AN EXPLORATION OF THE STRATEGIES INFORMATION ASSURANCE TECHNOLOGISTS NEED TO IMPROVE INFORMATION SECURITY PRACTICES IN AN SCHOOL DISTRICT

A Dissertation Presented in Partial Fulfillment of the Requirements for the Degree of Doctor of Computer Science

By

Travis Paakki

Colorado Technical University

June, 2019

Committee

James O. Webb, Jr., Ph.D, Chair

Jeffrey Butler, Ph.D, Committee Member

James Prunier, D.Cs., Committee Member

_____

June 4, 2019

Abstract

Even with the increasing warnings and evidence of how K-12 education is being specifically targeted for cyberattack, district leaders are unable to provide information assurance technologists in K-12 education with the strategies they need to improve information security. This systemic failure has led to high-profile breaches, compromises of student and staff data and FBI warnings to parents and families that promote demanding action from their school systems to address cybersecurity. This exploratory study made use of qualitative semi-structured interviews to determine the strategies present in other industries that are used to improve information security in those organizations. Subject matter experts were selected from a group of high-scoring participants in an information security certification testing body, as well as those who list their title as Chief Information Security Officer on Linked.com in the United States at organizations who did not engage in information security as their primary business. Six themes emerged from the data after a three-tiered analysis process: The need for laws, regulations, and standards, the need for appropriate staffing and funding, the need for a culture of security that starts at the top of the organization, the need for K-12 information assurance technologists to leverage and implement a security framework, augmenting security teams, and leveraging the use of auditors. By implementing these strategies, district leaders can ensure that information assurance technologists in their organizations are empowered to improve information security to aid in meeting the expectations of stakeholders in and outside of the organization as well as meet the standards of due diligence.

Keywords: Information security risk tolerance, Information security maturity, K-12 cybersecurity, K-12 information security, FERPA, COPPA, CIPA, Student data privacy, School district business systems, Information security posture, K-12 information technology

Dedication

This dissertation has seen the skylines of Austin, Chicago, Las Vegas, Seattle, Phoenix, Orlando, Portland, Denver, San Diego, New Orleans, Cozumel, San Antonio, San Jose, Cabo San Lucas, and Vancouver, B.C. from the desks by windows of hotel rooms and countless more cities from the windows of planes and airports. It has seen the seasons change, children grow and graduate, and the passing of a great number of rare sunny days. I dedicate this to any first generation college student who has opted to return to finish their terminal degree while also trying to balance family and a profession. More so, it is also dedicated to the families of those who have engaged in this pursuit, as without the love and support of mine, my goals would have not been attainable.

Acknowledgments

I want to thank the knowledgeable Computer Science staff at Colorado Technical University. In particular, I would like to thank Dr. James Webb for his guidance in this process. Additionally, I would like to thank the members of my committee, Dr. Jeffrey Butler and Dr. James Prunier. I want to thank the information security community for not only their guidance but also their participation in the study and their selfless sacrifice of time to do so. Lastly, I would like to thank my family, who has supported the late nights, the tired days, and encouraged me to keep going.

Table of Contents

Table of Contents v

List of Tables ix

List of Figures x

Chapter One 1

Topic Overview/Background 3

Problem Statement 5

Purpose Statement 6

Research Question 7

Propositions 7

Conceptual Framework 7

Assumptions/Biases 10

Significance of the Study 11

Delimitations 12

Limitations 12

Definition of Terms 13

General Overview of the Research Design 16

Summary of Chapter One 17

Organization of Study 19

Chapter Two 20

Previous Studies of K-12 Information Security 22
Information Security Maturity 24
Governance, Risk, and Compliance 26
Information Security Posture 31
Best Practices for Information Security 34
Stakeholder Demands 38
Economic Constraints 39
Risk Tolerance 43
Stakeholder Security Expectations 44
Staff Constraints 46
Gap Identified in the Body of Knowledge 47
Methods 49
Conceptual Framework 50
Summary of Literature Review 53
Chapter Three 55
Research Tradition 55
Research Question 57
Research Design 58
Population and Sample 58
Sampling Procedure 59

