secure environment can be established (Nagurney, 2017). Marchany (2014) also revealed that 37% of the institutions in the study reported information security making up between one to six percent of their overall IT budget. Although this is true, many higher education institutions, like other business organizations, may pull budget money from other IT-related budgets to meet the need of information security gaps or tools needed; this is also found to be true in other areas of the budgetary process (Marchany, 2014). Most higher education institutions fund their budget with a combination of money from the government and student tuition money; with governments pulling money from higher education in most cases, the budget process for higher education can be very difficult (Subsermsri, 2015). Many articles discuss the fact that given the lower IT budget in higher education it is even more crucial that institutions are able to balance their budget and needs appropriately (Radulescu, 2016). Higher education, as well as other areas, must begin to develop their information security budget by weighing the amount spent on the information security budget compared to the cost of repair and recovery from an attack that occurs (Radulescu, 2016). It is important that this is done throughout virtually all levels of the

budget process so that everyone is on the same page and so the budget is developed efficiently (Liu, 2016).

Administration and other decision makers in higher education must work on developing a balance between the efficiency of the IT system, the security, and the amount set aside for these areas in the budget (Liu, 2016). The administration is also responsible for examining the users' needs and the abilities required of the technology when trying to find the proper balance in their budget (Subsermsri, 2015). This is vital because having the proper administrative team in place to set the appropriate priorities within an information security budget can help in determining its success or its failure; these priorities are determined by the institution's needs and their current IT environment (Dreyfuss, 2016). Another aspect of higher education budgets that are addressed through literature is the difference between an IT budget and an information security budget, where an information security budget focuses specifically on security-related issues (Kim, 2014). Imboden (2014) stated that the size of a nonprofit institution or organization's budget is a primary factor in predicting whether the organization has an information security policy. Several institutions generally just role the information security budgetary needs into the overall IT budget, if there is no information security budget present (Imboden, 2014). However, even with the limitations of information security budgets, higher education can still provide students with information security training as part of their IT program, allowing for students to leave informed about security issues (Kim, 2014). Given the nature of higher education institutions, this isn't surprising, but one limiting factor on the amount of students' knowledge about information security upon leaving an institution is the amount of money available to spend on security hardware, making the budget just as important on the academic side as on the operational side of higher education (Kim, 2014). Literature is readily available when looking at the topic of higher education

budgets, but very few articles examine the IT budget or information security budget within higher education (Imboden, 2014). As briefly discussed in this section there is a difference between information technology budgets and information security budgets; in order to gain a better understanding, the next two sections will explore the differences and examine what literature has been written about each type of budget.

Information Technology Budgets. Given the nature of information technology in today's business world, it is easy to see that the IT budget can constitute a large amount of the overall organizational budget and that these costs are an ever-growing part of the organizational budget (Gercek, 2016). Within IT, the size of the budget can drastically change and limit the best practices and can have detrimental effects on the health of the IT system (Hryszkiewicz, 2015). The literature for this study focuses mainly on budgets and the effects on information technology, but there are articles that also visit the important role that information technology plays in assisting the overall organization, even outside of information security protection (Mushtaque, 2015). As shown in other articles, the amount of a budget is only one piece of the information security plan puzzle; proper planning must also be considered when establishing a plan (Boon, 2015). Studies have shown that certain information technology budgets do not plan accordingly for breaches and other technology issues; therefore, their budgets are exceeded trying to fix the problems that were not protected against (Shahpasand, 2015). Literature has shown that the amount of an IT budget and proper planning are essential in establishing an effective information security system, but other factors easily come into play with any IT department, causing difficulties in proper security plan deployment (Kaptein, 2015). Filkins (2016) discovered that information security budgets must be given priority in certain circumstances and there are several different ways to justify that such as complying with regulatory requirements, aligning with business objectives,

reducing security events, improving risk profile, reducing staffing costs, and improving overall system efficiency. Time and budget constraints in an IT budget can prevent an organization from implementing all required components of an information security policy at once, causing a gap in the desired protection (Kaptein, 2015). Studies have found that this can lead to having IT based projects finishing over-budget as the products have changed since the budget was developed and pricing is different when implementation was carried out compared to when the budget was developed, or that the technology had changed and needed to be altered from the time the budget was made; this can also lead to cutting corners to try and stay within budget and then causing other IT related problems for an organization (Obeidat, 2014).

Having the proper components installed and configured correctly has shown in many articles to be the most effective way for a security plan to be efficient and to be properly installed once an information security plan is established (Abdelwahed, 2017). The sequence in which components are adopted within an information security policy is also relevant and it can affect how effective an organization's security policy can be despite a limited budget (Kaptein, 2015). Some articles show that even when an information security plan is set up correctly, a security attack or a number of attacks could change the way in which an IT department handles their budget money (Bere, 2015). In light of information security attacks increases and the sheer number that has occurred, IT budgets are now having to divert budget money that was originally going to be used to upgrade and improve systems to now ensuring that systems are more secure (Bere, 2015). Literature is also indicating now that proper planning and even diverting funds to allocate for proper protection may not be enough in some cases, as IT departments now have to include in their budgets the handling of new technologies and other devices in some instances (Boon, 2015). Boon's study shows that

companies that embrace Bring Your Own Device (BYOD) could save on IT budgets because employees would be providing the devices they are working on (Boon, 2015). While there are many articles on information technology budgets, there are a minimal number of articles that discuss how the budget affects the overall effectiveness of an information security plan, helping with the justification process of the budget (Kaptein, 2015). The justification process of any budget can be difficult, but given the proper documentation and a cost-analysis of cyber-attacks and other IT needs, the justification of an IT or information security budget should be easy to supply (Iosifovitch, 2016). Although many organizations utilize the IT budget to handle their information security plans, there are some companies now that have focused their budgets more and developed an information security budget that strictly handles the information security portion of the IT department.

Information Security Budgets. Information security budgets are a fairly new concept and have not caught on in all areas of industry or higher education, but they are becoming more popular given the importance of information security in today's environment (Kim, 2014). Preliminary security budgets had trouble estimating the cost of effective security protection, and the cost functions well exceeded the budget (Nagurney, 2017). Many other studies have shown that the budget for an information security plan is difficult to plan and calculate given the irregular nature of software development, the evolving nature of hackers, and the unpredictability of security attacks; then there are also the different areas of the budget that must be explored like breach containment, crisis management, investigations, customer compensation, damaged system replacements, and any other penalties that the organization accrued in light of an attack (Kayode, 2016). And despite the increased number of cyber-attacks and security breaches over the years, the organizational budget for

information security continues to remain low, especially considering the potential loss for an individual or business if a successful attack were to occur (Choong, 2017).

In fact, different studies have shown that a proper information security budget could end up saving the organization money, and at the very least protect the brand or the reputation of the organization as well as reduce the negative exposure and negative press that can occur in the event of a data breach (Adler, 2015). While literature is discussing information security budgets more frequently in the last five years, there is still limited information available on different areas of information security (Shahpasand, 2015). A promising trend though is that certain studies show that many organizations are building into their information security budget amounts to be used to recover from an attack or data breach, to recuperate costs from losses as needed (Adler, 2015). Whatever areas are being considered for a budget, finding the balance in a budget is a delicate process, and an information security budget is no different; focusing part of the budget on targeted cyber-attacks and another portion on mass cyber-attacks is crucial in developing a well-balanced information security plan (Gao, 2015). Articles have shown that many information security models and methods do not consider limited budgets when considering information security effectiveness (Shahpasand, 2015).

The way in which newer information security budgets interact with the development and implementation of an information security budget is one of the more commonly researched topics in recent literature (Kayode, 2016). Shahpasand (2105) revealed that organizations trying to establish a cost-effective budget many times do not allow for beneficial information security policies and procedures. With many organizations just beginning to develop an information security budget, the proper development process should be taken; different studies have shown different models that build a budget using threat reports, logging, and other IT tools (Shahpasand, 2015). Then there is also the thought

process that goes into the budget process. Certain stigmas have to be overcome in order to develop a proper information security budget; one stigma still present in businesses today is when senior management believes information security is strictly addressing disaster recovery and not dealing with real-time protection (Alavi, 2016). Given the importance of information security plans, many organizations, businesses, and higher education institutions are beginning to make the information security budget a smaller portion of their overall IT budget (Shamala, 2015). Shamala (2015) revealed that 58.75% of their respondents indicated that their organizations allocate more than five percent of their total IT budgets to set aside for information security. Kayode (2016) found in her study that the average organization invested a total of 64.14% of their total IT budget to information security. Literature also shows that this trend is not just taking place in the United States; it is also happening in all around the world, although different countries handle their percentages and their overall information security budgets differently (Hryszkiewicz, 2015).

Different countries prioritize and budget for information security differently; for instance, Polish industry on average has information security comprising of only 2.7% of the overall IT budget (Hryszkiewicz, 2015). On average the worldwide spending on information security is 3.8% of the IT budget, with many countries varying plus or minus one to two percent (Hryszkiewicz, 2015). In many instances, it is found that although this amount may seem like a large amount for an information security budget, having a budget that is several hundred thousand to even $1 million is understandable given that one security breach can cost an organization several hundred million dollars at a time (Romanosky, 2016). Exploring information security budgets also had articles exploring additional topics, such as how information security budgets can affect the overall IT department and what the budgets can be used for throughout the department and even the company (Nagurney, 2017). The

information security budget can affect different things, like the vendors that are used and the products utilized in securing a system (Nagurney, 2017). The different ways that an information security budget can be used aside from developing and implementing an information security plan can also be found in a few different articles recently (Kim, 2014). One of the best uses of an information security budget is to develop a comprehensive information security awareness program for users so that these users can realize the importance of information security in an organization (Kim, 2014). Even though information security budgets are fairly new throughout industry, the importance and benefit of establishing a separate budget from general IT budgets can be found throughout many recent articles; indicating that this may be a trend that is going to continue to happen (Nagurney, 2017).

Summary

Information technology encompasses a variety of different aspects and subjects including cyber-security, and now virtually all aspects of security are handled within information technology, cyberwarfare, including the various areas of the world that are affected by cyberwarfare, infrastructure, end-user support, and many others; making information technology a difficult subject to broach (Raha, 2015). The area of cybersecurity or information security has quickly elevated to being included in discussions across every facet of business and other industries (Prislan, 2016). Information security and cybersecurity have also shown that attacks and breaches do not limit themselves to one type of business or industry; small, large, profit, non-profit, industry, education--all areas are affected by information security (Shamala, 2015). Given the recent spike in information security, the diverse nature of information technology, and the ever-changing nature of technology in general, the creation of information security plans have been vital in virtually every business or organization to ensure that company and client information is as safe as possible (Kaptein,

2015). Literature encompassing these topics of information technology, information security, cybersecurity, and information security plans can easily be found, showing significant studies done in this area; however, what is lacking is studies looking at the correlation of an information security plan's effectiveness and the budget amount that was spent on that plan (Marchany, 2014).

The need for information security plans is shown in the number of attacks and breaches that are occurring across the world, and the protection of company, employee, and customer data is very important (Choong, 2017). Cybersecurity breaches can have different short term and long-term effects for organizations, employees, and all those that are involved with the organization, costing some organizations everything (Zafar, 2016). Given the diversity of information technology, information security breaches can occur in just as many ways; including but not limited to data breaches, privacy violations, security incidents and more (Romanosky, 2016). Whatever type of breach that occurs within an organization, one repeating theme is the fact that user error or lack of information security training is what leads to the breach (Flores, 2014). The number of attacks, the type of attacks, and whom the attack affect has been covered significantly in literature, but one area that is still lacking in the aftermath of a breach is how a security breach affects the organization and all those affected after the incident (Choong, 2017).

Information security breaches and information security protection is highly dependent on the amount of money spent on developing and implementing proper information security protection; this causes the exploration of budgets to be crucial in the fight against cybercrime and cyber-criminals (Nagurney, 2017) Discussion of information technology and budgets is found in numerous articles and published works but, when exploring the effectiveness of an information security system and the budgets that are associated with that system, there is very

little research done on this subject (Shahpasand, 2015). The budget process is long and difficult in every facet of industry and around the world, but the inclusion of information technology, and now information security, has been found to be essential in ensuring that an organization has a proper system in place to aid and protect the organization (Zaveri, 2015). One fact found in numerous articles is how the size of an organization makes a significant difference in the extensiveness and amount of information security protection that can be put into place (Imboden, 2014). Information security budgets are a fairly new subset of an information technology budget but have been found in many articles to save organizations money and help with information security attacks and breaches, saving many organizations from losing thousands if not millions of dollars in successful attacks (Adler, 2015). There are several studies done concerning the subject of budgets within higher education, but there are virtually no articles dealing with IT or information security budgets within higher education (Imboden, 2014). These different topics through this chapter demonstrated that separately the topics of information technology, cybersecurity, information security plans, budgets, IT budgets, and information security budgets are all researched thoroughly; but the specific topic of information security budgets and their relationship with an effective information security plan has very little if any literature published on it, demonstrating the need for this study (Shahpasand, 2015). As this chapter has laid out a review of the literature that has been completed concerning the subject of this study, the next chapter explores the research method being used to conduct this study.

Chapter 3: Research Method

The purpose of this quantitative correlational study was to determine if a relationship exists between the budget and the effectiveness of an information security plan (Marchany, 2014). The problem is that some organizations face challenges implementing an effective information security plan due to inadequate budget funds (Marchany, 2014). Some organizations cannot develop an information security policy without the proper IT budget in place (Imboden, 2014). Information security attacks have become more consistent and aggressive which warrants a security policy or protection plan in virtually every industry (Abdelwahed, 2017). Some of the larger organizations have adequate funds to build effective information security plans, while small and medium-sized companies, colleges, universities, and other entities are not able to spend that amount of money on security (Choong, 2017). The ability to determine the correlation between an effective security defense and the amount of money spent on that defense will allow organizations with smaller information security budgets to determine if a proper security policy is possible without using funds that are hard to come by or are not available (Abdelwahed, 2017). The learner will explore the relationship between an information security plan and an information security budget. The ability for an organization to apply an effective and cost-saving information security policy can end up saving organizations in the long run; and for smaller organizations, this can make or break their business (Adler, 2015).

This study consists of using public data that is found through publicly released information from websites, databases, and other online sources. Using this data, the study worked to find the number of times a higher education entity was attacked by cyber-terrorists and examine the type of security currently in place and the amount of money that was spent

on an information security plan. Given the formula, calculated using the G*Power application the sample needed for this study would be a total of 66 different schools, with 22 being from the three different areas of higher education. A custom questionnaire was developed to answer the questions needed to provide the data for this quantitative study; this questionnaire consisted of questions pertaining to the number of cyber-attacks that have taken place and their effects, as well as the type of institution and their annual information security budget. To collect this data, research was conducted through online sources to find past instances of cyber events and budgets that have been published publicly. Upon finding this data, it was analyzed using statistical tools and algorithms to obtain the results desired for this study. It is recognized that the format in which this study was conducted does have limitations and delimitations, but this study was guided by the standards set forth through Northcentral University's Institutional Review Board (IRB) because the data found was all publicly released data that could already be discovered on the internet. The result of the methods used to complete this study indicated if information security budgets within an organization had any bearing on the effectiveness of a security plan.

Throughout this chapter, information related to the research method was examined, including the methodology and design, population and sample, data collection, materials used and much more. Beginning with demonstrating that this study was a correlational quantitative study, using statistical data to explore if there is a correlation between information security budgets and information security effectiveness, this chapter explored other aspects of the research design (Grant, 2014). To conduct this study the population and the sample were explored as well, ensuring an understanding of what the population is and why it is being used in the study (Harris, 2014). The materials used in the study, as well as the different variables in the study, were examined in this chapter to ensure a better understanding of why these

different aspects of the research are needed (Reimer, 2015). The procedures used in this study, in addition to the data collection and analysis, were examined in this chapter, looking at how these affect the independent and dependent variables (O'Connor, 2017). Continuing through the chapter, the assumptions, limitation, and delimitations were all taken into consideration to ensure that all the downsides to the study were examined to ensure the study was carried out in the most efficient way as possible. The last topic in this chapter explored the ethical assurances in the study to ensure that no rights and privileges of the parties being studied were exploited. The inclusion of these mentioned topics helped to ensure that this study was carried out as effectively and efficiently as possible, as well as ensuring that the research carried out met the needs of the study.

Research Methodology and Design

This study consisted of a correlational quantitative study based on the statistical data that was collected and analyzed to understand whether a correlation exists between information security budgets and information security effectiveness. The methodology used throughout this study consisted of either ratio or interval methods or a mixed method of both given the fact that the data was collected from publicly released information. The way in which the data was needed to perform the necessary statistical analysis made the correlational method using the ratio and interval types of measurement appropriate, to show the cause and effect of different information security methods used by different organizations (Filkins, 2016). In examining the problem proposed by this study, the research methods and design were advantageous because there have already been similar studies that have been conducted using the same type of design and method to arrive at their results (Weishaupl, 2015). Given the purpose of this study was to find a correlation between the amount of information security budgets and their effectiveness; a correlation study is appropriate given the nature of the

design and the study making comparisons between the different security plans and the amount of money spent on those plans. Similarly, as with the purpose of this study and the problem of this study, the research questions also pertain to the design and methods of this study given that all three research questions were examining the relationship between the higher education entity's information security funding and their security effectiveness. Additional research methods and designs were considered for this study but were found to not fit the needs of the study; therefore, the methods that were used were selected.

