2018

An Analysis of the Preparedness of Educational Institutions to Ensure the Security of Their Institutional Information

Vikram Ahmed
University of Central Florida

AN ANALYSIS OF THE PREPAREDNESS OF EDUCATIONAL INSTITUTIONS TO ENSURE THE SECURITY OF THEIR INSTITUTIONAL INFORMATION

by

VIKRAM AHMED
M.B.A. East Carolina University, 2002

A dissertation in practice submitted in partial fulfillment of the requirements
for the degree of Doctor of Education
in the School of Teaching, Learning, and Leadership
in the College of Education and Human Performance
at the University of Central Florida
Orlando, Florida

Summer Term
2018

Major Professor: Jerry Johnson

ABSTRACT

The purpose of this exploratory study was to analyze and examine the differences in the preparedness of educational institutions toward ensuring the security of their data by comparing their self-reported perceptions of security risks and their assessments of the corresponding risk-mitigating practices. Factors that were studied with reference to securing institutional data were aligned with the five components of information systems: hardware, software, data, procedures and people. The study examined the perceptions of security threats associated with these factors and explored the perceptions of the effectiveness of critical measures with respect to these factors within the constraints applicable to educational institutions. Given the dynamic nature of the threats to information security, this study further explored mechanisms and frequencies with which the different types of educational institutions conduct key security practices and stay up-to-date in their information security policies and procedures. The population of interest for this study consisted of a cross-sectional representation of the following types of educational institutions in the state of Florida: public and private PK-12 institutions, public and private universities, and virtual schools. At every stage of this explorative study, comparative analyses were conducted. The researcher found no statistically significant differences between the types of educational institutions in their perceptions of security risks. However, in terms of their perceptions of the effectiveness of security measures, frequencies of key security practices and policy updates, budget allocations, and overall assessment of security preparedness, the educational institutions showed statistically significant differences.

To Kakoli, Meghna, and Jelly Bean

ACKNOWLEDGMENTS

I would like to express my appreciation for my committee chair, Dr. Jerry Johnson, for his guidance, encouragement and support throughout this process. I would also like to thank my committee members - Dr. Kenneth Murray, Dr. Shahram Amiri, and Dr. Lee Baldwin for their support, advice and expertise. I am also thankful for my wonderful colleagues in my cohort; I have learned a lot from our discussions and experiences in and out of class.

I would also like to thank my family. My daughter Meghna and my doggy-son Jelly Bean were extremely patient and understanding when I was busy and did not have enough time to spend with them. Finally, and most importantly, I want to thank my wife Kakoli, who has always supported me in everything I have done. In fact, she was the one who had encouraged me to apply for the Ed.D. program at the University of Central Florida.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

Background of Study

As businesses, educational institutions and individuals rely more and more on technology for operational and decision-support activities, the importance of cyber-security cannot be over stated. This is because as technological advances happen, so do the advances in sophistication of cyber-crimes. Data breaches costing millions of dollars happen every year (Gardner & Thomas, 2014). Different breach tracking sources report different data breach numbers, but they all unanimously report that breaches in educational institutions remain high. In fact, according to the Privacy Rights Clearinghouse Chronology of Data Breaches report that tracks all reported data breaches starting from 2005, almost 25 million user records have been breached in educational institutions. In between 2005 and April 2018, there have been 815 reported data breaches in educational institutions (Chronology of Data Breaches, 2018). In the 2017 and 2018 editions of the annual data breach investigations report published by Verizon Enterprises, a total of 747 incidents were identified in educational institutions in 2016 and 2017 alone, 174 with confirmed data disclosure (Data Breach Investigations Report, 2017/2018).

Educational institutions often store a significant amount of private information, including educational and health records, and identity information of all personnel involved which may include students, teachers, faculty, administrators and staff (Levy & Ramim, 2016). Unfortunately, the security measures adopted by educational institutions are often not up to the standards desired in the world of information systems (Cavusoglu, Cavusoglu, Son, & Benbasat, 2015). Analyses of cyber-security often reveal that educational institutions do not adequately address the cyber-security issues by having appropriate plans in place. Further, such analyses

also reveal that information security is often not considered a key requirement in many educational institutions. Consequently, the volume of data breaches affecting educational institutions has grown (Powerhouses and Benchwarmers, 2014).

A data breach is defined as an incident in which an individual's identifying information which may include a social security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure. These breaches result in identity theft, privacy violations and fraud (Data Breaches, 2018). Educational institutions are in a unique position as compared to their industry counterparts as their user-bases have been primarily comprised of children and young adults whose identity information once compromised may not be misused instantly, but rather years later when they move to the workforce. As such, a detection of a breach is more challenging (Farina, 2015). In addition, the educational institutions are subject to different federal and state statutes that regulate data privacy such as the Family Educational Rights and Privacy Act [FERPA], The Payment Card Industry Data Security Standards [PCI-DSS], Gramm-Leach-Bliley Act [GLBA], Red Flags Rule, The Federal Information Security Management Act [FISMA], and the Health Insurance Portability and Accountability Act [HIPAA] (Powerhouses and Benchwarmers, 2014). Further, they can be subject to class action lawsuits in the wake of a data breach (IT Security for Higher Education: A Legal Perspective, 2003). Finally, significant costs, both tangible and intangible are incurred by an affected institution whenever a breach happens (Gardner & Thomas, 2014). In an era where budget shortage in the field of education is a recurring phenomenon, any significant un-budgeted costs can prove to be devastating for affected institutions (Mitchell, Palacios, & Leachman, 2014).

Statement of the Problem

The problem that was investigated in this study was the level of preparedness of educational institutions to ensure the security of their information. The threats to data and information security are constantly evolving, and becoming increasingly sophisticated with time (Vacca, 2012). Interestingly, educational institutions have endured a significant number of data breaches in recent times. In fact, almost 25 million user records have been breached in educational institutions between 2005 and April 2018 (Chronology of Data Breaches, 2018). The cost incurred by an educational institution in the event of a data breach has increased. It was $260 per record breached in 2017 with a four-year average of $200 per record (Cost of Data Breach Study, 2017). Historically, there has been a reluctance on the part of educational institutions to designate information security as a top-most priority, often due to cultural and budgetary reasons. As such, information security practices and procedures followed in these institutions have often been inadequate in countering the threat of sophisticated data breaches (Powerhouses and Benchwarmers, 2014). Consequently, they are the victims in a very high proportion of reported data breaches. Although extensive research exists in identifying and quantifying security threats that apply universally to all kinds of institutions, there have been few studies focused on preparedness of educational institutions in combating such threats and identifying areas where they are the most vulnerable.

Purpose of the Study

The purpose of this exploratory study was to analyze the preparedness of educational institutions toward ensuring the security of their data by comparing their self-reported perceptions of security risks and their assessments of the corresponding risk-mitigating practices.

Factors that were studied with reference to securing institutional data were aligned with the five components of any information system: hardware, software, data, procedures, and people (Kroenke & Boyle, 2015). The researcher examined the security threats associated with these factors and explored the critical measures with respect to these factors that can enhance security within the constraints applicable to educational institutions. Given the dynamic nature of the threats to information security, this study was also conducted to further explore the frequencies with which the different types of educational institutions undertake critical security practices and stay up-to-date in their information security policies and procedures. Finally, the culture of educational institutions, with respect to implementing information security measures as reflected in their allocation of budgets for the same, was explored. Obtaining this information could potentially allow for educational leaders to formulate and enforce policies and practices that will enhance their preparedness in securing their institutional data. At every stage of this explorative study, comparative analyses were made about the level of preparedness among different types of educational institutions with respect to their information security related measures.

Significance of the Study

The landscape of information security in educational institutions is changing rapidly. The concept of a lone hacker creating viruses in a basement has been relegated to the background (Zalaznick, 2013). Instead, data breaches conducted by sophisticated foreign governments as cyber espionage are the top cybersecurity threat today (Data Breach Investigations Report, 2017). Today's hackers are now being deployed around the clock to steal intellectual property, sensitive research, and personal information, potentially costing educational institutions millions of dollars and badly damaging their reputations (Thompson, 2015). These institutions are

susceptible to numerous kinds of data breaches due to the open welcoming environment in which they operate and the vast amount of data they compile from students, teachers, faculty, employees, and other affiliated individuals. Thus, they need to balance the security of their information systems with their focus on the uninterrupted flow of information (Amigud, Arnedo-Moreno, Daradoumis, & Geurrero-Roldan, 2018). This exploratory study was intended to provide leaders in educational institutions with relevant information relating to the self-reported preparedness of institutions to tackle the ever-increasing threats to their data. This study may assist in providing the decision makers with information relating to certain key areas where they need to focus to optimize the conflicting requirements of security and convenience. This study may also assist the decision makers with information on how to handle a post-breach situation with respect to the various legal implications involved.

Definition of Terms

For the purpose of this explorative study, the following operational definitions were used for key terms that pertain directly to the research being conducted.

Any information system is comprised of five components. Those are hardware, software, data, procedure and people (Kroenke & Boyle, 2015). At least one or all the five components are typically involved in a data breach.

Hardware - Hardware is the part of an information system that can be touched – the physical components of the technology. Computers, keyboards, disk drives, iPads, and flash drives are all examples of information systems hardware (Bourgeois, 2014).

Software - Software is a set of instructions that tells the hardware what to do. Software is not tangible – it cannot be touched. When programmers create software programs, what they are

really doing is simply typing out lists of instructions that tell the hardware what to do. There are several categories of software, with the two main categories being operating-system software, which makes the hardware usable, and application software, which does something useful. Examples of operating systems include Microsoft Windows on a personal computer and Google's Android on a mobile phone. Examples of application software are Microsoft Excel and Google Drive (Bourgeois, 2014).

Data - Data are comprised of a collection of facts. For example, street address, the city where one lives in, and phone number are all pieces of data. Like software, data are also intangible. By themselves, pieces of data are not really very useful. But aggregated, indexed, and organized together often into a database, data can become a powerful tool for decision-making purposes. Institutions collect all kinds of data and use it to make decisions (Bourgeois, 2014). One of the most critical pieces of data that are stored by an institution are personally identifiable information (PII) of its constituent individuals and entities. PII may include social security numbers, tax identification numbers and similar unique identifiers. This is the data component that is most routinely targeted by perpetrators (Levy & Ramim, 2016).

Procedure - A procedure is a series of steps undertaken to achieve a desired outcome or goal (Stair & Reynolds, 2013).

People – People are the creators, operators and consumers of an information system. People buy hardware, code software, analyze data, design procedures and finally make decisions. An information system cannot function without the involvement of people. From programming to data entry to the final decision making, people are involved (Stair & Reynolds, 2013).

There are essentially four components involved in any data breach situation applicable to educational institutions. Those are threat, vulnerability, safeguard and target (Kroenke & Boyle, 2015).

Threat - A threat is an entity that attempts to obtain and manipulate information systems data via illegal and secretive means (Jouini, Rabai, & Aissa, 2014).

Vulnerability - A vulnerability is the opportunity that a threat may utilize to accomplish its objectives (Austin, Holmgreen, & Williams, 2013).

Safeguard - A safeguard is the shield that blocks a threat from accomplishing its motives (Fay & Patterson, 2018).

Target - A target is what is being coveted by the threat (Fay & Patterson, 2018).

These four components work together in the event of a data breach. For a data breach to happen, a threat uses one or more vulnerabilities to bypass installed safeguards to reach the target. In an educational institution, targets typically comprise user identity information. Examples of threats include hacking, phishing, malware and ransomware that may exploit vulnerabilities like weak passwords, user ignorance and insecure systems. These may be prevented by adequate safeguards like firewalls, encrypted data, strong passwords and proper training (Kroenke & Boyle, 2015).

Figure 1 shows a threat/loss scenario which illustrates the inter-play of threats, vulnerabilities, safeguards and targets.

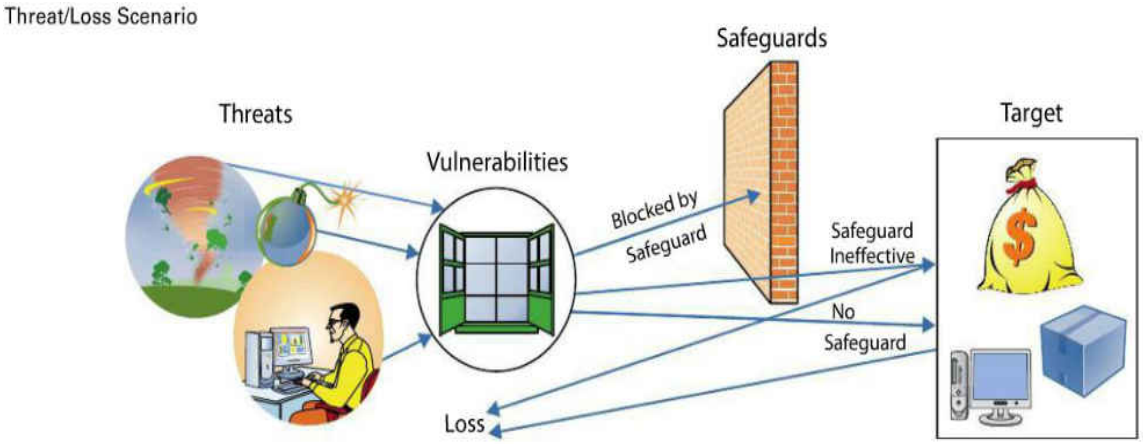


Figure 1. Threat/loss scenario

Source: Kroenke, D., & Boyle, R. (2015). *Experiencing MIS*. Harlow, Essex, England: Pearson

Research Questions

To analyze the preparedness of educational institutions toward ensuring the security of their data by comparing their assessments of security risks and their corresponding risk-mitigating practices, the following three research questions were created. The questions were sequentially placed as they relate to institutions' recognition, influence, and application of factors and their indication of the same in the research instrument used for this study.

1. What is the level of preparedness to counter threats to information security among educational institutions with respect to identification and classification of threats, and how do results vary across the types of institutions?

   This question was further divided into five sub-questions based on the five factors of information systems (Kroenke & Boyle, 2015):

1.1. What differences (if any) exist in the perception of security risks for hardware-oriented threats among the different types of educational institutions?

1.2. What differences (if any) exist in the perception of security risks for software-oriented threats among the different types of educational institutions?

1.3. What differences (if any) exist in the perception of security risks for data-oriented threats among the different types of educational institutions?

1.4. What differences (if any) exist in the perception of security risks for procedure-oriented threats among the different types of educational institutions?

1.5. What differences (if any) exist in the perception of security risks for people-oriented threats among the different types of educational institutions?

2. What is the level of preparedness to counter threats to information security among educational institutions with respect to institutional safeguards, frequency of critical measures and security policy updates, and budgetary allocation, and how do results vary across the types of institutions?

   This question was further divided into eight sub-questions based on the five factors of information systems (Kroenke & Boyle, 2015), frequency of critical measures and security policy updates, and budgetary allocation:

   2.1. What differences (if any) exist in the perception of the effectiveness of hardware-oriented security measures among the different types of educational institutions?

2.2. What differences (if any) exist in the perception of the effectiveness of software-oriented security measures among the different types of educational institutions?

2.3. What differences (if any) exist in the perception of the effectiveness of data-oriented security measures among the different types of educational institutions?

2.4. What differences (if any) exist in the perception of the effectiveness of procedure-oriented security measures among the different types of educational institutions?

2.5. What differences (if any) exist in the perception of the effectiveness of people-oriented security measures among the different types of educational institutions?

2.6 What differences (if any) exist in the frequencies of implementation of high-frequency critical practices among the different types of educational institutions?

2.7. What differences (if any) exist in the frequencies of implementation of low-frequency critical practices and security policy updates among the different types of educational institutions?

2.8. What differences (if any) exist in budgetary allocation related to information security among the different types of educational institutions?

3. What is the overall self-reported level of preparedness among educational institutions with respect to information security, and how do results vary across the types of institutions?

Review of Extant Literature

This analysis focusses on the level of preparedness of educational institutions to ensure the security of their data. Much research has been done within the field of identifying the threats to information security; however, there is dearth of research pertaining to the self-reported preparedness of educational institutions to handle information security threats.

Latest published literature and investigation reports often identify the frequencies, threats, motives and the types of data that are compromised during security breaches in educational institutions and compare them to the full picture of all areas and types of industries. For example, 75% of all reported beaches across all industries were conducted by outsiders and only 25% involved insiders. In contrast, 30% of insiders were involved in all reported breaches in educational institutions. Reports have also shown the changing distribution of threats in educational institutions. In 2016, Cyber-espionage was present in 26% of breaches, with User Errors closely behind at 22%. The previous year, the Cyber-espionage pattern accounted for only 5% of breaches while Web Application Attacks were the dominant threat. The trend in increased espionage breaches can be possibly attributed to access to research studies across a variety of disciplines conducted at universities. These studies are often coveted by state-affiliated groups. The breach findings have further shown that over half of the incidents in educational institutions involved the compromise and disclosure of stored personal information of both students and employees, with a little over 25% resulting in the disclosure of intellectual property. Educational

institutions face numerous challenges that are unique when it comes to keeping sensitive information secure. A significant challenge is often the prevalent inclusive culture based on the free and open exchange of ideas and information. The profile of the student/user population whose varying degrees of technical skills and curiosity must be considered, not to mention their roles as data subjects, whose personally identifiable information (PII) and other information must be protected (Data Breach Investigations Report, 2017).

Research and findings have often suggested that compromised identifying information of students is often not used immediately for financial transactions, keeping in mind the low-income status of the student stage. Only when they have an established career do perpetrators attempt identity-theft related activities. Thus, there is often a significant time lag between compromise of information and its subsequent detection. This feature is often unique to educational institutions (Farina, 2015).

The significantly high number of breaches occurring due to user errors (22%), notably mis-delivery of sensitive data and publishing errors as seen in educational institutions in 2016 further suggest the lack of adequate training and preparation of support staff as compared to their counterparts in the private industry (Data Breach Investigations Report, 2017). Compounding the problem is the often the lack of budgetary support for information security prevalent in educational institutions (Powerhouses and Benchwarmers, 2014). Furthermore, there are often differences among the type of educational institutions with respect to their security policies, technical expertise, content management, infrastructure, and budget allocations which makes difficult the process of generalizing the picture applicable to all educational institutions (Hentea, 2005).

These findings indicate that the cyber security landscape is changing. In fact, it is changing very fast. The question is whether educational institutions are acknowledging the threats and preparing themselves to handle them. Implementing security controls with reduced budgets and training opportunities while still maintaining the culture of openness is, thus, a balancing act that educational institution leaders have to endure. This exploratory study was aimed at ascertaining educational institutions' preparedness and how their preparations differed based on types of educational institutions.

Methodology

Only after receiving the approval of the University of Central Florida's Institutional Review Board (Appendix A), was research for this study initiated. The data for this study were collected using an instrument created by the researcher specifically for this study. This questionnaire-based instrument was used to measure the preparedness of educational institutions to ensure the security of their institutional information. The questionnaire primarily focused on four institution-specific areas that reflected their preparedness to counter security threats. Those are threat identification, threat mitigation practices, frequency of key security practices and updates of established security policies and practices, and budgetary allocations to enable security measures. The questions pertaining to these areas were further classified according to the five components of information systems – hardware, software, data, people, and procedures (Kroenke & Boyle, 2015). Responses to the questionnaire were obtained from five different types of educational institutions namely PK-12 Public Schools, PK-12 Private Schools, PK-12 Virtual Schools, Public Colleges/Universities, and Private Colleges/Universities in the state of Florida. Thereafter, the responses were aggregated based on the type of institution. Comparative

analyses using statistical tools such as the ANOVA and correlation analysis were performed on the data obtained from the different types of educational institutions.

Population

The population of interest for this study consisted of a cross-sectional representation of the following types of educational institutions in the state of Florida: PK-12 Public Schools, PK-12 Private Schools, PK-12 Virtual Schools, Public Colleges/Universities, and Private Colleges/Universities. Because the threat to institutional data applies to all educational institutions, a representation of different types of educational institutions was necessary for an accurate analysis as they are subjected to different levels of constraints with respect to ensuring information security.

Instrumentation

The Information Security Preparedness Instrument (ISPI©), created by the author for this study, was used to measure the preparedness of the educational institutions to combat information security threats. The ISPI©, shown in Appendix B, includes sections which were used to answer the research questions which guided this study. A draft version of the ISPI© was created first with relevant questions aimed at answering the study's research questions. Thereafter, it was reviewed by an expert panel and necessary revisions were made. A cognitive laboratory approach (Jobe, 1990) was then used to gauge comprehension and assess the cognitive burden placed on respondents. Finally, the instrument was checked for reliability using Chronbach's alpha (Gliem & Gliem, 2003) (see Appendix C).

Procedures

In March 2018, the chief information officers or their equivalent in selected educational institutions in Florida were sent an email requesting them to complete the online ISPI©. A hyperlink was provided in the email for the respondents to click and begin completing the instrument. Prior to beginning the instrument, the respondents were asked for their consent to take part in this study (Appendix D). They had to agree to participate in the ISPI© instrument before they were able to begin. Once they were in the online instrument, the respondents were asked to read each item carefully and select the option(s) that most closely resembled their self-perception and experience related to information security in their respective institutions.

The respondents were reminded in the informed consent that participating in this study was voluntary and that they had the option to change their minds and stop at any time. They also had the option to not answer any ISPI© instrument item for any reason and to withdraw at any time. The ISPI© instrument was open for 24 days. To facilitate a high response rate, follow-up e-mail messages were sent prior to the closing of the ISPI© instrument.

Analysis of Data

To answer Research Question 1, the respondents were asked to provide on the ISPI© instrument their perceptions of the security risks associated with all recognized threats on a scale of 1-5 as they applied to their institutions. The data hereby obtained for the threats were aggregated to the level of the five factors of information systems: hardware, software, data, people, and procedures (i.e., the group mean was calculated for individual items within each of the five factor groups). Thereafter, responses from similar institutions were grouped together (i.e., the group mean was calculated for each item by institution type) to obtain response profiles

for the different types of institutions. The analysis of the data collected was a combination of descriptive statistics to ascertain the overall response profiles at the factor-level and thereafter at the type of institution level. Five separate one-way ANOVA procedures were conducted to compare threat perceptions across the different types of educational institutions. The dependent variables were the threats aggregated to the level of the five factors of information systems (hardware, software, data, people, and procedures) and the independent variable was the institution type.

To answer Research Question 2, the respondents were asked to provide on the ISPI© instrument their perceptions of the effectiveness of recognized security threat prevention measures on a scale of 1-5 as they applied to their institutions. Thereafter, they were asked to indicate on the ISPI© instrument the time intervals at which their respective institutions reviewed and updated their specific security policies. Finally, the focus shifted to ascertaining the institutional cultures in acknowledging the threats to data and implementing measures to prevent breaches. Respondents were asked to answer questions on the ISPI© instrument about their institutional allocation of operational and personnel budgetary funds and the reporting lines of the head of information technology for this purpose. The data obtained for the threat prevention measures were aggregated to the level of the five factors of information systems: hardware, software, data, people, and procedures (i.e., the group mean was calculated for individual items within each of the five factor groups). Thereafter, responses from similar institutions were grouped together (i.e., the group mean was calculated for each item by institution type) to obtain response profiles for the different types of institutions. The analysis of the data collected was a combination of descriptive statistics to ascertain the overall response

profiles at the factor-level and thereafter at the type of institution level. Five separate one-way ANOVA procedures were conducted to compare threat prevention measures across the different types of educational institutions. The dependent variables were the threat prevention measures aggregated to the level of the five factors of information systems (hardware, software, data, people, and procedures) and the independent variable was the institution type. The responses about frequencies of key security measures and security policy updates were analyzed using descriptive statistics to ascertain the overall response profiles at the institutional level. Two separate ANOVA procedures were conducted to compare the frequencies of key security measures across the different types of educational institutions. The dependent variables were the frequencies of key security measures and the independent variable was the institution type. Finally, the responses obtained from similar institutions for the budget allocation percentages were grouped together (i.e., the group mean was calculated by institution type) to obtain response profiles for the different types of institutions. The analysis of the data collected was completed using descriptive statistics to ascertain the overall response profiles at the type of institution level. An ANOVA procedure was conducted to compare budget allocations for information security across the different types of educational institutions. The dependent variable was the budget allocations and the independent variable was the institution type.

To answer Research Question 3, the respondents were asked to rank their overall information security preparedness on a scale of 1-5. The responses obtained from similar institutions were grouped together (i.e., the group mean was calculated by institution type to obtain response profiles for the different types of institutions). The analysis of the data collected was completed using descriptive statistics to ascertain the overall response profiles at the type of

institution level. An ANOVA procedure was conducted to compare the overall threat preparation index across the different types of educational institutions. The dependent variable was the self-reported information security preparedness level and the independent variable was the institution type.

In addition, analyses correlating the institutional threat identifications, threat prevention measures, frequency of critical measures and security policy updates, and budgetary allocations with the overall institutional information security preparedness were performed. A comparative analysis of security measures that the institutions indicated that they did not perform was also completed.

Variables

The dependent variables for this study were the institutions' self-reported perceptions of security threats and effectiveness of threat prevention initiatives aggregated to the level of the five factors of information systems (hardware, software, data, people, and procedure) along with frequencies of key security measures and allocation of institutional budgets for information security. The independent variable for this study was the different types of educational institutions in the state of Florida involved in the study, namely public and private PK-12 institutions, public and private universities, and virtual schools.