Instrumentation 61

Validity 62

Reliability 64

Data Collection 66

Data Analysis 69

Ethical Considerations 70

Summary of Chapter Three 71

Chapter Four 73

Participant Demographics 73

Presentation of the Data 75

The Need for Laws and Regulations 77

The Need for Staffing and Funding 79

The Need for a Culture of Security 81

The Use of Frameworks 86

Augmenting Security Teams 88

Auditors 90

Miscellaneous 92

Presentation and Discussion of Findings 93

Summary of Chapter Four 96

Chapter Five 99

Findings and Conclusions 100

Theme 1: The Need for Prescriptive Laws, Regulations, and Standards 102

Theme 2: Engage in Appropriate Staffing and Funding for Information Security 103

Theme 3: Foster a Culture of Security 105

Theme 4: Implement and Follow a Security Framework 107

Theme 5: Augment Security Teams 108

Theme 6: Leverage the Use of Auditors 108

Conclusions 109

Limitations of the Study 110

Implications for Practice 112

Implications of Study and Recommendations for Future Research 116

REFERENCES 123

APPENDIX A 139

APPENDIX B 142

APPENDIX C 145

APPENDIX D 148

List of Tables

Table 1 *Strategies Examined in the Study* 20

Table 2 *Search Terms Used for the Study* 22

Table 3 *Significant K-12 Laws Pertaining to Information Security* 30

Table 4 *Research Participants, Industry, Gender, Years at Organization, and Coverage* 74

Table 5 *Interview Questions for the Study* 75

Table 6 *The Major Themes Identified in the Study* 77

Table 7 *Respondents Affected by Laws, Regulations, and Standards* 78

Table 8 *Infosec Team Size Comparison to IT by Budget and Staff* 81

Table 9 *End User Training Methods and Frequency* 82

Table 10 *Stakeholders Listed and Frequency* 83

Table 11 *Concerns About Information Security Threats and Frequency* 84

Table 12 *Participant Observations on the Level of Security Awareness by Population* 85

Table 13 *Frameworks Used by Respondents* 86

Table 14 *Options Used to Augment Information Security Teams Capabilities* 89

Table 15 *Auditor Sentiment and Remediation Expectations* 91

Table 16 *Responses to the Question Prompting for Additional Strategies* 93

Table 17 *Themes That Emerged from the Study and Their Frequency of Occurrence* 94

List of Figures

Figure 1. The Gartner model for assessing organizational information security maturity 25

Figure 2. The conceptual framework for the strategies needed to improve information security in a school district 33

Figure 3. Best practices for information security. 38

Figure 4. The conceptual framework for the strategies needed by IATs for improving information security in a school district 53

Figure 5. The questions that determined the need for laws and regulations 79

Figure 6. The questions that determined the need for staffing and funding 81

Figure 7. The questions which determined the need for a culture of security 86

Figure 8. The questions which determined the requirement for the use of frameworks 88

Figure 9. The questions contributing to the finding of the need to augment security teams 90

Figure 10. The questions contributing to the finding of the need to engage auditors 92

Figure 11. The strategies needed by IATs in a K-12 school district to improve information security 110

CHAPTER ONE

Culnan and Williams (2009) reported that information security is one of the most challenging obligations to meet for any organization but they have a moral obligation to do so, but this difficulty is even more so for information assurance technologists (IATs) working in the field of primary and secondary education. This collection of grades is known as K-12, indicating a span from Kindergarten to twelfth grade, as reported by Zhong (2017). Information security is challenging for IATs to provide in the K-12 environment because many of the strategies that exist in other industries that IATs can leverage to ensure information security are not present in K-12 (Brown, 2016; Nyachwaya, 2013). As a result, best practices are not followed and are possibly not yet established. Thus, the lack of these strategies being available leads to persistent information security vulnerabilities and the perception that information security in K-12 lags behind that of other industries contributing to further attacks.

The lack of information security in K-12 organizations is despite a genuine threat. On September 13, 2018, the Federal Bureau of Investigation made a public service announcement that warned K-12 institutions of threats by groups of actors looking to exploit the vast amounts of information that organizations possess regarding students. Further, privacy violations such as the viewing of records that are not specific to an educational need-to-know were also being exploited (Federal Bureau of Investigation, 2018). With estimated losses from a breach being more than $350 thousand per organization (Nyachwaya, 2013), school districts cannot afford poor information security practices.

The goal of the study was to explore the strategies that IATs in industries other than K-12 use to ensure and improve information security in their organizations. These strategies provide paths for IATs in K-12 organizations to follow to more readily implement information security

best practices as advocated by Okoye (2017). The study identified which strategies K-12 organizations can implement in the short-term and which may need more robust and long-term action plans and advocacy to put into place. However, implementations of strategies in K-12 can be impaired by a lack of financial resources, qualified staff, and prioritization (Brown, 2016).