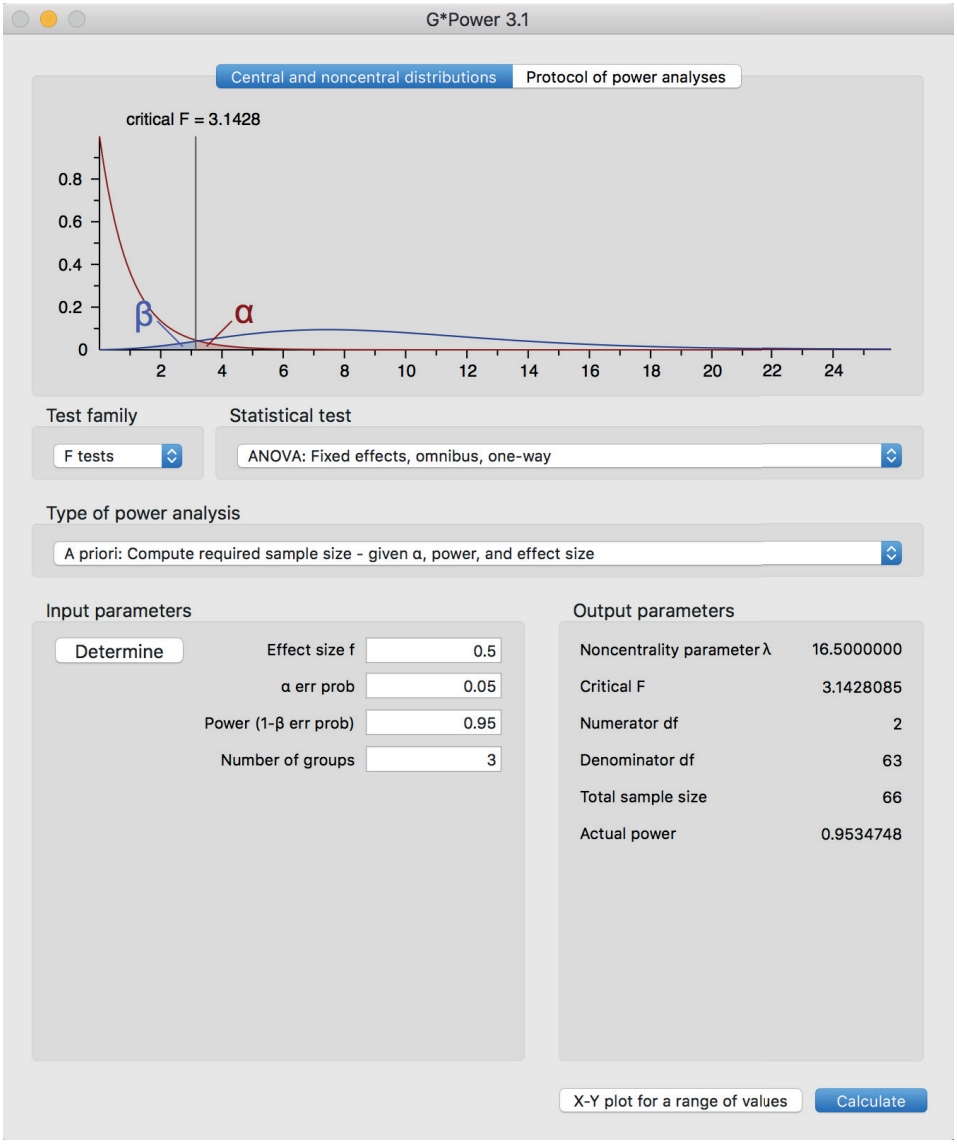
When examining different research methods, first quantitative was chosen over qualitative because statistical analysis was going to be taking place, because this study was going to be number-based rather than text-based, and because the response options were more fixed looking at budgets and the number of attacks taking place. The fact that this study was being conducted using archived data and not utilizing focus groups and interviews was another reason to use a quantitative approach, getting the desired information to address the hypotheses of the study. In addition to the quantitative design that was decided upon, the approach of a correlational experimental design was used in this study because of the relationship being proposed in the study; by attempting to find the correlation of the amount of money spent on an information security budget and the effect that the budget has on the overall effectiveness, this study fell within the correlational experiment realm (Grant, 2014). With this type of research design, different levels of measurement were needed; this study used a combination of ratio and interval types of measurement. This is because interval, which measures the distance between attributes, will help to tell us the difference between the amount of money needed to make an effective security plan, if such an amount exists (Silk, 2014). Ratio was the other level of measurement used in this study to help to determine if there is an effective ratio of budget money spent on information security and the effectiveness

of information security (Silk, 2014). Utilizing these different research methods and techniques combined for a thorough approach to the study and brought forth the most accurate data, although this was dependent on the population and sample size gathered.

Population and Sample

The sample for this study played an important part in receiving correct and accurate data to help ensure the research questions were answered correctly and that the hypothesis could be tested (Harris, 2014). Using G*Power and the values of an effect size of 0.5, an Alpha value of 0.05, a Power value of 0.95, and using three different groups (two-year or community colleges, four-year public colleges, and private higher education institutions) an overall sample size of 66 was calculated. This sample size of 66 was then broken down into the three different groups to give a sample size of 22 per group in the study; the calculations for this can be found in G*Power Figure below.

G*Power Figure. Software Displaying Sample Size Information



G*Power *Figure. G*Power Software showing the Sample size needed for the study.*

This sample size corresponds to the variables of this study because each group corresponds to a different type of higher education institution. The population of the different colleges and higher education institutions across the United States is equal to 5,300 colleges; so, the population is 5,300; showing that the sample size of colleges is a small portion of the overall population size, but the sample size should still help to indicate what differences if any persist between the different institutions. Including this sample size covered approximately

one percent of all the population size across the United States. The schools were broken down in order to find if there is a correlation between the different higher education information security budgets and their overall security effectiveness; the difference between these institution's funding, tuition, and other financial awards indicated if a difference existed between the institutions. Given that the problem relates to establishing an effective information security plan with a fixed amount of an information security budget; this sample examined three areas where budgets were the most challenged, higher education (Marchany, 2014). The purpose of this was trying to determine if there is a correlation between the budget and effectiveness of an information security plan; the sample size of 66 different higher education institutes gave an adequate number of references to be able to calculate and show whether a correlation exists (Adler, 2015). Being that the research questions were already broken up into three separate questions, examining the different aspects of these questions helped observe how higher education's budgets are different from other industries; and that within higher education there are differences (Subsermsri, 2015).

The sample size was broken into three different categories to examine the differences among two-year community colleges, four-year public colleges, and private colleges in order to show a true representation of the population, which is all the higher education institutions in the United States, and to see how all of these institutions differ across information security budgets and their effectiveness. This aspect of the study was important in order to illustrate that differences among these types of institutions do exist and that their own environments can differentiate with budgets that are developed and how information security effectiveness can differ (Coman, 2016). These samples were crucial to the study because they addressed the problem, the purpose and the research questions that were explored in this study. The problem of this study addressed the challenges of establishing an effective information

security plan due to budgetary issues; the samples of this study addressed this because they offered three different perspectives of higher education institutes and the varying budgets and information security protection they can provide (Marchany, 2014). While the purpose of this study was to discover if a correlation between information security budgets and security effectiveness exists, the three samples helped in confirming or denying if a correlation existed by examining three different aspects (Abdelwahed, 2017). In relation to the research questions in this study, the sample examined conveyed directly to the three different types of higher education institutions and helped in displaying the relationship, if any, between their budgets and their information security protection.

The data for this study was gathered using archival data; this was carried out using public information from websites and public databases. These data sources were used to find the budgets for the given higher education institutions and any information about security attacks. Examples of these public sources included databases and websites such as itdashboard.gov, usaspending.gov, veriscommunity.net, www.air.org, informationisbeautiful.net., www.statescoop.com, and www.dhs.gov in addition to other scholarly journals and periodicals. The data researched for this study consisted of budgets and attacks that have occurred in the past five years in order to ensure the findings of this study were relevant to current institutions and security measures. The geographical location of this study resided in the United States in order to compare similar budget types and similar information security habits within schools in the United States. This manner of gathering data refrained from attempting to gather information that organizations might be unwilling to give and depending on questionnaires that might or might not be returned, therefore resulting in data that has already been verified (Grant, 2014).

Materials/Instrumentation

The materials used in conducting the research for this study were strictly archival, as they were gathered using the public databases and websites containing previous attacks and budgets that have been either peer-reviewed or verified by a verifiable source (Reimer, 2015). Because the data being gathered has either been previously released in peer-reviewed articles or has been released to the public through websites or databases, the data can then be trusted as reliable and valid because of the validity process they have already been through (Reimer, 2015). Utilizing public information ensured that no field testing or pilot testing was required and that no testing of any kinds was required because the data was already released to the public (Alam, 2013). Given the manner in which the data was collected ensured that it was ready for data analysis and no further manipulation of an instrument was necessary (Reimer, 2015). The use of archival and public data also ensured that permission and approval to conduct the study required less work by the approval board, considering that the data has already been published and released to the public (Newman, 2013).

Operational Definitions of Variables

Within this study there were primarily two variables examined in order to find and measure results; the two variables were the independent variable, information security budgets, and the dependent variable, cyber-attacks. Information security budgets have become crucial in virtually every aspect of industry and education; measuring the effect of an information security budget in relation to an information security plan's effectiveness helped to determine if an effective plan can be established on a fixed budget (Subsermrsi, 2015).

Information Security Budget. An information security budget is an estimate of income and expenditure for a set period of time or the amount of money needed for a specific purpose (Nagurney, 2017). This variable would be considered the independent variable; and

it served more as a predictor variable in order to discover if there is a correlation between this variable and the dependent variable (Das, 2016). This variable was used to measure the amount of money that is utilized to offer an information security plan, providing the equipment, tools, training, and manpower to ensure the plan is kept functional. The measurement of this variable was a combination of both interval and ratio as it depended on the findings to determine if a relationship exists; this had a ratio measurement to be used to show the amount of a budget in comparison to a plan's effectiveness, or if a breakdown of amounts and a corresponding effectiveness could be found, then interval measurements would be utilized (Filkins, 2016). The measurements for this variable varied depending on the amounts of the budgets but consisted of values ranging from 0-$1,000,000 with a slight chance of running higher if institutions had budgets exceeding that amount. The information security budget information was gathered from the specific institution's websites; given that public higher education institutions must post their budgets through board of trustee minutes and meetings, budget information can be gathered in this manner. For those budgets that could not be located in this way, then certain databases and websites were used such as: www.oecd.org (Online Education Database), http://nces.ed.gov (National Center for Education Statistics), www.ncsl.org, and www.usa.gov/higher-education.

Cyber-attacks. A cyber-attack is an attempt by hackers to focus an attack or destroy a computer network or system (Gao, 2015). This variable was considered the dependent variable; it served more as a criterion variable in order to discover if there was a correlation between this variable and the information security budget (Mommer, 2015). This variable was used to count the number of security attacks that have occurred over the past five years; these attacks included anything from a computer virus outbreak to vicious malware that had infected an institution's network. This information was collected using databases and

websites like www.csis.org, which is the Center for Strategic and International Studies, to find the number of attacks that have occurred in higher education. The measurement of this variable was a combination of both interval and ratio as it depended on the findings to determine if a relationship existed; this had a ratio measurement used to show the number of attacks that occurred in relationship with the budget, or if there was a breakdown of the number of attacks and the amount of money spent on security budgets found, then interval measurements were utilized (Jogulu, 2011). The measurements for this variable varied depending on the number of attacks or breaches that occurred within an institution but consisted of values ranging from 0-500.

Study Procedures

This study collected data by performing a public search using the keywords for information security breaches or information security attacks on higher education institutions within the past five years. This search utilized peer-reviewed journals, public database, and reputable public websites in order to widen the search and find the information needed to conduct a thorough study. The sites and databases which helped in finding the information regarding cyber-attacks included the following: www.csis.org (The Center for Statistical and International Studies), www.air.org (American Institute of Research), www.statescoop.com, www.itdashbord.gov, and www.dhs.gov (The Department of Homeland Security). After finding the required number of samples and then searching the affected institution's websites and public budget information, the amount of budget money that was spent on information security in the past five years was found. Using additional public databases and websites such as www. oecd.org, http://nces.ed.gov, www.ncsl.org, and www.usa.gov/higher-educationas helped to find the information required to conduct the necessary statistical analysis. Other online resources like usaspending.gov, veriscommunity.net, and itdashbaord.gov helped in

finding additional budget information about higher education institutions. After the data was collected, statistical analysis was run in order discover if a relationship existed between the amount of money spent on information security and the overall number of attacks that occurred within the past five years. Using correlation statistics and measuring the value of *r* on a scatterplot helped to answer the research questions within this study. These analyses were calculated using computer software such as SPSS or Microsoft Excel to ensure accurate information; this information examined how many attacks occurred in an institution compared to the amount of money that was spent on the same institution's information security budget. This allowed for proper analysis to prove or disprove the research questions and the hypothesis of this study.

Data Collection and Analysis

The data collection for this study consisted of a certain type of statistical tool, a regression analysis, in order to ensure the most accurate results were obtained (Ferreira, 2015). This type of analysis allowed for the data to show if a relationship existed between the independent variables/predictor and criterion variable, information security budgets, and the dependent variable, an effective information security plan (O'Connor, 2017). The regression analysis was utilized because the dependent variable in this study should only produce one outcome, which is a continuous variable and there is only one independent variable which is also producing a continuous value. Because of these different values and the nature of the variables used in this study, the type of test used for each of the hypotheses consisted of either an ANOVA test or a Friedman test. The ANOVA test was utilized with parametric data, whereas the Friedman test was used if the data was nonparametric data. These tests were used because the independent variable consisted of three different environments, two-year public schools, four-year schools, and private schools. This was also the case because the dependent

variable resulted in continuous variables with the number of security attacks. Examining these different variables when progressing through a statistical decision tree helped in determining that a regression analysis was the best suited for this study (Trajkovski, 2016). This type of analysis was completed with the use of computer software such as SPSS statistical software. Because the type of analysis taking place measured the presence or lack of a relationship between the two variables, this ensured that the data being collected was analyzed correctly and that the results addressed the problem statement, the research questions, and the hypothesis (O'Connor, 2017).

Assumptions

Information security plans are vital to the success of many information technology departments within an organization, but an assumption that took place in this study was that all organizations have an information security plan in effect; while this should be the case in most institutions, it may not, in fact, be true in every instance (Choong, 2017). In addition to this assumption, there was an assumption that IT departments have a separate information security budget within their department; while this may not always be the case, it generally is the case in the majority of the IT departments in today's business world (Abdelwahed, 2017). The availability of information security budgets through the institution's websites was another assumption made for this study; while higher education institutions are required to publish and make their budgets public, this might not happen at all institutions, making the budget information hard to locate (Marchany, 2014).

Limitations

Certain limitations existed in this study, one being that data was collected and used through publicly released sources instead of conducting a study where information is gathered directly from the organizations themselves. This was done because many organizations do

not freely give out security breach or security attack information and fail to admit all the breaches that take place; by using public information all the data collected was kept reliable and valid (Marchany, 2014). The limitations of budgets also existed in this study; by only examining IT and information security budgets, there was a chance that certain budget items might be overlooked or omitted, but by looking at the individual institutions for their specific budgets, this limitation should not hinder the findings of the study (Filkins, 2016). In order to mitigate these limitations, the data was considered to be gathered by survey or questionnaire; but the general consensus across most information security departments is that they are unwilling to forgo the information needed because of privacy issues and the chance of further attacks, therefore archival data was used for the study (Filkins, 2016).

Delimitations

Delimitations existed in this study as well; for instance, this study only explored and gathered security breaches from the last five years. Although security attacks have been occurring for much longer than five years, this kept the information gathered more current, giving results that can be more applicable to today's information security environment (Abdelwahed, 2017). This delimitation provided more valid information given the fact that the information technology field changes so rapidly; if this study were to expand and look further than five years into the past, then some of the data would be too dated to provide reliable information (Vadursi, 2016). Having the study limited to higher education institutions was another delimitation; this was done in order to concentrate on organizations that tend to work off limited budgets and have a harder time getting a large enough IT security budget to make security work more efficiently (Huertas-Garcia, 2016).

Ethical Assurances

The research performed during this study sought approval from Northcentral University's Institutional Review Board by gathering data that was available through online databases and websites. The issue of confidentiality and anonymity was minimal in this study as individuals and human interaction were not required (Weishaupl, 2015). Although certain risk could be an issue, no individuals were identified in this study, only institutions in interest of developing a more cost-effective information security environment for our higher education institutions. Confidentiality was established in this study by assigning the selected higher education institutions an identification number instead of using any identifying information in the results of the study. The issue of security when storing and saving the data was alleviated because all data that was collected was stored on personal password protected data drives, but the data would also have been publicly released. The analyzed data that was gathered and calculated was stored on personal password protected storage and was backed up regularly to ensure that the data was safe and was not able to be accessed. The researcher in this study has over fifteen years of information technology and information security experience and is currently teaching computer science, information technology, and information security at a junior college. The information gathered and the study performed related to higher education due to the interest of the researcher, looking to further the understanding of the information technology field in higher education. The analysis and the study were not influenced or biased given the fact that the researcher strictly teaches the information and does not have influence over the information technology decisions that are made to develop a security plan.