Delimitations

Certain delimitations existed within this study. This research focused on analyzing the preparedness of educational institutions to ensure information security. The data collected for this research took place during the month of March 2018. The research population included chief information officers or equivalent or their designees in a cross section of educational institutions.

This study did not measure the long-term effects of any security measure that these institutions may have undertaken. This study did not make any recommendations to these institutions to implement any particular information security policy or measure.

Limitations

Certain limitations existed within this explorative study. The selected sample was not expected to be representative of the population of interest (the state of Florida), and thus findings were not generalizable although some findings had the potential to be generalized with caution. The researcher examined the characteristics of the sample ex post facto to determine the extent to which the sample might be representative of the population. In addition, this study included responses from the persons in charge of information security at different types of educational institutions. Differences exist in administration of security policies across similar type of institutions and those may not be properly reflected in any conclusion drawn from the responses. In contrast, any specific security measure adopted in an institution with some degree of success may not have the same effect in a similar institution due to other factors. Respondents selected to take part in this study completed the self-reported ISPI©; as such, it is possible for them to either over rate or under rate their security policies and perceptions of security threats.

Assumptions

This study was conducted with the following assumptions: (a) the respondents responded to the ISPI© accurately and honestly; (b) respondents voluntarily completed the ISPI© and could have withdrawn from the study at any point in time; (c) respondents understood the vocabulary and concepts associated with the ISPI©; and (d) the interpretation of the data accurately reflected the perceptions of the respondents.

Organization of the Study

The report of this exploratory research study is organized into five separate chapters. Chapter 1 describes the background of the study, statement of the problem, purpose of the study, significance of the study, definition of terms, conceptual framework, research questions, methodology, limitations, delimitations, and the assumptions of the study. Chapter 2 presents a review of the existing literature on this topic. Chapter 3 describes the methodology and procedures which were used in this study. It includes the selection of participants, instrumentation, data collection, and data analysis procedures. Chapter 4 presents the study's findings including the results of the data analyses for the three research questions which guided the study. Chapter 5 contains a summary of the entire study, discussion of the findings, implications of the findings for theory and practice, recommendations for further research, and conclusions.

CHAPTER 2
REVIEW OF LITERATURE

Introduction

Educational institutions have always been affected significantly by data breaches. According to the Privacy Rights Clearinghouse Chronology of Data Breaches report that tracks all reported data breaches starting from 2005, almost 25 million user records have been breached in educational institutions. In between 2005 and April 2018, there have been 815 reported data breaches in educational institutions (Chronology of Data Breaches, 2018). In the 2017 and 2018 editions of the annual data breach investigations report published by Verizon Enterprises, a total of 747 incidents were identified in educational institutions in 2016 and 2017 alone, 174 with confirmed data disclosure (Data Breach Investigations Report, 2017/2018). Much research has been conducted within the fields of identifying the threats to data security, assessing their impacts, and implementing safeguards to counter them; however little research has been conducted pertaining to (a) the preparedness of educational institutions to handle data security threats and (b) security practices and preparedness across different types of educational institutions.

Information security is a dynamic area that is constantly changing (Vacca, 2012). To keep up with this constantly changing environment, educational institutions need to identify their existing gaps in information security areas by conducting effective risk assessments and address those gaps with implementations of effective security measures with adequate budgetary support (Eling & Loperfido, 2017). The unique characteristics of educational institutions, however, often pose a challenge to attainment of this objective.

In terms of storage of personal identifying information (PII), educational institutions have requirements and practices that are like those of their counterparts in industry. Educational institutions store a significant amount of PII, including educational and health records, and identity information of all personnel involved which may include students, parents, teachers, faculty, administrators and staff (Levy & Ramim, 2016). An average educational institution, however, often lags behind an average industrial enterprise in terms of monetary investment and technical infrastructure necessary for securing such PII adequately. The security measures adopted by educational institutions are often not up to the standards desired in the world of information systems (Cavusoglu et al., 2015). Analyses of cyber-security often reveal that educational institutions have not adequately addressed the cyber-security issues by having appropriate plans in place. Furthermore, such analyses also reveal that information security has often not been considered a key requirement in many educational institutions. Consequently, the volume of data breaches affecting educational institutions has constantly grown. (Powerhouses and Benchwarmers, 2014). Data breaches are expensive. Once their security infrastructure is breached, educational institutions often incur additional expenses in the terms of legal costs, post-breach remedial costs and intangible costs like loss of goodwill (Gardner & Thomas, 2014). Also, they can be subject to class action lawsuits in the wake of a data breach (IT Security for Higher Education: A Legal Perspective, 2003). In an era, where budget shortage in the field of education is a recurring phenomenon, all these factors may continue to contribute to the existing monetary investment deficit for information security that educational institutions have with industrial enterprises (Mitchell et al., 2014).

In terms of timings of breach detection, educational institutions are in a disadvantageous position as compared to their industry counterparts. The user-base of educational institutions has typically been comprised of children and young adults whose identity information once compromised may not be misused instantly, but often years later when they move to the workforce. As such, a detection of a breach is more challenging (Farina, 2015).

In terms of operating culture, there are differences too between educational institutions and industrial enterprises. Although industrial enterprises tend to operate in a profit-centric closed environment, educational institutions have a relatively open culture focused on learning and learner convenience. Thus, the dilemma of balancing the conflicting needs of security and convenience is much higher in educational institutions (Strawser & Joy, 2015).

Thus, information security has been and continues to be a critical yet relatively neglected area in educational institutions. Furthermore, there are potential differences among the types of educational institutions in terms of operating media (example virtual schools vs traditional schools), budgetary support, data breach targets (protected research materials in universities vs PII in schools), security policies, technical expertise, content management, infrastructure, and budget allocations. This makes the process of generalizing the picture applicable to all educational institutions difficult (Hentea, 2005). A comparative analyses of security preparedness among the different types of educational institutions is essential.

This chapter, based on review of literature pertaining to information security in educational institutions, consists of eight sections. The first section concentrates on the characteristics of data stored in educational institutions and their vulnerabilities. The second section illustrates some major data breaches in educational institutions that occurred in recent

years. The third section illustrates the costs of a data breach, highlighting the difficulties of ascertaining such costs. The fourth section highlights the post-breach requirements and legal implications. The fifth section identifies the known common threats that take advantage of vulnerabilities in the five components of information systems. The sixth section concentrates on the known safeguards against data breaches. The seventh section identifies critical measures that institutions need to perform frequently to better protect themselves from security threats, and finally the eighth section illustrates the impact of budgetary support for information security in educational institutions.

An understanding of the literature pertaining to information security discussed in the following eight sections was instrumental in designing the Information Security Preparedness Instrument (ISPI©) that was created and used exclusively for this study.

Data in Educational Institutions

The bulk of the data stored in information systems maintained for educational institutions can be classified into three main categories: (a) personal identifying information from school records, (b) information stored in medical centers, and (c) financial information (Kroenke & Boyle, 2015). Following are descriptions of the data in each of these categories.

Personal identifying information from school records (PII) refers to attributes that can uniquely identify a person. These data can include name, address, birth-date, social security number, and financial information (Chen, Wu, Shen, & Ji, 2011). Educational institutions store a large volume of personal information data from students, faculty, teachers, parents, staff and administrators (Markos, Labrecque, & Milne, 2018). Data breaches of PII in recent times have

occurred in relatively smaller educational institutions as well as in premier institutions of higher education (Chronology of Data Breaches, 2018).

In regard to information stored in medical centers, many educational institutions, particularly higher education institutions have medical centers on or off campus that treat students, staff and often the public as well. In case of large universities that have a medical school, such centers are part of the institution itself. These medical centers store PII and medical records of patients. In recent times, the number of healthcare data breaches in such medical centers have continued to increase. Sometimes breaches are targeted at campus student health centers, rather than large-scale medical centers (McLeod & Dolezel, 2018). Under section 13402(e)(4) of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), institutions that experience a breach of unsecured protected health information affecting 500 or more individuals must report to the Secretary of the Department of Health and Human Services, who then must report a list of the breaches. Therefore, the institutions are required to publicize any large-scale compromise of confidential or sensitive information that they have experienced (Breaches Affecting 500 or More Individuals, 2018).

Student financial information which includes account balances, loan history, credit information, credit cards, debit cards, and other payment forms is often stored in the information systems maintained by educational institutions. Many institutions have put in place payment card systems that allow students to make payments on-campus and at certain off-campus venues (Ngai, Hu, Wong, Chen & Sun, 2011). Additionally, these institutions often use consumer credit reports for background checks on employees and for determining if students should obtain loans (Kroenke & Boyle, 2015). This wide array of financial information is extremely valuable to

perpetrators interested in identity theft and is therefore very vulnerable to data breaches (Shannon & Farley, 2012).

Breaches in Educational Institutions – Case Studies

Breaches Involving Personal Identifying Information

On February 4, 2016, The University of Central Florida (UCF) notified current and former students of a data breach when they discovered unauthorized access into the university system. Two groups of individuals associated with UCF were primarily affected. The first group included some current student-athletes, as well as some former student-athletes who last played for UCF in 2014-15. This group also included some student staff members, such as managers, supporting UCF teams. The second group included current and former university employees in a category known as OPS, or Other Personal Services. Examples of positions in this category include undergraduate student employees (including those in work-study positions), graduate assistants, housing resident assistants, adjunct faculty instructors, and student government leaders. The University responded by offering free credit monitoring services, launching a large-scale investigation into the breach, and holding information sessions on information security (Data Security/Data Breach, 2016).

On September 15, 2015, Louisiana State University (LSU) reported that a doctor associated with the LSU Health New Orleans School of Medicine had his laptop stolen which may have exposed the personal information of 5,000 patients. The laptop computer was stolen from the doctor's vehicle when it was parked in front of his home on July 16 or 17. The theft was reported, but the item was not recovered at the time of the report. The information contained on

this laptop included names, dates of birth and medical information of the affected patients. LSU offered a one-year subscription to a credit monitoring service for any patients affected by the breach (LSU doc's stolen laptop, 2015).

On October 1, 2014, the Provo City School District notified employees of a "phishing" attack attempted on Monday September 29, 2014 which allowed access to employee's email accounts. Some employee email accounts contained files that may have had personally identifiable information (Provo City School District, 2014).

On February 18, 2014, the University of Maryland reported a breach of data systems by a computer security attack. The breached database included 287,580 records of students, staff, faculty, and affiliated persons. The data accessed included names, dates of birth, University identification numbers, and social security numbers of affected individuals. The University responded by offering free credit monitoring services, launching a large-scale investigation into the breach, and holding information sessions on data privacy (UMD Data Breach, 2014).

On February 25, 2014, Indiana University notified the Indiana Attorney General that personal data for students and recent graduates might have potentially been exposed, including names, addresses, and social security numbers for roughly 146,000 individuals. The University opened a call center to establish whether or not any of the individuals were victims of identity theft. Because the data were encrypted, it was difficult for hackers to decode and ultimately, no cases of identity theft were found. In July 2014, the University shut down the call center and closed the investigation, but not until after spending a reported $130,000.67 (IU says no victims reported in data breach, 2014).

Personal information can also be found in admissions records stored in educational institutions. In March 2013, hackers accessed a database of student admission records at Kirkwood Community College in Cedar Rapids, Iowa. They used an international Internet Protocol (IP) address to unlawfully access a website maintained by the college with archived application information. The information accessed may have included applicant names, birthdates, race, contact information and social security numbers. The Community College responded by alerting law enforcement, hiring an outside firm to do a forensic analysis of the breach, and offering credit monitoring to affected individuals (Kirkwood Website Experienced Unlawful Access, 2013).

Breaches Involving Medical Records

On November 26, 2013, the University of Pennsylvania reported a paper breach that affected 3,000 individuals. Additionally, there was a paper theft on the same campus affecting 661 individuals that occurred from May 1, 2014 to June 19, 2014. The paper theft involved stolen receipts from a locked office that included information such as patient name, date of birth, and the last four digits of credit card numbers. The University sent notification letters and began an internal investigation (Burling, 2014).

In March 2014, the University of California – Irvine experienced a breach of student information. Three computers in the Student Health Center were infected with a keylogging virus that captured keystrokes as the user typed and transmitted that information to hackers. The information collected included names, unencrypted medical information, bank names as well as addresses and other medical information. The University offered free credit reporting services to affected students (UC Irvine Student Heath Center, 2014).

Cost of Data Breaches

Data breaches cost money. In some cases, the cost of a data breach is so large that it can put an enterprise out of business. The cost of data breaches often includes regulatory fines such as HIPAA/HITECH and PCI DSS. Other costs result from loss of business, state notification laws, and fixing the security issues that lead to the breach (Gardner & Thomas, 2014). It is often extremely difficult to determine the full extent of the financial and data losses due to a security breach. As a result, a relatively small number of organizations calculate such costs due to the complexity and unknowns involved, and even fewer publish such findings (Furnell, 2009). In 2015, Kroenke and Boyle reported there were no standards for tallying and calculating cyber-crime costs. Moreover, they raised some unanswered questions:

a. Does the cost of a cyber-attack include lost employee time, lost revenue and long-term revenue losses due to loss of clients or customers?
b. What is the cost that may result from the loss of goodwill or reputation that an institution invariably endures after a data breach?
c. If an equipment for example a laptop worth $1,500 is stolen, does the replacement cost include the value of the data that was stored in it or the cost of the time necessary to replace it or re-install software on it?

Studies to determine cost of cyber-crimes have almost always been based on surveys. Often different respondents interpret terms differently (Leveson, 2012). Moreover, there are some organizations that do not report all their losses and there are some that do not report cyber-crime losses at all (Kroenke & Boyle, 2015). In the absence of standards and accurate ways of gathering crime data, estimates are not always reliable (Leveson, 2012).

One potential helpful metric is year-to-year trend analysis, assuming the same methodology is used by the various survey respondents. Table 1 shows the results of such a survey completed over four years from 2010 to 2013 (Cost of Cyber Crime Study – Ponemon Institute, 2013). Amounts shown are in millions of US dollars and indicate computer crime costs per organizational respondent. This survey was commissioned by Hewlett-Packard and performed by the Ponemon Institute, a consulting group that specializes in computer crime.

Table 1

Computer Crime Costs: Ponemon Institute*

Costs	2010	2011	2012	2013
Maximum	$51.9	$36.5	$46.0	$58.1
Median	$3.8	$5.9	$6.2	$9.1
Minimum	$1.0	$1.5	$1.4	$1.3

Note. Costs shown in millions of US dollars
Source. Cost of Cyber Crime Study – Ponemon Institute (2013).

These data underline the problems of tallying crime data from surveys. For example, in 2013, no organization reported a figure less than $1.3 million in loss. It is reasonable to assume that the survey did not include small companies that incurred much smaller losses. Given the large number of small companies, those unknown and unaccounted losses could be substantial (Cost of Cyber Crime Study – Ponemon Institute, 2013).

Recent studies have indicated that the cost incurred by an educational institution in the event of a data breach is increasing and was $260 per record breached in 2017 with a 4-year average of $200 per record (“Cost of Data Breach Study”, 2017).

Post-Breach Requirements

The most critical component of a data breach for an educational institution is its financial implications. Some of these institutions, particularly the smaller ones are not prepared for the high costs of remedying and recovering from a breach and providing services to victims of the breach (O'Neil, 2014). In addition, only a few institutions have had cyber insurance to help offset these costs. Post-breach expenses can include forensics consultants, lawyers, call centers, websites, mailings, identity-protection and credit-check services, and litigation. An intangible expense is the damage to an institution's reputation that occurs when it experiences a breach of data security (O'Neil, 2014). It can be especially difficult for public institutions that rely on state funding to absorb the costs of a cyber-attack (Bielski, 2005).

Data breach insurance is available to educational institutions to help protect them in case a breach occurs. As the threat of cyber-attacks has increased, so have the number of companies buying cyber insurance. Some insurance carriers have begun to specifically market cyber insurance for educational institutions. Insurance benefits may include protections for breach of contract claims, computer forensics, notification costs, regulatory actions, healthcare protections in the case of an on-campus medical center, and hacker damage (Young, Lopez, Rice, Ramsey & McTasney, 2016).

Unfortunately, cyber insurance is expensive and often difficult to obtain. Some insurance companies have required institutions to have strong security procedures in place to be eligible for insurance. If the educational institutions are implementing proper procedures per the FERPA guidelines and the GLBA Safeguard Procedures, their chances of obtaining such insurance increase (Fernandes, 2014).

Timely notification is important. It is important for educational institutions to be familiar with their state's data breach notification laws. There is a wide variation in the laws of each state with respect to the definition of what constitutes a data breach, what a timely notification is, and who needs to be notified. Moreover, some states impose data protection laws on out-of-state entities, which means physical presence in the state is often not required for an institution to be subject to the law. Therefore, if an institution has students from a wide array of states, it may be subject to the notification requirements of each state (Bakhshi, Papadaki & Furnell, 2009).

In Florida, the notification must occur no later than 30 days following determination of the breach. Some state statutes do not have any set amount of time but rather require notification in the most expedient time possible (Burdon, Reid & Low, 2010).

Most educational institutions deal with breaches by offering free credit monitoring to the affected individuals which may include students, faculty, teachers and staff. This involves significantly high costs which might make it more difficult for smaller entities to fund (Young et al., 2016). Offering credit monitoring is often a positive response to a data breach that might convince victims not to sue and convince the court not to levy too harsh a penalty in the case of a suit (UMD Data Breach, 2014).

Legal Implications of Data Breaches

Educational institutions are subject to federal regulations and state statutes which dictate the legal implications of a data breach. Some of the most important ones include the following: Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), FERPA and Cloud Computing, FERPA and Online Educational Services, State Consumer Protection Statutes. These are discussed in the following paragraphs

Health Insurance Portability and Accountability Act (HIPAA) focuses on health insurance portability and on the prevention of health care fraud and abuse by the adoption of standards and requirements for electronic transmission of health information. There are three separate part of HIPAA's information security component: the privacy regulations, the electronic transaction standards, and the security regulations. These three parts regulate the security standards for protected health information, the privacy of patient-identifiable information, and the standardization of electronic transactions (Sitko, 2003).

Education institutions fall under the definition of an entity covered under HIPAA if they provide health care services and engage in one or more covered electronic transactions. Electronic transactions include health care claims, health care payments, coordination of benefits, eligibility for a health plan, and enrollment in a health plan (Liginlal, Sim, Khansa, & Fearn, 2012). Many educational institutions fall under HIPAA because they provide health services to students and often run medical centers in association with their medical programs. However, because of the exception for FERPA educational records, if a center solely services students, it may be exempt from HIPAA (Sitko, 2003).

The Health Information Technology for Economic and Clinical Health (HITECH) Act covers electronic medical records and requires a covered entity to notify affected individuals when unsecured personal health information has been breached. It extended application of both the security and privacy rules of HIPAA. It also amended HIPAA to increase civil and criminal penalties, require notification of data breaches, and change disclosure rules, among others (Stark, 2010).

The Family Educational Rights and Privacy Act (FERPA) covers educational institutions that receive funds for programs administered by the Department of Education. The information covered includes education records, defined as records that contain information directly related to a student and are maintained by the educational institution. Additionally, directory information is covered, defined as information that would not generally be considered harmful or an invasion of privacy if disclosed. Because directory information is not harmful, all that is required of a covered educational institution is public notice of the categories of information which it has designated as such information. Like HIPAA, FERPA does not establish a private cause of action. Only the Secretary of Health and Human Services can bring an action to enforce FERPA (Hillison, Pacini, & Williams, 2001). In Gonzaga University v. Doe, the Supreme Court held that a plaintiff could not sue for damages under 28 U.S.C. §1983 to enforce a FERPA provision (Gonzaga University v. Doe, 2002).

The use of cloud computing has increased significantly in recent years. Some critics have suggested amendment of FERPA with respect to cloud computing to promote more efficient usage. Educational institutions are beginning to take advantage of the convenience of cloud computing as they are drawn to its increased efficiency, mobile access, innovation and access to new services. They are moving storage, messaging, video conferencing and computing power to the cloud (Chopra, Mung, & Chopra, 2013).

In recent years, online education has increased significantly. This has caused a significant increase in the use of online educational services including software, mobile applications, and web-based tools created by third parties by educational institutions. Some of these services use

FERPA-protected information, while others collect metadata related to that information (Moore & Shelton, 2013).

Most states have data breach notification laws. While many such laws have broad provisions that hold anyone in possession of personal information liable for a data breach, some of them are considerably narrower in that they only require notification by specific agencies or businesses in the event of a breach. Moreover, states differ as to who must be notified; some require notification only to consumers, while others require entities to notify credit reporting agencies or the government (Romanosky, Telang, & Acquisti, 2008).

Threats Affecting Educational Institutions

A threat is an entity that attempts to obtain and manipulate information systems data via illegal and secretive means (Jouini et al., 2014). The many threats that are encountered today in the world of information systems that may apply to educational institutions can be broadly grouped into five main categories based on the components of information systems: (a) hardware, (b) software, (c) data, (d) procedures and (e) people (Kroenke & Boyle, 2015). The following paragraphs provide additional detail regarding each of these five main categories.

Hardware-Oriented Threats

Theft

Theft of electronic devices is a major source of data breaches. These devices can include laptops, desktop computers, portable electronic devices such as smart phones, or intact hard drives. A study conducted in 2010 found that theft of such devices compromised seven million

sensitive medical records, and student personal information records from 2009 to the beginning of 2010 (Rhodes & Polley, 2014).

Many educational institutions have a Bring Your Own Device (BYOD) policy that allows users to use their personal devices for professional work (Nicholson & O'Reardon, 2009). Allowing personal devices often allows the transfer of confidential institutional information to the device. Because the device is personal, the educational institution cannot adequately control its security protocols and access policies. Thus, the theft of such personal devices, which are often not encrypted, can put student information at risk (Rhodes & Polley, 2014).

Natural Disasters

This category includes fires, floods, hurricanes, earthquakes and other natural disasters that an educational institution may encounter. For example, given their geographic location, educational institutions in Florida are often prone to exposure by hurricanes every year. Extensive loss to institutional data might take place due to natural disasters if adequate measures are not undertaken. Most educational institutions have extensive disaster recovery plans to help them recover quickly in the event a natural disaster takes place. (Conrad, Misenar, & Feldman, 2016).

Sniffing

Sniffing is a technique for intercepting network-based traffic and communications between a source and a destination computer. If wired networks are involved, this technique relies on physical connectivity. However, with wireless networks which are used heavily nowadays, no such physical connection is necessary. Network sniffers simply take devices with wireless connections through an area and search for unprotected wireless networks. If they find

one, they can easily monitor and intercept wireless traffic. Sometimes, even wireless networks that are protected are vulnerable if the security protocols enforced are not strong enough (Singleton, Singleton & Gottlieb, 2006).

Payment Card Skimmers

Payment card skimmers are often used by perpetrators to electronically capture a victim's personal information from their credit or debit cards. This information can be subsequently used by identity thieves. The skimmer is a small device that scans a credit card and captures the personal information contained in the magnetic strip of the credit card. Educational institutions that deploy payment terminals that accept credit or debit card payments are often vulnerable to have users' PII stolen using such skimmers. Duplicate cards are often created using that information and used thereafter, almost immediately, before such a fraudulent use can be detected (Rockwell, 2013).

Software-Oriented Threats

Ransomware

Ransomware is a form of software that prevents or limits users from accessing their systems or personal computers. This type of software forces its victims to pay a demanded ransom through certain specified online payment methods to regain access to their systems, or to reclaim their data back. The ransom price is often quoted in its bitcoin equivalent. It is important to note that paying the ransom does not guarantee that users eventually regain access to the infected system. In certain cases, they only reclaim part of the data (Al-rimy, Maarof, & Shaid, 2018).

Users may encounter this threat through a variety of means. Ransomware can be inadvertently downloaded by unsuspecting users if they visit malicious or compromised websites. Some ransomware is often delivered as an attachment to an email. Once executed in the system, ransomware can either lock the computer screen or encrypt predetermined files with a key. In the first scenario, ransomware shows a full-screen image or notification, which prevents victims from using their system. This notification typically delivers the instructions on how users can pay for the ransom. The second type of ransomware locks files like documents, spreadsheets and other important files (Mansfield-Devine, 2017).

Two very common and fast-spreading ransomwares are the WannaCry and the LOCKY. These ransomwares spread typically via attachments to emails often as a JavaScript-file. They can also be spread through executable files. Once the attachment is accessed, the JavaScript runs a program that encrypts all files on the user's computer including those on network drives, removes the originals and deletes any system restore point so that the machine can never be reverted to an earlier state. It then creates a desktop message (as shown in Figure 2) that asks the user to pay the ransom using bitcoins via a TOR browser (Furnell & Emm, 2017).

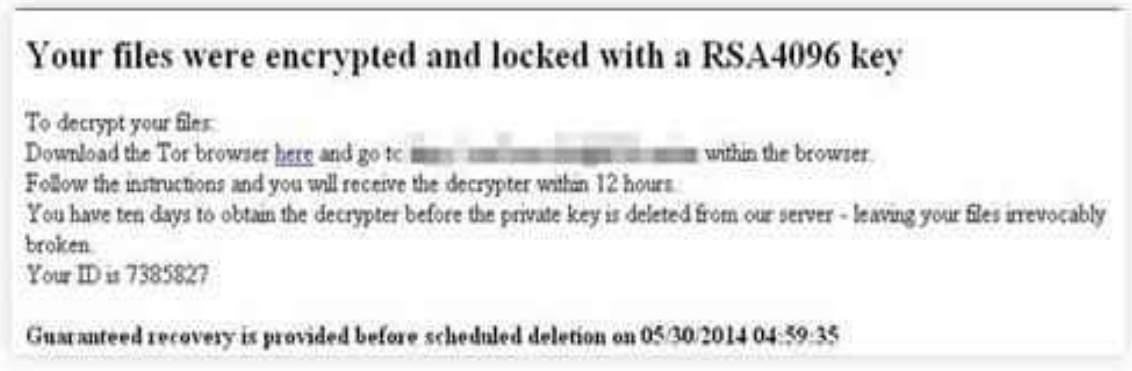


Figure 2. Ransomware – LOCKY.