Renaud (2016) wrote that organizations of all sizes struggle to maintain adequate levels of information security, but the problem was particularly acute in small to medium-sized organizations. Thus understanding the strategies that IATs can leverage, such as regulations or compliance requirements, mandatory budgetary allocations, staff training, or stakeholder education can uncover paths for advocacy and long-term budget strategies that can aid in improving information security (Aloul, 2012; Behara & Huang, 2013). Toward this end, Cox (2012) wrote that the strategies that IATs need are dependent upon the information security risk tolerance of the organization, the assets requiring protection, and the security expectations of the constituents.

Ahmad, Maynard, and Park (2014) wrote that well-established information security strategies are vital to the success of an information security program. Thus, understanding and leveraging strategies discovered in the study can allow K-12 IATs and their leadership to advocate for the implementation of such strategies. With these strategies available in an organization, IATs can reduce breaches of security and privacy and reduce how attractive their organization is to a potential attacker. The primary concern that an IAT must address using the strategies to improve information security is the protection of the sensitive information for which they are responsible. In the case of K-12 organizations, Trainor (2015) wrote that both the standard business information of any enterprise as well as the sensitive data on students and families must be protected.

The K-12 industry needs to define the strategies for successful information security program implementation, funding, and function. Both Brown (2016) and Nyachwaya (2013) discovered that IATs in K-12 are skilled, competent, and aware of standard information security controls. However, since strategies to improve information security have not been established in the context of K-12 specifically (Brown, 2016; Nyachwaya, 2013), focused research is necessary to determine those strategies and how they may apply to K-12. By leveraging these strategies, IATs can improve information security practices in K-12 organizations so that the level of information security can be parallel with that of organizations in other industries.

Topic Overview/Background

Ajredini, Ebibi, Fetaji, M. and Fetaji, B. (2013) wrote that as recently as the late 1990s education record keeping was performed mainly on paper, but the demand for computerization continued to grow as administrators realized that electronic records were the only viable way to stay ahead of the explosion in demand for timely and actionable data. While these systems have improved, they have also increased the K-12 attack surface (Brown, 2016) exposing that data to the potential for unauthorized access by bad actors over the internet or internally. While in industry, information security practices have improved due to laws, stockholder demands, breach insurance compliance agreements and other factors (Strauss, 2016), in K-12, the level of information security has remained relatively stagnant. Choraś, Churchill, Kozik, and Yautsiukhin (2016) reported that the threat landscape, however, has not, placing K-12 organizations at risk.

McLaughlin wrote in 2011 that K-12 organizations, like all organizations connected to the internet, are under constant attack from those who may wish to exploit the organization's resources for gain. IATs had little leverage to influence budget or policy to improve information security in their organizations in spite of this threat. Toward this end, research investigations have indicated a gap in the knowledge that is needed to ensure information security in K-12

organizations which is the strategies used in other industries to ensure information security which can apply in the K-12 context. The lack of available strategies is leading IATs to implement measures that cannot be successful in improving information security (Nyachwaya, 2013). Therefore research is needed to determine those strategies that IATs need to improve information security in K-12 environments.

The review of past and current research offered views of the state of information security in a K-12 setting. However, practitioners and researchers have given only nominal thought as to the human experience of attempting to implement and sustain information security in a K-12 environment (Brown, 2016; Nyachwaya, 2013) either regionally or nationally. While research has eluded to the fact that the state of the information security in K-12 is below the level expected in other industries (Lestch, 2015), and that there is a multitude of contributing causes, there has been little exploration as to remediating strategies to address this (Brown, 2016). Thus, from these initial determinations, it is necessary to explore the successful strategies that IATs make use of in other industries to understand those strategies that may translate to the K-12 environment to improve information security.

K-12 IATs have typically understood the need to have reliable strategies to leverage to ensure that information security remains a priority in their organizations. Overall information security strategies, those drivers and requirements that IATs can leverage to influence policy and compete for budget dollars, play a central role in establishing and maintaining good information security practice for an organization (Ahmad et al., 2014). Earlier research has exposed that K-12 information security lags behind the information security level of other industries (Brown, 2016). This lag exists even though the professionals responsible for this information security are typically well aware of the requirements and how to technically implement them.