Summary

The research method for this study consisted of several different types of research methods and measurements; all of these ensured proper handling of data and valid results. This chapter has given the proper information needed to conduct the research, starting with the population and the sample sizes needed; using the G*Power application it was found that 66 was the total sample size, allowing for 22 sample sizes per distinct higher education type. After determining the population size and sample size, it was determined that the two different types of measurements being used in this study would be either ratio or interval; these were due to the fact that this study explored the relationship between information security budgets in higher education and their effective security plan (Jogulu, 2011). Additional types of research methods and designs were clarified in this section as well; this included showing that the study was a quantitative study and that the study was performing a correlation study (Grant, 2014). The population and samples were then further elaborated on by exploring the different types of samples, the two-year community colleges, four-year public schools, and private higher education schools. This included exploring how the data would be retrieved, examining that the data collected for this study would be done through archival data and that it would be collected through public websites and databases. The way in which the data was collected limited some of the materials and instrumentation that were needed for the study (Reimer, 2015). The data collected used previously-released peer-reviewed articles and public information that had been released and verified beforehand (Alam 2013). The operational variables were also explored in this chapter, looking at the independent variables that could also be considered predictors and criterion variables and examining the types of values that were expected for these variables (Das, 2016). Study procedures were also explored as was the data collection and analysis type; these two areas

helped to show that the proper analysis was conducted to correspond to the research questions and the hypothesis, showing that the ANOVA and simple regression techniques would be used for the statistical analysis (O'Connor, 2017). In addition to the different types of techniques and designs used in this study, the assumptions, limitations, and delimitations were explored to help understand the study at a deeper level. Some of the assumptions and delimitations examined in this chapter looked at the fact that the study would be limited to the past five years in order to keep the data current (Abdelwahed, 2017). Similarly, some of the limitations discussed in this chapter dealt with the fact that all the data collected was publicly released data and was not gathered using an instrument or tool of some kind (Marchany, 2014). The last portion of this chapter explored the ethical assurances needed to conduct this study. Because the study used archival data and did not involve any human interaction in the study, ensuring ethical standards was quite simple. The methodology and design of this study helped to lead to the findings and resulted in the upcoming chapters, demonstrating that performing this study in the manner it was designed helped in collecting the correct type of data and the amount of data needed. The findings in the following chapter communicate what was found while conducting the research for this study and how these findings can be interpreted.

Chapter 4: Findings

The purpose of this quantitative study was to determine if there is a correlation between the budget and the effectiveness of an information security plan (Marchany, 2014). This study concentrated on the specific area of higher education in an effort to see if a cost-effective information security plan can be developed and still be effective. This chapter includes the examination of the validity and reliability of the data, ensuring that the research data that was collected was collected in such a way that ensures it adhered to NCU IRB's research standards. This section of the chapter is followed by investigating how the results relate to each of the research questions; looking at whether a relationship exists between the three different higher education entities examined in this study. Considering higher education entities such as two-year or community colleges, four-year public colleges or universities, and private colleges or universities helped in determine if a relationship exists. The extent of a relationship, if one is present, are in the statistical methods used for this study; including ANOVA methods, correlational methods, and ratio or interval methods (Comiksey, 2016). Exploring these different types of statistical tools helps determine whether there is a correlation between the amount in an information security budget and the effectiveness of an information security plan (Tiwari, 2017). Determining if a correlation between information security budgets and the effectiveness of an information security plan can then help to determine if an effective information security plan can be established in higher education at a lower effective budget. The validity and reliability of the data will be the next part of this chapter to be explored to ensure that the data was handled correctly and that the proper tests were used in representing the data set.

Validity and Reliability of the Data

The data set used for this study consisted of two main bodies of data, which is why this study used both ratio and interval methods; a ratio scale was used on the number of cyber-attacks, which is the dependent variable, that have occurred because if there is a zero value then it indicates that no attacks have occurred, this is vital information for this study (Filkins, 2016). The information security or information technology budget, which is the independent variable, represented in this study are also ratio methods because also the value of zero shows that no budget was allotted to information technology within the higher education entity (Filkins, 2016). Although both of these values use the ratio method, intervals are still present in both data sets (Jogulu, 2011). Both the independent and dependent variables for this study dealt with higher education entities; therefore, this study consisted of a population estimated at 53,000, which represents all of the higher education institutions within the United States. Because of the values shown using the G*Power application, it was concluded that a sample of 66 schools would be needed to give a fair representation of the overall population; this would depict approximately one percent of the higher education institutions in the United States. The sample size of 66, was broken down into the three different areas examined in this study, twenty-two two-year or community colleges, twenty-two four-year public colleges or universities, and twenty-two private colleges or universities. In order to ensure reliable data within this study, research was conducted within peer-reviewed databases as well as through trustworthy online sources. Conducting this research was completed by searching for higher education institutions that had experienced a cyber-security breach within the past five years; once a subject was found, then it was verified by searching the institutions public website to another reputable source such as www.databreach.net. This process was completed over 80 times to give ample subjects in the study; therefore, if an institution did not meet the

needs of the study, it could be removed and there would still be the 66 sample size schools needed. This was done through public-released information on the internet and through public databases, demonstrating that no preference or requirements were needed to acquire the data. The data collected for this study was done randomly with names of higher education institutions removed, the only commonality between the institutions being that they have been successfully attacked and affected by a security breach. This helped to ensure that the data used for this study was reliable, objective, accurate, and free from error (Comiskey, 2016). Once the required number of subjects were found in the research process, the subjects were double-checked to ensure that there were no duplications in the data so that it would be reliable. The data for the independent variable for this study was collected after the dependent variable information was discovered, because the IT security budget was needed for the higher education institution involved in the cyber-attack. Once the names of the institutions were identified, then the budget information was gathered through their public website information or through other public means, ensuring that this study could be duplicated given the proper citation information. Given that this budget information was gathered from the individual higher education institution's own website, the information should be viable, but it was verified with a minimum of one additional source. After all data for both the independent and dependent variable was verified through two to three sources then the identifying information (the school name) was deleted from the data set and replaced with identifiers such as CC1, CC2, etc. to indicate a two-year or community college, PR1, PR2, etc. to indicate a private college or university, and PU1, PU2, etc. to indicate a public college or university. These identifiers allowed for the data to identify the different types of institutions, without giving school names or identifying them in any other manner. With each of the different types of higher education entities, the budget amounts for the overall school budget, the IT

budget, and the information security budget were all verified to ensure the data set information was complete in order to move forward with the statistical tests. These different institutions were found only in the United States and only fell into one of the three categories described previously--a two-year or community college, a private college or university, or a public college or university. This was all done as stated in chapter three of this study. The higher education institutions were verified that they were all valid two-year, private, or public schools by either public verification or through peer-reviewed journals and studies. The budget amounts were verified by ensuring they were monetary amounts and by ensuring that the IT budget and the IT security budget consisted of a small portion or percentage of the overall school budget. Once all the data was collected to perform the needed statistical tests and the data was verified, then it was narrowed down to reach the required sample size of 66 required by the student; this was accomplished by removing institutions that were outliers and either highly above or highly below the mean of other institutions in either IT budget or IT security budget. After completing this task, it was determined that because so few schools either possessed or publicized their IT security budgets, that for the sake of this study general IT budgets would have be used as the independent variable. This is outside the original design of the study, but it was found that many of the schools found in this data set still operate their IT security budget within their over IT budget (Shamala, 2015). In addition to the information previously discussed, there were several statistical assumptions that were utilized throughout this study. The first statistical assumption was one of normality, which was tested originally using the ANOVA test; this assumption assumes that there are variables in the study that are normally distributed which can be seen with a p value of less than .05 in most cases. In our study the normality assumption proved to be true only when looking at the two-year colleges, as that was the only data set that indicated the p value of less than .05 as

you can see in the U.S. Demographic Data for Higher Education Table. The next statistical assumption seen in this study is linearity which assumes a linear relationship is present between the independent and dependent variable; this assumption was seen because of the use of the Pearson Correlation that was performed in the study. Because these assumptions were not met, a chi-square test was used to see if the values were met under the test conditions; as seen on Chi-Square Table, the chi-square value was at .02 showing that this test value was met.

Chi-Square Table

Chi-Square test results for all higher education institutions

	Value	**Dg**	**Asymptotic Significance (2-sided)**
Pearson Chi-Square	3712.000[a]	3654	.247
Likelihood Ratio	517.428	3654	1.000
Linear-by-Linear Association	.031	1	.861
N of Valid Cases	64		

[a.] 3776 cells (0.00%) have expected count less than five. The minimum expected count is .02.

Note. Chi-Square test results when comparing all higher education budgets to the number of attacks and the number of records affected.

These different statistical assumptions were in addition to the other results that were found for this study which are discussed next in this chapter.

Results

This study attempted to discover if there is a correlation between the amount of money spent in an IT security budget and the effectiveness of an IT security plan, focusing on higher education institutions. The data showed that several schools have not only been affected by cyber-security attacks over the past five years but also, had millions of records affected in the

process. Data for this study was collected from higher education institutions from all over the United States as seen in the U.S. Demographic Data for Higher Education Table.

U.S. Demographic Data for Higher Education Table

Demographic data from all higher education institutions found in study.

ID	Location	Type of School	IT Budget	School Budget	# of Attacks	Records affected
CC 1	Iowa	two-year college	$ 3,631,796.00	$ 336,529,014.00	1	125,000
CC 2	Arizona	two-year college	$ 18,959,154.00	$ 733,181,797.00	3	2,400,000
CC 3	Missouri	two-year college	$ 3,875,802.00	$ 149,399,466.00	1	4,000
CC 4	New York	two-year college	$ 7,845,000.00	$ 415,447,000.00	2	113,000
CC 5	Florida	two-year college	$ 984,150.00	$ 11,547,845.00	1	24,000
CC 6	Tennessee	two-year college	$ 1,747,517.00	$ 64,445,580.00	1	222
CC 7	California	two-year college	$ 2,039,274.15	$ 200,587,073.00	1	unknown
CC 8	Massachusetts	two-year college	$ 36,000,000.00	$ 347,000,000.00	1	5,100
CC 9	Texas	two-year college	$ 18,000,000.00	$ 437,367,742.00	1	unknown
CC 10	Kansas	two-year college	$ 628,448.00	$ 16,037,257.00	1	unknown
CC 11	Florida	two-year college	$ 2,182,072.00	$ 283,547,989.00	3	18,000
CC 12	California	two-year college	$ 500,000.00	$ 63,847,988.00	1	28,000
CC 13	Oregon	two-year college	$ 7,594,994.00	$ 218,133,874.00	1	2,500
CC 14	Florida	two-year college	$ 1,000,000.00	$ 83,063,183.00	1	2,040
CC 15	California	two-year college	$ 57,540,000.00	$ 5,800,000,000.00	2	1,900
CC 16	Illinois	two-year college	$ 3,000,000.00	$ 69,100,000.00	1	1,000
CC 17	California	two-year college	$ 1,281,254.00	$ 125,516,808.00	2	1,000
CC 18	New York	two-year college	$ 1,085,000.00	$ 38,433,000.00	1	45,900
CC 19	California	two-year college	$ 1,305,400.00	$ 50,614,278.00	1	1,200

CC 20	Pennsylvania	two-year college	$ 2,406,875.00	$ 42,997,414.00	1	280
CC 21	New Mexico	two-year college	$ 6,296,800.00	$ 251,704,222.00	1	3,000
CC 22	California	two-year college	$ 2,894,135.00	$ 69,618,340.00	2	3,020
CC 23	Massachusetts	two-year college	$ 780,191.00	$ 26,888,794.00	1	24,000
CC 24	North Carolina	two-year college	$ 1,215,799.53	$ 89,271,210.00	1	5,300
CC 25	California	two-year college	$ 1,052,035.48	$ 80,925,806.00	1	1,910
PR 1	Florida	Private University	$ 150,000.00	$ 3,300,000.00	2	2,100,000
PR 2	Utah	Private University	$ 531,708.00	$ 5,567,486.00	2	2,200,000
PR 3	California	Private University	$ 96,000,000.00	$ 6,800,000,000.00	3	82,000
PR 4	Connecticut	Private University	$ 121,600,000.00	$ 3,800,000,000.00	2	159,000
PR 5	New York	Private University	$ 88,968,276.00	$ 2,688,081,017.00	2	61,001
PR 6	North Carolina	Private University	$ 610,000.00	$ 1,657,000.00	10	540,000
PR 7	Rhode Island	Private University	$ 102,512.00	$ 2,784,376.00	2	1,100
PR 8	Washington	Private University	$ 671,000.00	$ 2,377,000.00	4	290,700
PR 9	Tennessee	Private University	$ 971,000.00	$ 69,200,000.00	1	24
PR 10	Utah	Private University	$ 363,400.00	$ 15,800,000.00	2	600
PR 11	Missouri	Private University	$ 790,000.00	$ 365,900,000.00	2	1,300
PR 12	Virginia	Private University	$ 46,900.00	$ 292,200.00	1	1,400,000,000
PR 13	Texas	Private University	$ 494,252,776.00	$ 3,718,871,628.00	2	33,000
PR 14	New York	Private University	$ 235,287.00	$ 3,888,916.00	2	3,000
PR 15	California	Private University	$ 4,900.00	$ 649,600.00	1	2,580
PR 16	Wisconsin	Private University	$ 247,500.00	$ 10,180,100.00	1	9,500
PR 17	Pennsylvania	Private University	$ 1,784,642.00	$ 300,915,680.00	1	1,020
PR 18	Washington D.C.	Private University	$ -	$ 113,934,622.00	1	1,400

PR		Private	$	$		
19	Virginia	University	5,357,000.00	48,700,000.00	1	110
PR		Private	$	$		
20	Delaware	University	1,100,000.00	50,000,000.00	1	100
PR		Private	$	$		
21	Vermont	University	-	94,000,000.00	1	14,127
PR		Private	$	$		
22	California	University	7,237,161.00	551,581,397.00	1	940
PR		Private	$	$		
23	Maine	University	378,000.00	7,000,000.00	2	493
PR	Pennsylvani	Private	$	$		
24	a	University	1,955,295.00	43,451,000.00	1	10,000
PR		Private	$	$		
25	Oregon	University	596,654.00	118,147,399.00	1	1,536
PU		Public	$	$		
1	Ohio	University	494,932.00	7,177,472.00	2	820,000
PU		Public	$	$		
2	California	University	58,000,000.00	2,900,000,000.00	2	240,000
PU		Public	$	$		
3	Maryland	University	143,438,901.00	2,090,367,669.00	1	300,000
PU		Public	$	$		
4	Florida	University	9,100,000.00	1,730,936,530.00	1	63,000
PU		Public	$	$		
5	Wisconsin	University	5,500,000.00	653,000,000.00	2	173,000
PU		Public	$	$		
6	Vermont	University	4,935,224.00	669,300,000.00	1	37,000
PU		Public	$	$		
7	Iowa	University	1,005,000.00	739,700,000.00	2	30,250
PU	Connecticu	Public	$	$		
8	t	University	13,000,000.00	1,329,800,000.00	3	336,400
PU		Public	$	$		
9	Indiana	University	-	3,700,000,000.00	1	146,000
PU		Public	$	$		
10	Virginia	University	2,620,000.00	3,472,300,000.00	2	1,001,900
PU		Public	$	$ 14,174,274,000.0		
11	California	University	1,045,903.00	0	2	16,000
PU		Public	$	$		
12	California	University	9,228,494.00	415,665,742.00	1	15,000
PU		Public	$	$		
13	Virginia	University	-	1,795,143.00	1	1,880
PU		Public	$	$		
14	Oklahoma	University	34,553,522.00	1,299,092,966.00	1	280,000
PU		Public	$	$		
15	Arizona	University	3,087,000.00	2,586,000,000.00	2	33,000
PU		Public	$	$		
16	New York	University	11,059,994.00	1,136,798,128.00	1	2,690
PU		Public	$	$		
17	Texas	University	844,302.81	2,586,000,000.00	1	114,000

PU 18	South Carolina	Public University	$ 21,569,044.00	$ 1,635,776,458.00	1	3,000
PU 19	Pennsylvania	Public University	$ 1,400,000.00	$ 347,009,000.00	2	48,000
PU 20	North Dakota	Public University	$ 3,612,414.00	$ 94,790,100.00	1	15,000
PU 21	Virginia	Public University	$ -	$ 64,332,963.00	1	381,000
PU 22	Florida	Public University	$ -	$ 44,787,545.00	1	20
PU 23	New York	Public University	$ 135,120,000.00	$ 3,378,000,000.00	1	350
PU 24	Alabama	Public University	$ 20,552,430.00	$ 1,271,000,000.00	1	13,700
PU 25	California	Public University	$ 108,000.00	$ 542,000,000.00	1	500

Note. Data from IT Budgets from various educational sites (2016-2019), for Number of attacks form Data Breaches (2016), and from Number of affected records from Cybersecurity Ventures (2018).

As the U.S. Demographic Data for Higher Education Table indicates, all states within the United States were considered although not all were present in this study; also, the different types of higher education institutions were present throughout all of the United States. While this study looked at higher education institutions as a whole, the evaluation of the three different types of higher education institutions was also explored; the different types of higher education can be further explored in the research question and hypotheses section of this chapter. In addition to how each of these different types of schools relate between IT budgets and cyber-security attacks, the question of what this data shows in relation to the different research questions is one of the main points of this study; this is examined in the next section of this chapter.