Source: Stetson University. (2018). *Information Security Handbook*. DeLand, FL.

Unless the user has the data backed up in an alternate location, data-loss is inevitable in such a scenario. A South Carolina school district paid an estimated $10,000 in 2016 when cyber-criminals locked its computer servers. As per the Federal Bureau of Investigation, cyber-criminals collected $209 million using ransomware in the first three months of 2016 by extorting businesses and institutions to unlock computer servers. (Fitzpatrick & Griffin, 2016).

Malware

The term malware refers to an assortment of viruses, spyware, and other unwanted software that can get installed on a users' computers or mobile devices without their knowledge or consent. This often happens when a user visits a malicious website or downloads an unauthorized program from the web (Noor, Abbas, & Shahid, 2018). These programs can cause the device to crash. More importantly, they can be used to monitor and control the user's online activity. They can often make the device deliver unwanted or inappropriate ads (Pectas & Acarman, 2017).

There are many different types of malware, from spyware to key loggers, to computer viruses. Some types of malware, such as financial malware, which is designed to scan a computer system for information related to financial transactions, are more common than other types (Noor et al., 2018). One example is a malware named Cridex. It monitors login pages, cookies and steals user credentials (Touchette, 2016). Other common ones like the FAKEAV malware trick users into purchasing bogus anti-malware software by showing fake anti-malware scanning results (Pectas & Acarman, 2017).

Structured Query Language (SQL) Injection

SQL injection is a type of security attack in which the attacker adds Structured Query Language (SQL) code to a web form input box, which in turn makes changes to data within the database. This allows the perpetrator to gain access to unauthorized resources and information. This information may include sensitive institutional data, user lists or personal information of users, which are typically used for subsequent fishing attacks (Cherry, 2015).

Web Application Attacks

Web application attacks are conducted using software programs that are written to probe a user's computer and automatically exploit security holes or vulnerabilities if any. Such exploits may provide a path into the user's system core for subsequent deeper intrusions (Wilhelm, 2013). Some hackers may inject malicious code within vulnerable web applications to trick users and redirect them towards phishing sites that they maintain. This technique is called cross-site scripting and may be used even when there are no vulnerabilities in the associated web servers and database engines. (Razzaq, Latif, Ahmad, Hur, Anwar, & Bloodsworth, 2014).

Outdated Anti-Virus and Anti-Malware Software

Anti-virus and anti-malware software on personal computers and servers protect the machines from viruses and other malware threats. However, if these software programs are not kept up to date, they lose their efficiency and effectiveness as they cannot detect any newer threats that are created almost on a daily-basis (Bourne, 2014).

Data-Oriented Threats

Unpatched systems

Computer systems and machines that have not been kept up to date with the latest security patches are the most vulnerable to be exploited. Unfortunately, some institutions are never up-to-date with their patching process due to lack of resources or personnel. In fact, patching computers is sometimes regarded as a tedious exercise and is not always seen as a vulnerability concern. Institutions often shy away from addressing regular patches and routine software upgrades because they have concerns about price, time, and complexity. Therefore, exploitation of unpatched systems remains a serious risk to institutions and the underlying cause of many data breaches (Andress, 2014). Recent years have seen significant advances in automated patching mechanisms, yet managing updates remains a challenge. Factors like the sheer number of updates, limited bandwidth, lack of security personnel can discourage institutions from patching as often as they should. This creates a security gap which can expose institutional data for unauthorized access (Furnell, Niekerk, & Clarke, 2014).

Cyber – espionage

The term cyber-espionage stands for a set of processes that deals with the theft of intellectual property and confidential information from computer systems. Often these processes are politically motivated (Shakarian, Shakarian, & Ruef, 2013). In the education sector, cyber-espionage primarily targets institutions of higher education, especially research universities as they usually store a vast collection of expensive and often unpublished research work (Thompson, 2015).

Institutional Data on Personal Devices

Increased use of personally owned devices offers convenience, productivity gains, and job satisfaction. Many educational institutions have a Bring Your Own Device (BYOD) policy that allows users to use their personal smart phones, tablets or laptops for professional work (Nicholson & O'Reardon, 2009). There are, however, significant risks of data exposure if these devices are accessed by unauthorized individuals or entities. In addition, there is always a risk that data used on a personal device might violate institutional contracts or violate state or federal laws and regulations (Rhodes & Polley, 2014).

Unencrypted Data Transfers

Educational institutions receive and send a large volume of data as part of their routine operations. Such data is transmitted through computer networks all the time. To maintain the security of the data being transferred, it needs to be encrypted with security keys which can only be decrypted by the intended recipient. If left unencrypted, sensitive data may be intercepted and exposed (Rashti, Sabin, & Kettimuthu, 2016).

Institutional Data on Third Party Services

With the advent of cloud-based services, more and more institutional data are being shared with third-party providers of cloud-based services to conduct business. Institutional data remains vulnerable if adequate security measures are not implemented by such third-party providers (Tan, Hijazi, Lim, & Gani, 2018).

Procedure-Oriented Threats

Hacking

Hacking involves breaking into computers, servers, or networks to steal data such as customer lists, product inventory data, employee data, and other proprietary and confidential data (Kroenke & Boyle, 2015). Typically, inadequate security protocols implemented by the system administrators or unsafe practices by its users facilitate the processes involved in hacking. Those include weak passwords, short passwords, and commonly-used passwords among others. Short passwords are especially vulnerable to a brute force attack in which the password cracker tries every possible combination of characters. The shorter the password, the higher the chances of it being cracked. Commonly-used passwords like "password" are relatively easy to guess (Shen, Yu, Xu, Yan, & Guan, 2016). Sophisticated probing processes used by hackers often scan browser cookies on public computers. Browser cookies are small files that a browser stores on a user's computer. When the user visits web sites, cookies enable access to sites without having to sign in every time, and they speed up processing on some sites. However, some cookies also contain sensitive security data from visited authenticated sites that may be read by malicious hackers (Gold, 2011).

Spoofing

Spoofing is term used to describe someone pretending to be someone else. Internet Protocol (IP) spoofing occurs when an intruder uses another web-site's IP address to masquerade as the original web-site (Kroenke & Boyle, 2015). By modifying the source address of attacking traffic to an address assigned to others or not assigned, or by using a proxy-machine with a fake

IP address, attackers can hide their actual locations, or bypass established access control rules (Yao, Bi, & Xiao, 2013).

Denial of Service

A denial of service (DoS) is a type of attack where the attackers attempt to prevent legitimate users from accessing a service. In a DoS attack, the attacker sends an extremely high number of bogus messages asking the network or server to authenticate requests which in turn have invalid return addresses. Consequently, the network or server is unable to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more bogus authentication messages with invalid return addresses. Hence, the process of authentication and server wait will resume, keeping the network or server extremely busy and inaccessible for legitimate users (Oliveira, Laranjeiro, & Vieira, 2015).

Elevation of Privilege

A privilege elevation attack is a type of network intrusion that takes advantage of errors in programming logic or flaws in design to grant the attacker elevated access to the network. Elevation of privilege results from an attacker gaining authorization permissions above and beyond those originally granted. For example, an attacker with a privilege set of read only permissions somehow elevates the set to include read and write (Knapp & Langill, 2015).

Inadequate Security Monitoring

Even the most sophisticated security measures can be rendered ineffective without adequate monitoring. Monitoring a computer system typically includes installing software on the

network that sends alerts to the administrators of the system about any issues that the system may be experiencing. Additional benefits of real-time analytics may be obtained by using such monitoring software. Unfortunately, some institutions are not pro-active in implementing security monitoring which increases the possibilities of intrusion attempts going undetected (Sanders, 2014).

Inadequate Backups of Institutional Data

Inadequate data backups invariably cause critical data losses. Data volume, limited storage capacity, and inadequate backup and restore policies are backup related challenges. At the time of the present study, explosive data growth had further compounded these performance and capacity issues. To maintain efficiency of institutional operations, data needs to be backed up frequently, restored quickly, and protected constantly (Kroenke & Boyle, 2015).

People-Oriented Threats

Improper Disposal Practices

Although most personal information is now stored electronically, there can be breaches resulting from an improper disposal of paper records involving personally identifiable information (Leveson, 2012). These paper breaches make up nearly 26% of breaches (Chronology of Data Breaches, 2018). Sometimes the breach comes from something as simple as a user throwing confidential institutional information in the trash as opposed to taking more secure measures such as shredding them before disposing. The same issue can arise with electronic records due to the improper disposal of hard drives or other media in publicly accessible places (Leveson, 2012).

User Errors

User errors may result from accidental and/or negligent human actions. For example, a school system database administrator may inadvertently install an old database on top of an existing one causing loss or corruption of data. In contrast, a school administrative staff-member may store a data file with confidential information on a publicly accessible folder, thereby exposing it to the whole world via the web (Leveson, 2012).

Phishing

Phishing is a technique for obtaining unauthorized data that primarily happens via email messages. The perpetrator claims to be a legitimate company and sends an email (that looks very similar to the original site in look and feel) requesting confidential data, such as social security numbers, and account passwords, among others (Kroenke & Boyle, 2015). Often, they send a link in an email that takes the user to a fake login page that looks very similar to one that the recipient is accustomed to visit. The unsuspecting user may enter his credentials on such a page thereby exposing them to the perpetrator (Aleroud & Zhou, 2017).

Weak Passwords

Some passwords are easy to guess or crack with password identification algorithms. These include weak passwords, short passwords, and commonly used passwords among others. Short passwords are especially vulnerable to a brute force attack in which the password cracker tries every possible combination of characters. The shorter the password, the higher the chances of it being cracked. Commonly-used passwords like “password” are relatively easy to guess (Shen et al., 2016).

Malicious Insider

Malicious insider threats refer to deliberate attempts by an insider to access and potentially harm an organization's data, systems or IT infrastructure often for financial gain, retribution, or some other motivation (Jones, 2008). These types of threats are often extremely difficult to detect and mitigate, as an insider may potentially be more knowledgeable than an external attacker about the target system and is therefore more effective at defeating security controls that mainly defend against external attacks (Liu, Wang, & Camp, 2008).

Safeguards against Data Breaches

Information is one of the most prominent assets for educational institutions and therefore needs to be protected from security threats. Prevention of data breach initiatives involve applying safeguards at both personal and institutional levels (Joshi & Singh, 2017). Some critical safeguards classified using the five factors of information systems (hardware, software, data, procedures, and people) are as follows:

Hardware-Oriented safeguards

Removing Stored Personal Identifying Information from Computers and Mobile Devices

Computers and mobile devices may potentially store personal identifying information (PII) of the owner. By using secure encryption techniques or by relying on biometric characteristics, such storage of PII may be avoided. In the event such devices are stolen or accessed by an unauthorized person, the absence of any PII on such devices may limit further damage of such being exposed (Lee, 2017).

Using Biometric Authentication for Accessing Secure Areas

Biometric authentication is a security process that relies on the unique biological characteristics of individuals to verify their identities. Finger-prints are the most commonly used biometric characteristics that uniquely identify an individual. In recent times, eye-retina and face-recognitions have been increasingly used by institutions as well. Biometric authentication systems compare a biometric data capture to stored, authentic data in a secure database. If both match, authentication is confirmed. Typically, biometric authentication has been used to manage access to resources such as buildings, rooms and mobile devices (Ogbanufe & Kim, 2018).

Software-Oriented Safeguards

Clearing Browsing History, Temporary Files and Cookies from Public Computers

Using cookies and browsing history that are stored on a user's machine may result in information may be obtained that may subject a user's account to unauthorized access. Further, a user may leave the machine without logging out from all services. Thus, on a public machine, the next user may get access to the previous user's information. A critical safeguard in this situation for educational institutions is to program the system so that cookies and browsing history are removed from the browser when the user signs off. A provision to time out the user session once the user leaves his machine unattended after a certain amount of time has elapsed is helpful as well (Jia, Chen, Dong, Saxena, Mao, & Liang, 2015).

Regularly Updating Anti-Virus and Anti-Malware Software

Anti-virus and anti-malware software on all institutional computers and servers protect those machines from virus and malware threats. However, if they are not kept up to date, they

lose their efficiency as they cannot detect new threats. Thus, keeping them automatically updated is critical for educational institutions(Townsend, 2010).

Installing Institutional Firewall

To protect the institutional network from security threats on the public internet, an educational institution may implement a firewall at the intersection of the institutional network boundary and the internet. The border firewall operates a "default deny" policy. This means that only traffic that has been specifically permitted is allowed through the firewall (Goralski, 2017).

Installing Institutional Virtual Private Network

A VPN, or Virtual Private Network, is a service that allows a user to connect to the internet via a server run by a VPN provider. All data traveling between the user's computer, phone or tablet and this "VPN server" is securely encrypted. Educational institutions may allow access to critical web-based services and applications from off-campus locations only via the VPN to prevent network-based intrusions (Richter & Wood, 2016).

Data-Oriented Safeguards

Using Central Authentication and Single Sign on

Central authentication allows applications to authenticate the user based on credentials stored in a single repository. Single sign on allows users to access multiple applications after providing their credentials only once. In other words, a user can login to multiple web-applications using the same username and password. Once the users are logged in to one web-application, they are not required to provide their credentials for accessing another web-application. They are signed on by default. Implementing both these measures allows the educational institutions to focus on implementing advanced security protocols at the sign in stage

which by design extend to all applicable web applications (Nacer, Djebari, Slimani, & Aissani, 2017).

Using Multi-factor Authentication

Multifactor authentication (MFA) is a security protocol that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. In an MFA scenario, users are initially presented a login screen to a web-application. Once they successfully enter their credentials, the system requires them to validate the authentication on another device, typically the user's mobile phone to complete the process. The idea behind this safeguard is the reasoning that even if perpetrators know a users' usernames and passwords, the possibility of their having access to a second device (the mobile phone in the example) at the same time is remote (Velasquez, Caro, & Rodriguez, 2018).

Using Encryption for Data Transfer and Storage

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data are commonly referred to as ciphertext, and unencrypted data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by educational institutions. Two main types of data encryption exist--asymmetric encryption, also known as public-key encryption, and symmetric encryption (Kroenke & Boyle, 2015).

User Authorization

Authorization is the process of giving someone access and privileges to specific components of an information system. In multi-user computer systems, a system administrator defines for the system which users are allowed what levels of access to the system and what are

the privileges of use (example file directories, data access etc.). If done effectively and adequately, authorization can prevent data exposure by restricting access as necessary. (Information Resources Management Association, 2017).

Procedure-Oriented Safeguards

Implementing a Password Policy for Strong, Complex and Long Passwords

Researchers have shown that strong, long and complex passwords are a big deterrent to cyber perpetrators as they get exponentially difficult for them to crack them. Some rules for password complexity may include: creating passwords that are at least 8 characters long and containing one uppercase letter[A-Z], one lowercase letter[a-z], one numeric character [0-9] and one special character from the set: ` ! @ $ % ^ & * ( ) - _ = + [ ] ; :. Certain attributes like login ID, email address, first, or last name are not recommended to be a part of the password (Shen et al., 2016).

To get an idea about the time it may take for a perpetrator using brute force methods to crack a password, modern algorithms show that the length plays the biggest role in establishing complexity. For example, nine-character passwords may take five days to break, 10-character passwords may take four months, and 11-character passwords may take ten years. If the length is increased to 12 characters, it may take up to 200 years to crack (Estimating Password Cracking Times, 2018).

Making Users Change Passwords Frequently

Password breaches may not be detected right after they happen. Often, they are not discovered until months go by. Having a policy of frequent password changes (at least once in three months) is a vital safeguard. This is critical for institutions as users often tend to use the

same password for multiple sites. If a perpetrator can guess a user's password for one site, the other applicable sites to which that user has access may also be at risk as the potential for the password to be the same for multiple sites is relatively high (Woods & Siponen, 2018).

Taking Regular Backups of Key Data

A good backup strategy is essential for data security. A backup is the last line of defense against data loss, providing a way to restore original data (Groot, 2017). Backups are even more crucial if they are completed in real-time. This is because restoring from a backup even a day-old can result in partial data-loss especially for transactions or changes that happened after the last backup was taken (Cherry, 2015). This is a critical component for business continuity and disaster recovery protocols, especially for institutions in states like Florida that are prone to natural disasters and may experience data loss due to them (Torres & Alsharif, 2016).

Implementing Post-intrusion Attempt Remediation Procedures

A data-breach comes with legal implications which force educational institutions to take additional post-intrusion remediation steps. Some common procedures include informing the authorities, blocking rogue IP addresses, offering credit monitoring for affected users (Young et al., 2016).

Applying Critical Server and System Patches Regularly

A patch is a specialized software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and system malfunctions, also known as bugs. Thus, such fixes are called bug fixes. Institutions need to perform this critical step of applying patches and bug fixes on their information systems on a regular basis to improve their security, usability, and performance (Bourne, 2014).

People-Oriented Safeguards

Avoid Opening Emails from Unknown Sources

Emails are the primary media for directing users to phishing scam web-sites which are usually presented as links within the email. Educating the user base on the dangers of phishing and instructing them to avoid clicking on links in the email unless they are sure of their authenticity is a critical security measure (Vayansky & Kumar, 2018).

Avoid Opening Attachments to Emails from Unknown Sources

Attachments containing harmful malware and ransomware are often circulated using emails. Educating users about dangers of such attachments is critical so that they are careful about ignoring attachments from unknown sources (Sammons & Cross, 2017).

Avoid Visiting Unauthorized Websites on Work Computers

Unauthorized websites may contain hidden viruses that may get downloaded on the computers from which they are accessed and may subsequently damage institutional data by propagating through the institutional network. Some institutions enforce safe-use policies for work machines that prohibit users from visiting such unauthorized and black-listed websites (Tanaka, Akiyama, & Goto, 2017).

Avoiding Sending Valuable and Confidential Data via Email or Instant Messages

It is important to avoid sending confidential data using emails as messages may get intercepted in transit or be accidentally delivered to an unauthorized recipient if the email address is entered incorrectly. In addition, there is no guarantee that the recipients' email addresses are always accurate or have not been compromised. Thus, sending emails, while not

being completely sure of their intended destination, might expose such confidential data (Sammons & Cross, 2017).

Check for Https in Website Addresses That Require Authentication

Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data are sent between the users' browsers and the websites that they are connected to. The 'S' at the end of HTTPS stands for Secure. It means all communications between the user's browser and the website are encrypted. Thus, checking for the presence of the https protocol is critical especially for websites that require users to enter credentials to verify their identity (Virvilis, Mylonas, Tsalis, & Gritzalis, 2015).

Employ a Dedicated Information Security Officer

The Chief Information Security Officer (CISO) is a senior-level executive responsible for developing and implementing an information security program, which includes procedures and policies designed to protect enterprise communications, systems and assets from both internal and external threats. Information security is a specialized dynamic area that requires expertise and training for optimal utility. Those institutions that invest in employing a dedicated CISO show the commitment to stay ahead of the information security challenge-curve (Hooper & McKissack, 2016)

Training Users on New Security Threats

The world of security threats changes constantly. New threats are launched regularly. It is imperative for an institution focused on information security to continually train its users on new security threats to keep them up to date (Caballero, 2017).

Frequency of Critical Measures

Implementation of data security measures in institutions is not enough by itself. The implemented measures need to be repeated at an acceptable frequency for them to remain effective. Some critical measures applicable to educational institutions are described in this section. They are classified as high or low frequency measures depending on the number of repetitions that can be completed within a year (Caballero, 2017).

High Frequency Measures

Measures that need to be repeated multiple times in a year for optimal effectiveness are classified as high frequency measures (Caballero, 2017). Three measures are discussed in the following paragraphs: (a) honey pot experiments, (b) social engineering experiments to enforce security protocols, and (c) log review and monitoring.

A honeypot is a computer system (typically a server on the network) that is set up by security administrators of an institution to act as a decoy to lure cyber-attackers. This is done by relaxing security protocols on the server, thereby making it visible and inducing cyber-attackers to attempt to get into it. No confidential information is stored on that server, but some fake information may be entered to make the data look authentic. The purpose of such honeypot experiments is to gain an insight into attempts to gain unauthorized access to information systems as they apply to that institution so that they can be better prepared to counter them (Christopher, Choo, & Dehghantanha, 2017).

To ensure that their users are following adequate security protocols, institutions may send communications like phishing emails on a periodic basis to a cross-section of their user-base to check the responses. The selection of users identified to receive such emails may initially be

made at random but later targeted to ensure that repeat offenders or those with a propensity to be phished are always included. Penalties for clicking on the links in the email include curbing access to critical services for such users, pending their passing compulsory security classes. For repeat offenses, their access may be suspended or in more severe cases, the employee may be terminated (Gardner & Thomas, 2014; Stetson University, 2018).

A breach can be identified much before it is reported to have happened. Any access or attempts to access an institution's servers and network are recorded in system and server logs. Administrators could review and monitor these logs for clues and patterns that may help them identify potential breaches or intrusion attempts to access the institution's information systems (Wang, Liu, Pitsilis, & Zhang, 2018).

Low Frequency Measures

Due to the time and resources involved, some of the critical measures are not cost-effective enough to be repeated multiple times a year. Often these measures require the involvement of outside agencies. They are classified as low-frequency measures (Caballero, 2017) and are discussed in the following paragraphs.

Internal Security Audit

A security audit of an institution's information security infrastructure and policies may be conducted by the internal audit unit of the institution to identify areas where improvement is needed. Some institutions have dedicated internal audit teams that conduct such procedures routinely. Because such audits are completed by employees of the institution, there are no extra costs associated with the process, and there is no additional risk of institutional data being exposed to a third-party (Steinbart, Raschke, Gal, & Dilla, 2012). Some higher education

institutions often allow students enrolled in a computer security class at the institution to perform an internal security audit for the institution as a part of their coursework (Stetson University, 2018).

External security Audit

A security audit of an institution's information security infrastructure and policies may be conducted by an external independent agency to rectify shortcomings and identify areas of improvement. These audits are typically carried out by experts in their fields. Consequently, there is a significant cost associated with this process. Specialized tools and software are often used for external audits. Because they are conducted by people outside the institution, internal biases are avoided (Kovacich & Halibozek, 2017).

Review of Institutional Security Policies and Change Management Policies

Information security is a dynamic field. As security threats change and become more sophisticated, an institution's security policies and change management policies also need to change to keep up. Therefore, institutional security policies and change management policies need to be reviewed periodically to ensure that they are updated with the necessary changes (Adi, Hamza, & Pene, 2018).

Attendance of Information Technology Personnel at Information Security Classes

Staff working in information security areas can be more productive and efficient if they can enhance their skills and knowledge by attending information security classes. Some of these classes prepare security personnel with the concepts of ethical hacking that allow them to enhance their skills in tackling security threats more efficiently (Caballero, 2017).

Mandatory Training on Security Topics for all Employees

Threats to information security change constantly. Adequate training on a regular basis can keep institutional staff updated about the latest threats and applicable safeguards so that they can implement those in practice. There is never a substitute for relevant training. An institution that regularly trains its staff, especially on security aspects, is usually well-prepared to tackle the ever-changing security threats. If such trainings are made mandatory and routinely enforced, an institution can ensure that none of its staff are left behind in any area related to threats and safeguards (Caldwell, 2016)

Review of Data Breach Remediation Procedures

Breach remediation procedures that include cyber insurance policies, post-breach actions need to be reviewed by the institutions periodically to keep them up to date (Young et al., 2016).

Review of Business Continuity and Disaster Recovery Policies

Data breaches, unauthorized access, malware or natural disasters can affect an institution's business continuity. In cases of technical or natural disasters, an institution needs to have plans in place to recover from any disruption of service quickly and resume normal operations efficiently. These business continuity and disaster recovery plans need to be reviewed periodically to ensure accuracy, reliability, and adaptability (Snedaker & Rima, 2014).

Review of Data Backup Policies

An efficient data backup policy is essential for data security. A backup is the last defense against data loss, providing a way to restore original data. This data policy is expected to be reviewed periodically to ensure that data are backed up optimally while considering advanced

methods of data backup to enhance efficiency in creating backups and restoring from them (Cherry, 2015).

Budget Allocations for Information Security

In recent years, especially after the economic downturn towards the end of the last decade, almost all states in the United States had to endure budget cuts, especially in the field of education (Serneels, Beegle, & Dillon, 2017). This, in turn, has negatively impacted the ability of educational institutions to implement sophisticated information security related initiatives. Budgets allocated for information security in educational institutions form a part of the total budget for information technology initiatives which experienced cuts due to the overall budgetary situation of education in general. Private institutions that did not typically rely on state funding, but were instead funded by revenue generated from enrollments, were also negatively impacted due to the economic downturn which caused lower enrollments in such institutions (Urquiola, 2016). However, with the relative stabilization of the economy in recent years, enrollments in private institutions have increased (Serneels et al., 2017).