Information security strategies are necessary for improving information security in K-12 organizations. These strategies can take the form of appropriate staffing and budgeting levels, the proper establishment of policies and the documented information security risk tolerance that states that dictates following policies, appropriate prioritization of information security work by IT, and access to laws and compliance frameworks that mandate a particular level of information security. These critical components in information security are essential to the present and future security posture of the organization (Ahmad et al., 2014) and the protection of both business data as written by Ekelhart, Grill, Kiesling, Strauss, and Stummer (2016) as well as the sensitive student and family information. However, work in information assurance continues to advance and evolve. Thus, present-day attacks, stakeholder expectations, and laws are forcing IATs to seek out strategies to improve the information security of their organizations (Brown, 2016). As such, K-12 IATs need to evolve to incorporate strategies that allow them to become more effective in their goals of improving information security maturity.

Problem Statement

The problem the study examined is that a lack of strategies that information assurance technologists need to improve information security in K-12 organizations has led to information security best practices not being followed (Brown, 2016; Nyachwaya, 2013). The lack of information security best practices is especially troubling since the advent of student information systems that aim to place the majority of data involving students into systems in which information security practices have not evolved to keep pace with the increased exposure. Additionally, employees and students often lack information security awareness training (Nyachwaya, 2013). Additionally, all the above with constrained budgets and staffing and the information technology assets of school districts at increasing risk (Brown, 2016). This

combination of factors has left school district information security often lagging behind that of other industries, making them appealing targets (Brown, 2016).

Purpose Statement

The purpose of the qualitative exploratory study was to explore the strategies information assurance technologists need to improve information security practices in a school district. By understanding what these strategies are, K-12 IATs can aim to implement them in their organization to improve information security. Changing these strategies may prove difficult as Hambright and Diamantes (2004) indicated that the implementation of security strategies is a significant change for an organization. In a K-12 organization, this may involve culture transformation, funding prioritization, and advocacy for more comprehensive K-12 information privacy regulations (Brown, 2016).

The study explored those strategies through semi-structured interviews with subject matter experts in information security regarding the strategies they employ to improve information security in their organizations. These subject matter experts were identified by their membership in the GIAC advisory board ("GIAC Advisory Board", n.d.) and several vetting questions designed to identify the responsible parties for information security in organizations outside of the education industry with successful, multi-year experience in their role, or identified as a Chief Information Security Officer (CISO) on LinkedIn.com. These individuals were asked a series of questions that will discern the tools and tactics that are vital to ensure that information security best practices are followed in their organizations (Ahmad et al., 2014). These were analyzed and synthesized into a list of strategies that IATs can incorporate into their organizations in the United States.

Research Question

The question to be answered in the study was: What are the strategies information assurance technologists can use to improve information security practices in a school district? This research question was the guiding force of the study (Law, 2004). By following this guiding question, the instrument and research design are formed to ensure that each contributes to answering the question (Mason, 2002).

Propositions

The proposition associated with the study was that by understanding the strategies that IATs in other industries leverage to improve information security in their organizations, IATs in K-12 districts can implement and, as suggested by Kovács, Nemeslaki, Orbók, and Szabó (2017), then advocate for those same strategies and use them to improve information security in their school districts. The information security of districts could improve by making these strategies available to IAT's in K-12. These strategies are essential to influence the practice of information security in an organization towards maturity (Ahmad et al., 2014).

Conceptual Framework

The researcher has created a conceptual framework for the study that examines the role of information security maturity in organizations and how that drives demands for information security practices as well as the organization's capability to deliver the intended outcome of those practices and absorb the organizational impact of those practices. Also examined is the role of information security posture, which is defined as the organizational risk tolerance and the organization's awareness of information security issues and its subsequent demand for solutions. At the intersection of information security posture and maturity are the strategies that information assurance technologists use to improve information security in their organizations.

By examining the intersection of information security maturity and the information security posture for an organization, the researcher can determine responses that most readily translate into a K-12 environment. An organization with a security posture that dictates a near zero risk tolerance will spend whatever it takes to avoid the exposure to information security risk and is very unlike K-12 organizations. Posture is moderated by the information security maturity of an organization having a near zero information security budget and thus a low maturity (Edwards, M., 2018) but is very like most K-12 organizations. By using organizations from other industries with similar constraints, the researcher is bound to performing research in organizations with strategies that could apply to K-12 organizations as well. By examining the experiences of subject matter experts that are responsible for information security in their environments, the study sought to extrapolate from the lived experiences of the subjects who practice information security in other industries into strategies for improving K-12 information security (Kovács et al., 2017).