Research Question 1/Hypothesis $H1_0$

The first research question looked at the relationship between the IT budget and the number of attacks or affected records among two-year or community colleges. After seeing the results of all the higher education institutions included in the previous section of this

chapter; this section explores two-year or community colleges to see if a correlation exists between IT budgets and the number of attacks. The statistical assumptions with this research question included linear assumptions and equality of variance because an ANOVA was utilized. The linear assumption included assuming that a correlation would exist and that there would be a negative linear relationship between the amount of money spent in information technology budgets and the number of cyber-attacks that took place, where the less money spent on information security budgets meant more cyber-attacks. The other statistical assumption was one of equality of variance, assuming that all groups within the sample were equal; and thus, assuming all higher education information security departments are the same across the different groups. As seen in the Correlational Two-Year College Table; compared to the data from all the higher education institutions there is a level of significance when looking at both the number of attack and the number of affected records with this schools. As you can also see in the Two-Year School's Scatterplot of Attacks and Affected Records Figures, the scatterplots for two-year or community colleges when comparing IT budgets, the number of attacks, and the number of affected records; show a correlation that is slightly positive.

Correlational Two-Year College Table.

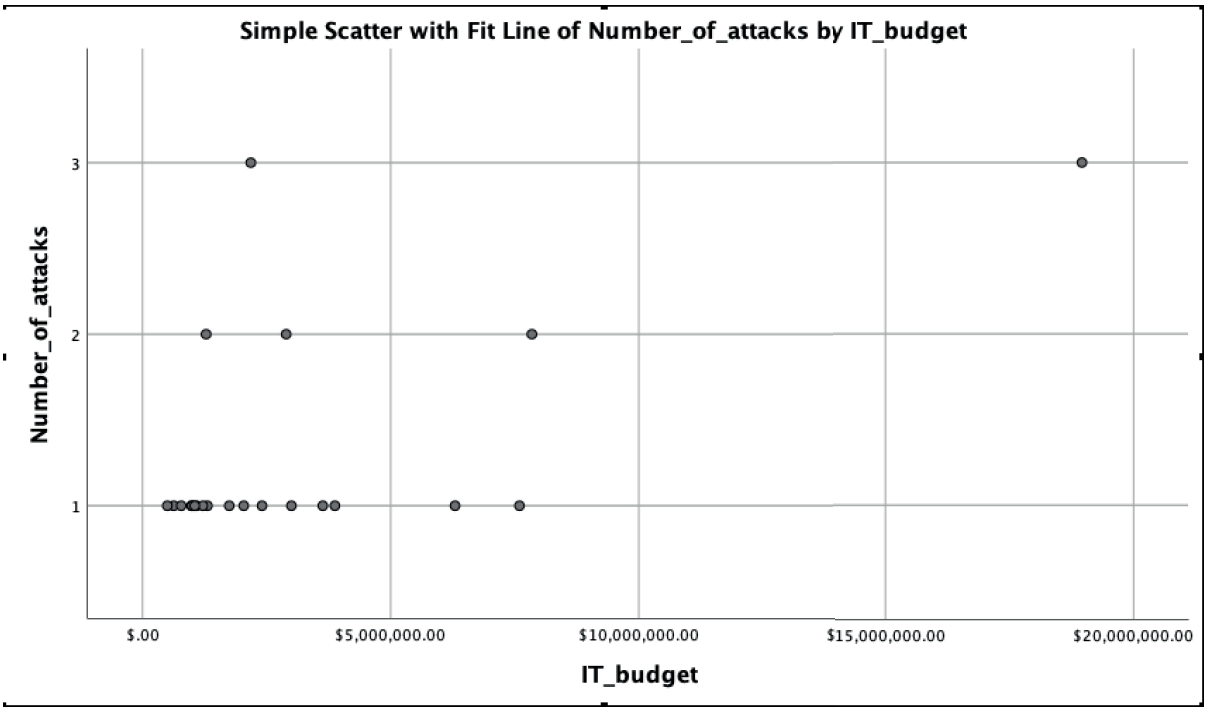
Correlational table showing the relationship between the IT budget and number of attacks and number of affected records for all two-year or community college

		IT Budget	Number of Attacks	Number of Affected Records
IT Budget	Pearson Correlation	1	.561**	.864**
	Sig. (2-tailed)		.007	.000
	N	22	22	20
Number of Attacks	Pearson Correlation	.561**	1	.585**
	Sig. (2-tailed)	.007		.007

	N	22	23	20
Number of Affected Records	Pearson Correlation	.864**	.585**	1
	Sig. (2-tailed)	.000	.007	
	N	20	20	20
** Correlation is significant at the 0.01 level (2-tailed).				

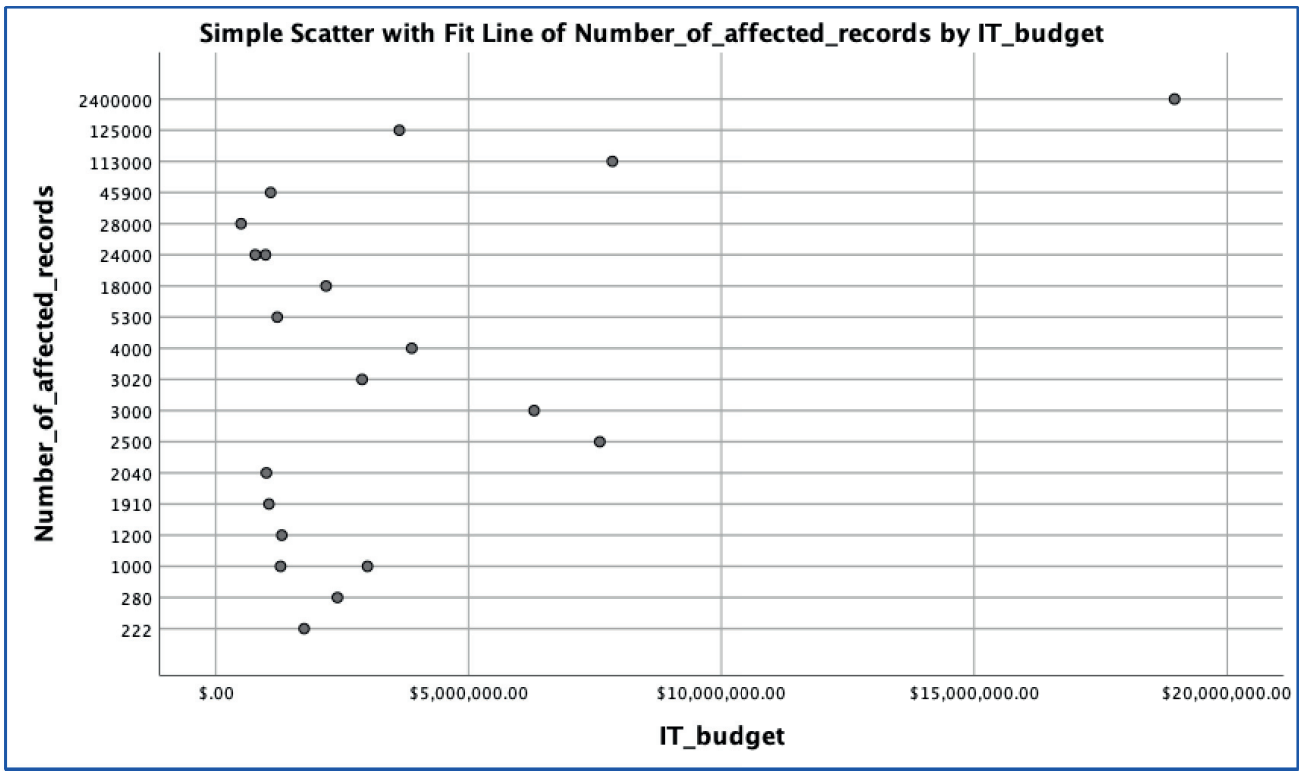
Note. Data from IT Budgets from various educational sites (2016-2019)), for Number of attacks form Data Breaches (2016), and from Number of affected records from Cybersecurity Ventures (2018).

Two-year School's Scatterplot of Attacks Figure



Two-year schools' scatterplot of Attacks: A scatterplot of two-year or community college schools and the number attacks

Two-year School's Scatterplot of Affected Records Figure



Two-year schools' scatterplot of affected records: A scatterplot of two-year or community college schools and the number of affected records

This table and these figures show a slight correlation compared to all the higher education schools, but there is also another option to consider, which is how this data set compares when looking at private colleges and universities. As stated previously, research question one is:

> To what extent, if any, is there a relationship in two-year or community college higher education entities between information security funding and information security effectiveness?

This research question corresponds to the hypotheses of $H1_0$ and $H1_a$, both of which state:

> **$H1_0$.** A correlation does exist when comparing the amount of money spent on information security protection within a two-year or community college organization

and the number of successful attacks and/or breaches that organization has experienced.

$H1_a$. A significant correlation does not exist when comparing the amount of money spent on information security protection within a two-year or community college organization and the number of successful attacks and/or breaches that organization has experienced.

Referring to the Correlational Two-Year College Table and the Two-Year School's Scatterplot of Attacks and Affected Records Figures displaying the results for two-year or community colleges with this data set and using the program SPSS, it was found that there was a correlation between the IT budget, the number of attacks, and the number of affected records within two-year community colleges. As seen in the Correlational Two-Year College Table, the Pearson Correlational test was conducted on these different pieces of data, and it was found that there is a correlation with both the IT budget and the number of attacks as well as with the IT budget and the number of affected records. Given that the G*Power program showed our level of significance to be at .05, the Correlational Two-Year College Table shows that both of the correlations show a significance level even as low as .001. With both of the significant values within the Correlational Two-Year College Table showing to be positive value, then a positive correlation is seen in both of the scatterplots. This information leads this study to adopt hypothesis $H1_0$ which states that a correlation does exist between the amount of money spend on information security within a two-year or community college organization and the number of successful attacks and/or breaches that organization has experienced.

Research Question 2/Hypothesis $H2_0$

The second research question looked at a relationship between the IT budget and the number of attacks and number of affected records among four-year public colleges. After taking exploring this data set, the second data set to consider is that of public colleges and universities. The statistical assumptions with this research question were the same as with the first research question including linear assumptions and equality of variance because an ANOVA was utilized. The linear assumption included assuming that a correlation would exist and that there would be a negative linear relationship between the amount of money spent in information technology budgets and the number of cyber-attacks that take place, where the less money spent on information security budgets meant more cyber-attacks. The other statistical assumption is one of equality of variance assuming that all groups within the sample are equal and therefore assuming all higher education information security departments are the same across the different groups. This data set can be found in the Correlational Public College Table and in the Public School's Scatterplot of Attacks and Affected Records Figures which show the correlational table and the scatterplots between IT budgets and the number of attacks and number of affected records.

Correlational Public College Table

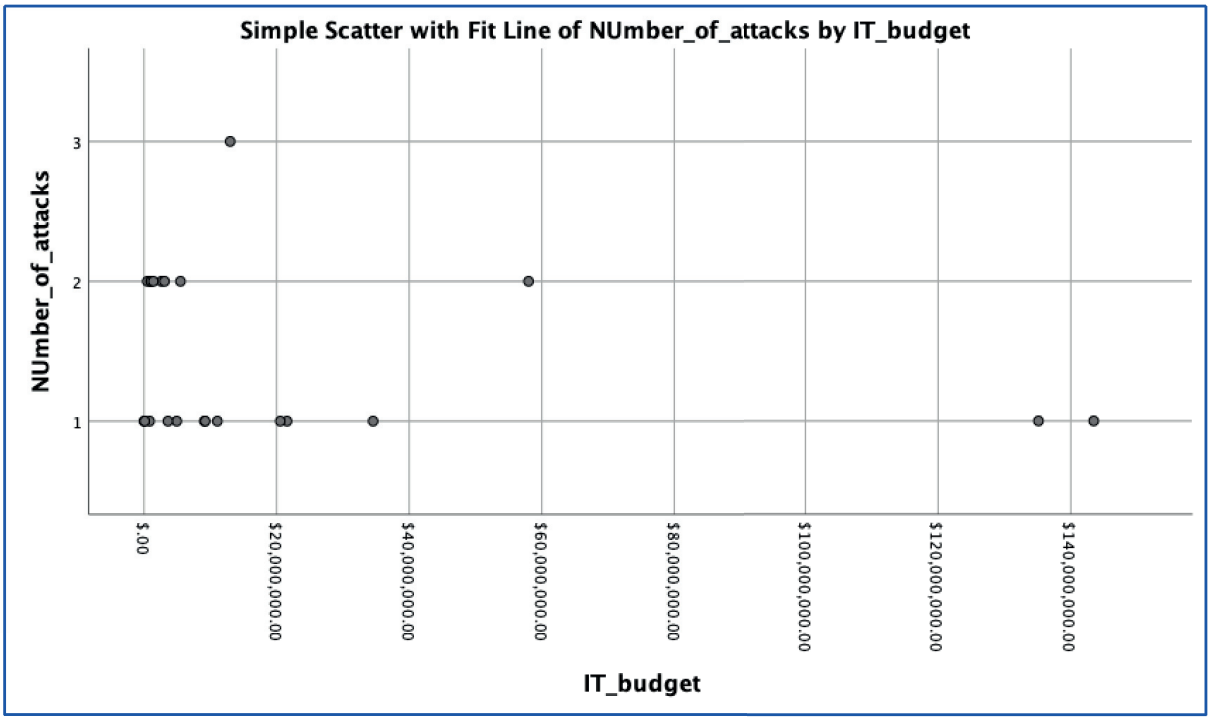
Correlational table showing the relationship between the IT budget and number of attacks and number of affected records for all Public college and university institutions.

		IT Budget	Number of Attacks	Number of Affected Records
IT Budget	Pearson Correlation	1	-.235	-.003
	Sig. (2-tailed)		.291	.990
	N	22	22	22
Number of Attacks	Pearson Correlation	-.235	1	.426*
	Sig. (2-tailed)	.291		.048
	N	22	23	22
	Pearson Correlation	-.003	.426*	1

Number of Affected Records	Sig. (2-tailed)	.990	.048	
	N	22	22	22
* Correlation is significant at the 0.05 level (2-tailed).				

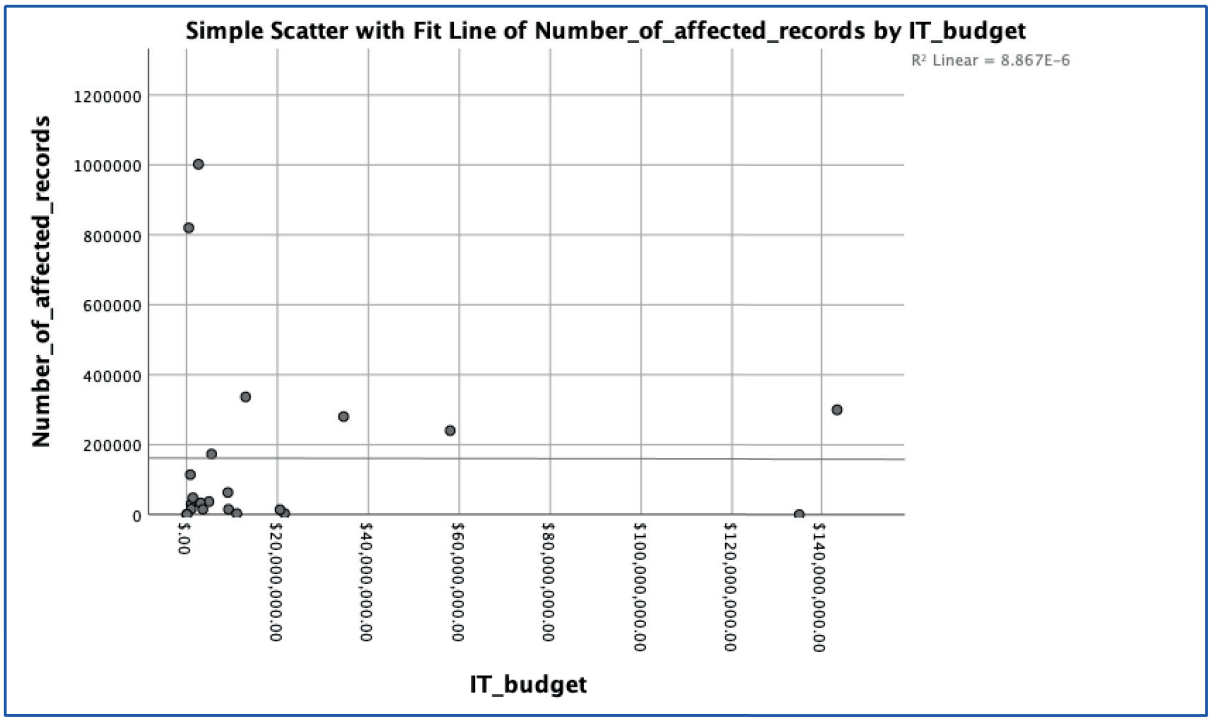
Note: Data from IT Budgets from various educational sites (2016-2019)), for Number of attacks form Data Breaches (2016), and from Number of affected records from Cybersecurity Ventures (2018).

Public School's Scatterplot of Attacks Figure



Public schools' scatterplot of attacks: A scatterplot of Public college schools and the number attacks

Public School's Scatterplot of Affected Records Figure



Public schools' scatterplot of affected records: A scatterplot of Public college schools and the number of affected

As stated previously, research question 2 is:

To what extent, if any, is there a relationship in four-year public college higher education entities between information security funding and information security effectiveness?

This research question corresponds to the hypotheses of $H2_0$ and $H2_a$, both of which state:

$H2_0$. A correlation does exist when comparing the amount of money spent on information security protection within a four-year public college organization and the number of successful attacks and/or breaches that organization has experienced.