Information technology (IT) budgets are typically allocated as a function of the total operating budget of an institution which, in turn, is related to its revenue and size. Interestingly, the allocation of funds for information technology has been higher for smaller institutions. According to a recent 2018 publication, the average small institution (less than $50 million in revenue) spends 6.9% of their revenue on IT; Mid-sized institutions (between $50 million – $2 billion) spend 4.1%, while larger institutions (over $2 billion) spend a relatively tiny 3.2%. The relatively smaller allocation in larger institutions is probably related to economies of scale obtained from operational efficiencies (How Much Should a Company Spend on IT?/Business

Guide, 2018). Institutions spend on an average 5.6% of the overall IT budget on information security and risk management with a range of 1% to 13% (Gartner Says Many Organizations Falsely Equate IT Security Spending with Maturity, 2016).

In recent years, a majority of proposed and enacted budget proposals at both the state and federal levels have curtailed budgets allocated for the fields of education. Technology and personnel budgets have thus been impacted across most educational institutions. Although some premier higher education institutions have used donor, endowment and grant money to power technology initiatives, the impact on state run public schools due to the budget cuts has been the most significant (Kelly & Rohland, 2017). Often, schools have no dedicated full-time personnel allocated for information technology and security areas. Those who oversee those areas have other responsibilities as well. In a specialized area such as information security, a lack of specialization has had detrimental effects (Fay & Patterson, 2018).

Critical issues like teacher shortages and school closures have affected education at its very core. Areas like information security, although serious, have not historically ranked very high in the list of priorities for educational institutions and are facing continuous challenges. In such an environment, keeping up with constant changes in the field of information security for educational institutions dealing with budget cuts has been increasingly difficult (Furnell et al., 2017).

Summary

Information security is a dynamic concept. Threat mitigation mechanisms that were prevalent and effective in the past may not be valid today as the threats themselves constantly change. To keep up in this dynamic environment, educational institutions need to constantly

evaluate their existing security practices and make necessary enhancements as needed to protect their confidential information, which includes the personal identity information (PII) of their users. Adequate infrastructure, personnel, and budgetary support are necessary for educational institutions to achieve this objective, but they lag behind industrial enterprises in this regard. Moreover, infrastructure, personnel, and budgetary differences may exist between the types of educational institutions. A review of relevant literature pertaining to information security in educational institutions showed a dearth of research pertaining to the preparedness of educational institutions to handle data security threats and any associated research comparing information security practices and preparedness across different types of educational institutions. Thus, this chapter focused on research of attributes necessary to conduct such a comparative analysis of different types of educational institutions with respect to their information security preparedness. The information obtained was instrumental in designing the Information Security Preparedness Instrument (ISPI©) that was created and used exclusively for this study.

CHAPTER 3
METHODOLOGY

Introduction

The primary goal of this study was to investigate the research questions that relate to the preparedness of educational institutions toward ensuring the security of their institutional information as stated in Chapter 1. A survey instrument titled Information Security Preparedness Instrument (ISPI©) was created exclusively for this study by the researcher. An online survey tool named Qualtrics was used to distribute the survey instrument and obtain the data for the study. The methodology used to investigate the research questions is presented in this chapter which has been organized into five sections: (a) research questions, (b) selection of participants, (c) instrumentation, (d) data collection and, (e) data analysis.

Research Questions

The following research questions were used to guide this study:

1. What is the level of preparedness to counter threats to information security among educational institutions with respect to identification and classification of threats, and how do results vary across the types of institutions?

   This question was further divided into five sub-questions based on the five factors of information systems (Kroenke & Boyle, 2015):

   1.1. What differences (if any) exist in the perception of security risks for hardware-oriented threats among the different types of educational institutions?

1.2. What differences (if any) exist in the perception of security risks for software-oriented threats among the different types of educational institutions?

1.3. What differences (if any) exist in the perception of security risks for data-oriented threats among the different types of educational institutions?

1.4. What differences (if any) exist in the perception of security risks for procedure-oriented threats among the different types of educational institutions?

1.5. What differences (if any) exist in the perception of security risks for people-oriented threats among the different types of educational institutions?

2. What is the level of preparedness to counter threats to information security among educational institutions with respect to institutional safeguards, frequency of critical measures and security policy updates, and budgetary allocation, and how do results vary across the types of institutions?

   This question was further divided into eight sub-questions based on the five factors of information systems (Kroenke & Boyle, 2015), frequency of critical measures and security policy updates, and budgetary allocation:

   2.1. What differences (if any) exist in the perception of the effectiveness of hardware-oriented security measures among the different types of educational institutions?

2.2. What differences (if any) exist in the perception of the effectiveness of software-oriented security measures among the different types of educational institutions?

2.3. What differences (if any) exist in the perception of the effectiveness of data-oriented security measures among the different types of educational institutions?

2.4. What differences (if any) exist in the perception of the effectiveness of procedure-oriented security measures among the different types of educational institutions?

2.5. What differences (if any) exist in the perception of the effectiveness of people-oriented security measures among the different types of educational institutions?

2.6 What differences (if any) exist in the frequencies of implementation of high-frequency critical practices among the different types of educational institutions?

2.7. What differences (if any) exist in the frequencies of implementation of low-frequency critical practices and security policy updates among the different types of educational institutions?

2.8. What differences (if any) exist in budgetary allocation related to information security among the different types of educational institutions?

3. What is the overall self-reported level of preparedness among educational institutions with respect to information security, and how do results vary across the types of institutions?

Selection of Participants

The population of interest for this study consisted of a cross-sectional representation of the following types of educational institutions in the state of Florida: public and private PK-12 institutions, public and private universities, and virtual schools. Because the threat to institutional data applies to all educational institutions, a representation of different types of educational institutions was necessary for an accurate analysis, as they are subjected to different levels of constraints with respect to ensuring information security.

The information systems in PK-12 Public Schools in Florida are managed at the school-district level. There are 67 school districts in Florida, one for each county. Each of the 67 school districts operate virtual schools (Virtual Education, 2018). In addition, there is a state-run Florida Virtual School along with several virtual schools both tuition free and private that are not operated by the state (Online Learning with a K12 Education, 2018). There are also 3,072 PK-12 Private Schools that operate in Florida (Private School Directory, 2018). Finally, there are 85 Public Colleges/Universities and 57 Private Colleges/Universities in the state (Florida Colleges and Universities – Colleges Search by State/Cappex, 2018).

The criterion for selection of the participant institutions for the study was the online availability of contact information of their respective heads of information technology. The contact information for the heads of information technology for PK-12 Public Schools was available online for all 67 school districts. Similarly, the contact information for the heads of

information technology for PK-12 Virtual Schools was available online for all 67 school districts, the Florida Virtual School, and two non-state-run virtual schools, thereby totaling 70 virtual schools. The numbers of PK-12 Private Schools, Public Colleges/Universities, and Private Colleges/Universities for which the contact information for the heads of information technology was available online were 20, 30, and 30 respectively. Thus, using a method of criterion-based purposive sampling, a total of 218 institutions were chosen for the study.

A researcher-created survey, Information Security Preparedness Instrument (ISPI©), was used for this study. Emails containing a link to this researcher-created survey were sent in March 2018 to the respective heads of information technology at the 218 selected educational institutions.

Data Collection

Approval was obtained from the Institutional Review Board (IRB) at the University of Central Florida. The approval can be seen in Appendix A. The data for this study were obtained from the respondents using a survey instrument titled Information Security Preparedness Instrument (ISPI©) which was based on the Qualtrix Survey tool and created exclusively for this study by the researcher (See Appendix B). This 68-question online survey was designed to take approximately 10-15 minutes to complete. Given the nature of the questions involved regarding institutional information security and to protect the confidentiality of the respondents, the survey was designed to be anonymous. The researcher provided all respondents involved in the study with an informed consent form (Appendix D), which includes a clause stating that the participant can withdraw from the study at any time. The consent form was added as an attachment to the email that was sent to the respondents. The email briefly explained the research study being

conducted and provided the respondent with a choice to participate and a link to access the web-based ISPI© instrument. Prior to beginning the instrument, the respondents were asked to confirm their consent to take part in this study. They had to agree to participate in the ISPI© instrument before being able to begin.

Web-based surveys are a convenient and popular method of data collection, especially if they are directed toward an internet-savvy population. However, a "survey-overload" is often created as many research initiatives and other data collection initiatives use this method. Consequently, the response rate for such surveys has declined over the years (Morton et al, 2012). Nulty (2008) in comparing response rates to online surveys showed that they can range anywhere from 20% to 47%. Another publication indicated that web-based response rates for surveys are usually around 42% (Dilman, Smyth & Christian, 2014). Bennett and Nair (2009) contended, however, that there is no magic formula by which a response rate can be identified as "acceptable." Furthermore, there is no evidence that online surveys with lower response rates produce biased evaluations (Layne, DeCristoforo, & McGinty, 1999; Porter, 2004). Although a higher response rate is certainly desirable, valid and reliable results have been generated from online surveys with low response rates of 30% (Bennett & Nair, 2009).

This study was exploratory in nature. The selected sample was not expected to be representative of the population of interest, and thus findings were not immediately generalizable, though some cautious generalizations were inferred and are presented. The researcher was attentive to recommended minimums to achieve a reliable and valid result and attempted to obtain a survey response rate of at least 42% (Dilman et al., 2014).

The initial email to the respondents was sent on March 7, 2018. The survey was available to complete from March 7, 2018 through March 31, 2018. Two follow-up emails were sent prior to the survey closing date to remind respondents to complete it. Of the 218 institutional respondents who were contacted, 93 responded. Thus, the survey had an overall response rate of 42.66%.

Data Analysis

Data Analysis for Research Question 1

To answer Research Question 1, the respondents were asked to provide on the ISPI© instrument their perceptions of the security risks associated with all recognized threats on a scale of 1-5 with 1 being the least risky and 5 being the riskiest as they applied to their respective institutions. The data obtained for the threats was aggregated to the level of the five factors of information systems: hardware, software, data, people, and procedures (i.e., the group mean was calculated for individual items within each of the five factor groups). The association of the selected security threats and the five factors of information systems is shown in Table 2. Any given security risk may be associated with more than one information security factors. However, for this study, any given risk was classified only under one factor based on the one on which it had the maximum impact.

Responses from similar institutions were grouped together (i.e., the group mean was calculated for each item by institution type) to obtain response profiles for the different types of institutions. The analysis of the data collected was a combination of descriptive statistics to ascertain the overall response profiles at the factor-level and at the type of institution level. Five

separate one-way ANOVA procedures were conducted to compare threat perceptions across the different types of educational institutions, one for each dependent variable. The dependent variables were the security threats aggregated to the level of the five factors of information systems (hardware, software, data, people, and procedure) and the independent variable was the institution type.

Table 2

Association of Security Risks with Five Factors of Information Systems

Risk	Factor
Ransomware	Software
Cyber – espionage	Data
Phishing	People
Sniffing	Hardware
Hacking	Procedure
Denial of service	Procedure
Natural disasters	Hardware
Theft	Hardware
Improper disposal	People
Malicious insider	People
Spoofing	Procedure
Malware	Software
SQL injection	Software
Web application attacks	Software
Payment card skimmers	Hardware
Weak passwords	People
Elevation of privilege	Procedure
User errors	People
Unpatched systems	Data
Institutional data on personal devices	Data
Unencrypted data transfers	Data
Institutional data on third party services	Data
Outdated anti-virus and anti-malware software	Software
Inadequate security monitoring	Procedure
Inadequate backups of institutional data	Procedure

Data Analysis for Research Question 2

To answer Research Question 2, the respondents were asked to provide on the ISPI© instrument their perceptions of the effectiveness of recognized security threat prevention measures on a scale of 1-5 with 1 being the least effective and 5 being the most effective as they applied to their respective institutions. Thereafter, they were asked to indicate on the ISPI© instrument the time intervals at which their respective institutions performed critical security practices and reviewed their specific security policies. Finally, the focus shifted to ascertaining the institutional cultures in acknowledging the threats to data and implementing measures to prevent breaches. Respondents were asked to answer questions on the ISPI© instrument about their institutional allocation of operational and personnel budgetary funds, and the reporting lines of the head of information technology for this purpose.

The data obtained for the threat prevention measures were aggregated to the level of the five factors of information systems: hardware, software, data, people, and procedures (i.e., the group mean was calculated for individual items within each of the five factor groups). The association of the selected threat prevention measures and the five factors of information systems is shown in Table 3. Any given security risk may be associated with more than one information security factor. However, for this study, only the primary factor was associated.

Responses from similar institutions were grouped together (i.e., the group mean was calculated for each item by institution type) to obtain response profiles for the different types of institutions. The analysis of the data collected was a combination of descriptive statistics to ascertain the overall response profiles at the factor-level and at the type of institution level. Five separate one-way ANOVA procedures were conducted to compare threat prevention measures

across the different types of educational institutions, one for each dependent variable. The dependent variables were the threat prevention measures aggregated to the level of the five factors of information systems (hardware, software, data, people, and procedures) and the independent variable was the institution type.

Table 3

Association of Threat Prevention Measures with Five Factors of Information Systems

Risk	Factor
Instructing users to not click on links in emails from unknown sources	People
Instructing users to not open attachments from emails from unknown sources	People
Instructing users to avoid visiting unauthorized websites on work computers	People
Implementing a password policy for strong, complex and long passwords for all users	Procedure
Making users change passwords frequently	Procedure
Avoiding sending valuable and confidential data via email or instant messages	People
Instructing users to check for https in any website address that require authentication	People
Removing stored personal identifying information from computers and mobile devices	Hardware
Clearing browsing history, temporary files and cookies from public computers	Software
Regularly updating anti-virus and anti-malware software on all institutional machines	Software
Taking regular backups of key data	Procedure
Using central authentication and single sign on	Data

Risk	Factor
Using multi-factor authentication	Data
Using encryption for data transfer and storage	Data
Using biometric authentication for accessing secure areas	Hardware
User authorization	Data
Employing a dedicated Information Security Officer	People
Installing institutional firewall	Software
Installing institutional virtual private network	Software
Training users on new security threats	People
Implementing post-intrusion attempt remediation procedures	Procedure
Applying critical server and system patches regularly	Procedure

The responses about frequencies of critical security practices and security policy updates were first differentiated between high frequency and low frequency based on their relative frequency of occurrence. Practices that are typically undertaken multiple times a year were classified as high frequency practices and those that were performed yearly or less frequently were classified as low frequency practices. These practices are listed in Table 4. The responses were then grouped together (i.e., the group mean was calculated by institution type) to obtain response profiles for the different types of institutions. The data were analyzed using descriptive statistics and two ANOVA procedures, one each for high frequency and low frequency practices to ascertain the overall response profiles at the institutional level. For the ANOVA procedures, the dependent variables were the frequencies of critical security practices and security policy updates and the independent variable was the institution type.

Table 4

Typical Frequencies of Critical Security Practices

Measure	Frequency
Honey pot experiments	High
Social engineering experiments to enforce security protocols	High
Log review and monitoring	High
Internal security audit	Low
External security audit	Low
Review of institutional security policies and change management	Low
Sending information technology personnel to attend information security classes	Low
Mandatory training on security topics for all employees	Low
Review of data breach remediation procedures	Low
Review of business continuity and disaster recovery policies	Low
Review of data backup policies	Low

Note. High = Multiple times a year, Low = Yearly or less frequent

Finally, the responses obtained from similar institutions for the budget allocation metrics were grouped together (i.e., the group mean was calculated by institution type) to obtain response profiles for the different types of institutions. The budget allocation metrics are listed in Table 5. The analysis of the data was completed using descriptive statistics to ascertain the overall response profiles at the type of institution level. An ANOVA procedure was conducted to compare budget allocations for information security across the different types of educational institutions. The dependent variable was the budget allocations and the independent variable was the institution type.

Table 5

Budget Allocation Metrics

Budget Measure	Score
Percentage of Annual Operating Budget allocated to Information Technology (IT)	
Less than 3%	1
3% to 10%	2
10% to 15%	3
Greater than 15%	4
Percentage of IT Budget allocated to Information Security	
Less than 3%	1
3% to 10%	2
10% to 15%	3
Greater than 15%	4
Dollar Amount of IT Budget per Employee	
Less than $5,000	1
$5,000 to $10,000	2
$10,000 to $20,000	3
Greater than $20,000	4

Data Analysis for Research Question 3

To answer Research Question 3, respondents were asked to rank their overall information security preparedness on a scale of 1-5 with 1 being the least prepared and 5 being the most prepared. The responses obtained from similar institutions were grouped together (i.e., the group mean was calculated by institution type to obtain response profiles for the different types of institutions). The analysis of the data was completed using descriptive statistics to ascertain the overall response profiles at the type of institution level. An ANOVA procedure was conducted to compare the overall security preparation scores across the different types of educational

institutions. The dependent variable was the self-reported information security preparedness level and the independent variable was the institution type.

Ancillary Data Analyses

Additional analyses were conducted to further analyze the initial findings related to the research questions and to establish identifiable patterns, if any, within the scope of the study. These analyses included a correlation analysis and a N/A response analysis.

The correlation analysis was conducted using the responses obtained in the ISPI© to investigate how each of the mean scores of security threat risk perception factors, threat prevention measure effectiveness perception factors, frequency of key security practices, and budget allocations correlated with the overall preparedness scores for each educational institution who participated in the survey. The purpose of this analysis was to further investigate the factors to determine which had the most impact on the overall institutional threat preparedness.

Respondents of the ISPI© had the option to indicate N/A for any item on the survey, be it a security threat risk perception score, threat prevention measure effectiveness perception score, or a frequency of a key security measure. An N/A response meant that the item concerned did not apply to the institution concerned. In other words, the institution concerned did not implement the item concerned as a threat prevention measure or did not consider the item concerned as a significant risk. An analysis was completed to identify the 10 items on the ISPI© that had the most N/A responses and how such N/A responses were distributed across the different types of educational institutions. The averages of the percentage distributions of the identified N/A response items were then calculated for each type of educational institution. The

purpose of this analysis was to help identify how the N/A responses were distributed across the types of educational institutions which, in turn, helped identify the types of educational institutions that were failing to implement key security measures the most.

Summary

The methods used to conduct this study have been presented in this chapter. The purpose of the study and the research questions were restated. The selection of participants, instrumentation, data collection, and data analysis were also presented. Results of the data analysis are presented in Chapter 4.

CHAPTER 4
RESULTS

Introduction

This exploratory study was conducted to analyze the preparedness of educational institutions toward ensuring the security of their data by comparing their self-reported perceptions of security risks and their assessments of the corresponding risk-mitigating practices. Factors that were studied with reference to securing institutional data were aligned with the five components of any information system (Kroenke & Boyle, 2015): hardware, software, data, procedures, and people. The researcher examined the security threats and the critical measures associated with these factors that can enhance security within the constraints applicable to educational institutions. Given the dynamic nature of the threats to information security, the researcher further explored the frequencies with which the different types of educational institutions undertake critical security practices and stay up-to-date in their information security policies and procedures. Finally, the culture of educational institutions with respect to implementing information security measures as reflected in their allocation of budgets for the same was explored. This chapter presents the data for the three research questions and is divided into three sections: (a) Data Collection Response Details, (b) Results, and (c) Summary.

Data Collection Response Details

A researcher-created survey named Information Security Preparedness Instrument (ISPI©) was used in this study. Emails containing a link to this researcher-created survey were sent on March 7, 2018 to individuals overseeing information security at 218 educational institutions. Institutions included 20 PK-12 Private Schools, 30 Public Colleges or Universities,

30 Private Colleges or Universities, the Florida Virtual School, 70 PK-12 Virtual Schools, and all 67 PK-12 Public School districts. The survey remained open through March 31, 2018. A total of 93 responses were received, 31 of which were from PK-12 Public Schools, 10 were from PK-12 Private Schools, 17 were from PK-12 Virtual Schools, 20 were from Public Colleges or Universities and 15 were from Private Colleges or Universities. The response rate was the highest for Public Colleges or Universities at 66.66% and was the lowest for PK-12 Virtual Schools at 24.28%. The overall response rate was 42.66%.

Results

Research Question 1

What is the level of preparedness to counter threats to information security among educational institutions with respect to identification and classification of threats, and how do results vary across the types of institutions?

The analysis of the data collected was a combination of descriptive statistics to ascertain the overall response profiles at the factor level and at the type of institution level. Five separate one-way ANOVA procedures were conducted to compare threat perceptions across the different types of educational institutions, one for each dependent variable. The dependent variables were the security threats aggregated to the level of the five factors of information systems (hardware, software, data, people, and procedures), and the independent variable was the institution type. The research question was further divided into five sub-questions, one for each dependent variable. The analyses to respond to the five sub-questions for Research Question 1 are presented in the sections.

Research Question 1.1. Hardware-Oriented Threats

What differences (if any) exist in the perception of security risks for hardware-oriented threats among the different types of educational institutions?

The descriptive statistics can be seen in Table 6. The respondents rated their perceptions of security risks for hardware-oriented threats on a scale of 1-5 with 1 being the least risky and 5 being the riskiest. The mean risk score for hardware-oriented threats across all types of educational institutions was 3.52. PK-12 Public Schools had the highest mean risk score of 3.62 and PK-12 Private Schools had the lowest mean risk score of 3.10. The risk score varied the most among PK-12 Public Schools and PK-12 Virtual Schools with a standard deviation of 0.71 and varied the least among Public Colleges/Universities with a standard deviation of 0.45.

Table 6

Descriptive Statistics of Perceptions of Hardware-Oriented Threats by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	3.62	0.71	[3.36, 3.88]	1.25	5.00
PK-12 Private School	10	3.10	0.61	[2.66, 3.54]	2.25	3.75
PK-12 Virtual School	17	3.69	0.71	[3.33, 4.06]	2.00	5.00
Public College/University	20	3.43	0.45	[3.21, 3.64]	2.50	4.25
Private College/University	15	3.52	0.41	[3.29, 3.74]	2.75	4.00
Total	93	3.52	0.62	[3.39, 3.65]	1.25	5.00

Note. *N* = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the perception of hardware-oriented threats among institutional types (see Table 7). The results from the analysis revealed that there were no statistically significant differences among the types of institutions with respect to hardware-oriented threat perceptions at the $p < 0.05$ level [$F(4, 88) = 1.85$, $p = 0.13$].

Table 7

ANOVA: Perceptions of Hardware-oriented Threats by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	2.76	4	0.69	1.85	0.13
Within Groups	32.74	88	0.37		
Total	35.50	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

Research Question 1.2. Software-Oriented Threats

What differences (if any) exist in the perception of security risks for software-oriented threats among the different types of educational institutions?

The descriptive statistics can be seen in Table 8. The respondents rated their perceptions of security risks for software-oriented threats on a scale of 1-5, with 1 being the least risky and 5 being the riskiest. The mean risk score for software-oriented threats across all types of educational institutions was 3.56. PK-12 Virtual Schools had the highest mean risk score of 3.69, and PK-12 Private Schools had the lowest mean risk score of 3.28. The risk score varied the

most among PK-12 Virtual Schools with a standard deviation of 0.64 and varied the least among Private Colleges/Universities with a standard deviation of 0.42.

Table 8

Descriptive Statistics of Perceptions of Software-oriented Threats by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	3.63	0.53	[3.43, 3.82]	2.80	5.00
PK-12 Private School	10	3.28	0.54	[2.89, 3.66]	2.40	4.00
PK-12 Virtual School	17	3.69	0.64	[3.36, 4.02]	2.60	5.00
Public College/University	20	3.45	0.50	[3.21, 3.68]	2.40	4.20
Private College/University	15	3.63	0.42	[3.39, 3.85]	3.00	4.40
Total	93	3.56	0.54	[3.45, 3.67]	2.40	5.00

Note. N = Number of Participants; SD = Standard Deviation; CI = Confidence Interval

A one-way ANOVA was performed to investigate differences in the perceptions of software-oriented threats among institutional types (see Table 9). The results from the analysis revealed that there were no statistically significant differences among the types of institutions with respect to software-oriented threat perceptions at the $p < 0.05$ level [$F(4, 88) = 1.35$, $p = 0.26$].

Table 9

ANOVA: Perceptions of Software-oriented Threats by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	1.53	4	0.38	1.35	0.26
Within Groups	24.94	88	0.28		
Total	26.48	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

Research Question 1.3. Data-Oriented Threats

What differences (if any) exist in the perception of security risks for data-oriented threats among the different types of educational institutions?

The descriptive statistics can be seen in Table 10. The respondents rated their perceptions of security risks for data-oriented threats on a scale of 1-5 with 1 being the least risky and 5 being the riskiest. The mean risk score for data-oriented threats across all types of educational institutions was 3.79. Private Colleges/Universities had the highest mean risk score of 3.89, and PK-12 Public Schools had the lowest mean risk score of 3.74. The risk score varied the most among PK-12 Public Schools with a standard deviation of 0.66 and varied the least among Private Colleges/Universities with a standard deviation of 0.38.

Table 10

Descriptive Statistics of Perceptions of Data-oriented Threats by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	3.74	0.66	[3.50, 3.98]	1.80	5.00
PK-12 Private School	10	3.86	0.57	[3.44, 4.27]	2.40	4.40
PK-12 Virtual School	17	3.80	0.64	[3.47, 4.12]	2.20	5.00
Public College/University	20	3.76	0.40	[3.57, 3.94]	2.60	4.40
Private College/University	15	3.89	0.38	[3.68, 4.10]	3.40	4.80
Total	93	3.79	0.55	[3.68, 3.90]	1.80	5.00

Note. N = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the perceptions of data-oriented threats among institutional types (see Table 11). The results of the analysis revealed that there were no statistically significant differences among the types of institutions with respect to data-oriented threat perceptions at the $p < 0.05$ level [$F(4, 88) = 0.24$, $p = 0.92$].

Table 11

ANOVA: Perceptions of Data-oriented Threats by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	0.30	4	0.08	0.24	0.92
Within Groups	27.58	88	0.31		
Total	27.88	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

Research Question 1.4. Procedure-Oriented Threats

What differences (if any) exist in the perception of security risks for procedure-oriented threats among the different types of educational institutions?

The descriptive statistics can be seen in Table 12. The respondents rated their perceptions of security risks for procedure-oriented threats on a scale of 1-5 with 1 being the least risky and 5 being the riskiest. The mean risk score for procedure-oriented threats across all types of educational institutions was 3.67. Private Colleges/Universities had the highest mean risk score of 3.78 and PK-12 Private Schools had the lowest mean risk score of 3.45. The risk score varied the most among PK-12 Public Schools with a standard deviation of 0.76 and varied the least among Private Colleges/Universities with a standard deviation of 0.27.

Table 12

Descriptive Statistics of Perceptions of Procedure-oriented Threats by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	3.68	0.76	[3.40, 3.96]	1.25	5.00
PK-12 Private School	10	3.45	0.50	[3.09, 3.80]	2.50	4.00
PK-12 Virtual School	17	3.76	0.58	[3.45, 4.05]	2.67	5.00
Public College/University	20	3.60	0.38	[3.42, 3.77]	2.67	4.00
Private College/University	15	3.78	0.27	[3.62, 3.92]	3.17	4.17
Total	93	3.67	0.57	[3.55, 3.78]	1.25	5.00

Note. N = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the perceptions of procedure-oriented threats among institutional types (see Table 13). The results from the analysis revealed that there were no statistically significant differences among the types of institutions with respect to procedure-oriented threat perceptions at the $p < 0.05$ level [$F(4, 88) = 0.68$, $p = 0.61$].

Table 13

ANOVA: Perceptions of Procedure-oriented Threats by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	0.89	4	0.22	0.68	0.61
Within Groups	28.77	88	0.33		
Total	29.66	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

Research Question 1.5. People-Oriented Threats

What differences (if any) exist in the perception of security risks for people-oriented threats among the different types of educational institutions?

The descriptive statistics can be seen in Table 14. The respondents rated their perceptions of security risks for people-oriented threats on a scale of 1-5 with 1 being the least risky and 5 being the riskiest. The mean risk score for people-oriented threats across all types of educational institutions was 3.80. PK-12 Virtual Schools had the highest mean risk score of 3.99, and PK-12 Private Schools had the lowest mean risk score of 3.54. The risk score varied the most among

PK-12 Public Schools with a standard deviation of 0.58 and varied the least among Private Colleges/Universities with a standard deviation of 0.31.

Table 14

Descriptive Statistics of Perceptions of People-oriented Threats by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	3.76	0.58	[3.55, 3.97]	2.20	5.00
PK-12 Private School	10	3.54	0.47	[3.20, 3.87]	2.60	4.20
PK-12 Virtual School	17	3.99	0.53	[3.71, 4.26]	3.00	5.00
Public College/University	20	3.79	0.35	[3.62, 3.95]	3.20	4.40
Private College/University	15	3.83	0.31	[3.65, 3.99]	3.40	4.20
Total	93	3.80	0.48	[3.69, 3.89]	2.20	5.00

Note. *N* = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the perceptions of people-oriented threats among institutional types (see Table 15). The results from the analysis revealed that there were no statistically significant differences among the types of institutions with respect to people-oriented threat perceptions at the $p < 0.05$ level [$F(4, 88) = 1.46$, $p = 0.22$].

Table 15

ANOVA: Perceptions of People-oriented Threats by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	1.34	4	0.33	1.46	0.22
Within Groups	20.10	88	0.23		
Total	21.44	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

Research Question 2

What is the level of preparedness to counter threats to information security among educational institutions with respect to institutional safeguards, frequency of critical practices and security policy updates, and budgetary allocation, and how do results vary across the types of institutions?

The analysis of the data collected for threat prevention measures was a combination of descriptive statistics to ascertain the overall response profiles at the factor-level and at the type of institution level. Five separate one-way ANOVA procedures were conducted to compare threat prevention measures across the different types of educational institutions, one for each dependent variable. The dependent variables were the threat prevention measures aggregated to the level of the five factors of information systems (hardware, software, data, people, and procedures) and the independent variable was the institution type.

The data for frequency of key security practices were analyzed using descriptive statistics and two separate one-way ANOVA procedures, one each for high frequency and low frequency practices to ascertain the overall response profiles at the institutional level. For both the ANOVA

procedures, the dependent variables were the frequencies of critical security practices and security policy updates; and the independent variable was the institution type.

The analysis of the data collected for budget allocation was completed using descriptive statistics to ascertain the overall response profiles at the type of institution level. An ANOVA procedure was conducted to compare budget allocations for information security across the different types of educational institutions. The dependent variable was the budget allocations, and the independent variable was the institution type.

The research question was further divided into eight sub-questions, one for each dependent variable. The analyses to respond to the eight sub-questions for Research Question 2 are presented in this section.

Research Question 2.1. Hardware-Oriented Measures

What differences (if any) exist in the perception of the effectiveness of hardware-oriented security measures among the different types of educational institutions?

The descriptive statistics can be seen in Table 16. The respondents rated their perceptions of effectiveness for hardware-oriented security measures on a scale of 1-5 with 1 being the least effective and 5 being the most effective. The mean effectiveness score for hardware-oriented measures across all types of educational institutions was 3.19. Private Colleges/Universities had the highest mean effectiveness score of 3.80, and PK-12 Private Schools had the lowest mean effectiveness score of 2.85. The effectiveness score varied the most among PK-12 Virtual Schools with a standard deviation of 1.00 and varied the least among Private Colleges/Universities with a standard deviation of 0.53.

Table 16

Descriptive Statistics of Perceptions of Hardware-oriented Measures by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	3.03	0.71	[2.77, 3.29]	1.00	5.00
PK-12 Private School	10	2.85	0.58	[2.43, 3.26]	2.00	4.00
PK-12 Virtual School	16	2.94	1.00	[2.40, 3.46]	1.00	5.00
Public College/University	20	3.35	0.65	[3.04, 3.65]	2.00	5.00
Private College/University	15	3.80	0.53	[3.50, 4.09]	3.00	4.50
Total	92	3.19	0.77	[3.03, 3.34]	1.00	5.00

Note. N = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the perceptions of effectiveness of hardware-oriented measures among institutional types (see Table 17). The results from the analysis revealed that there were significant differences among the types of institutions with respect to the perceptions of effectiveness of hardware-oriented measures at the $p < 0.05$ level [$F(4, 88) = 4.38$, $p = 0.00$].

Table 17

ANOVA: Perceptions of Hardware-oriented Measures by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	9.04	4	2.26	4.38	0.00
Within Groups	44.88	87	0.52		
Total	53.92	91			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

A Tukey HSD post hoc test was performed to determine which specific pairs of groups showed statistically significant differences in their perceptions of hardware-oriented measures (see Table 18). Based on the results, statistically significant differences existed between Private Colleges/Universities and PK-12 Public Schools, Private Colleges/Universities and PK-12 Private Schools, and Private Colleges/Universities and PK-12 Virtual Schools.

Table 18

Tukey HSD Post-hoc Test of Scores of Hardware-oriented Measures by Institution Type

Type of Educational Institution		*MD*	*SE*	*Sig*	*95% CI*
PK-12 Public School	PK-12 Private School	0.18	0.26	0.96	[-0.54, 0.90]
	PK-12 Virtual School	0.09	0.22	0.99	[-0.52, 0.71]
	Public College/University	-0.32	0.21	0.54	[-0.89, 0.25]
	Private College/University	-0.77	0.23	0.01	[-1.39, -0.13]
PK-12 Private School	PK-12 Public School	-0.18	0.26	0.96	[-0.90, 0.54]
	PK-12 Virtual School	-0.09	0.29	1.00	[-0.89, 0.71]
	Public College/University	-0.50	0.28	0.38	[-1.27, 0.27]
	Private College/University	-0.95	0.29	0.01	[-1.76, -0.13]
PK-12 Virtual School	PK-12 Public School	-0.09	0.22	0.99	[-0.71, 0.52]
	PK-12 Private School	0.09	0.29	1.00	[-0.71, 0.89]
	Public College/University	-0.41	0.24	0.43	[-1.08, 0.25]
	Private College/University	-0.86	0.26	0.01	[-1.58, -0.14]
Public College/University	PK-12 Public School	0.32	0.21	0.54	[-0.25, 0.89]
	PK-12 Private School	0.50	0.28	0.38	[-0.27, 1.27]
	PK-12 Virtual School	0.41	0.24	0.43	[-0.25, 1.08]
	Private College/University	-0.45	0.25	0.36	[-1.13, 0.23]
Private College/University	PK-12 Public School	0.77	0.23	0.01	[0.13, 1.39]
	PK-12 Private School	0.95	0.29	0.01	[0.13, 1.76]
	PK-12 Virtual School	0.86	0.26	0.01	[0.14, 1.58]
	Public College/University	0.45	0.25	0.36	[-0.23, 1.13]

Note. MD = mean difference; *SE* = standard error; *CI* = confidence interval

Research Question 2.2. Software-Oriented Measures

What differences (if any) exist in the perception of the effectiveness of software-oriented security measures among the different types of educational institutions?

The descriptive statistics can be seen in Table 19. The respondents rated their perceptions of effectiveness for software-oriented measures on a scale of 1-5 with 1 being the least effective

and 5 being the most effective. The mean effectiveness score for software-oriented measures across all types of educational institutions was 3.43. Public Colleges/Universities had the highest mean effectiveness score of 3.63, and PK-12 Virtual Schools had the lowest mean effectiveness score of 3.11. The effectiveness score varied the most among PK-12 Virtual Schools with a standard deviation of 0.69 and varied the least among Private Colleges/Universities with a standard deviation of 0.40.

Table 19

Descriptive Statistics of Perceptions of Software-oriented Measures by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	3.42	0.41	[3.26, 3.56]	2.67	4.25
PK-12 Private School	10	3.33	0.47	[2.98, 3.66]	2.75	4.25
PK-12 Virtual School	17	3.11	0.69	[2.75, 3.46]	1.00	4.00
Public College/University	20	3.63	0.41	[3.43, 3.81]	3.00	5.00
Private College/University	15	3.62	0.40	[3.39, 3.83]	2.50	4.00
Total	93	3.43	0.50	[3.32, 3.53]	1.00	5.00

Note. *N* = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the perceptions of effectiveness of software-oriented measures among institutional types (see Table 20). The results from the analysis revealed that there were significant differences among the types of institutions

with respect to the perceptions of effectiveness of software-oriented measures at the $p < 0.05$ level [$F(4, 88) = 3.47$, $p = 0.01$].

Table 20

ANOVA: Perceptions of Software-oriented Measures by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	3.17	4	0.79	3.47	0.01
Within Groups	20.06	88	0.23		
Total	23.22	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

A Tukey HSD post hoc test was performed to determine which specific pairs of groups showed statistically significant differences in their perceptions of software-oriented measures (see Table 21). Based on the results, statistically significant differences existed between Private Colleges/Universities and PK-12 Virtual Schools and between Public Colleges/Universities and PK-12 Virtual Schools.

Table 21

Tukey HSD Post-Hoc Test of Scores of Software-oriented Measures by Institution Type

Type of Educational Institution		*MD*	*SE*	*Sig*	*95% CI*
PK-12 Public School	PK-12 Private School	0.09	0.17	0.98	[-0.39, 0.57]
	PK-12 Virtual School	0.31	0.14	0.21	[-0.09, 0.71]
	Public College/University	-0.21	0.14	0.55	[-0.58, 0.17]
	Private College/University	-0.20	0.15	0.67	[-0.61, 0.21]
PK-12 Private School	PK-12 Public School	-0.09	0.17	0.98	[-0.57, 0.39]
	PK-12 Virtual School	0.22	0.19	0.78	[-0.31, 0.74]
	Public College/University	-0.30	0.18	0.49	[-0.81, 0.21]
	Private College/University	-0.29	0.19	0.57	[-0.83, 0.25]
PK-12 Virtual School	PK-12 Public School	-0.31	0.14	0.21	[-0.71, 0.09]
	PK-12 Private School	-0.22	0.19	0.78	[-0.74, 0.31]
	Public College/University	-0.52	0.16	0.01	[-0.95, -0.07]
	Private College/University	-0.51	0.17	0.03	[-0.98, -0.03]
Public College/University	PK-12 Public School	0.21	0.14	0.55	[-0.17, 0.58]
	PK-12 Private School	0.30	0.18	0.49	[-0.21, 0.81]
	PK-12 Virtual School	0.52	0.16	0.01	[0.07, 0.95]
	Private College/University	0.01	0.16	1.00	[-0.44, 0.46]
Private College/University	PK-12 Public School	0.20	0.15	0.67	[-0.21, 0.61]
	PK-12 Private School	0.29	0.19	0.57	[-0.25, 0.83]
	PK-12 Virtual School	0.51	0.17	0.03	[0.03, 0.98]
	Public College/University	-0.01	0.16	1.00	[-0.46, 0.44]

Note. MD = mean difference; *SE* = standard error; *CI* = confidence interval

Research Question 2.3. Data-Oriented Measures

What differences (if any) exist in the perception of the effectiveness of data-oriented security measures among the different types of educational institutions?

The descriptive statistics can be seen in Table 22. The respondents rated their perceptions of effectiveness for data-oriented measures on a scale of 1-5 with 1 being the least effective and 5 being the most effective. The mean effectiveness score for data-oriented measures across all

types of educational institutions was 4.01. Private Colleges/Universities had the highest mean effectiveness score of 4.39, and PK-12 Virtual Schools had the lowest mean effectiveness score of 3.55. The effectiveness scores varied the most among PK-12 Virtual Schools with a standard deviation of 1.06 and varied the least among Private Colleges/Universities with a standard deviation of 0.34.

Table 22

Descriptive Statistics of Perceptions of Data-oriented Measures by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	3.84	0.62	[3.60, 4.06]	3.00	5.00
PK-12 Private School	10	3.98	0.56	[3.57, 4.37]	2.50	4.67
PK-12 Virtual School	17	3.55	1.06	[3.00, 4.10]	1.00	5.00
Public College/University	20	4.38	0.40	[4.19, 4.57]	3.67	5.00
Private College/University	15	4.39	0.34	[4.20, 4.57]	3.75	4.75
Total	93	4.01	0.71	[3.86, 4.15]	1.00	5.00

Note. N = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the perceptions of effectiveness of data-oriented measures among institutional types (see Table 23). The results from the analysis revealed that there were significant differences among the types of institutions with respect to the perceptions of effectiveness of data-oriented measures at the $p < 0.05$ level [$F(4, 88) = 5.59$, $p = 0.00$].

Table 23

ANOVA: Perceptions of Data-oriented Measures by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	9.42	4	2.36	5.59	0.00
Within Groups	37.06	88	0.42		
Total	46.48	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

A Tukey HSD post hoc test was performed to determine which specific pairs of groups showed statistically significant differences in their perceptions of data-oriented measures (see Table 24). Based on the results, statistically significant differences existed between Private Colleges/Universities and PK-12 Virtual Schools, between Public Colleges/Universities and PK-12 Virtual Schools, and between PK-12 Public Schools and Public Colleges/Universities.

Table 24

Tukey HSD Post-Hoc Test of Scores of Data-oriented Measures by Institution Type

Type of Educational Institution		*MD*	*SE*	*Sig*	*95% CI*
PK-12 Public School	PK-12 Private School	-0.14	0.24	0.98	[-0.79, 0.51]
	PK-12 Virtual School	0.28	0.20	0.60	[-0.26, 0.82]
	Public College/University	-0.55	0.19	0.03	[-1.06, -0.02]
	Private College/University	-0.55	0.20	0.06	[-1.12, 0.01]
PK-12 Private School	PK-12 Public School	0.14	0.24	0.98	[-0.51, 0.79]
	PK-12 Virtual School	0.42	0.26	0.48	[-0.29, 1.14]
	Public College/University	-0.41	0.25	0.49	[-1.10, 0.29]
	Private College/University	-0.41	0.26	0.53	[-1.15, 0.32]
PK-12 Virtual School	PK-12 Public School	-0.28	0.20	0.60	[-0.82, 0.26]
	PK-12 Private School	-0.42	0.26	0.48	[-1.14, 0.29]
	Public College/University	-0.83	0.21	0.00	[-1.42, -0.23]
	Private College/University	-0.83	0.23	0.00	[-1.47, -0.19]
Public College/University	PK-12 Public School	0.55	0.19	0.03	[0.02, 1.06]
	PK-12 Private School	0.41	0.25	0.49	[-0.29, 1.10]
	PK-12 Virtual School	0.83	0.21	0.00	[0.23, 1.42]
	Private College/University	-0.01	0.22	1.00	[-0.62, 0.61]
Private College/University	PK-12 Public School	0.55	0.20	0.06	[-0.01, 1.12]
	PK-12 Private School	0.41	0.26	0.53	[-0.32, 1.15]
	PK-12 Virtual School	0.83	0.23	0.00	[0.19, 1.47]
	Public College/University	0.01	0.22	1.00	[-0.61, 0.62]

Note. MD = mean difference; *SE* = standard error; *CI* = confidence interval

Research Question 2.4. Procedure-oriented Measures

What differences (if any) exist in the perception of the effectiveness of procedure-oriented security measures among the different types of educational institutions?

The descriptive statistics can be seen in Table 25. The respondents rated their perceptions of effectiveness for procedure-oriented measures on a scale of 1-5 with 1 being the least effective

and 5 being the most effective. The mean effectiveness score for procedure-oriented measures across all types of educational institutions was 3.70. Private Colleges/Universities and PK-12 Private Schools had the highest mean effectiveness score of 3.96, and PK-12 Virtual Schools had the lowest mean effectiveness score of 3.41. The effectiveness score varied the most among PK-12 Virtual Schools with a standard deviation of 0.82 and varied the least among Public Colleges/Universities with a standard deviation of 0.33.

Table 25

Descriptive Statistics of Perceptions of Procedure-oriented Measures by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	3.61	0.42	[3.45, 3.76]	3.00	4.40
PK-12 Private School	10	3.96	0.44	[3.64, 4.27]	3.40	5.00
PK-12 Virtual School	17	3.41	0.82	[2.99, 3.83]	1.00	4.40
Public College/University	20	3.77	0.33	[3.61, 3.92]	3.00	4.40
Private College/University	15	3.96	0.44	[3.71, 4.20]	3.40	4.80
Total	93	3.70	0.53	[3.59, 3.81]	1.00	5.00

Note. N = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the perceptions of effectiveness of procedure-oriented measures among institutional types (see Table 26). The results from the analysis revealed that there were significant differences among the types of

institutions with respect to the perceptions of effectiveness of procedure-oriented measures at the $p < 0.05$ level [$F(4, 88) = 3.37$, $p = 0.01$].

Table 26

ANOVA: Perceptions of Procedure-oriented Measures by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	3.45	4	0.86	3.37	0.01
Within Groups	22.57	88	0.26		
Total	26.03	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

A Tukey HSD post hoc test was performed to determine which specific pairs of groups showed statistically significant differences in their perceptions of procedure-oriented measures (see Table 27). Based on the results, statistically significant differences existed between Private Colleges/Universities and PK-12 Virtual Schools.

Table 27

Tukey *HSD Post-Hoc Test of Scores of Procedure-oriented Measures by Institution Type*

Type of Educational Institution		*MD*	*SE*	*Sig*	*95% CI*
PK-12 Public School	PK-12 Private School	-0.35	0.18	0.32	[-0.86, 0.16]
	PK-12 Virtual School	0.20	0.15	0.70	[-0.22, 0.62]
	Public College/University	-0.16	0.15	0.80	[-0.56, 0.24]
	Private College/University	-0.35	0.16	0.19	[-0.79, 0.09]
PK-12 Private School	PK-12 Public School	0.35	0.18	0.32	[-0.16, 0.86]
	PK-12 Virtual School	0.55	0.20	0.06	[-0.01, 1.11]
	Public College/University	0.19	0.20	0.87	[-0.35, 0.73]
	Private College/University	0.00	0.21	1.00	[-0.57, 0.57]
PK-12 Virtual School	PK-12 Public School	-0.20	0.15	0.70	[-0.62, 0.22]
	PK-12 Private School	-0.55	0.20	0.06	[-1.11, 0.01]
	Public College/University	-0.36	0.17	0.21	[-0.82, 0.10]
	Private College/University	-0.55	0.18	0.02	[-1.04, -0.04]
Public College/University	PK-12 Public School	0.16	0.15	0.80	[-0.24, 0.56]
	PK-12 Private School	-0.19	0.20	0.87	[-0.73, 0.35]
	PK-12 Virtual School	0.36	0.17	0.21	[-0.10, 0.82]
	Private College/University	-0.19	0.17	0.81	[-0.67, 0.29]
Private College/University	PK-12 Public School	0.35	0.16	0.19	[-0.09, 0.79]
	PK-12 Private School	0.00	0.21	1.00	[-0.57, 0.57]
	PK-12 Virtual School	0.55	0.18	0.02	[0.04, 1.04]
	Public College/University	0.19	0.17	0.81	[-0.29, 0.67]

Note. MD = mean difference; *SE* = standard error; *CI* = confidence interval

Research Question 2.5. People-Oriented Measures

What differences (if any) exist in the perception of the effectiveness of people-oriented security measures among the different types of educational institutions?

The descriptive statistics can be seen in Table 28. The respondents rated their perceptions of effectiveness for people-oriented measures on a scale of 1-5 with 1 being the least effective

and 5 being the most effective. The mean effectiveness score for people-oriented measures across all types of educational institutions was 3.06. PK-12 Private Schools had the highest mean effectiveness score of 3.306, and PK-12 Virtual Schools had the lowest mean effectiveness score of 2.97. The effectiveness score varied the most among PK-12 Virtual Schools with a standard deviation of 0.68 and varied the least among PK-12 Private Schools with a standard deviation of 0.41.

Table 28

Descriptive Statistics of Perceptions of People-oriented Measures by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	2.99	0.46	[2.81, 3.15]	2.00	4.14
PK-12 Private School	10	3.30	0.41	[3.00, 3.58]	2.57	3.71
PK-12 Virtual School	17	2.97	0.68	[2.62, 3.31]	1.00	4.00
Public College/University	20	3.03	0.58	[2.75, 3.30]	2.29	4.29
Private College/University	15	3.20	0.52	[2.91, 3.49]	2.14	4.14
Total	93	3.06	0.54	[2.95, 3.17]	1.00	4.29

Note. *N* = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the perceptions of effectiveness of procedure-oriented measures among institutional types (see Table 29). The results from the analysis revealed that there were no statistically significant differences among

the types of institutions with respect to the perceptions of effectiveness of people-oriented measures at the $p < 0.05$ level [$F(4, 88) = 1.02$, $p = 0.40$].

Table 29

ANOVA: Perceptions of People-Oriented Measures by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	1.18	4	0.29	1.02	0.40
Within Groups	25.39	88	0.29		
Total	26.57	92			

Note. SS = sum of squares; df = degrees of freedom; MS = mean square

Research Question 2.6. High Frequency Practices

What differences (if any) exist in the frequencies of implementation of high-frequency critical practices among the different types of educational institutions?

The descriptive statistics can be seen in Table 30. The respondents indicated the frequencies with which they performed critical security practices. For practices that were typically performed multiple times a year, the responses were scored on a scale of 1-5 with 1 being the least frequent and 5 being the most frequent. The mean score for high frequency practices across all types of educational institutions was 1.24. Private Colleges/Universities had the highest mean score of 3.24, and PK-12 Virtual Schools had the lowest mean score of 0.29. The score varied the most among Public Colleges/Universities with a standard deviation of 2.20 and varied the least among PK-12 Virtual Schools with a standard deviation of 0.65.

Table 30

Descriptive Statistics of Frequencies of High Frequency Practices by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	0.40	0.85	[0.08, 0.70]	0.00	2.67
PK-12 Private School	10	0.43	0.77	[-0.11, 0.98]	0.00	2.00
PK-12 Virtual School	17	0.29	0.65	[-0.04, 0.63]	0.00	1.67
Public College/University	20	2.27	2.20	[1.23, 3.29]	0.00	5.00
Private College/University	15	3.24	2.08	[2.09, 4.39]	0.00	5.00
Total	93	1.24	1.84	[0.86, 1.62]	0.00	5.00

Note. N = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the frequencies of implementation of high-frequency critical practices among institutional types (see Table 31). The results from the analysis revealed that there were significant differences among the types of institutions with respect to the frequencies of implementation of high-frequency critical practices at the $p < 0.05$ level [$F(4, 88) = 14.73$, $p = 0.00$].

Table 31

ANOVA: Frequencies of High Frequency Practices by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	125.05	4	31.26	14.73	0.00
Within Groups	186.76	88	2.12		
Total	311.81	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

A Tukey HSD post hoc test was performed to determine which specific pairs of groups showed statistically significant differences in their frequencies of implementation of high-frequency critical practices (see Table 32). Based on the results, Private Colleges/Universities showed statistically significant differences from PK-12 Public Schools, PK-12 Private Schools and PK-12 Virtual Schools respectively. In addition, Public Colleges/Universities showed statistically significant differences from PK-12 Public Schools, PK-12 Private Schools and PK-12 Virtual Schools respectively.