$H2_a$. A significant correlation does not exist when comparing the amount of money spent on information security protection within a four-year public college organization

and the number of successful attacks and/or breaches that organization has experienced.

Referring to the Correlational Public College Table and the Public School's Scatterplot of Attacks and Affected Records Figures displaying the results for public colleges with this data set and using the program SPSS, it was found that there was a correlation between the IT budget, the number of attacks, and the number of affected records within four-year public colleges. As seen in the Correlational Public College Table the Pearson Correlational test was conducted on these different pieces of data, and it was found that there is no correlation when considering both the IT budget and the number of attacks as well as with the IT budget and the number of affected records. Given that the G*Power program showed our level of significance to be at .05, the Correlational Public College Table shows that both of the areas dealing with the IT budget were way above this significance level. This information leads this study to adopt hypothesis $H2_a$ which states that a correlation does not exist between the amount of money spend on information security within a four-year public college organization and the number of successful attacks and/or breaches that organization has experienced.

Research Question 3/Hypothesis $H3_0$

The third research question looked at a relationship between the IT budget and the number of attacks and number of affected records among private colleges. The statistical assumptions with this research question are the same as the previous two research questions, including linear assumptions and equality of variance because an ANOVA was utilized. The linear assumption included assuming that a correlation would exist and that there would be a negative linear relationship between the amount of money spent in information technology budgets and the number of cyber-attacks that take place, where the less money spent on

information security budgets meant more cyber-attacks. The other statistical assumption is one of equality of variance assuming that all groups within the sample are equal and therefore assuming all higher education information security departments are the same across the different groups. The set of data exploring the effects on private colleges can be found in the Correlational Private College Table below and in the Private School's Scatterplot of Attacks and Affected Records Figures, which show the scatterplots of the IT budgets and the number of attacks and the number of affected records in relation to private colleges and universities.

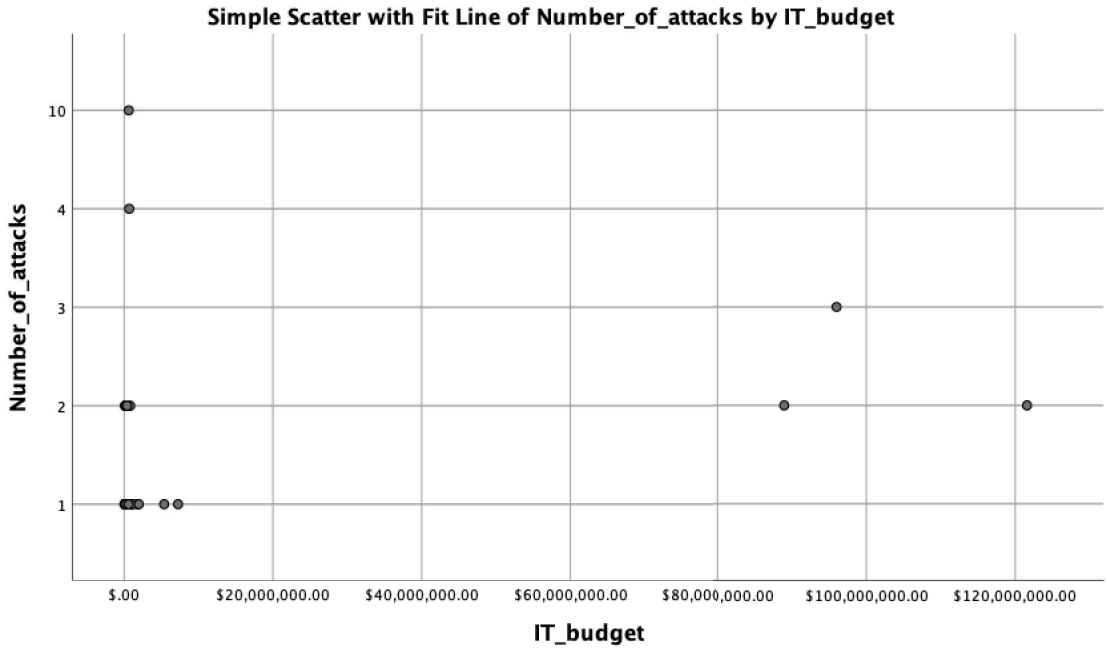
Correlational Private College Table

Correlational table showing the relationship between the IT budget and number of attacks and number of affected records for all Private college and university institutions.

		IT Budget	Number of Attacks	Number of Affected Records
IT Budget	Pearson Correlation	1	.046	-.135
	Sig. (2-tailed)		.837	.551
	N	22	22	22
Number of Attacks	Pearson Correlation	.046	1	.119
	Sig. (2-tailed)	.837		.599
	N	22	23	22
Number of Affected Records	Pearson Correlation	-.135	.119	1
	Sig. (2-tailed)	.551	.599	
	N	22	22	22

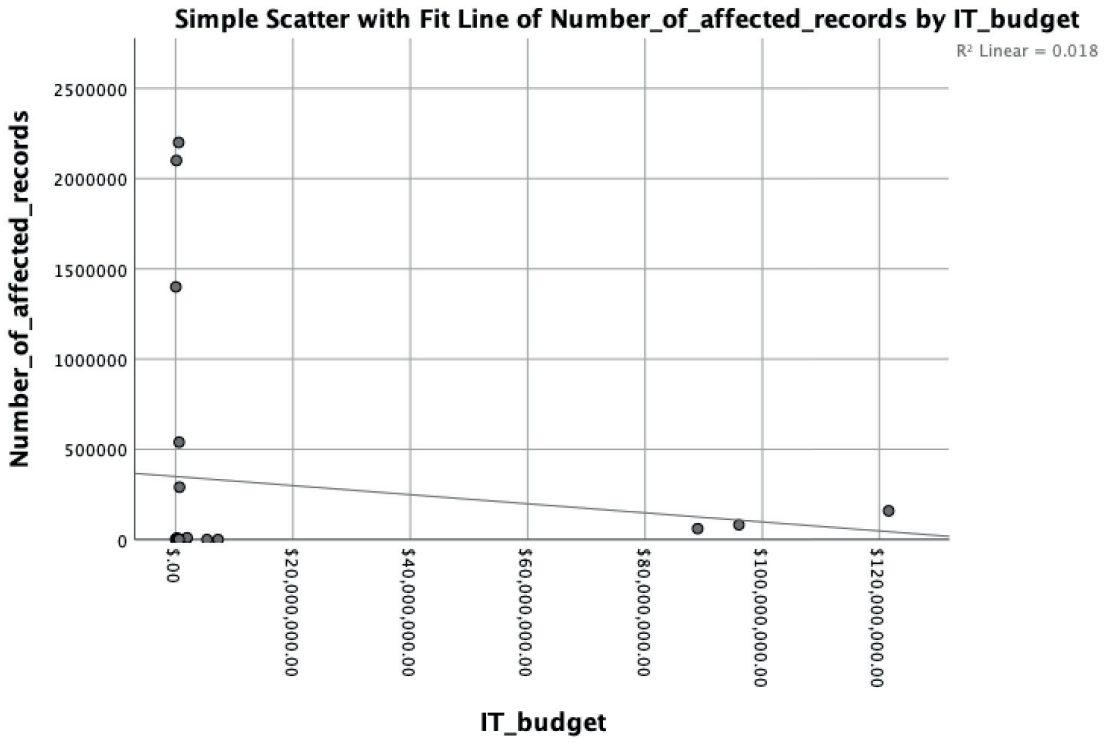
Note. Data from IT Budgets from various educational sites (2016-2019)), for Number of attacks form Data Breaches (2016), and from Number of affected records from Cybersecurity Ventures (2018).

Private School's Scatterplot of Attacks Figure



Private schools' scatterplot of attacks: A scatterplot of Private college schools and the number attacks

Private School's Scatterplot of Affected Records Figure



Private schools' scatterplot of affected records: A scatterplot of Private college schools and the number of affected

It can be seen in the table and in both of the scatterplots that there is no significance between the IT budget and the number of attacks or the number of affected records when considering private schools. As stated previously, research question 3 is:

> To what extent, if any, is there a relationship in private college higher education entities between information security funding and information security effectiveness?

This research question corresponds to the hypotheses of $H3_0$ and $H3_a$, both of which state:

> **$H3_0$.** A correlation does exist when comparing the amount of money spent on information security protection within a private college organization and the number of successful attacks and/or breaches that organization has experienced.
>
> **$H3_a$.** A significant correlation does not exist when comparing the amount of money spent on information security protection within a private college organization and the number of successful attacks and/or breaches that organization has experienced.

Referring to the Correlational Private College Table and the Private Schools Scatterplot of Attacks Figure and displaying the results for private colleges with this data set and using the program SPSS, it was found that there was a correlation between the IT budget, the number of attacks, and the number of affected records within private colleges. As seen in the Correlational Private College Table, the Pearson Correlational test was conducted on these different pieces of data, and it was found that there is no correlation when considering both the IT budget and the number of attacks as well as with the IT budget and the number of affected records. Given that the G*Power program showed our level of significance to be at .05, the Correlational Private College Table shows that both of the areas dealing with the IT budget were way above this significance level. This information leads this study to adopt

hypothesis $H3_a$ which states that a correlation does not exist between the amount of money spent on information security within a private college organization and the number of successful attacks and/or breaches that organization has experienced. In addition to these three different research questions, there is also data present examining all of the higher education institutions. Using the program SPSS, a correlation table was developed to show the correlation between the different institution's IT budget and the number of attacks that have occurred as well as the number of records that were affected. Please see the Correlational Table of All Higher Education Institutions.

Correlational Table of All Higher Education Institutions

Correlational table showing the relationship between the IT budget and number of attacks and number of affected records for all higher education institutions.

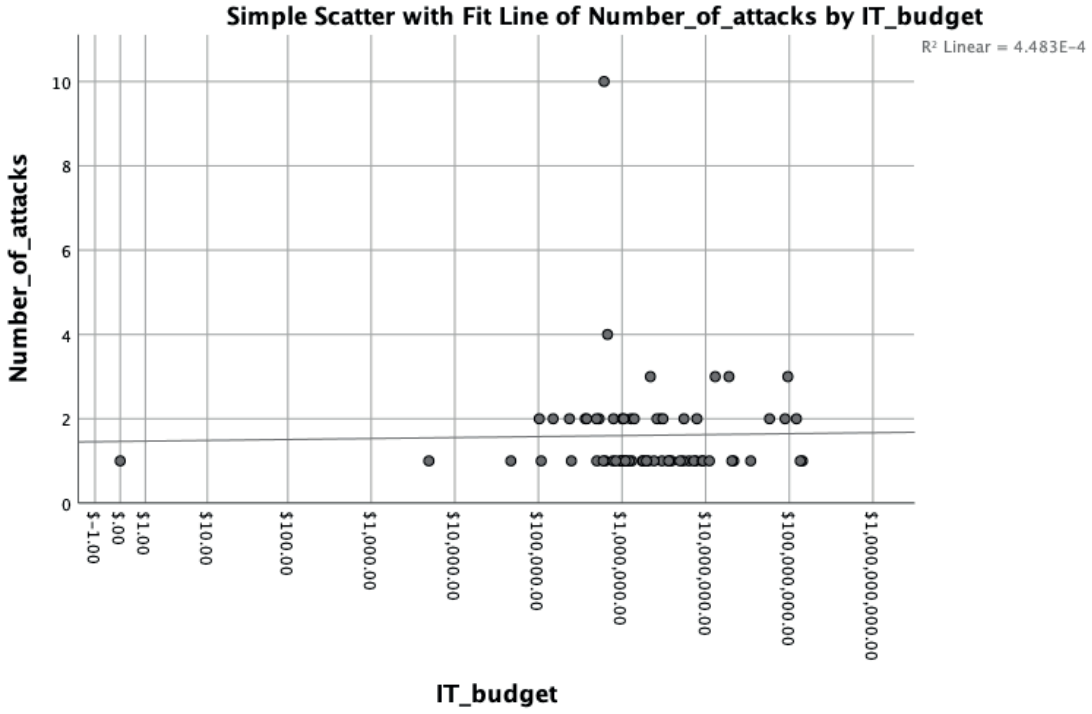
		IT Budget	Number of Attacks	Number of Affected Records
IT Budget	Pearson Correlation	1	.012	-.054
	Sig. (2-tailed)		.923	.672
	N	66	66	64
Number of Attacks	Pearson Correlation	.012	1	-.062
	Sig. (2-tailed)	.923		.627
	N	66	67	64
Number of Affected Records	Pearson Correlation	-.054	-.062	1
	Sig. (2-tailed)	.672	.627	
	N	64	64	64

Note. Data from IT Budgets from various educational sites (2016-2019)), for Number of attacks form Data Breaches (2016), and from Number of affected records from Cybersecurity Ventures (2018).

As seen in this table, the correlation between the IT budget and the number of attacks at all the different higher education institutions is equal to .012, while the correlation between the IT budget and the number of records affected throughout all institutions is equal to -.054. These two values also indicate that the IT budget and number of attacks has a significance

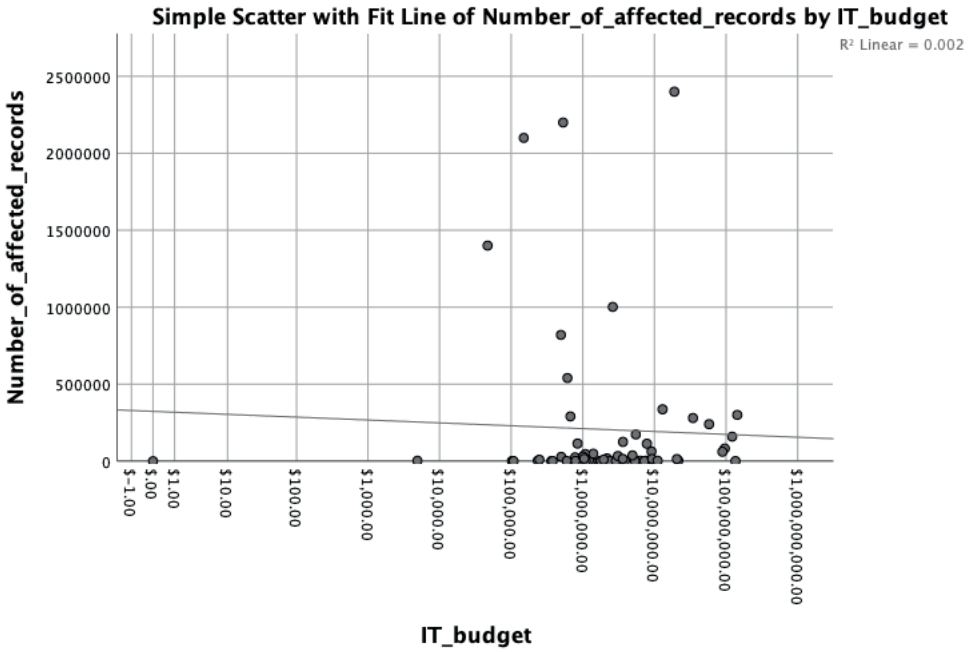
value of .923 and the IT budget and number of affected records has a significance value of .672. Both of these values are much higher than that previous significance value of 0.05 given using the G*Power program (see the G*Power Figure); this indicates that when looking at the IT budget and including all higher education institutions, a correlation does not exist. This can also be seen in the All Schools Scatterplot of Attacks and Affected Records Figures, a scatterplot of all this data that produced the correlational table in the Correlational Table of All Higher Education Institutions.

All Schools Scatterplot of Attacks Figure



All schools' scatterplot of attacks: A scatterplot of all schools and the number of attacks on the schools

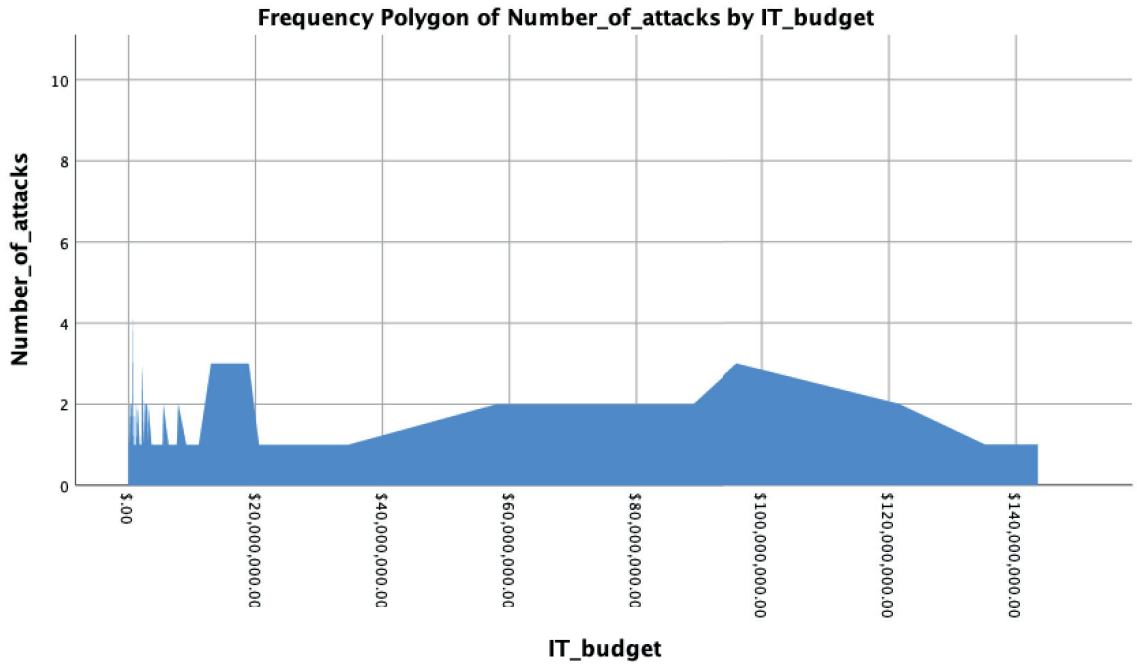
All Schools Scatterplot of Affected Records Figure



All schools' scatterplot of affected records: A scatterplot of all schools and the number of affected records

As seen on both of these scatterplots, a linear regression is present but there is no correlation present between these different variables. In addition to these scatterplots, a histogram can be seen in the All Schools Histogram of Attacks Figure showing the overall number of attacks related to the IT budget for all higher education institutions found in the study.