Table 32

Tukey HSD Post-Hoc Test of Scores of High Frequency Practices by Institution Type

Type of Educational Institution		*MD*	*SE*	*Sig*	*95% CI*
PK-12 Public School	PK-12 Private School	-0.04	0.53	1.00	[-1.51, 1.44]
	PK-12 Virtual School	0.10	0.44	1.00	[-1.12, 1.32]
	Public College/University	-1.87	0.42	0.00	[-3.03, -0.70]
	Private College/University	-2.85	0.46	0.00	[-4.12, -1.57]
PK-12 Private School	PK-12 Public School	0.04	0.53	1.00	[-1.44, 1.51]
	PK-12 Virtual School	0.14	0.58	1.00	[-1.47, 1.75]
	Public College/University	-1.83	0.56	0.01	[-3.40, -0.26]
	Private College/University	-2.81	0.59	0.00	[-4.46, -1.15]
PK-12 Virtual School	PK-12 Public School	-0.10	0.44	1.00	[-1.32, 1.12]
	PK-12 Private School	-0.14	0.58	1.00	[-1.75, 1.47]
	Public College/University	-1.97	0.48	0.00	[-3.31, -0.63]
	Private College/University	-2.95	0.52	0.00	[-4.38, -1.51]
Public College/University	PK-12 Public School	1.87	0.42	0.00	[0.70, 3.03]
	PK-12 Private School	1.83	0.56	0.01	[0.26, 3.40]
	PK-12 Virtual School	1.97	0.48	0.00	[0.63, 3.31]
	Private College/University	-0.98	0.50	0.29	[-2.36, 0.40]
Private College/University	PK-12 Public School	2.85	0.46	0.00	[1.57, 4.12]
	PK-12 Private School	2.81	0.59	0.00	[1.15, 4.46]
	PK-12 Virtual School	2.95	0.52	0.00	[1.51, 4.38]
	Public College/University	0.98	0.50	0.29	[-0.4, 2.36]

Note. MD = mean difference; *SE* = standard error; *CI* = confidence interval

Research Question 2.7. Low Frequency Practices

What differences (if any) exist in the frequencies of implementation of low-frequency critical practices among the different types of educational institutions?

The descriptive statistics can be seen in Table 33. The respondents indicated the frequencies with which they performed critical security practices and reviewed security related policies and procedures. For practices that were typically performed once a year or less, the responses were scored on a scale of 1-5 with 1 being the least frequent and 5 being the most frequent. The mean score for low frequency practices across all types of educational institutions was 1.10. Private Colleges/Universities had the highest mean score of 1.60, and PK-12 Virtual Schools had the lowest mean score of 0.74. The score varied the most among PK-12 Public Schools with a standard deviation of 0.68 and varied the least among PK-12 Virtual Schools with a standard deviation of 0.43.

Table 33

Descriptive Statistics of Frequencies of Low Frequency Practices by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	0.83	0.68	[0.58, 1.08]	0.00	2.25
PK-12 Private School	10	1.15	0.54	[0.76, 1.53]	0.13	2.00
PK-12 Virtual School	17	0.74	0.43	[0.51, 0.95]	0.00	1.38
Public College/University	20	1.44	0.53	[1.19, 1.69]	0.25	2.13
Private College/University	15	1.60	0.44	[1.35, 1.84]	0.75	2.13
Total	93	1.10	0.65	[0.97, 1.23]	0.00	2.25

Note. N = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the frequencies of implementation of low-frequency critical practices among institutional types (see Table 34). The results from the analysis revealed that there were significant differences among the types of institutions with respect to the frequencies of implementation of low-frequency critical practices at the $p < 0.05$ level [$F(4, 88) = 8.44$, $p = 0.00$].

Table 34

ANOVA: Frequencies of Low Frequency Practices by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	10.63	4	2.66	8.44	0.00
Within Groups	27.70	88	0.32		
Total	38.32	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

A Tukey HSD post hoc test was performed to determine which specific pairs of groups showed statistically significant differences in their frequencies of implementation of low-frequency critical practices (see Table 35). Based on the results, Private Colleges/Universities showed statistically significant differences with PK-12 Public Schools and PK-12 Virtual Schools respectively. In addition, Public Colleges/Universities showed statistically significant differences with PK-12 Public Schools and PK-12 Virtual Schools respectively.

Table 35

Tukey HSD Post-Hoc Test of Scores of Low Frequency Practices by Institution Type

Type of Educational Institution		*MD*	*SE*	*Sig*	*95% CI*
PK-12 Public School	PK-12 Private School	-0.32	0.20	0.53	[-0.88, 0.25]
	PK-12 Virtual School	0.10	0.17	0.98	[-0.37, 0.56]
	Public College/University	-0.61	0.16	0.00	[-1.06, -0.16]
	Private College/University	-0.77	0.18	0.00	[-1.25, -0.27]
PK-12 Private School	PK-12 Public School	0.32	0.20	0.53	[-0.25, 0.88]
	PK-12 Virtual School	0.41	0.22	0.35	[-0.2, 1.03]
	Public College/University	-0.29	0.22	0.66	[-0.89, 0.31]
	Private College/University	-0.45	0.23	0.29	[-1.08, 0.18]
PK-12 Virtual School	PK-12 Public School	-0.10	0.17	0.98	[-0.56, 0.37]
	PK-12 Private School	-0.41	0.22	0.35	[-1.03, 0.2]
	Public College/University	-0.71	0.19	0.00	[-1.22, -0.19]
	Private College/University	-0.86	0.20	0.00	[-1.41, -0.31]
Public College/University	PK-12 Public School	0.61	0.16	0.00	[0.16, 1.06]
	PK-12 Private School	0.29	0.22	0.66	[-0.31, 0.89]
	PK-12 Virtual School	0.71	0.19	0.00	[0.19, 1.22]
	Private College/University	-0.16	0.19	0.93	[-0.68, 0.37]
Private College/University	PK-12 Public School	0.77	0.18	0.00	[0.27, 1.25]
	PK-12 Private School	0.45	0.23	0.29	[-0.18, 1.08]
	PK-12 Virtual School	0.86	0.20	0.00	[0.31, 1.41]
	Public College/University	0.16	0.19	0.93	[-0.37, 0.68]

Note. MD = mean difference; *SE* = standard error; *CI* = confidence interval

Research Question 2.8. Budget Allocations

What differences (if any) exist in budgetary allocation related to information security among the different types of educational institutions?

The descriptive statistics can be seen in Table 36. The respondents indicated on the ISPI© the allocations for their institutional budgets for information technology with a focus on information security. The responses were scored on a scale of 1-5 with 1 being the lowest budget allocation and 5 being the highest budget allocation. The mean score for budget allocations across all types of educational institutions was 1.44. Private Colleges/Universities had the highest mean score of 2.11, and PK-12 Public Schools had the lowest mean score of 1.10. The score varied the most among Public Colleges/Universities with a standard deviation of 0.64 and varied the least among PK-12 Virtual Schools with a standard deviation of 0.42.

Table 36

Descriptive Statistics of Perceptions of Budget Allocation by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	1.10	0.29	[0.99, 1.20]	0.67	2.00
PK-12 Private School	10	1.30	0.43	[0.99, 1.60]	1.00	2.00
PK-12 Virtual School	17	1.29	0.42	[1.07, 1.51]	1.00	2.00
Public College/University	20	1.67	0.64	[1.36, 1.96]	1.00	2.67
Private College/University	15	2.11	0.59	[1.78, 2.43]	1.00	3.00
Total	93	1.44	0.59	[1.32, 1.56]	0.67	3.00

Note. N = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the budgetary allocation related to information security among institutional types (see Table 37). The results from the analysis revealed that there were significant differences among the types of institutions with respect to the budgetary allocation related to information security at the $p < 0.05$ level [$F(4, 88) = 13.46$, $p = 0.00$].

Table 37

ANOVA: Perceptions of Budget Allocation by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	11.99	4	3.00	13.46	0.00
Within Groups	19.60	88			
Total	31.59	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

A Tukey HSD post hoc test was performed to determine which specific pairs of groups showed statistically significant differences in their budget allocations (see Table 38). Based on the results, Private Colleges/Universities showed statistically significant differences with PK-12 Public Schools, PK-12 Private Schools and PK-12 Virtual Schools respectively. In addition, Public Colleges/Universities showed statistically significant differences with PK-12 Public Schools.

Table 38

Tukey HSD Post-Hoc Test of Scores of Budget Allocation by Institution Type

Type of Educational Institution		*MD*	*SE*	*Sig*	*95% CI*
PK-12 Public School	PK-12 Private School	-0.20	0.17	0.76	[-0.68, 0.27]
	PK-12 Virtual School	-0.20	0.14	0.64	[-0.59, 0.19]
	Public College/University	-0.57	0.14	0.00	[-0.94, -0.19]
	Private College/University	-1.01	0.15	0.00	[-1.42, -0.60]
PK-12 Private School	PK-12 Public School	0.20	0.17	0.76	[-0.27, 0.68]
	PK-12 Virtual School	0.01	0.19	1.00	[-0.51, 0.52]
	Public College/University	-0.37	0.18	0.27	[-0.87, 0.14]
	Private College/University	-0.81	0.19	0.00	[-1.34, -0.27]
PK-12 Virtual School	PK-12 Public School	0.20	0.14	0.64	[-0.19, 0.59]
	PK-12 Private School	-0.01	0.19	1.00	[-0.52, 0.51]
	Public College/University	-0.37	0.16	0.13	[-0.80, 0.06]
	Private College/University	-0.82	0.17	0.00	[-1.28, -0.35]
Public College/University	PK-12 Public School	0.57	0.14	0.00	[0.19, 0.94]
	PK-12 Private School	0.37	0.18	0.27	[-0.14, 0.87]
	PK-12 Virtual School	0.37	0.16	0.13	[-0.06, 0.80]
	Private College/University	-0.44	0.16	0.05	[-0.89, 0.00]
Private College/University	PK-12 Public School	1.01	0.15	0.00	[0.60, 1.42]
	PK-12 Private School	0.81	0.19	0.00	[0.27, 1.34]
	PK-12 Virtual School	0.82	0.17	0.00	[0.35, 1.28]
	Public College/University	0.44	0.16	0.05	[0.00, 0.89]

Note. MD = mean difference; *SE* = standard error; *CI* = confidence interval

Research Question 3

What is the overall self-reported level of preparedness among educational institutions with respect to information security, and how do results vary across the types of institutions?

Descriptive statistics were used to ascertain the overall response profiles at the type of institution level. An ANOVA procedure was conducted to compare the overall security

preparedness scores across the different types of educational institutions. The dependent variable was the self-reported information security preparedness level and the independent variable was the institution type.

The descriptive statistics can be seen in Table 39. The respondents rated their overall security preparedness on a scale of 1-5 with 1 being the least prepared and 5 being the most prepared. The mean preparedness score across all types of educational institutions was 2.60. Private Colleges/Universities had the highest mean preparedness score of 3.40 and PK-12 Public Schools had the lowest mean preparedness score of 2.16. The risk score varied the most among PK-12 Public Schools with a standard deviation of 1.07 and varied the least among PK-12 Private Schools with a standard deviation of 0.67.

Table 39

Descriptive Statistics of Perceptions of Overall Security Preparedness by Institution Type

Institution Type	*N*	*Mean*	*SD*	*95% CI*	*Min*	*Max*
PK-12 Public School	31	2.16	1.07	[1.76, 2.55]	1.00	5.00
PK-12 Private School	10	3.00	0.67	[2.52, 3.47]	2.00	4.00
PK-12 Virtual School	17	2.29	1.05	[1.75, 2.83]	1.00	4.00
Public College/University	20	2.75	0.85	[2.35, 3.14]	1.00	4.00
Private College/University	15	3.40	0.74	[2.99, 3.8]	2.00	4.00
Total	93	2.60	1.02	[2.39, 2.81]	1.00	5.00

Note. N = Number of Participants; *SD* = Standard Deviation; *CI* = Confidence Interval

A one-way ANOVA was performed to investigate differences in the overall self-reported level of preparedness among institutional types (see Table 40). The results from the analysis revealed that there were significant differences among the types of institutions with respect to their overall self-reported level of preparedness at the $p < 0.05$ level [$F(4, 88) = 5.48$, $p = 0.00$].

Table 40 ANOVA: Perceptions of Overall Security Preparedness by Institution Type

Source	*SS*	*Df*	*MS*	*F*	*Sig.*
Between Groups	19.21	4	4.80	5.48	0.00
Within Groups	77.07	88	0.88		
Total	96.28	92			

Note. SS = sum of squares; *df* = degrees of freedom; *MS* = mean square

A Tukey HSD post hoc test was performed to determine which specific pairs of groups showed statistically significant differences in their overall self-reported preparedness (see Table 41). Based on the results, Private Colleges/Universities showed statistically significant differences with PK-12 Public Schools and PK-12 Virtual Schools respectively.

Table 41

Tukey HSD Post-Hoc Test of Scores of Overall Security Preparedness by Institution Type

Type of Educational Institution		*MD*	*SE*	*Sig*	*95% CI*
PK-12 Public School	PK-12 Private School	-0.84	0.34	0.11	[-1.78, 0.10]
	PK-12 Virtual School	-0.13	0.28	0.99	[-0.91, 0.65]
	Public College/University	-0.59	0.27	0.19	[-1.33, 0.15]
	Private College/University	-1.24	0.29	0.00	[-2.05, -0.41]
PK-12 Private School	PK-12 Public School	0.84	0.34	0.11	[-0.10, 1.78]
	PK-12 Virtual School	0.71	0.37	0.33	[-0.33, 1.74]
	Public College/University	0.25	0.36	0.96	[-0.75, 1.25]
	Private College/University	-0.40	0.38	0.83	[-1.46, 0.66]
PK-12 Virtual School	PK-12 Public School	0.13	0.28	0.99	[-0.65, 0.91]
	PK-12 Private School	-0.71	0.37	0.33	[-1.74, 0.33]
	Public College/University	-0.46	0.31	0.58	[-1.31, 0.40]
	Private College/University	-1.11	0.33	0.01	[-2.02, -0.18]
Public College/University	PK-12 Public School	0.59	0.27	0.19	[-0.15, 1.33]
	PK-12 Private School	-0.25	0.36	0.96	[-1.25, 0.75]
	PK-12 Virtual School	0.46	0.31	0.58	[-0.4, 1.31]
	Private College/University	-0.65	0.32	0.26	[-1.54, 0.24]
Private College/University	PK-12 Public School	1.25	0.29	0.00	[0.41, 2.05]
	PK-12 Private School	0.40	0.38	0.83	[-0.66, 1.46]
	PK-12 Virtual School	1.11	0.33	0.01	[0.18, 2.02]
	Public College/University	0.65	0.32	0.26	[-0.24, 1.54]

Note. MD = mean difference; *SE* = standard error; *CI* = confidence interval

Ancillary Analyses

Additional analyses were conducted to further analyze the initial findings related to the research questions and to establish identifiable patterns, if any, within the scope of the study. These analyses included a correlation analysis and a N/A response analysis.

Correlation with Overall Preparedness

A bivariate correlation analysis was conducted using the responses obtained in the ISPI© to investigate how the overall preparedness scores for each educational institution that participated in the survey correlated with the mean scores calculated for 25 security threat risk perception factors, 22 threat prevention measure effectiveness perception factors, 11 key security practice frequencies, and 3 budget allocation factors respectively. The results are summarized in Table 42. All the correlations were statistically significant at 0.01 level except for *People-Oriented Threats* and *Software-Oriented Measures* which were significant only at the 0.05 level. All the security threat risk perception scores showed a negative correlation with overall preparedness scores, while prevention measure effectiveness perception scores, frequency of key security practices, and budget allocations showed a positive correlation with overall preparedness scores. In other words, higher overall preparedness scores were associated with lower security threat risk perception scores. Similarly, higher overall preparedness scores were associated with higher prevention measure effectiveness scores, higher frequency of key security practices, and higher budget allocations.

Table 42

Correlation with Overall Preparedness

Item	*Correlation Coefficient*	*Sig.*
Hardware-Oriented Threats	-0.29	0.004
Software-Oriented Threats	-0.29	0.005
Data-Oriented Threats	-0.28	0.008
People-Oriented Threats	-0.22	0.031
Procedure-Oriented Threats	-0.28	0.008
Hardware-Oriented Measures	0.39	0.000
Software-Oriented Measures	0.25	0.014
Data-Oriented Measures	0.40	0.000
People-Oriented Measures	0.40	0.000
Procedure-Oriented Measures	0.40	0.000
High Frequency Practices	0.57	0.000
Low Frequency Practices	0.73	0.000
Budget Allocations	0.68	0.000

Note. All correlations are significant at the 0.05 level.

Analysis of N/A responses

Respondents of the ISPI© had the option to indicate N/A for any item on the survey, be it a security threat risk perception score, threat prevention measure effectiveness perception score, frequency of a key security measure, or a budget allocation item. The N/A response meant that the item did not apply to the institution concerned. An analysis was completed to find out which items on the ISPI© had the most N/A responses. Table 43 lists the 10 items that had the most N/A responses and shows the percentage distribution of each N/A response across the different types of educational institutions. An analysis of the items identified as having the most N/A responses revealed that all these items were key security measures. An average of the percentage distributions for each type of educational institution is provided at the end of the table. PK-12

Public Schools had the highest percentage of N/A responses followed closely by PK-12 Virtual Schools. Private Colleges/Universities had the least percentage of N/A responses.

Table 43

Analysis of Not Applicable (N/A) responses

Item	*N*	*PK-12 Public Schools*	*PK-12 Private Schools*	*PK-12 Virtual Schools*	*Public College/ Univ.*	*Private College /Univ.*	*All*
Honey pot experiments	76	97%	100%	100%	65%	40%	82%
Social engineering experiments to enforce security protocols	71	94%	90%	100%	55%	33%	76%
Using biometric authentication for accessing secure areas	70	90%	80%	76%	75%	40%	75%
Log review and monitoring	56	81%	70%	82%	40%	13%	60%
Sending information technology personnel to attend information security classes	55	74%	60%	88%	40%	20%	59%
Using multi-factor authentication	49	74%	60%	59%	35%	20%	53%
Internal security audit	48	61%	40%	82%	35%	27%	52%
Mandatory training on security topics for all employees	47	65%	70%	71%	25%	20%	51%
Review of data breach remediation procedures	46	71%	60%	59%	25%	20%	49%
Employing a dedicated Information Security Officer	38	71%	40%	41%	20%	7%	41%
Average		78%	67%	76%	42%	24%	60%

Summary

The results of the data analysis for each research question were presented in this chapter along with applicable descriptive statistics. For Research Question 1, using separate ANOVA analyses for each of the security risk categories, the researcher found no statistically significant differences between the types of educational institutions in their assessments of security risks. For Research Question 2, using separate ANOVA analyses, the researcher found significant differences between the types of educational institutions in their perceptions of the effectiveness of security measures, frequencies of key security practices and policy updates, and budget allocations. Using post-hoc analyses, these differences were isolated to the types of educational institutions involved. Finally, for Research Question 3, using an ANOVA analysis, the researcher found that the educational institutions showed statistically significant differences in terms of their overall assessment of their security preparedness. Using post-hoc analyses, these differences were isolated to the types of educational institutions involved. A separate analysis revealed correlations between the overall preparedness of the educational institutions with their assessments of security risks, their perceptions of the effectiveness of security measures, frequencies of key security practices and policy updates, and budget allocations. Finally, an analysis of the not applicable (N/A) responses indicated a distribution of the critical security measures that were not being implemented by the educational institutions. A summary of the study, discussion, and recommendations are presented in Chapter 5.

CHAPTER 5
DISCUSSION

Introduction

In the preceding chapter, the results of the data analyses were presented. This chapter includes a summary of the study and a five-part discussion of findings: (a) Research Question 1 which includes assessments of the different security risks by the different types of educational institutions, (b) Research Question 2 which includes perceptions of the effectiveness of security measures, frequencies of key security practices and policy updates, and budget allocations by the different types of educational institutions, (c) Research Question 3 which includes an overall assessment of security preparedness by the different types of educational institutions, (d) additional findings from supplementary analyses, and (e) an overall summary of findings from the discussion. Implications for practice and recommendations for further research are also included.

Summary of the Study

The purpose of this exploratory study was to analyze the preparedness of educational institutions toward ensuring the security of their data by comparing their self-reported perceptions of security risks and their assessments of the corresponding risk-mitigating practices. The five different types of educational institutions that were included in this study were PK-12 Public Schools, PK-12 Private Schools, PK-12 Virtual Schools, Public Colleges/Universities, and Private Colleges/Universities in the state of Florida. Factors that were studied with reference to securing institutional data were aligned with the five components of any information system (Kroenke & Boyle, 2015): hardware, software, data, procedures, and people. The researcher

examined the security threats associated with these factors and explored the critical measures with respect to the factors that can enhance security within the constraints applicable to educational institutions. Given the dynamic nature of the threats to information security, the researcher further explored the frequencies with which the different types of educational institutions undertake critical security practices and stay up-to-date with their information security policies and procedures. Finally, the culture of educational institutions with respect to implementing information security measures, as reflected in their allocation of budgets for the same, was explored.

Data for this study were collected using an instrument created by the researcher exclusively for this study. This questionnaire-based instrument, the Information Security Preparedness Instrument (ISPI©), was distributed using the survey tool Qualtrix and was used to measure the preparedness of educational institutions to ensure the security of their institutional information. The questionnaire primarily focused on four institution specific areas that reflected institutional preparedness to counter security threats (i.e., threat identification, threat mitigation practices, frequency of key security practices and updates of established security policies and practices, and budgetary allocations to enable security measures). The questions pertaining to these areas were further classified according to the five components of information systems – hardware, software, data, people, and procedures (Kroenke & Boyle, 2015). Emails containing a link to the questionnaire were sent on March 7, 2018 to individuals overseeing information security at 218 educational institutions in the state of Florida. A total of 20 PK-12 Private Schools, 30 Public Colleges or Universities, 30 Private Colleges or Universities, the Florida Virtual School, 70 PK-12 Virtual Schools, and all 67 PK-12 Public School districts were

included. The survey remained open through March 31, 2018. A total of 93 responses (42.66% response rate) were received of which 31 were from PK-12 Public Schools, 10 were from PK-12 Private Schools, 17 were from PK-12 Virtual Schools, 20 were from Public Colleges or Universities and 15 were from Private Colleges or Universities.

The following research questions were used to guide this study:

1. What is the level of preparedness to counter threats to information security among educational institutions with respect to identification and classification of threats, and how do results vary across the types of institutions?

   This question was further divided into five sub-questions based on the five factors of information systems (Kroenke & Boyle, 2015):

   1.1. What differences (if any) exist in the perception of security risks for hardware-oriented threats among the different types of educational institutions?

   1.2. What differences (if any) exist in the perception of security risks for software-oriented threats among the different types of educational institutions?

   1.3. What differences (if any) exist in the perception of security risks for data-oriented threats among the different types of educational institutions?

   1.4. What differences (if any) exist in the perception of security risks for procedure-oriented threats among the different types of educational institutions?

1.5. What differences (if any) exist in the perception of security risks for people-oriented threats among the different types of educational institutions?

2. What is the level of preparedness to counter threats to information security among educational institutions with respect to institutional safeguards, frequency of critical measures and security policy updates, and budgetary allocation, and how do results vary across the types of institutions?

   This question was further divided into eight sub-questions based on the five factors of information systems (Kroenke & Boyle, 2015), frequency of critical measures and security policy updates, and budgetary allocation:

   2.1. What differences (if any) exist in the perception of the effectiveness of hardware-oriented security measures among the different types of educational institutions?

   2.2. What differences (if any) exist in the perception of the effectiveness of software-oriented security measures among the different types of educational institutions?

   2.3. What differences (if any) exist in the perception of the effectiveness of data-oriented security measures among the different types of educational institutions?

   2.4. What differences (if any) exist in the perception of the effectiveness of procedure-oriented security measures among the different types of educational institutions?

2.5. What differences (if any) exist in the perception of the effectiveness of people-oriented security measures among the different types of educational institutions?

2.6. What differences (if any) exist in the frequencies of implementation of high-frequency critical measures among the different types of educational institutions?

2.7. What differences (if any) exist in the frequencies of implementation of low-frequency critical measures and security policy updates among the different types of educational institutions?

2.8. What differences (if any) exist in budgetary allocation related to information security among the different types of educational institutions?

3. What is the overall self-reported level of preparedness among educational institutions with respect to information security, and how do results vary across the types of institutions?

To answer Research Question 1, the respondents were asked to provide on the ISPI© instrument their perceptions of the security risks associated with all recognized threats on a scale of 1-5 as they applied to their institutions. The data obtained for the threats were aggregated to the level of the five factors of information systems: hardware, software, data, people, and procedures (i.e., the group mean was calculated for individual items within each of the five-factor groups). Thereafter, responses from similar institutions were grouped together (i.e., the group mean was calculated for each item by institution type) to obtain response profiles for the

different types of institutions. The analysis of the data collected was a combination of descriptive statistics to ascertain the overall response profiles at the factor-level and thereafter at the type of institution level. Five separate one-way ANOVA procedures were conducted to compare threat perceptions across the different types of educational institutions. The dependent variables were the threats aggregated to the level of the five factors of information systems (hardware, software, data, people, and procedures) and the independent variable was the institution type.

To answer Research Question 2, the respondents were asked to provide on the ISPI© instrument their perceptions of the effectiveness of recognized security threat prevention measures on a scale of 1-5 as they applied to their institutions. Thereafter, they were asked to indicate on the ISPI© instrument the time intervals at which their respective institutions review and update their specific security policies. Finally, the focus shifted to ascertaining the institutional cultures in acknowledging the threats to data and implementing measures to prevent breaches. Respondents were asked to answer questions on the ISPI© instrument about their institutional allocation of operational and personnel budgetary funds, and the reporting lines of the head of information technology for this purpose. The data obtained for the threat prevention measures were aggregated to the level of the five factors of information systems: hardware, software, data, people, and procedures (i.e., the group mean was calculated for individual items within each of the five factor groups). Thereafter, responses from similar institutions were grouped together (i.e., the group mean was calculated for each item by institution type) to obtain response profiles for the different types of institutions. The analysis of the data collected was a combination of descriptive statistics to ascertain the overall response profiles at the factor-level and thereafter at the type of institution level. Five separate one-way ANOVA procedures were

conducted to compare threat prevention measures across the different types of educational institutions. The dependent variables were the threat prevention measures aggregated to the level of the five factors of information systems (hardware, software, data, people, and procedures), and the independent variable was the institution type. The responses about frequencies of key security measures and security policy updates were analyzed using descriptive statistics to ascertain the overall response profiles at the institutional level. Two separate ANOVA procedures were conducted to compare the frequencies of key security measures across the different types of educational institutions. The dependent variables were the frequencies of key security measures and the independent variable was the institution type. Finally, the responses obtained from similar institutions for the budget allocation percentages were grouped together (i.e., the group mean was calculated by institution type) to obtain response profiles for the different types of institutions. The analysis of the data collected was completed using descriptive statistics to ascertain the overall response profiles at the type of institution level. An ANOVA procedure was conducted to compare budget allocations for information security across the different types of educational institutions. The dependent variable was the budget allocations, and the independent variable was the institution type.

To answer Research Question 3, the respondents were asked to rank their overall information security preparedness on a scale of 1-5. The responses obtained from similar institutions were grouped together (i.e., the group mean was calculated by institution type to obtain response profiles for the different types of institutions). The analysis of the data collected was performed using descriptive statistics to ascertain the overall response profiles at the type of institution level. An ANOVA procedure was conducted to compare the overall threat preparation

index across the different types of educational institutions. The dependent variable was the self-reported information security preparedness level, and the independent variable was the institution type.

Additional analyses were conducted to further analyze findings from the data analyses for the research questions and to establish identifiable patterns, if any, within the scope of the study. These analyses included a correlation analysis and a not applicable (N/A) response analysis.

The correlation analysis was conducted using the responses obtained in the ISPI© to investigate how each of the mean scores of security threat risk perception factors, threat prevention measure effectiveness perception factors, frequency of key security practices, and budget allocations correlated with the overall preparedness scores for each educational institution that participated in the survey. The purpose of this analysis was to investigate which of the factors had the most impact on the overall institutional threat preparedness.

Respondents to the ISPI© had the option to indicate N/A for any item on the survey, be it a security threat risk perception score, threat prevention measure effectiveness perception score, or a frequency of a key security measure. A not applicable (N/A) response meant that the item concerned did not apply to the institution concerned. In other words, the institution concerned did not implement the item as a threat prevention measure or did not consider the item as a significant risk. An analysis was performed to identify the 10 items on the ISPI© that had the most N/A responses and how such N/A responses were distributed across the different types of educational institutions. The averages of the percentage distributions of the identified N/A response items were then calculated for each type of educational institution. The purpose of this analysis was to help identify how the N/A responses were distributed across the types of

educational institutions which, in turn, assisted in the identification of the types of educational institutions that were most frequently failing to implement key security measures.

Discussion of the Findings

Research Question 1

The respondents rated their perceptions of security risks for threats on a scale of 1-5 on the ISPI© with 1 being the least risky and 5 being the riskiest. The responses were aggregated based on the five components of information systems (Kroenke & Boyle, 2015): hardware, software, data, procedures, and people; and group means were calculated. Participants from Private Colleges/Universities showed the least variance in their responses. Five separate ANOVA tests (one for each component) revealed no statistically significant differences between the types of educational institutions in their assessments of security risks. Perceptions of people-oriented threats had the highest aggregate mean of 3.80. This finding matched a finding in a prior study by Keller et al. (2005).

The findings revealed that the different types of educational institutions identified information security risks in similar ways. Given that the security risks identified for this survey were dynamic in nature, it can be inferred that at present, different educational institutions have similar perceptions of security threats and are keeping up with the knowledge of the continuous changes in the field of information security in similar ways.

Research Question 2

The respondents rated their perceptions of the effectiveness of measures to counter security risks for threats on a scale of 1-5 on the ISPI© with 1 being the least effective and 5 being the most effective. The responses were aggregated based on the five components of

information systems (Kroenke & Boyle, 2015): hardware, software, data, procedures, and people; and group means were calculated. Participants from Public Colleges/Universities and Private Colleges/Universities showed the least variance in their responses. Perceptions of the effectiveness of data-oriented measures had the highest mean overall effective score of 4.01. Four of five separate ANOVA tests (one for each component) revealed significant differences between the types of educational institutions in their perceptions of the effectiveness of security measures. The only component that did not show any significant difference between the different types of educational institutions was the perception of effectiveness of people-oriented measures. Post-hoc tests conducted on the components that showed significant differences revealed the source of such differences between the types of educational institutions. Private Colleges/Universities were involved in most of such differences.

The respondents included in the ISPI© the frequencies with which they performed critical security practices and review their security policies and procedures. In addition, the respondents answered questions in the ISPI© regarding their institutional budget allocations for information security. Private Colleges/Universities had the highest mean scores for the frequencies of security practices and policy updates as well as for the allocation of budgets. Two separate ANOVA tests were run for the frequency responses (one each for low frequency measures and high frequency measures). An ANOVA test was run for the budgetary responses as well. These tests revealed significant differences between the types of educational institutions in their frequencies of critical security practices and review of security policies as well as in their budget allocations. Post-hoc tests conducted revealed the source of such differences between the

types of educational institutions. Private Colleges/Universities were again involved in most of such differences.

The findings revealed that the educational institutions had differences in their perceptions of effectiveness of their security risk mitigation practices, including the frequencies of occurrence. However, the perceptions of effectiveness of people-oriented risk mitigation practices did not show any difference across the different types of educational institutions. Because these risk mitigation practices and their frequencies of operation are universal, it can be inferred that there could be differences in their implementation across the different types of educational institutions. In addition, because these measures incur an expenditure, a corresponding difference in the budgetary allocation scores for information security related activities was an expected finding. An analysis of the budgetary allocation scores did reveal such differences across the different educational institution types.

An interesting finding was that no significant difference was observed for the perception of effectiveness of people-oriented measures across the different educational institution types. It can thus be inferred that educational institutions have been undertaking security measures that involve people in similar ways. One possible explanation for this is the relatively lower cost of implementation of people-centric security practices which are primarily based on user training and instruction as compared to the more sophisticated and expensive measures that apply to the other factors (hardware, software, data, and procedures). This allows most institutions to implement similar user-oriented practices with similar effects in risk prevention. A possible counter explanation could be that institutions find people-oriented measures ineffective, irrespective of the cost involved, as human behaviors are the most difficult to manage and

predict; thus, they rate their effectiveness with similar scores which are typically low. In this study the mean of the people-oriented measures was 3.05, which is somewhere in the middle of the 1-5 range. So, the first explanation seems more plausible, but the counter explanation cannot be discounted.

Research Question 3

The respondents rated their overall information security preparedness on a scale of 1-5 on the ISPI© with 1 being the least prepared and 5 being the most prepared. The responses were aggregated based on the five components of information systems (Kroenke & Boyle, 2015): hardware, software, data, and procedures and people; and group means were calculated. Participants from PK-12 Private Schools showed the least variance in their responses, and Private Colleges/Universities had the highest mean preparedness score of 3.40. An ANOVA test that was conducted showed significant differences between the types of educational institutions in their perceptions of their overall information security preparedness. Post-hoc tests conducted revealed the source of such differences to be between Private Colleges/Universities and PK-12 Public Schools and between Private Colleges/Universities and PK-12 Virtual Schools.

In a review of the overall mean scores (Table 39), participants from PK-12 Public Schools averaged an overall preparedness score of 2.16 and those from PK-12 Virtual Schools averaged an overall preparedness score of 2.29. Compared to the average score of 3.40 for Private Colleges/Universities, the scores of PK-12 Public Schools and PK-12 Virtual Schools were significantly lower.

Ancillary Analyses Findings

A correlation analysis was conducted to determine how each of the security threat risk scores, threat prevention measure effectiveness scores, frequency of key security practices, and budget allocations correlated with overall preparedness scores across all educational institutions. The results were summarized in Table 42. All of the correlations were significant at the 0.05 level and the 0.01 level except for those with people-oriented threats and with software-oriented measures which were significant only at the 0.05 level. All the security threat risk scores showed a negative correlation with overall preparedness scores, but prevention measure effectiveness scores, frequency of key security practices, and budget allocations showed a positive correlation with overall preparedness scores. In other words, higher overall preparedness scores were correlated with lower security threat risk scores. Similarly, higher overall preparedness scores were correlated with higher prevention measure effectiveness scores, higher frequency of key security practices, and higher budget allocations. The strongest correlations were observed for the overall preparedness score with Low Frequency Practices, Budget Allocations and High Frequency Practices (correlation coefficients of 0.73, 0.68 and 0.57 respectively). On further review of the post-hoc tests done after the ANOVA tests for Low Frequency Practices, Budget Allocations and High Frequency Practices, it was observed that significant differences existed between Private Colleges/Universities and PK-12 Private Schools and PK-12 Virtual Schools respectively. Thus, it can be inferred that frequency of security practices and budget allocations are the strongest contributors to the overall preparedness score for an institution.

Respondents of the ISPI© had the option to indicate N/A for any item on the survey be it a security threat risk score, threat prevention measure effectiveness score, or a frequency of a key

security measure. The N/A response meant that item did not apply to the institution concerned. An analysis was completed to identify which items on the ISPI© had the most N/A responses. Table 43 lists the 10 items that had the most N/A responses and shows the percentage distribution of each type of educational institution that responded with an N/A response. All these items are key security measures. PK-12 Public Schools had the highest percentage of N/A responses followed closely by PK-12 Virtual Schools. Private Colleges/Universities had the least percentage of N/A responses.

Thus, it can be observed that PK-12 Public Schools and PK-12 Virtual Schools were not conducting a significant number of key security measures. It can be inferred from this finding that these institutions were having to deal with a lack of adequate personnel or expertise to perform these key security procedures which in turn can be associated with a smaller budget allocation. This finding confirms the earlier finding of frequency of security practices and budget allocations to be the strongest contributors to the overall preparedness score for an institution.

Implications for Practice

This researcher grouped responses about threat perceptions, security measures and overall preparedness by the type of institution and analyzed them based on the five factors of information systems: hardware, software, data, people, and procedures. These metrics show the differences in self-reported security preparedness among the types of institutions. Educational institutions are always in the process of balancing the conflicting demands of open culture, convenience of users and information security. In addition, there are other implications for the

information security environment of an educational institution. Personnel, employee certification, and outsourcing security pose constraints in the discussion of implications.

The presence of a dedicated information security department can make a substantial difference in terms of an educational institution's security policies and procedures. The number of employees dedicated to implement and manage information security also speaks to the importance of security issues. Some of these employees often have duties assigned to them other than information security. Medium to small institutions often have only one person, and sometimes in a part-time capacity, taking on the information security duties.

The security certification of the employee(s) in charge of security is a significant factor. Given the salaries certified professionals are presently enjoying, most schools and smaller colleges find it difficult to be competitive, and most of the educational institutions often try to grow the person from within. When institutions do take the time to train information security staff, they are very likely to be hired away from them.

To offset the lack of personnel or lack of expertise in the areas of information security, some institutions (especially smaller ones) may consider security as a service, essentially outsourcing the security management responsibilities to an outside company. This may prove to be a cost-effective solution for some institutions.

Suggestions for Future Research

This exploratory study concentrated on self-reported preparedness of educational institutions. Because such institutions are always in the process of balancing the contrasting requirements of culture, convenience and security, such responses may only reflect what they

feel they are doing right. Gaps may still exist in their actual security preparedness and what they perceive it to be.

Student population size is an important factor in information security in educational institutions because it often directly affects the institution's budget allocation. In other words, the smaller the institution, the fewer resources it typically has to allocate towards information security initiatives. This study did not differentiate the selected educational institutions in terms of this factor. A future study may be considered where institutions may be differentiated in terms of student population size. For example, small (0-15,000), medium (15001-60,000) and large (60,001 and above).

This study focused on a cross-section of educational institutions in the state of Florida. To study far-reaching trends and eliminate any regional or state-wide bias, a future study may need to be conducted that would include responses from educational institutions nationwide.

Future research may also include a design of an "information security matrix" which dynamically assigns weights to threats and measures based on their severity and prevalence with time. This matrix may then evaluate the preparedness of each institution by comparing their measures with established standards dynamically and making necessary adjustments based on budgets, school-size, profile and other parameters. The output from this matrix-based process would be a score that will reflect the actual preparedness of each institution. This could potentially be designed along the lines of the framework used by the corporate credit-rating agencies like Moody's Investor Service, Standard & Poor, and Fitch Ratings, that evaluate investment products like bonds and by individual credit-rating agencies like Experian, Equifax and Trans Union, that evaluate credit scores of individuals on pre-set parameters. To ensure

compliance, such a matrix-based security preparedness evaluation tool may be maintained at the state-level and be used to evaluate the information security performance of each institution on an annual basis.

Summary

This exploratory study was an attempt to find any significant differences in the information security preparedness among different types of educational institutions. The researcher found that though institutions differed in terms of their perceptions of effectiveness of security measures, frequencies of security operations and policy reviews, and budgetary allocations, they had very similar understandings of the risks associated with the security threats. This study was conducted to analyze the security practice gaps that were revealed, to identify potential causes and explore options by which gaps may be bridged.

APPENDIX A
IRB APPROVAL

University of Central Florida Institutional Review Board Office of Research & Commercialization 12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246
Telephone: 407-823-2901 or 407-882-2276
www.research.ucf.edu/compliance/irb.html

Determination of Exempt Human Research

From: **UCF Institutional Review Board #1**
FWA00000351, IRB00001138

To: **Vikram Ahmed, EdD**

Date: **December 21, 2017**

Dear Researcher:

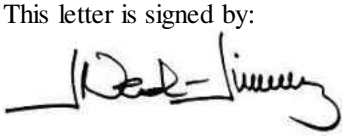
On , the IRB reviewed the following activity as human participant research that is exempt from regulation:

Type of Review:	Exempt Determination – Category #2 – Online Survey in Adults
Project Title:	An analysis of the preparedness of educational institutions to ensure the security of their institutional information
Investigator:	Vikram Ahmed, EdD
IRB Number:	SBE-17-13607
Funding Agency:	
Grant Title:	
Research ID:	N/A

This determination applies only to the activities described in the IRB submission and does not apply should any changes be made. If changes are made and there are questions about whether these changes affect the exempt status of the human research, please contact the IRB. When you have completed your research, please submit a Study Closure request in iRIS so that IRB records will be accurate.

In the conduct of this research, you are responsible to follow the requirements of the Investigator Manual.

This letter is signed by:



Signature applied by Jennifer Neal-Jimenez on 12/21/2017 11:15:23 AM EST

Designated Reviewer

APPENDIX B
INFORMATION SECURITY PREPAREDNESS INSTRUMENT (ISPI) SCREEN CAPTURES

0% 100%

UNIVERSITY OF CENTRAL FLORIDA

College of Education and Human Performance

EDUCATIONAL LEADERSHIP PROGRAM

Title of Study: An analysis of the preparedness of educational institutions to ensure the security of their institutional information

Principal Investigator: Vikram Ahmed, M.B.A.

Co-Investigator and Faculty Supervisor: Jerry Johnson, Ed.D.

You are being requested to take part in a research study being conducted by researchers at the University of Central Florida concerning the preparedness of educational institutions to ensure the security of their institutional information. We are requesting you to take part in this study since you have been identified as an institutional leader overseeing information security at your institution. Your answers to this survey will be anonymous.Your participation in this study is completely voluntary. Even if you decide to participate now, you may change your mind and stop at any time. You may choose not to answer any survey question for any reason. If you decide to take part, you are free to withdraw at any time.

Purpose of the Study: The purpose of this exploratory study is to analyze the preparedness of educational institutions toward ensuring the security of their data by analyzing their self-reported perceptions of security risks and their assessments of the corresponding risk-mitigating practices. Given the dynamic nature of the threats to information security, this study will further explore mechanisms by which the different types of educational institutions are staying up-to-date in their information security policies and procedures. Finally, the culture of educational institutions with respect to implementing information security measures as reflected in their allocation of budgets for the same will be explored.

What you will be asked to do in the study: You will be asked to complete a 68-question survey that will ask you to rate information security risk factors, risk-mitigating measures and overall information security preparedness as they apply to your institution. In addition, you will be asked some general questions about frequency of occurrences of security measures, information systems personnel hierarchy, budgetary allocations for information security, and past data breaches if applicable.

Participation time required: It is estimated that the survey will take approximately 10-15 minutes to complete.

Study contact for questions about the study or to report a problem: If you have questions, concerns, or complaints, please contact:

Vikram Ahmed, M.B.A., Principal Investigator, College of Education and Human Performance, University of Central Florida by email at vahmed@knights.ucf.edu or by phone at (979) 220-6952.

Jerry Johnson, Ed.D., Faculty Supervisor, College of Education and Human Performance, University of Central Florida by email at Jerry.Johnson@ucf.edu or by phone at (407) 823-3278.

By completing the survey you confirm you are at least 18 years of age.

IRB contact about your rights in the study or to report a complaint: Research at the University of Central Florida involving human participants is carried out under the oversight of the Institutional Review Board (UCF IRB). This research has been reviewed and approved by the IRB. For information about the rights of people who take part in research, please contact: Institutional Review Board, University of Central Florida, Office of Research & Commercialization, 12201 Research Parkway, Suite 501, Orlando, FL 32826 or by telephone at (407) 823-2901.

To begin the survey, please click on the yellow "Next >>" button below.

Next >>

For questions 1-25, choose on a scale of 1 to 5 (1 being very low risk to 5 being very high risk) the level you perceive for the following security threats as they apply to your institution. Choose N/A for threats that do not apply.

(For a brief explanation of each of the security threats, please click on the respective threat items. The explanation will open in a new window on your browser. When you are done reading the explanation, please close the explanation window to return to the survey).

	1	2	3	4	5	N/A
1) Ransomware	○	○	○	○	○	○
2) Cyber - espionage	○	○	○	○	○	○
3) Phishing	○	○	○	○	○	○
4) Sniffing	○	○	○	○	○	○
5) Hacking	○	○	○	○	○	○
6) Denial of service	○	○	○	○	○	○
7) Natural disasters	○	○	○	○	○	○

	1	2	3	4	5	N/A
8) Theft	○	○	○	○	○	○
9) Improper disposal	○	○	○	○	○	○
10) Malicious insider	○	○	○	○	○	○
11) Spoofing	○	○	○	○	○	○
12) Malware	○	○	○	○	○	○
13) SQL injection	○	○	○	○	○	○
14) Web application attacks	○	○	○	○	○	○

	1	2	3	4	5	N/A
15) Payment card skimmers	○	○	○	○	○	○
16) Weak passwords	○	○	○	○	○	○
17) Elevation of privilege	○	○	○	○	○	○
18) User errors	○	○	○	○	○	○
19) Unpatched systems	○	○	○	○	○	○
20) Institutional data on personal devices	○	○	○	○	○	○
21) Unencrypted data transfers	○	○	○	○	○	○

	1	2	3	4	5	N/A
22) Institutional data on third party services	○	○	○	○	○	○
23) Outdated anti-virus and anti-malware software	○	○	○	○	○	○
24) Inadequate security monitoring	○	○	○	○	○	○
25) Inadequate backups of institutional data	○	○	○	○	○	○

<< Previous

Next >>

UNIVERSITY OF CENTRAL FLORIDA

For questions 26-47, choose on a scale of 1 to 5 (1 having very low effect to 5 being very effective) the level you perceive for the following security measures as they apply to your institution. If an item does not apply to your institution, please select N/A.

(For a brief explanation of each of the security measures, please click on the respective measure items. The explanation will open in a new window on your browser. When you are done reading the explanation, please close the explanation window to return to the survey).

	1	2	3	4	5	N/A
26) Instructing users to not click on links in emails from unknown sources	○	○	○	○	○	○
27) Instructing users to not open attachments from emails from unknown sources	○	○	○	○	○	○
28) Instructing users to avoid visiting unauthorized websites on work computers	○	○	○	○	○	○
29) Implementing a password policy for strong, complex and long passwords for all users	○	○	○	○	○	○
30) Making users change passwords frequently	○	○	○	○	○	○
31) Avoiding sending valuable and confidential data via email or instant messages	○	○	○	○	○	○

	1	2	3	4	5	N/A
32) Instructing users to check for https in any website address that require authentication	○	○	○	○	○	○
33) Removing stored personal identifying information from computers and mobile devices	○	○	○	○	○	○
34) Clearing browsing history, temporary files and cookies from public computers	○	○	○	○	○	○
35) Regularly updating anti-virus and anti-malware software on all institutional machines	○	○	○	○	○	○
36) Taking regular backups of key data	○	○	○	○	○	○
37) Using central authentication and single sign on	○	○	○	○	○	○

	1	2	3	4	5	N/A
38) Using multi-factor authentication	○	○	○	○	○	○
39) Using encryption for data transfer and storage	○	○	○	○	○	○
40) Using biometric authentication for accessing secure areas	○	○	○	○	○	○
41) User authorization	○	○	○	○	○	○
42) Employing a dedicated Information Security Officer	○	○	○	○	○	○
43) Installing institutional firewall	○	○	○	○	○	○

	1	2	3	4	5	N/A
44) Installing institutional virtual private network	○	○	○	○	○	○
45) Training users on new security threats	○	○	○	○	○	○
46) Implementing post-intrusion attempt remediation procedures	○	○	○	○	○	○
47) Applying critical server and system patches regularly	○	○	○	○	○	○

<< Previous

Next >>

UNIVERSITY OF CENTRAL FLORIDA

For the following periodic security measures listed in questions 48-58, please indicate the frequency of occurrence as they apply to your institution. If an item does not apply to your institution, please select N/A.

(For a brief explanation of each of the periodic security measures, please click on the respective measure items. The explanation will open in a new window on your browser. When you are done reading the explanation, please close the explanation window to return to the survey).

	Occurs every month	Occurs every 3 months	Occurs every 6 months	Occurs every year	Occurs every 3 years	N/A
48) Honey pot experiments	○	○	○	○	○	○
49) Social engineering experiments to enforce security protocols	○	○	○	○	○	○
50) Log review and monitoring	○	○	○	○	○	○
51) Internal security audit	○	○	○	○	○	○

	Occurs every month	Occurs every 3 months	Occurs every 6 months	Occurs every year	Occurs every 3 years	N/A
52) External security audit	○	○	○	○	○	○
53) Review of institutional security policies and change management	○	○	○	○	○	○
54) Sending information technology personnel to attend information security classes	○	○	○	○	○	○
55) Mandatory training on security topics for all employees	○	○	○	○	○	○

	Occurs every month	Occurs every 3 months	Occurs every 6 months	Occurs every year	Occurs every 3 years	N/A
56) Review of data breach remediation procedures	○	○	○	○	○	○
57) Review of business continuity and disaster recovery policies	○	○	○	○	○	○
58) Review of data backup policies	○	○	○	○	○	○

<< Previous

Next >>

UNIVERSITY OF CENTRAL FLORIDA

59) Please indicate the title of the institutional official to whom the head of Information Technology in your institution reports to:

60) Please indicate the percentage of the total institutional annual operating budget allocated to information technology in your institution:

- Less than 3%
- 3% to 10%
- 10% to 15%
- Greater than 15%

61) Please indicate the percentage of the total annual information technology budget allocated to information security in your institution:

- Less than 3%
- 3% to 10%
- 10% to 15%
- Greater than 15%

62) Please indicate the dollar amount of the total annual information technology budget per employee in your institution:

- Less than $5,000
- $5,000 to $10,000
- $10,000 to $20,000
- Greater than $20,000

<< Previous

Next >>

63) Did you ever encounter any data breach incident in your institution?

Yes	Maybe	No

64) If yes, did you invoke your cyber insurance?

Yes	No

65) On a scale of 1 to 5 (1 being the least prepared to 5 being the most prepared), choose the level you perceive for the overall information security preparedness of your institution :

	1	2	3	4	5
Overall information security preparedness	○	○	○	○	○

<< Previous Next >>

Powered by Qualtrics

UNIVERSITY OF CENTRAL FLORIDA

66) Please indicate the type of educational institution where you currently work:

- PK-12 Public School
- PK-12 Private School
- PK-12 Virtual School
- Public College/University
- Private College/University

67) Please indicate what your job title is:

68) Please select the option that best represents the time you have been in your current position:

- Less than 1 year
- 1 - 3 years
- 4 - 6 years
- 7 - 9 years
- More than 10 years

<< Previous Next >>

Powered by Qualtrics

APPENDIX C
CHRONBACH'S ALPHA TEST FOR RELIABILITY

The Information Security Preparedness Instrument (ISPI©) used in this study was checked for reliability and consistency using Chronbach's Alpha. The results are as follows:

Reliability Statistics for ISPI©

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.767	.788	14

The Reliability Statistics shows the value of the Chronbach's Alpha coefficient. If the coefficient is above 0.70, the instrument has high internal consistency. In this case the coefficient was 0.767 which shows that the ISPI© had high internal consistency and was thus reliable.