All Schools Histogram of Attacks Figure



All schools' histogram of attacks: A histogram of all schools and the number of cybersecurity attacks related to the IT budget for the schools.

Evaluation of the Findings

Given the results shown in the previous section in relation to the research questions and the different hypotheses, the theoretical framework must also be re-evaluated. In this study the theoretical framework followed the theory of resourced-based view (RBV), which establishes that different information security investments are used to obtain security assets to protect investments (Weishaupl, 2015). This theory explores the use of tangible and intangible resources such as firewalls, security knowledge and other areas used to protect and cover IT information; while these different areas were not directly evaluated in this study, indirectly they are measured through the number of attacks and the number of affected records at each higher education institution (Weishaupl, 2015).

Research Question 1/Hypothesis $H1_0$

Looking at the first research question and given the results found in the Correlational Two-year College Table it can be seen that the investments made by two-year or community colleges did, at some level, protect the assets of the information security system given that there is a positive correlation between the IT budget or the investments in IT security and the number of attacks and number of affected records. Similar data can be found in other studies that showed having IT security infrastructure in place can aid in the protection against cyber-attacks (Hosban, 2015). Additional studies have now shown how employees within a school or organization can help in protecting against cyber-attacks as well, while they are working with the tools that are in place (Wong, 2015). Many of these two-year schools show that not only does having an IT security plan and tools in place help keep their data and system safe, but the added protection of a disaster recovery plan, can aid in keeping data protected from cyber-terrorists (El-Temtamy, 2016). Although these findings are similar in certain studies, it is also found that even with a multitude of information security tools and plenty of protection, cyber-attacks and breaches still occur (Shamala, 2015).

Research Question 2/Hypothesis $H2_0$

Another data set of the study, four-year public school did not show a correlation between the IT budget or the investment and the overall IT security system; this does not necessarily mean that the RBV theory is untrue as it is outside the realm of this study to see the number of attacks that would have occurred if no IT budget or investment was made at the different institutions. When observing the second research question and hypotheses $H2_0$ and $H2_a$ it was found that there was no correlation, and as seen in the Correlational Public College Table there is no significance in the data sets. This indicates, according to our study, that there is no correlation between the amount of money spent on information security and the number of cyber-attacks. This is seen in many articles in the last five years, indicating that in

four-year public schools if cyber-terrorists want the data at a school, they will find a way to get it (Sembiring, 2015). Additional studies have shown this to be true on other fronts within the public-school area as well, in particular the portion dealing with the amount of training that is given to all support staff in a school. Public schools can have a tendency to employ more support staff to support the large number of students but, if they are not trained properly, they will allow cyber-attacks to occur (Kaptein, 2015). Other articles dealing with four-year public schools show that part of the cyber-terrorist threat occurs because many higher education institutions are ill-prepared due to overall budget constraints within higher education and smaller or non-existent information security budgets (Marchany, 2014). Studies have also indicated that cyber-attacks will occur no matter what, so an information security budget may help in some form but will not make a significant difference (Imboden, 2014).

Research Question 3/Hypothesis $H3_0$

The final research question and $H3_0$ and $H3_a$ addressed the relationship between information security and budgets in private higher education institutions. If you refer to the Correlational Private College Table you are able to see that there is no correlation between the amount of the information security budget and the number of cyber-security attacks; in fact, just as with the last research question, it can also be seen in the Correlational Private College Table that there is no significance between the different variables. As with the other two subsets of this study, the private schools are also likely to get attacked because of their lack of preparation or secure network (El-Temtamy, 2016). Given that private schools, like public and even some two-year schools, have massive amounts of data also makes them a bigger target which could affect the number of attacks related to the budget money they spend each year (Abdelwahed, 2017). Another factor that comes into place with both public and private

schools is the fact that cyber-attacks and cyber-crimes have grown exponentially over the last ten years, meaning that at some point no matter how much money is spent on information security, attacks and breaches are going to occur anyway (Prislan, 2016). With all these different aspects of information security and information security budgets, at least it is clear that the goals of this study were achieved by determining which hypotheses to adopt and which research questions were proven true and which were proven false. This study completed the task of using the same sample size of 66 higher education institutions that was established previously and then breaking that sample size into three different categories, which included two-year or community colleges, four-year public colleges, and private colleges; then, using public information gathered pertaining to these entities, the previous data was extracted. This data simply showed that when looking at the different research questions within this study, research question one was the only one that indicated a correlation exists between information security funding and information security effectiveness. This also showed that research question two and three did not show a correlation between information security funding and information security effectiveness. These pieces of information indicate that hypothesis $H1_0$ can therefore be adopted and both $H2_a$ and $H3_a$ null hypotheses have to be adopted when considering other higher education institutions. The only conclusion that can be derived from this information is that two-year or community colleges do have a positive correlation between information security funding and information security effectiveness, indicating that on this level the amount of money spent on information security will determine how effective an information security plan will be in thwarting attacks and breaches at an institution.

Summary

Throughout this chapter different aspects of this study and the methods needed to perform the data analytics were discussed, starting with a look into this quantitative study. Examining the different types of methods used in this study, including an ANOVA test, and using programs like G*Power provided the proper information to start the data sets for this chapter, by determining the proper population and sample size that is needed to conduct a study like this. Throughout the validity and reliability section of this chapter, it was found that both the independent and dependent variables used ratio and interval data recording IT budgets and the number of attacks and number of affected records at each higher education institution. The data for this study was also collected by using public-released websites and databases and by researching higher education institutions that had suffered from a cyber-attack within the last five years; then, once the list of schools was discovered and verified, their public websites or other publicly-released information was researched to find the corresponding school's budget information. This research was conducted approximately 80 times in order to find the required sample size of 66; within this sample size were three distinct types of higher education institutions: two-year or community colleges, four-year public colleges, and four-year private colleges. After finding the required data for the study the data was then verified; the number of attacks were verified by other peer-reviewed articles and journals and the budgets were verified by examining the monetary amounts and comparing the percentage of the IT budget to the overall school budget. At the conclusion of all the data verification process, all the identifying markers were removed, and the schools were given corresponding variables, consisting of CC# for the community colleges, PU# for the public colleges, and PR# for the private colleges. In addition to verifying the data used in the study, the validity and reliability section of the chapter also examined some of the

statistical assumptions that were addressed in this study. Some of the assumptions included normality, which was explored using an ANOVA test, and a linear assumption using the Pearson Correlation; since the linear test was not met, a Chi-Square test was run, but it also failed to meet the requirements. The examination of the data and how it related to the research questions and the different hypotheses was also discussed. Using the Pearson Correlation test it was found that our first section, which deals with two-year or community colleges, contained a correlation between IT budgets and the number of attacks and the number of affected records. This can be seen in the Correlational Two-year College Table and the Public School Scatterplot of Attacks and Affected Records Figures. The same tests were run on the second and third sets of data, which dealt with four-year public colleges and private colleges, and it was found that neither of these data sets contained a correlation between the IT budgets and the number of attacks and the number of records affected. The study concluded by accepting the hypothesis $H1_o$ and accepting the null hypotheses of $H2_a$ and H3; this corresponded to accepting research question one and rejecting research questions two and three. The only conclusion that can be drawn from this chapter is that two-year or community colleges do have a relationship between IT budgets and effective IT security, while the other two data sources in this study do not have this same relationship.

Chapter 5: Implications, Recommendations, and Conclusions

The problem addressed in this study was that some organizations tend to have problems implementing an effective information security plan because of inadequate or low information security or information technology budgets (Marchany, 2014). Without proper preparation and installation of information technology and information security in an organization, there can be no consistency of information security protection, which can lead to damaging an organization's reputation, income, and overall business through unwanted attacks (Abdelwahed, 2017). The proper budget can assist any type of organization in developing and maintaining an information security plan that will help in protecting the organization's information (Imboden, 2014). The purpose of this quantitative study was to determine if there is a relationship between the budget money that is spent in an information security or information technology department and the effectiveness of that department's information security protection (Marchany, 2014). This correlational study was explored through studying both the budgets of information security departments and the number of successful attacks that have taken place within that department. The ability of an organization to take a smaller budget amount and ensure that information security is effective can help keep their business remain on top (Adler, 2015). This study was conducted using the resourced-based view (RBV) theory, which states that different resources can be purchased and used in order to protect information within an organization (Weishaupl, 2015). This study used both the ratio and interval types of research when dealing with the type of data collected to find the information desired (Filkins, 2016). The type of data used in this study included both information technology and information security budgets and the number of cyber-attacks that had successfully occurred in an organization within the past five years.

All of the data used in this study was collected through public databases and public websites, and all identifying information was removed from the data to ensure that proper anonymity could be safeguarded (Jogulu, 2011). In order to ensure this study was confined to a helpful arena, the data collected was limited to higher education institutions. The research questions and hypotheses for this study consisted of looking at three different categories of higher education institutions: two-year or community colleges, four-year public colleges or universities, and four-year private colleges or universities. Using statistical software, it was determined that approximately one percent or 66 higher education schools would be a valid sample size for the study; this sample size of 66 was then broken down into the three categories, which led to a sample size of 22 schools per category. After being collected, the data for this study was broken down into the three different categories and then all the data for the information technology budgets and the number of cyber-attacks that had occurred were compiled in order to complete the data. This data set was then given generic names of the three different types of categories of higher education institutions and the identifiable college names were removed in order to keep the study fair and ensure validity. The results of this study consisted of findings within each of the three categories and within all higher education institutions as a whole; each data set was run through the statistical tools in SPSS to find different aspects of a correlational relationship. The data found considering all higher education institutions was that there was no correlation present, with the significance value much higher than the required 0.05.

When exploring the different research questions and hypotheses, each one resulted in different outcomes. Research question one dealing with two-year or community colleges was the only data set that resulted in a correlation being seen; the data found from SPSS showed that the significance level when looking at two-year schools was well within the 0.05; it was

even within the 0.01 level within this study. This shows that when looking at two-year schools that there is a slight positive correlation between the amount of money spent on IT or information security budgets and the number of cyber-attacks that occur or the number of records that are affected because of attacks. The second research question explored four-year public schools and the data set showed through a correlation chart and scatterplot that there was no correlation present; the significance level being well over 0.05 making the data clear. The third and final research question examined private colleges and universities and the data set for this category of colleges showed similar data as the public schools did, with no correlation present and the significance level being well over 0.05.

Overall these findings show that the amount of money spent on information security does not directly affect the number of attacks that may occur within an institution; although two-year schools do show a slight correlational relationship, it isn't enough to refute the remainder of the findings. One reason that the first research question may have been the only data set to show a correlation is due to some of the limitations that this study possessed. The first limitation in this study is that the data was collected from archival data from public databases and websites; this is mainly because most organizations would be unwilling to release information security attack information in fear of another attack. There is also the limitation of the budget; the only budgets examined in this study were information technology and information security budgets. After acquiring and exploring all the data for the study, it was found that too few higher education institutions either did not have an information security budget or they did not make it public, this caused the information technology budget to be used in the confines of this study. The remainder of this chapter explores the implications of these findings and the recommendations for future research and possible security practices.

Implications

The findings of this study have several implications for both the world of higher education and information security. Research question one examined the relationship between the IT budget and the number of attacks and number of affected records within a two-year or community college, more specifically looking to see if a relationship between these two areas existed. As with most studies, there were some statistical assumptions, like linear assumption and equality of variance, both of which were addressed using additional testing. After the collection of the data, the hypothesis corresponding to this research question was accepted because it was found that there was a slight positive correlation between the amount of budget money spent on information technology and the number of attacks that were successful at the corresponding school. These findings did confirm what many articles found, and that is that cybercrimes are continuing to grow and will happen to organizations no matter how much money is spent on protection (Kayode, 2016). Even though when examining the two-year schools it was not possible to explore the details of their information security plan, the premise was that the development and contents of a sound information security plan can be seen in the number of attacks that took place in the two-year schools (Alavi, 2016). The fact that some studies have found that smaller IT security budgets and smaller schools or companies are in more danger from cyber-attackers was not confirmed in this research question (Marchany, 2014). Another area that this study did not explore but many articles focus on is how cyber-attacks and breaches affect the organization after they have been attacked; this study strictly looked at the relationship between the amount of money spent on information security and the number of attacks (Leukfeldt, 2015).

Looking at the second research question there are some similarities that can be found, but there are also several differences. Research question two examined whether a relationship

is present between a four-year public college's IT security budget and the number attacks that have taken place. As with the first research question, statistical assumptions were also present; the linear assumption and the equality of variance were both dealt by using additional testing. With the data that was collected the null hypothesis related to this research question was accepted; this was due to the fact that there was no correlation found between the IT budget of four-year public schools and the number of attacks or number of records affected. There are some factors that could have resulted in these findings as well, such as where the school is located and how popular or publicized the school is; these factors could draw in potential attackers. These findings appear to be more in line with other research that has been performed on this topic, showing that while colleges and businesses have spent billions of dollars on information security, cyber-attacks and security breaches still continue to occur (Filkins, 2016). Just as with examining the two-year schools, the ability to gain access to look at a school's IT department and their information security plan or system was not available; the assumption remains that there is some sort of coordinated information security plan in affect (Abdelwahed, 2017). The outcomes of this research question also support other research that states that more hackers and cyber-terrorists are being drawn to higher education because of the open-access philosophy and the knowledge of lower budget issues within these organizations (Dreyfuss, 2016). When compared with the first data group, these four-year public schools tend to have a much larger IT budget than the two-year schools in the study, but there is still the fact that many articles mention higher education budgets being only a fraction of industry and business budgets, thus making it harder to up with attackers (Liu, 2016).

The final research question also suggests some similarities with the two previous research questions, but there are still some minor differences. The third research question

examined whether a relationship exists between four-year private school's IT budgets and the number of attacks or the number of affected records. The same statistical assumptions that were present in the first two research questions were also assumed with this research question, and additional tests were used to verify the data. After the data was collected the null hypothesis on this research question was adopted, because just as with the second research question there was no evidence of a relationship between the schools' IT budgets and the number of attacks or number of affected records. Some of the same factors that were present with the four-year public schools also existed with this data set, like the location of the school and how it is publicized but being private schools, they are generally not as well known. Other factors like the number of donors that are present for these private colleges and the nature of their donations could play into how the private college's budget money is spent. This four-year private school data set also showed similar information that has been found in other studies such as how important it is to keep donor and other information confidential and safe from cyber-attacks (Mubarak, 2016). As with other higher education institutions, these private schools have to be very mindful of their budget and ensure there is a proper balance between the money spent on information security and the protection it provides; this process can take years to perfect (Radulescu, 2016). Without the ability to look into the inter-workings of the IT budget of these private schools, it was impossible to see if the correct type of information security budget was developed as is recommended in many articles on this subject (Subsermsri, 2015). These findings also show that precedence or some kind of priority must be given to information security budgets in order for them to make a noticeable effect on cyber-attacks (Filkins, 2016). As seen in many other articles this priority can alleviate the need for higher education institutions to divert and move money to information security as a result of attacks that occur due to the lack of proper development and budgeting

(Bere, 2015). Of course, as shown in many studies, even if the proper planning and budgeting take place and every possible proactive step is taken, cyber-attacks can still occur, making the job of protecting an institution's data especially difficult (Iosifovitch, 2016). The ending result in regard to all three data sets is that information security planning and development is always going to be difficult as hackers and cyber-terrorists are constantly changing and finding ways to get the data they want (Kayode, 2016). These implications have led to different recommendations in both practice and in future research, which is discussed in the next section of this chapter.

Recommendations for Practice

As seen in many articles related to information security and the protection of data, there is almost always room for recommendations to help keep organizations from being breached and from losing important data (Kayode, 2016). Because two of the three research questions ended up adopting the null hypothesis over the recommended hypothesis, a recommendation of developing an algorithm or process in which the proper budget money can be maintained and then applied to construct the most effective information security plan would be ideal. Although this recommendation sounds very unlikely or difficult to accomplish, through proper data analysis and planning an effective security plan can be established while spending only a certain required amount of money to ensure an organization is protected properly. As seen in other articles, this process has been attempted before and has had very little success; the proper development of IT rules and regulations coupled with an efficient budget can accomplish this goal (Hryszkiewicz, 2015). This process, although possible within the higher education world, would be much more difficult because it requires not only the development of proper policies and procedures but also a highly educated IT

security staff to perfect and carry out the plan; given the budget constraints in the education field, hiring such a staff would be difficult at best. (Abdelwahed, 2017).