APPENDIX D
INFORMED CONSENT

An analysis of the preparedness of educational institutions to ensure the security of their institutional information

Informed Consent

Principal Investigator:	Vikram Ahmed, MBA
Faculty Supervisor:	Jerry Johnson, Ed.D
Sponsor:	UCF College of Education and Human Performance
Medium:	Online Survey

Introduction:

Researchers at the University of Central Florida (UCF) study many topics. To do this we need the help of people who agree to take part in research studies. You are being requested to take part in such a research study being conducted by researchers at the UCF concerning the preparedness of educational institutions to ensure the security of their institutional information. We are requesting you to take part in this study since you have been identified as an institutional leader overseeing information security at your institution. You must be 18 years of age or older to be included in the research study.

The persons doing this research are UCF Professor Jerry Johnson along with graduate student Vikram Ahmed.

What you should know about a research study:

- The procedures involved in the research study will be explained to you.
- A research study is something you volunteer for.
- Whether or not you take part is up to you.
- You should take part in this study only because you want to.
- You can choose not to take part in the research study.
- You can agree to take part now and later change your mind.
- Whatever you decide it will not be held against you.

- Feel free to ask all the questions you want before you decide.

Purpose of the research study:
The purpose of this study is to ascertain the preparedness of educational institutions toward ensuring the security of their data by analyzing their self-reported perceptions of security risks and their assessments of the corresponding risk-mitigating practices. Factors to be studied in securing institutional data are aligned with the five components of any information system: hardware, software, data, procedures and people. The study will examine the security threats associated with these factors, and explore the critical measures with respect to these factors that can enhance security within the constraints applicable to educational institutions. Given the dynamic nature of the threats to information security, this study will further explore mechanisms by which the different types of educational institutions are staying up-to-date in their information security policies and procedures. Finally, the culture of educational institutions with respect to implementing information security measures as reflected in their allocation of budgets for the same will be explored.

What you will be asked to do in the study:
If you agree to participate in this study you will be asked to complete an online survey created exclusively for this study.

Location:
The survey will be conducted online.

Time required:
The survey contains 68 questions and will take approximately 10-15 minutes to complete.

Funding for this study:
Not Applicable.

Risks:
There are no reasonably foreseeable risks or discomforts involved in taking part in this study. Participating in this study will require you to click on the link provided for the survey and answer the questions online.

Benefits:
This research study will provide you with the opportunity to assess the relative criticality of the threat factors to information security as they pertain to your institution and assess the effectiveness of their corresponding security measures. In addition, this study will allow you the opportunity to analyze the frequency of reviews of the security policies currently in effect in your institution. So, in summary, this study may assist in providing you with information relating to certain key areas where you may need to focus on to optimize the conflicting requirements of security and convenience.

Compensation or payment:

There is no direct compensation or other payment to you for taking part in this study.

Confidentiality:

Data collection will take place in an online medium via an anonymous survey. You will not be required to provide your name or any other form of identifying information. In addition to the investigators, organizations that may inspect and review the survey responses include the IRB and other representatives of UCF.

Study contact for questions about the study or to report a problem:

If you have questions, concerns, or complaints, or think the research has hurt you, please contact:

Mr. Vikram Ahmed, Graduate Student, College of Education and Human Performance, phone (979) 220-6952 or email: vahmed@knights.ucf.edu OR

Dr. Jerry Johnson, Faculty Supervisor, College of Education and Human Performance, phone (407) 823-3278 or email: jerry.johnson@ucf.edu

IRB contact for questions about your rights in the study or to report a complaint:

Research at the University of Central Florida involving human participants is carried out under the oversight of the Institutional Review Board (UCF IRB). This research has been reviewed and approved by the IRB. For information about the rights of people who take part in research, please contact: Institutional Review Board, University of Central Florida, Office of Research & Commercialization, 12201 Research Parkway, Suite 501, Orlando, FL 32826-3246 or by telephone at (407) 823-2901. You may also talk to them for any of the following:

- Your questions, concerns, or complaints are not being answered by the research team.
- You cannot reach the research team.
- You want to talk to someone besides the research team.
- You want to get information or provide input about this research.

Withdrawing from the study:

You may withdraw from the study at any time.

Results of the research:

The results of the study will be shared with the public via conferences and peer-reviewed publications. If you wish to receive a summary of the results of the survey, please send an email to the principal investigator or the faculty supervisor.

REFERENCES

Adi, K., Hamza, L., & Pene, L. (2018). Automatic security policy enforcement in computer systems. *Computers & Security, 73*, 156-171. https://doi.org/10.1016/j.cose.2017.10.012

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*, 160-196. https://doi.org/10.1016/j.cose.2017.04.006

Al-rimy, B., Maarof, M., & Shaid, S. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security, 74*, 144-166. https://doi.org/10.1016/j.cose.2018.01.001

Amigud, A., Arnedo-Moreno, J., Daradoumis, T., & Geurrero-Roldan, A. (2018). An integrative review of security and integrity strategies in an academic environment: Current understanding and emerging perspectives. *Computers & Security, 76*, 50-70. https://doi.org/10.1016/j.cose.2018.02.021

Andress, J. (2014). *The basics of information security*. Waltham, MA: Syngress.

Austin, A., Holmgreen, C., & Williams, L. (2013). A comparison of the efficiency and effectiveness of vulnerability discovery techniques. *Information and Software Technology, 55*(7), 1279-1288. https://doi.org/10.1016/j.infsof.2012.11.007

Bakhshi, T., Papadaki, M. & Furnell, S. (2009). Social engineering: assessing vulnerabilities in practice. *Information Management & Computer Security 17*(1).

Bennett, L., & Nair. C. (2010). A recipe for effective participation rates for web-based surveys. *Assessment & Evaluation in Higher Education, 35*(4).

Bielski, L. (2005). Security breaches hitting home. *ABA Banking Journal*, *97*.

Breaches Affecting 500 or More Individuals (2018). US Department of Health and Human Services. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Bourgeois, D. T. (2014). *Information systems for business and beyond*. Saylor Academy.

Bourne, K. (2014). *Application administrator's handbook*. Waltham, MA: Elsevier.

Burdon, M., Reid, J., & Low, R. (2011). Encryption safe harbours and data breach notification laws. *Computer Law & Security Review, 26*(5), 520-534. https://doi.org/10.1016/j.clsr.2010.07.002

Burling, S. (2014). *Penn Medicine Rittenhouse has data breach*. Philly.com. Retrieved from http://articles.philly.com/2014-07-18/news/51663609_1_data-breach-social-security-numbers-identity-theft

Caballero, A. (2017). *Computer and information security handbook*. Cambridge MA: Morgan Kaufmann.

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security, 2016*(6), 8-14. https://doi.org/10.1016/S1361-3723(15)30046-4

Cavusoglu, H., Cavusoglu, H., Son, J., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management, 52*(4), 385-400. https://doi.org/10.1016/j.im.2014.12.004

Chen, J., Wu, G., Shen, L., & Ji, Z. (2011). Differentiated security levels for personal identifiable information in identity management system. *Expert Systems with Applications, 38*(11), 14156-14162. https://doi.org/10.1016/j.eswa.2011.04.226

Cherry, D. (2015). *Securing SQL server*. Waltham, MA: Elsevier.

Chopra, M., Mung, J., & Chopra, K. (2013). A survey on use of cloud computing in various fields. *International Journal of Science, Engineering and Technology Research, 2*.

Christopher, L., Choo, K., & Dehghantanha, A. (2017). *Contemporary digital forensic investigations of cloud and mobile applications*. Cambridge, MA: Elsevier.

Chronology of Data Breaches – Educational Institutions (2018). Privacy Rights Clearinghouse. Retrieved from https://www.privacyrights.org/data-breaches

Christopher, L., Choo, K., & Dehghantanha, A. (2017). *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Cambridge, MA: Elsevier.

Conrad, E., Misenar, S., & Feldman, J. (2016). *CISSP study guide.* Waltham, MA: Elsevier.

Cost of Cyber Crime Study – Ponemon Institute (2013). Ponemon Institute. Retrieved from http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

Cost of Data Breach Study – Ponemon Institute (2017). IBM. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

Data Breach Investigations Report – Verizon Enterprise Solutions (2017). Verizon Enterprise Solutions. Retrieved from http://www.verizonenterprise.com/DBIR/2017/.

Data Breach Investigations Report – Verizon Enterprise Solutions (2018). Verizon Enterprise Solutions. Retrieved from http://www.verizonenterprise.com/DBIR/2018/.

Data Breaches (2018). Identity Theft Research Center. Retrieved from https://www.idtheftcenter.org/data-breaches.html.

Data Security | Data Breach – Information and Updates on UCF's network intrusion (2016). University of Central Florida. Retrieved from http://www.ucf.edu/datasecurity/

Dilman, D., Smyth, J., & Christian, L. (2014). *Internet, phone, mail, and mixed-mode surveys: The tailored design method* (4th ed). Wiley.

Estimating Password Cracking Times. (2018). Better Buys. Retrieved from https://www.betterbuys.com/estimating-password-cracking-times/

Farina, K. (2015). *International encyclopedia of the social & behavioral sciences*. Amsterdam, Netherlands: Elsevier.

Fay, J., & Patterson, D. (2018). *Contemporary security management*. Cambridge, MA: Elsevier.

Fernandes, D. (2014) *More firms buying insurance for data breaches*. Boston Globe. Retrieved from https://www.bostonglobe.com/business/2014/02/17/more-companies-buying-insurance-against-hackers-and-privacy-breaches/9qYrvlhskcoPEs5b4ch3PP/story.html

Fitzpatrick, D., & Griffin, D. (2016). Cyber-extortion losses skyrocket, says FBI. *CNN Money*. Retrieved from http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/index.html?section=money_technology

Florida Colleges and Universities - Colleges Search by State | Cappex (2018). Cappex. Retrieved from https://www.cappex.com/colleges/states/Florida

Furnell, S. (2009). The irreversible march of technology. *Information Security Technical Report, 14*, 176-180. https://doi.org/10.1016/j.istr.2010.04.002

Furnell, S., & Emm, D. (2017). The ABC of ransomware protection. *Computer Fraud & Security, 10*, 5-11. https://doi.org/10.1016/S1361-3723(17)30089-1

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security, 2017*(2), 5-10. https://doi.org/10.1016/S1361-3723(17)30013-1

Furnell, S., Niekerk, J., & Clarke, N. (2014). The price of patching. *Computer Fraud & Security, 2014*(8), 8-13. https://doi.org/10.1016/S1361-3723(14)70521-4

Gardner, B., & Thomas, V. (2014). *Building an information security awareness program*: *Defending against social engineering and technical threats.* New York, NY: Syngress.

Gartner Says Many Organizations Falsely Equate IT Security Spending with Maturity. (2016). Gartner. Retrieved from https://www.gartner.com/newsroom/id/3539117

Gliem, J. A., & Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. *Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education*.

Gold, S. (2011). The Cookie Monster. *Computer Fraud & Security, 2011*(9), 12-15. https://doi.org/10.1016/S1361-3723(11)70091-4

Gonzaga University v. Doe - 536 U.S. 273 (2002).

Goralski, W. (2017). *The illustrated network*. Cambridge, MA: Morgan Kaufmann

Groot, M. (2017). *A primer in financial data management.* Cambridge, MA: Elsevier.

Hentea, M. (2005). A perspective on achieving information security awareness. Informing Science. *International Journal of an Emerging Transdiscipline*, *2*, 169-178.

Hillison, W., Pacini, C., & Williams, P. (2001). Confidentiality of student records in the electronic frontier: professors' and administrators' obligations. *Journal of Accounting Education, 18*(4), 301-313. https://doi.org/10.1016/S0748-5751(01)00003-3

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons, 59*(6), 585-591. https://doi.org/10.1016/j.bushor.2016.07.004

How Much Should a Company Spend on IT?|Business Guide (2018). Techvera. Retrieved from https://techvera.com/company-it-spend/

Information Resources Management Association. (2017). *Identity theft: Breakthroughs in research and practice.* Hershey, PA: IGI Global.

IT Security for Higher Education: A Legal Perspective (2003). Retrieved from https://www.educause.edu/ir/library/pdf/CSD2746.pdf

IU says no victims reported in data breach (2014). *Indianapolis Business Journal*. Retrieved from http://www.ibj.com/articles/48628-iu-says-no-victims-reported-in-data-breach

Jia, Y., Chen, Y., Dong, X., Saxena, P., Mao, J., & Liang, Z. (2015). Man-in-the-browser-cache: Persisting HTTPS attacks via browser cache poisoning. *Computers & Security, 55*, 62-80. https://doi.org/10.1016/j.cose.2015.07.004

Jobe, J.B. (1990). Cognitive laboratory approach to designing questionnaires for surveys of the elderly. *Public Health Reports, 105*(5), 518-524.

Jones, A. (2008). Catching the malicious insider. *Information Security Technical Report 13*(4), 220-224. https://doi.org/10.1016/j.istr.2008.10.008

Joshi, C., & Singh, U. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*, 128-137. https://doi.org/10.1016/j.jisa.2017.06.006

Jouini, M., Rabai, L., & Aissa, A. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489-496. https://doi.org/10.1016/j.procs.2014.05.452

Keller, S., Powell, A., Horstmann, B., Predmore, C., Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management*, *22*(2).

Kelly, P., & Rohland, C. (2017). The United States federal budget project. *Journal of Accounting Education, 41*, 48-57. https://doi.org/10.1016/j.jaccedu.2017.09.002

Kirkwood Website Experienced Unlawful Access (2013). Kirkwood Community College. Retrieved from http://kirkwoodonlinenews.org/?p=3947

Knapp, E., & Langill, J. (2015). *Industrial network security*. Waltham, MA: Elsevier.

Kovacich, G., & Halibozek, E. (2017). *Security metrics management*. Cambridge, MA: Elsevier

Kroenke, D., & Boyle, R. (2015). *Experiencing MIS*. Harlow, Essex, England: Pearson.

Layne, B., DeCristoforo, J., & McGinty, D. (1999). Electronic versus traditional student ratings of instruction. *Research in Higher Education*, *40*(2), 221–232.

Lee, P. (2017). Prints charming: how fingerprints are trailblazing mainstream biometrics. *Biometric Technology Today, 2017*(4), 8-11. https://doi.org/10.1016/S0969-4765(17)30074-7

Leveson, N. (2012). *Engineering a safer world*. Cambridge, MA: MIT Press.

Levy, Y., & Ramim, M. M. (2016). Towards an evaluation of cyber risks and identity information sharing practices in e-learning, social networking, and mobile texting apps. *Proceeding of the chais 2016 conference on innovative and learning technologies research*.

Liginlal, D., Sim, I., Khansa, L., & Fearn, P. (2012). HIPAA Privacy Rule compliance: An interpretive study using Norman's action theory. *Computers & Security, 31*(2)*,* 206-220. https://doi.org/10.1016/j.cose.2011.12.002

Liu, Wang, & Camp (2008). Game-theoretic modeling and analysis of insider threats. *International Journal of Critical Insider Protection, 1*, 75-80.

LSU doc's stolen laptop brings offer for free credit protection for NOLA area patients (2015). WGNO. Retrieved from http://wgno.com/2015/09/15/lsu-docs-stolen-laptop-brings-offer-for-free-credit-protection-for-nola-area-patients/

Mansfield-Devine, S. (2017). Ransomware: the most popular form of attack. *Computer Fraud & Security, 10*, 15-20. https://doi.org/10.1016/S1361-3723(17)30092-1

Markos, E., Labrecque, L., & Milne, G. (2018). A new information lens: The self-concept and exchange context as a means to understand information sensitivity of anonymous and personal identifying information. *Journal of Interactive Marketing, 45,* 46-62. https://doi.org/10.1016/j.intmar.2018.01.004

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems, 108,* 57-68. https://doi.org/10.1016/j.dss.2018.02.007

Mitchell, M., Palacios, V., & Leachman, M. (2014). States are still funding higher education below pre-recession levels. *Center on Budget and Policy Priorities.*

Moore, J., & Shelton, K. (2013). Social and student engagement and support: The Sloan-C quality scorecard for the administration of online programs. *Journal of Asynchronous Learning Networks, 17*(1).

Morton, S.M.B., Bandara, D. K., Robinson, E. M. & Carr, P. E. A. (2012). In the 21st century, what is an acceptable response rate? *Australian and New Zealand Journal of Public Health, 36*. 106–108.

Nacer, H., Djebari, N., Slimani, H., & Aissani, D. (2017). A distributed authentication model for composite Web services. *Computers & Security, 70*, 144-178. https://doi.org/10.1016/j.cose.2017.05.008

Ngai, E.W.T, Hu, Y., Wong, Y.H., Chen, Y. & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559-569. https://doi.org/10.1016/j.dss.2010.08.006

Nicholson, J. & O'Reardon, M. (2009), Data protection basics: A primer for college and university counsel. *Journal of College and University Law, 36*(1).

Noor, M., Abbas, H., & Shahid, W. (2018). Countering cyber threats for industrial applications: An automated approach for malware evasion detection and analysis. *Journal of Network and Computer Applications, 103*, 249-261. https://doi.org/10.1016/j.jnca.2017.10.004

Nulty, D. (2008). The adequacy of response rates to online and paper surveys: what can be done? *Assessment & Evaluation in Higher Education, 33*(3).

Ogbanufe, O., & Kim, D. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support Systems, 106*, 1-14. https://doi.org/10.1016/j.dss.2017.11.003

Oliveira, R., Laranjeiro, N., & Vieira, M. (2015). Assessing the security of web service frameworks against denial of service attacks. *Journal of Systems and Software, 109*, 18-31. https://doi.org/10.1016/j.jss.2015.07.006

O'Neil, M. (2014). Data breaches put a dent in colleges' finances as well as reputations. *Chronicle of Higher Education*. Retrieved from http://chronicle.com/article/Data-Breaches-Put-a-Dent-in/145341/

Online Learning with a K12 Education (2018). K12. Retrieved from https://www.k12.com/k12-education.html

Pectas, A., & Acarman, T. (2017). Classification of malware families based on runtime behaviors. *Journal of Information Security and Applications, 37*, 91-100. https://doi.org/10.1016/j.jisa.2017.10.005

Porter, S., (2004). *Overcoming survey research problems*. San Francisco: Jossey-Bass.

Powerhouses and Benchwarmers: Assessing the Cyber Security Performance of Collegiate Athletic Conferences (2014). Bitsight Technologies. Retrieved from http://media.scmagazine.com/documents/90/bitsight_insights_athletics_q3_22351.pdf

Private School Directory (2018). Florida Department of Education. Retrieved from http://www.floridaschoolchoice.org/information/PrivateSchoolDirectory/Default.aspx

Provo City School District warning employees of data breach (2014). Fox. Retrieved from http://fox13now.com/2014/10/01/provo-city-school-district-warning-employees-students-of-data-breach/

Rashti, M., Sabin, G., & Kettimuthu, R. (2016). Long-haul secure data transfer using hardware-assisted GridFTP. *Future Generation Computer Systems, 56*, 265-276. https://doi.org/10.1016/j.future.2015.09.014

Razzaq, A., Latif, K., Ahmad, H., Hur, A., Anwar, Z., & Bloodsworth, P. (2014). Semantic security against web application attacks. *Information Sciences, 254,* 19-38. https://doi.org/10.1016/j.ins.2013.08.007

Rhodes, J. & Poley, V. (2014). *The aba cybersecurity handbook: A resource for attorneys, law firms, and business professionals*. New York, NY: American Bar Association Book Publishing.

Richter, A., & Wood, J. (2016). *Practical deployment of Cisco identity services engine (ISE).* Waltham, MA: Elsevier.

Rockwell, L. (2013). Payment Cards. *Encyclopedia of Forensic Sciences*. https://doi.org/10.1016/B978-0-12-382165-2.00219-1

Romanosky, S., Telang, R., & Acquisti, A (2008). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management, 30*(2).

Sammons, J., & Cross, M. (2017). *The basics of cyber safety*. Cambridge, MA: Elsevier.

Sanders, C. (2014). *Applied network security monitoring*. Waltham, MA: Elsevier.

Serneels, P., Beegle, K., & Dillon, A. (2017). Do returns to education depend on how and whom you ask? *Economics of Education Review, 60*, 5-19. https://doi.org/10.1016/j.econedurev.2017.07.010

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to Cyber-Warfare.* Waltham, MA: Elsevier.

Shannon, D., & Farley, J. (2012). *Privacy and network security liability in higher education.* Wells Fargo Insurance Services. Retrieved from http://www.dedcmdasfaa.org/docs/conferences/Conference2012Fall/presentations/PrivacyAndNetworkSecurityLiabilityInHigherEducation.pdf

Shen, C., Yu, T., Xu, H., Yan, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security, 61*, 130-141. https://doi.org/10.1016/j.cose.2016.05.007

Singleton, T., Singleton, A. & Gottlieb, G. (2006). Cyberthreats facing the banking industry. *Bank Accounting & Finance, 19*(2).

Sitko, T. (2003). Life with HIPAA: A primer for higher education. *Center for Applied Research*. Retrieved from https://net.educause.edu/ir/library/pdf/ERB0307.pdf

Snedaker, S., & Rima, C. (2014). *Business continuity and disaster recovery planning for it professionals*. Waltham, MA: Elsevier.

Stair, R., & Reynolds, G. (2013). *Principles of information systems*. Boston, MA: Course Technology Cengage Learning.

Stark, P. (2010). Congressional intent for the HITECH Act. *American Journal of Managed Care*. Retrieved from http://www.ajmc.com/publications/supplement/2010/AJMC_10dec_HIT/AJMC_10decHIT_Stark_SP24tp28/

Steinbart, P., Raschke, R., Gal, G., & Dilla, W. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems, 13*(3), 228-243. https://doi.org/10.1016/j.accinf.2012.06.007

Stetson University. (2018). *Information security handbook*. DeLand, FL:Stetson University.

Strawser, B., & Joy, D. (2015). Cyber security and user responsibility: surprising normative differences. *Procedia Manufacturing, 3*, 1101-1108. https://doi.org/10.1016/j.promfg.2015.07.183

Tan, C., Hijazi, M., Lim, Y., & Gani, A. (2018). A survey on proof of retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends. *Journal of Network and Computer Applications, 110*, 75-86. https://doi.org/10.1016/j.jnca.2018.03.017

Tanaka, Y., Akiyama, M., & Goto, A. (2017). Analysis of malware download sites by focusing on time series variation of malware. *Journal of Computational Science, 22*, 301-313. https://doi.org/10.1016/j.jocs.2017.05.027

Thompson, J. (2015). *High integrity systems and safety management in hazardous industries*. Waltham, MA: Elsevier.

Torres, H., & Alsharif, K. (2016). Reflecting on resilience in Broward County, Florida: A newspaper content analysis about Hurricane Wilma recovery. *International Journal of Disaster Risk Reduction, 19*, 36-46. https://doi.org/10.1016/j.ijdrr.2016.08.007

Touchette, F. (2016). The evolution of malware. *Network Security, 2016*(1), 11-14. https://doi.org/10.1016/S1353-4858(16)30008-3

Townsend, K. (2010). Anti-virus: a technology update. *Infosecurity 7*(6), 28-31. https://doi.org/10.1016/S1754-4548(10)70109-1

UMD Data Breach (2014). University of Maryland. Retrieved from http://www.umd.edu/datasecurity/

Urquiola, M. (2016). *Handbook of the economics of education*. Amsterdam: Elsevier

Vacca, J. R. (2012). *Computer and information security handbook*. Waltham, MA: Elsevier.

Vayansky, I., & Kumar, S. (2018). Phishing – challenges and solutions. *Computer Fraud & Security, 2018*(1), 15-20. https://doi.org/10.1016/S1361-3723(18)30007-1

Velasquez, I., Caro, A., & Rodriguez, A. (2018). Authentication schemes and methods: A systematic literature review. *Information and Software Technology, 94*, 30-37. https://doi.org/10.1016/j.infsof.2017.09.012

Virtual Education (2018). Florida Department of Education. Retrieved from http://www.fldoe.org/schools/school-choice/virtual-edu/

Virvilis, N., Mylonas, A., Tsalis, N., & Gritzalis, D. (2015). Security Busters: Web browser security vs. rogue sites. *Computers & Security, 52*, 90-105. https://doi.org/10.1016/j.cose.2015.04.009

Wang, W., Liu, J., Pitsilis, G., & Zhang, X. (2018). Abstracting massive data for lightweight intrusion detection in computer networks. *Information Sciences, 433-434*, 417-430. https://doi.org/10.1016/j.ins.2016.10.023

Woods, N., & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies, 111*, 36-48. https://doi.org/10.1016/j.ijhcs.2017.11.002

Yao, G., Bi, J., & Xiao, P. (2013). VASE: Filtering IP spoofing traffic with agility. *Computer Networks, 57*(1).

Young, D., Lopez, J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection, 14*, 43-57. https://doi.org/10.1016/j.ijcip.2016.04.001

Zalaznick, M. (2013). Cyberattacks on the rise in higher education, University Business. Retrieved from http://www.universitybusiness.com/article/cyberattacks-rise-higher-education