An additional recommendation is to attempt to acquire larger information security budgets in order to increase the tools and overall training of the information security staff in a higher education institution. Given that this study found the current budgets being spent on information security lead to attacks and in many cases a large number of records exposed, the introduction of more tools, new utilities, and proper education of employees could have a significant impact. With the increase of available information security tools and utilities an organization can both prevent information security attacks and at the very least can recover from any attack or breach much quicker, helping the organization in the future (Alavi, 2016). Many organizations have only minimal information security tools and nothing that is effective enough to allow for an organization to be proactive; with proper tools and utilities these organizations and schools could help catch harmful files and attacks either before they happen or quickly after they take place (Choong, 2017). In addition to the introduction of more tools and utilities, the proper and continual training of information security staff and overall employee staff would drastically improve an organization's information security outlook (Sommestad, 2015). Many studies have found that over half of the information security breaches that occur are because of employees improperly trained or educated in the area of information security; this recommendation could change the nature of information security if more employees were properly educated (Michelberger, 2016). In addition to these recommendations, the focus of future research can aid in the area of information security in higher education.

Recommendations for Future Research

As with many studies, certain questions get answered through the collection and analysis of the data, but during this process additional questions become clear and call for future research. This study suggests a few different areas of research that could be completed in the future, a deeper and better understanding of what organizations currently put into setting up their information security plan. Exploring the development of an information security plan could become much more effective with more collaboration between entities. In this study information security plans are discussed, and certain aspects are examined in more detail, but a complete and better understanding would help an organization to better defend and protect their digital assets (Prislan, 2016). The data was limited to only that of IT budgets and the number of attacks and the number of affected records were examined, by exploring information security plans in more depth a better understanding could allow for different results in a study like this moving forward. Having the ability to explore and gain a deeper understanding of an information security plan could aid all organizations in defending their networks; from this study it is seen that the amount of budget money spent on IT budgets does not directly affect the number of attacks in most cases, but a more thorough understanding of information security plans could help in future to produce different results in a study similar to this one (Ahmad, 2014). Future research in this area could also help to work within the current theoretical framework found in this study because a deeper understanding of an information security plan can help to see what assets were purchased or acquired in order to protect the investments of these organizations (Weishaupl, 2015). But, other areas of study can be derived from these results, instead of strictly focusing on the information security plan.

Another area where future researchers can improve on this study is expanding on the information gathered from the schools in higher education; this study conducted an archival

data gathering, whereas in the future, if researchers were able to get direct information from the universities and colleges in the study, then the outcomes could vary. By using direct data from schools in a study, further insight could be given as to exactly how money was spent in information security budgets as well as how many exact attacks took place and maybe even number of attempts that were made on the institution. Many organizations are skeptical in giving out this information at this time because of fear that it could lead to the possibility of divulging more information and leading to more attacks; whereas in the future this information could be gathered in a manner in which this information could be safeguarded (Choong, 2017).

A better understanding of the budget process will allow for future researchers to see where information security tools and utilities are being purchased or acquired and to see what areas could be approved upon in order to spend the information security budget more efficiently (Nagurney, 2017). As this study shows, the budget portion of information security is just one side of the an effective plan that helps to protect from cyber-attacks; the information security plan is just as vital as the budget process and without a proper plan in place that covers every aspect of information security an organization can be left unprotected (Gao, 2015). In addition to further insight into the information security budget and the information security plan, future researchers could gather direct information about the number of cyber-attacks and attempts that were made against the school; this could help to see if the correlations that were used in this study are accurate using direct information compared to archival data. Although studies have shown that no organization is completely secure, future researchers could use this direct information in order to determine whether or not there is a formula between the amount of budget money spent and the contents of an information security plan that works best to defend against cyber-attacks (Adler, 2015).

A third area that can be used for future research is in the comparison of findings in this study with how budgets and number of cyber-attacks relate to industry or corporate America. This study has shown that in most cases there is no correlation between the amount of information technology budget spent and the number of attacks that take place within a higher education institution; future researchers could try to find out if the same is true of industry businesses given that they generally have a much larger IT budget (Liu, 2016). One area that could be problematic for future researchers is that given that higher education institutions are hesitant to give up their information security information, businesses might be even more hesitant because of their competitive nature (Radulescu, 2016). This concern corresponds with the limitations within this study; but if that could be overcome by future researchers, the data that is collected might be very useful in helping to develop a sound information security plan.

Even though some of the higher education schools had very large IT budgets, there are a few areas that would different in the business world, which could provide good comparison information; the amount of money spent on an IT budget would be good to compare as would the number of information security budgets that are readily available compared to that of higher education. One of the limitations of this study was that very few information security budgets were available in the archival data that was presented, which lead to the use of IT budgets instead; this difference when examining businesses could make a large difference in the budget amount and how much is actually spent on information security. Certain areas of future research could be highly beneficial to the world of information security if done correctly, and in the way in which the data is collected to ensure the data is as accurate as possible; this among other topics will be elaborated on in the next section, the conclusion of this study.

Conclusions

Information security is a topic that is becoming more prevalent every passing day, and the manner in which we protect our information from cyber-attacks and cyber-terrorists is becoming more and more crucial (Zafar, 2016). This statement is true of all areas around the globe, but the emphasis of this study is in the area of higher education; this is done because many studies have found that higher education has to fight information security using a smaller budget and at times with a less knowledgeable information technology staff to get the job done (Imboden, 2014). Given these realities about higher education, the problem addressed in this study is that some organizations have problems implementing an effective information security plan because of inadequate or smaller budget (Marchany, 2014). This study is important from several different aspects for higher education; the IT budget was examined to ensure the information security was a priority in order to provide adequate protection, and the number of attacks were examined to show how effective IT budgets can be within a higher education institution. These different aspects of the study came together to show if a relationship between the amount of money spent on information security and the number of attacks that occurred was present, helping higher education institutions to see if an efficient and effective information security plan could be developed. As higher education entities generally have less money to spend on information security, the emphasis of this study was to show that the amount of money spent on information security is not directly related to the number of attacks that occur at an institution (Dreyfuss, 2016).

The data for this study was gathered using archival data available from free public locations, such as websites, databases, and articles; this limited some certain aspects of the study, but the data was still able to provide the information needed to form a firm conclusion. This data was then broken into three different data sets, each examining a different type of

higher education entity. The first looked at two-year or community colleges, the second looked at four-year public colleges, and the third looked at four-year private colleges. The data that was collected and examined gave slightly different results depending on the type of higher education system examined, but the same general result was found in two out of the three types of schools. When exploring the results within two-year schools, the data showed that there is a correlation between the amount of IT budget money that was spent and the number of attacks that occurred. In contrast, when exploring the data of both the four-year public and four-year private schools, it was found that there was no relationship between the amounts of money spent on IT budgets and the number of attacks.

The outcome to take from this study generally is that there is no relationship between the amount of money spent on information security and the number of attacks an institution will endure; this means that cyber-attacks or breaches will occur, no matter what protection plan is in effect. This does not mean that no protection should be in place; as seen with our two-year schools, proper information security protection can be achievable with smaller amounts of budget money. In relation to previous studies done on this topic, the results of this study are consistent with the fact that cyber-attacks will take place, no matter how many information security tools and systems are in place; having information security plans and budgets are helpful, but we are still a long way away from developing an efficient information security plan that can protect against everything (Prislan, 2016). As found in many previous studies and confirmed in this study, the development of an effective and efficient information security theory will be difficult at least in the foreseeable future because cyber-terrorists and other attackers continue to adapt and change to make these cyber-attacks possible and find new and improved ways to steal or damage data (Leukfeldt, 2015).

References

Abdelwahled, A., Mahmoud, A., & Bdair, R. (2017). Information security policies and their relationship with the effectiveness of the management information systems of major Palestinian Universities in the Gaza Strip. *International Journal of Information Science and Management, 15*(1), 1-26.

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., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intellectual Manufacturing, 25*(1), 357-370. doi:10.1007/s10845-012-0683-0

Alam B., Doja, M., Alam, M., & Malhotra, S. (2013). Security issues analysis for cloud computing. *International Journal of Computer Science and Information Security, 11*(9), 117-125.

Alavi, R., Islam, S., & Mouratidis, H. (2016). An information security risk-driven investment model for analyzing human factors. *Information & Computer Security, 24*(2), 205-227. doi:10.1108/ICS-01-2016-0006

Al-Mukahal, H., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations. *Information & Computer Security, 23*(1), 102-118. doi:10.1108/ICS-03-2014-0018

Bate, S., & Chatfield, M. (2016). Using the structure of the experimental design and the randomization to construct a mixed model. *Journal of Quality Technology, 48*(4), 365-387.

Bere, M., Bhunu-Shava, F., Gamundani, A., & Nhamu, I. (2015). How advanced persistent threats exploit humans. *International Journal of Computer Science Issues, 12*(6), 1694-1784. Retrieved from http://www.IJCSI.org

Berinato, S. (2002). Finally, a real return on security spending. *CIO, 1*(1), 1-9. Retrieved from https://www.cio.com.au/article/52650/finally_real_return_security_spending/

Bharadwaj, A. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly, 24*(1), 169-196.

Bianchi, I., & Sousa, R. (2016). IT governance mechanisms in higher education. *Procedia Computer Science, 100*(1), 941-946.

Boon, G., & Sulaiman, H. (2015). A review on understanding of BYOD issues, frameworks and policies. *The 3rd National Graduate Conference, 1*(1), 272-277.

Brand, J., Renen, W., & Rudman, R. (2015). Proposed practices to mitigate significant mobility security risks. *International Business & Economics Research Journal, 14*(1), 199-220.

Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Scientific Engineering Ethics, 20*(1), 701-715. doi:10.1007/s11948-0149551-y

Chen, M., Qian, Y., Mao, S., Tang, W., & Yang, X. (2016). Software-defined mobile networks security. *Mobile Networks Applications, 21*(1), 729-743. doi:10.1007/s11036-015-0665-5

Choong, P., Hutton, E., Richardson, P., & Rinaldo, V. (2017). Protecting the brand: Evaluating the cost of security breach from a marketer's perspective. *American Journal of Management, 11*(1), 59-68.

Comiskey, C., Dempsey, C. (2016). Importance and use of correlational research. *Nurse Researcher, 23*(6), 20-25.

Das, A., & Khan, H. (2016). Security behaviors of smartphone users. *Information & Computer Security, 24*(1), 116-134. doi:10.1108/ICS-04-2015-0018

Das, S., Mukhopadhyay, A., & Shukla, G. (2013). i-Hope framework for predicting cyber breaches: A logit approach. *Hawaii International Conference on System Sciences, 12*(1), 3008-3017. doi:10.1109/HICSS.2013.256

Diamantopoulou, V., Tsohou, A., Loukis, E., & Gritzalis, S. (2017). Does the development of information systems resources lead to the development of information security resources? An empirical investigation. *Twenty-third American Conference on Information Systems, 1*(1), 1-10.

Dragoi, A. (2015). Research regarding the risks in the audit mission of computerized systems. *Audit FinanciarXIII, 4*(124), 72-82.

Dreyfuss, M., & Giat, Y. (2016). Identifying security modules in a university's information system. *Information Science & IT Education Conference, 1*(1), 41-51.

El-Temtamy, O., Majdalawieh, M., & Pumphrey, L. (2016). Assessing IT disaster recovery plans. *Information & Computer Security, 24*(5), 514-533. doi:10.1108/ICS04-2016-0030

Ellis, T., & Levy, Y. (2008). Framework of problem-based research: A guide for novice researcher's development of a research-worthy problem. *Informing Science: The International Journal of an Emerging Transdisciple, 11*(1), 17-33.

Ferreira, A., & Kuniyoshi, M. (2105). Critical factors in the implementation process of integrated management systems. *Journal of Information Systems and Technology Management, 12*(1), 145-164. doi:10.4301/S1807-17752015000100008

Filkins, B., & Hardy, G. (2016). IT security spending trends. *A SANS Survey, 2*(1), 1-23.

Flores, W., Holm, H., & Svensson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviors in practice. *Information Management & Computer Security, 22*(4), 393-406. doi:10.1108/IMCS-11-2013-0083

Friberg, F., & Lyckhage, E. (2013). Changing essay writing in undergraduate nursing education through action research: A Swedish example. *Nursing Education Perspectives, 7*(1), 226-232.

Gao, X., & Zhong W. (2015). Information security investment for competitive firms with hacker behavior and security requirements. *Annual Operation Resources, 235*(1), 277-300. doi:10.1007/s10479-0151925-2

Garg, A., Shula, B., & Kendall, G. (2015). Barriers to implementation of IT in educational institutions. *The International Journal of Information and Learning Technology, 32*(2), 94-108.

Georgescu, C., & Tudor, M. (2015). Cyber terrorism threats to critical infrastructures NATO's role in cyber defense. *Knowledge Horizons – Economics, 7*(2), 115-118.

Gercek, G., Saleem, N., & Steel, D. (2016). Networked services outsourcing for small businesses: A lifecycle approach. *Journal of Global Business and Technology, 12*(1), 23-32.

Gharibi, W., & Ktaiman, H. (2016). Developing information security multimedia training program security analyst workbench. *Scientific International, 28*(2), 935-938.

Ghazizadeh, E., Zamani, M., Manan, J., & Alizadeh, M. (2014). Trusted computing strengths cloud authentication. *The Scientific World Journal, 2014*(1), 1-17. Retrieved from http://dx.doi.org/10.1155/2014/260187

Grant, C., & Osanloo, A. (2014). Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the Blueprint for your House. *Administrative Issues Journal, 4*(2), 11-26. Retrieved from https://dc.swosu.edu/aij/vol4/iss2/4

Harris, M., Furnell, S., & Patten, K. (2014). Comparing the mobile device security behavior of college students and information technology professionals. *Journal of Information Privacy and Security, 10*(1), 186-202. doi:10.1080/15536548.2014.974429

Harris, M., & Patten, K. (2014). Mobile device security considerations for small-medium-sized enterprise business mobility. *Information Management & Computer Security, 22(1), 97-114. doi:10.1108/IMCS-03-2013-0019*

Hosban, 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.

Huertas-Garcia, R., Nunez-Carballosa, A., & Miravitlles, P. (2016). Statistical and cognitive optimization of experimental designs in conjoint analysis. *Revista Eurpoea de Direccion y Economia de la Empresa, 25*(1), 142-149. Retrieved from http://dx.doi.org/10.1016/j.redee.2015.10.001

Hulbert, S. (2013). Affirmation of the Classical Terminology for Experimental Design via a Critique of Casella's Statistical Design. *Agronomy Journal, 105*(2), 412-418.

Hryszkiewicz, D., & Lubas, B. (2015). A qualitative security model for business processes. *Internal Security, 1*(1), 279-289.

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.

Imboden, T., Phillips, J., Seib, J., & Fiorentino, S. (2014). Information security in nonprofits: A first glance at the state of security in two Illinois regions. *Journal of Information Security Applied Research, 7*(2), 28-38.

Iosifovitch, L., & Podolyanets, L. (2016). Models of complex industrial facilities assessment based on risk approach. *International Review of Management and Marketing, 6*(55), 125-135. Retrieved from http://www.econjournals.com

Jain, A., & Pandey, U. (2013). Role of cloud computing in higher education. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(7), 966-972.

Jogulu, U., & Pansiri, J. (2011). Mixed methods: A research design for management doctoral dissertations. *Management Research Review, 34*(6), 687-701.

Kalliosaari, L., Taipale, O., Smolander, K., & Richardson, I. (2016). Adoption and use of cloud-based testing in practice. *Software Qualifications Journal, 24*(1), 337-364. doi:10.1007/s11219-014-9256-0

Kaptein, M. (2015). The effectiveness of ethics programs: The role of scope, composition, and sequence. *Journal of Business Ethics, 132*(1), 415-431. doi:10.1007/s10551-014-2296-3

Kayode, A., Arome, G., Iaeng, M., Tolulope, A., & Ajoke, A. (2016). Cost-benefit analysis of cyber-security systems. *World Congress on Engineering and Computer Science, 1*(1), 1-9.

Kearns, G. (2015). Computer forensics projects for accountants. *Computer Forensic Projects for Accountants, 10*(3), 7-34.

Kenney, M. (2015). Cyber-Terrorism in a post-stuxnet world. *Foreign Policy Research Institute, 12*(1), 111-128. doi:10.1016/j.orbis.2014.11.009

Kim, E. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security, 22*(1), 115-126. doi:10.1108/IMCS-01-2013-0005

Kim, S., Yang, K., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal, 2014*(1), 1-12.

Kwecka, R. (2016). Information in the area of security: New paradigms. *Journal of Defense Resources Management, 7*(2), 97-124.

Lee, M. (2014). IT governance implementation framework in small and medium enterprise. *International Journal of Management and Enterprise Development, 12*(6), 424-441. doi:10.1504/IJMED.2013.056445

Li, D. (2015). Online security performances and information security disclosures. *Journal of Computer Information Systems, 55*(2), 20-28.

Liu, M., Scheepbouwer, E., & Giovinazzi, S. (2016). Critical success factors for post-disaster infrastructure recovery. *Disaster Prevention and Management, 25*(5), 685-700. doi:10.1108/DPM-01-2016-0006

Maheux, B. (2014). Assessing the intentions and timing of malware. *Technology Innovation Management Review, 11*(1), 34-40.

Mangelsdorf, M. (2017). What executives get wrong about cybersecurity. *MITSloan Management Review, 58*(2), 21-25. Retrieved from http://mitsmr.com/2gDSjip

Manly, T., Leonard, L., & Riemenschneider, C. (2015). Academic integrity in the information age: Virtues of respect and responsibility. *Journal of Business Ethics, 127*(1), 579-590. doi:10.1007/s10551-014-2060-8

Marchany, R. (2014). Higher education: Open and secure? *SANS Institute, 1*(1), 1-25.

Markelj, B., & Bernik, I. (2016). Information security related to the use of mobile devices in Slovene Enterprises. *Journal of Criminal Justice and Security, 16*(2), 117-127.

Merriam-Webster. (2018, July). Retrieved from www.merriam-webster.com.

Michelberger, P., & Dombora, S. (2016). A possible tool for development of information security – Siem system. *Scientific Review Article, 62*(1), 125-140. doi:10.5937/ekonomika1601125m

Miron, W., & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review, 10*(1), 33-39.

Misra, A., & Misra, S. (2014). Conceptual modeling for knowledge management to support agile software development. *The Knowledge Engineering Review, 29*(2), 496-511. doi:10.1017/S0269888914000198

Mommer, M., Sommer, A., Schloder, J., & Bock, H., (2015). A nonlinear preconditioner for optimum experimental design problems. *Euro Journal of Computational Optimization, 3*(1), 131-146. doi:10.1007/s13675-015-0036-9

Mubarak, S. (2016). Developing a theory-based information security management framework for human service organizations. *Journal of Information, Communication, and Ethics in Society, 14*(3), 254-271. doi:10.1108/JICES-06-2015-018

Mushtaque, K., Ahsan, K., & Umer, A. (2015). Digital forensic investigation models: An evolution study. *Journal of Information Systems and Technology Management, 12*(2), 233-244. doi:10.4301/S1807-17752015000200003

Nagurney, A., Daniele, P., & Shukla, S. (2017). A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annual Operating Resolutions, 248*(1), 405-427. doi:10.1007/s10479-016-2209-1

Nawafleh, Y., Nawafleh, A., & Nawafleh, S. (2016). Cybercrimes: concept, forms and their civil liabilities. *International Journal of Arts & Sciences, 7*(5), 211-234.

Newman, I., & Covrig, D., (2013). Writer's Forum – Building consistency between title, problem statement, purpose, & research questions to improve the quality of research plans and reports. *New Horizons in Adult Education & Human Resources Development, 25*(1), 70-79.

O'Connor, B. (2017). A first steps guide to the transition from null hypothesis significance testing to more accurate and Informative Bayesian Analyses. *Canadian Journal of Behavioral Science, 49*(3), 166-182. Retrieved from http://dx.doi.org/10.1037/cbs0000077

Obeidat, M., & North, M. (2014). A comparative review of information technology project management in private and public sector organizations. *International Management Review, 10*(1), 55-67.

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity strategy's role in raising Kenyan awareness of mobile security threats. *Information & Security: An*

International Journal, 32(1), 3207-1-3207-20. Retrieved from http://dx.doi.org/10.11610/isij-3207

Olafare, O., Parhizakar, H., & Vem, S. (2015). A new secure mobile cloud architecture. *International Journal of Computer Science Issues, 12*(2), 161-174.

Peralta, K., & Klonowski, M. (2017). Examining conceptual and operational definitions of "first-generation college student" in research on retention. *Journal of College Student Development, 58*(4), 630-636.

Prislan, K. (2016). Efficiency of corporate security systems in managing information threats: An overview of the current situation. *Journal of Criminal Justice and Security, 16*(2), 128-147.

Pitcher, R. (2011). Doctoral students' conceptions of research. *The Qualitative Report, 16*(4), 971-983. Retrieved from http://www.nova.edu/ssss/QR/QR16-4/pitcher.pdf

Raha, M. (2015). Aerospace Power in the 21st Century. *VAYU, 1*(1), 46-52.

Radulescu, M. (2016). Considerations on the selection and prioritization of information security solutions. *Audit Financiar, 5*(137), 564-574.

Rege, A. (2014). Digital information warfare trends in Eurasia. *Security Journal, 27*(4), 374-398. Retrieved from http://www.palgrave-journals.com/sj/

Reimer, J., Schuerch, M., & Slawig, T. (2015). Optimization of model parameters and experimental designs with the Optimal Experimental Design Toolbox (v1.0) exemplified by sedimentation in salt marshes. *Geoscientific Model Development, 8*(1), 791-804. doi:10.5194/gmd-8-791-2015

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of CyberSecurity*, *2*(2), 121-135. doi:10.1093/cybsec/tyw001

Rowe, B., & Gallaher, M. (2006). Private sector cyber security investment strategies: An empirical analysis. *U.S. Department of Homeland Security, 1*(1), 1-23.

Sadovnikova, N., Klochkova, E., Dobrolyubova, E., & Alexandrov, O. (2015). Basic trends of information society development in Russia compared to world's leading countries. *International Review of Management and Marketing, 5*(1), 18-29. Retrieved from http://www.econjournals.com

Santos, L., & Santos, C. (2017). A study on the impact of non-operational mechanisms on the effectiveness of public information technology governance. *Revista de Administracao, 1*(1), 256-267. Retrieved from http://www.sciencedirect.com

Sembiring, J., Ramadam, M., Gondokaryono, Y., & Arman, A. (2015). Network security risk analysis using improved MulVAL Bayesian attack graphs. *International Journal of Electrical Engineering and Informatics, 7*(4), 735-753. doi:10.15676/ijeei.2015.7.415

Shahpasand, M., Shajari, M., Golpaygani, S., & Ghavamipoor, H. (2015). A comprehensive security control selection model for inter-dependent organizational assets structure. *Information and Computer Security, 23*(2), 218-242.

Shamala, P., Ahmad, R., Zolait, A., & Sahib, S. (2015). Collective information structure model for information security risk assessment (ISRA). *Journal of Systems and Information Technology, 17*(2), 193-219. Retrieved from http://www.emeraldinsight.com/1328-7265.htm

Silk, D., Kirk, P., Barnes, C., Toni, T., & Stumpf, M. (2014). Model selection in systems biology depends on experimental design. *PLOS Computational Biology, 10*(6), 1-14. Retrieved from http://www.ploscompbiol.org

Sindhuja, P. (2014). Impact of information security initiatives on supply chain performance. *Information Management & Computer Security, 22*(5), 450-473. doi:10.1106/IMCS-05-2013-0035

Sommestad, T., Karlzen, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security, 23*(2), 200-217. doi:10.1108/ICS-04-2014-0025

Subsermsri, P., Jairak, K., & Praneetpolgrang, P. (2015). Information technology governance practices based on sufficiency economy philosophy in the Thai university sector. *Information Technology & People, 28*(1), 195-223. doi:10.1108/ITP-10-2013-0188

Sung, P., Ku, C., & Su, C. (2014). Understanding the propagation dynamics of multipartite computer virus. *Industrial Management & Data Systems, 114*(1), doi:10.1108/IMDS-04-2013-0197

Syuntyurenko, O. (2015). Network technologies for information warfare and manipulation of public opinion. *Scientific and Technical Information Processing, 42*(4), 205-210.

Tahat, L., Elian, M., Sawalha, N., & Al-Shaikh, F. (2014). The ethical attitudes of information technology professionals: a comparative study between the USA and the Middle East. *Ethics in Information Technology, 16*(1), 241-249. doi:10.1007/s10676-014-9349-2

Tang, Y. (2007). IT capability, customer information handling, and privacy protection: A resource-based view of organizational performance. *A thesis in Information Systems.* Massey University, Auckland, New Zealand.

Taylor, R., & Robinson, S. (2014). The roles of positive and negative exemplars in information security strategy. *Academy of Information and Management Sciences Journal, 17*(2), 57-79.

Tiwari, M., Oasa, S., Yamamoto, J., Mikuni, S., Kinjo, M. (2017). A quantitative study of internal and external interactions of homodimeric glucocorticoid receptor using fluorescence cross-correlation spectroscopy in a live cell. *Scientific Reports, 7*(1), 1-17. doi:10:1038/s41598-017-04499-7

Trajkovski, V. (2016). How to select appropriate statistical test in scientific articles. *Journal of Special Education and Rehabilitation, 17*(4), 5-28. doi:10:19057/jser2016

Vaduris, M., Ceccarelli, A., Duarte Jr, E., & Mahanti, A. (2016). System and Network Security: Anomaly Detection and Monitoring. *Journal of Electrical and Computer Engineering, 2016*(1), 1-2. Retrieved from http://dx.doi.org/10.1155.2016.2093790

Vijayakumar, U., & Ilangovan, D. (2015). A quantitative approach to information systems audit in small and medium enterprises. *Infromatica Economica, 19*(3), 89-95. doi:10.12948/issn14531305/19.3.2015.08

Weishaupl, E., Yasasin, E., & Schryen, G. (2015). IT security investments through the lens of the resource-based view: A new theoretical model and literature review. *Twenty-Third European Conference on Information Systems, 1*(1), 1-19.

Wong, Z. (2015). Student attitudes toward information systems management as major and career options. *International Journal of Information and Education Technology, 5*(6), 409-413.

Wongpinunwatana, N. (2014). Creating self-efficacy in internal auditors from information technology audits: An on-the-job training perspective. *International Journal of Management & Information Systems, 18*(3), 213-222.

Yayla, M. (2014). Cyber terrorism from the criminal law perspective. *Law & Justice Review, 5*(1), 123-145.

Yuksel, A., Zaim, A., & Aydin, M. (2014). A comprehensive analysis of android security and proposed solutions. *International Journal of Computer Network and Information Security, 12*(1), 9-20.

Zafar, H., Ko, M., & Osei-Bryson, K. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontier, 18*(1), 1205-1215. doi:10.1007/sl10796-015-9562-5

Zavada, D., & Longo, R. (2014). AGA survey spotlights federal inspectors general. *The Journal of Government Financial Management, 63*(1), 50-54.

Zaveri, P. (2015). Digital disaster management in libraries in India. *Library Hi Tech, 33*(2), 230-244. doi:10.1108/LHT-09-2014-0090

Zezulka, L., & Seigfried-Spellar, K. (2016). Differentiating cyberbullies and internet trolls by personality characteristics and self-esteem. *JDFSL, 11*(3). 7-25.

Zheng, D., & Lewis, J. (2015). Cyber threat information sharing: Recommendations for congress and the administration. *Center for Strategic & International Studies, 3*(1), 1-13.

Appendix A:

Sample Information Security Plan

I. OBJECTIVE:

Our objective, in the development and implementation of this written information security plan, is to create effective administrative, technical and physical safeguards in order to protect our customers' non-public personal information.
The plan will evaluate our electronic and physical methods of accessing, collecting, storing, using, transmitting, protecting, and disposing of our customers' non-public personal information.

II. PURPOSES:

a) Ensure the security and confidentiality of our customers' information;

b) Protect against any anticipated threats or hazards to the security or integrity of our customers' information;

c) Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any of our customers.

III. ACTION PLANS:

a) Identify reasonably foreseeable internal and external threats that couldresult in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems;

b) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information;

c) Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

IV. ACTION STEPS:

a) Appoint a specific person or persons within the firm to be responsible for:
   1) initial implementation of the plan;
   2) training of employees;
   3) regular testing of the controls and safeguards established by the plan;
   4) evaluating the ability of prospective service providers to maintain appropriate information security practices, ensuring that such providers

are required to comply with this information security plan, and monitoring such providers for compliance herewith; and

5) periodically evaluating and adjusting the plan, as necessary, in light of relevant changes in technology, sensitivity of customer information, reasonably foreseeable internal or external threats to customer information, changes to our own business (such as mergers or acquisitions or outsourcing), and/or changes to customer information systems.

b) Conduct an annual training session for all owners, managers, employees and independent contractors—and periodic training for new employees—working for the firm on the elements of this information security plan, the contents of the firm's "Privacy Policy," and any other requirements of federal or state privacy laws. All persons in attendance should be required to certify their attendance at the training, their receipt of the firm's privacy policy, and their familiarity withthe firm's requirements for ensuring the protection of customers' non-public personal information.

c) Determine reasonably foreseeable **internal** threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems, assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information, and evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

Internal Threat	Risk Level	Response
Intentional or inadvertent misuse of customer information by current employees	Low	1) Dissemination of, and annual training, on privacy laws and firm privacy policy. 2) Incorporation of privacy policy guidelines into employee handbook. 3) Employment agreements amended to require compliance with privacy policy and to prohibit any nonconforming use of customer information during or after employment. 4) Employees encouraged to report any suspicious or unauthorized use of customer information. 5) Periodic testing to ensure these safeguards are implemented uniformly.
Intentional or inadvertent misuse of customer information by	Medium	1) Require return of all customer information in the former employee's possession (i.e., policies requiring return of

former employees subsequent to their employment		all firm property, including laptop computers and other devices in which records may be stored, files, records, work papers, etc… 2) Eliminate access to customer information (i.e., policies requiring surrender of keys, ID or access codes or badges, business cards; disable remote electronic access; invalidate voicemail, e-mail, internet, passwords, etc…, and maintain a highly secured master list of all lock combinations, passwords, and keys. 3) Change user-ID's and passwords for current employees periodically. 4) Amend employment agreements during employment to require compliance with privacy policy and to prohibit any nonconforming use of customer information during or after employment. 5) Send "pre-emptive" notices to clients when the firm has reason to believe a departed employee may attempt to wrongfully use customer information, informing them that the employee has left the firm. 6) Encourage employees to report any suspicious or unauthorized use of customer information. 7) Periodic testing to ensure these safeguards are implemented uniformly.
Inadvertent disclosure of customer information to the general public or guests in the office	Low	1) Prohibit employees from keeping open files on their desks when stepping away. 2) Require all files and other records containing customer records to be secured at day's end. 3) Use software program that requires each employee to enter a unique log-in ID to access computer records, and to re-log-in when the computer is inactive for more than a few minutes. 4) Change user-ID's and passwords for current employees periodically. 5) Restrict guests to one entrance point, require them to present a photo ID, sign-in,

		and wear a plainly visible "GUEST" badge or tag; restrict areas within the office in which guests may travel unescorted. 6) Use shredding machines on unused photocopies or other records being discarded before depositing in trash or recycling containers. 7) Ensure secure destruction of obsolete equipment, including computer hardware and software systems. 8) Encourage employees to report any suspicious or unauthorized use of customer information. 9) Periodic testing to ensure these safeguards are implemented uniformly. { VERY LARGE FIRMS MAY WISH TO CONSIDER ADDING THE FOLLOWING: } 10) Require all customer records to be maintained in locked desks or filing cabinets when the records are not being used, or when the office is closed. 11) Install security badge system, requiring employees to use photo ID badges with an electronic strip to open locked internal doors in the office.

d) Determine reasonably foreseeable **external** threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems, assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information, and evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

External Threat	Risk Level	Response

Inappropriate access to, or acquisition of, customer information by third parties	Low	1) Install firewalls for access to firm internet site. Include privacy policy on the site. 2) Require secure authentication for internet and/or intranet and extranet users. 3) Establish dial-in protections (such as Caller-ID, Callback, encryption) to prevent unauthorized access.

		4) Require encryption and authentication for all infrared, radio, or other wireless links. 5) Train employees to protect and secure laptops, handheld computers, or other devices used outside the office that contain customer information. 6) Install virus-checking software that continually monitors all files, downloads, floppy disks, CD's, all incoming and outgoing e-mail messages. 7) Establish uniform procedures for installation of updated software. 8) Establish systems and procedures for secure back-up, storage and retrieval of computerized and paper records. 9) Establish procedures to ensure external points of entry to the office are closed, locked and inaccessible to unauthorized persons when the office is closed. 10) Install burglar alarm or other security systems, with training for authorized persons on activation, deactivation, …. 11) Physically lock or otherwise secure the computer room, and if necessary, all areas in which paper records are maintained. 12) Use shredding machines on unused photocopies or other records being discarded before depositing in trash or recycling containers. 13) Ensure secure destruction of obsolete equipment, including computer hardware and software systems. 14) Encourage employees to report any suspicious or unauthorized use of customer information. 15) Periodic testing to ensure these safeguards are implemented uniformly.
Inappropriate use of customer information by third parties	Medium	1) Evaluate the ability of all prospective third-party service providers to maintain appropriate information security practices. 2) Provide all third-party service providers to whom contractual access to premises or records have been granted (including, but

		not limited to, insurance companies being solicited for new or renewal policies, mailing houses, custodial or plant services, equipment or services vendors, affiliates, non-affiliated joint marketing partners, …) with a copy of the Privacy Policy. 2) Require all such third-parties—**by written contract**—to adhere to the Privacy Policy, agree to make no use of any nonpublic personal information on your customers that would be prohibited thereby, or otherwise by law or contract, and agree to hold harmless and indemnify the firm for any inappropriate use of customer non-public personal information. 3) Require all such third-parties—**by written contract**—to return all customer information and all other firm property at the completion or termination, for whatever reason, of the agreement between the firm and the third-party. 4) Prohibit access to customer information (i.e., policies requiring surrender of keys, ID or access codes or badges, disabling remote electronic access; invalidating voicemail, e-mail, internet, passwords, etc…, if applicable) to all such third-parties upon completion or termination, for whatever reason, of the agreement between the firm and the third-party. 5) Change user-ID's and passwords for current employees periodically. 6) Send "pre-emptive" notices to clients when the firm has reason to believe a terminated third-party service provider may attempt to wrongfully use customer information, informing them that the agreement with the firm is no longer in effect. 7) Encourage employees to report any suspicious or unauthorized use of customer information. 8) Periodic testing to ensure these safeguards are implemented uniformly.