The research fits with other research in the information systems field that states that there is significant insight that to be gained from qualitative exploratory studies (Myers & Newman, 2007). While information security is often a technical pursuit, the decision-making process often does not lend itself to quantitative analysis (Albrechtsen & Hovden, 2009). Other research seeks to understand a level of K-12 information security, which is useful in establishing a starting point for improvement but does not necessarily address the causes of insufficient levels of information security in K-12 environments. While this previous research is useful in the assessment of individual organizations, it does not address the systemic and causal issues in the field of K-12 information security and its deficiencies.

Information security is often referred to as a human problem even in organizations with a strong information security posture; a human could easily compromise information security devices and policies with insufficient training (Butavicius, Jerram, McCormac, Parsons, & Pattinson, 2014). As such, it is unusual that any industry would be lacking in studies of the lived experiences of those implementing information security. Research states that there are relatively few academic studies of K-12 information security, and none of the lived experiences of IAT's in the field.

Additionally, in the field of K-12, the laws that mandate the protection of student data are permissive and vague, and a breach of data often does not result in a monetary penalty of any sort for the organization (Bennett & Brower, 2001). Other privacy laws aim to mandate protections at the state level that require organizations to protect student privacy but principally aim to keep student data away from marketers (Peterson, 2016). There is a concern that the lack of laws to insist organizations properly secure their data, and with a lack of penalties that private industry would face such as a loss of customers, or monetary penalties, or executive liability, there is little motive for school districts to place due diligence efforts in providing for their information assets.

A large portion of information security research examines establishing a measure and then measuring the level of information security for an organization. In K-12 information security, the two major works are quantitative assessments of the level of information security in an organization (Brown, 2016; Nyachwaya, 2013). These works examine the *what* regarding information security but mostly avoid the why or more importantly what to do about it. There are studies of the socio-technical necessities of information security and subsequent implementation and improvement strategies, but there are none in the field of K-12. This is in

significant contrast to studies in other fields that include assessments of security levels and well as qualitative studies of the impact of the human factor in information security as reported by Baskerville et al. (2013) in their survey of behavioral information security research.

Assumptions/Biases

Assumptions are the beliefs that are necessary to conduct the study but cannot be proven, such as assuming the honesty of the subjects (Goes & Simon, 2013). One of the key assumptions is that the researcher makes is that subjects are truthful in their qualifications. Another critical assumption by the researcher is that the size of the sample adequately reaches saturation (Cardon, Fontenot, Marshall, & Poddar, 2013). A third assumption is that the organizations the subjects are employed by do not perform information security as a primary function, and thus prioritizations of security spending must take place. The fourth assumption is that extrapolation is viable for the security strategies in use by the subjects in other industries. The assumptions of a researcher are necessary, and identifying them can aid in building an instrument that can facilitate rigorous and valid findings (Guba & Lincoln, 1986).

The documentation and acknowledgment of bias are essential as are documenting the steps that were taken to eliminate or reduce the bias (Goes & Simon, 2013). Bias in qualitative research is inevitable (Mehra, 2002). A fundamental bias is the work experience of the researcher (Noble & Smith, 2015). The researcher has a 25-year history in the field of information technology. Additionally, the researcher has a 15-year history in the area of information assurance and ten years of experience in information assurance in educational organizations. Based on this experience, the researcher will have preconceived notions of the discovered strategies in the study. An instrument has been created that restricts the ability of the researcher to lead the subject towards providing answers that fit those preconceived notions, thus controlling bias.

Significance of the Study

There remains a lack of documentation on the lived experiences of those implementing information security in K-12 organizations. Many of the school district in the United States, and subsequently, their IT departments are typically underfunded (Laboy, Schaffer, Stein, & Ware, 2013). Information security is often lacking, even though there is a growing list of systems that depend on internet connectivity to serve students (Brown, 2016). Further, there is a lack of documentation in information assurance studies regarding the strategies that information assurance technologists leverage to influence the improvement of information security in their organizations.

Interestingly, there are a wealth of studies that identify the tactics of implementing a particular information security function as a means to address specific information security maturity goal. However, there are almost no studies that directly identify the strategies that IAT's employ to ensure the addressing of information security posture. This lack of documentation leads to inconsistent implementations of security controls even within the same jurisdiction, or a lack of information system security implementations altogether (Brown, 2016).

By identifying strategies IATs can use to improve information security in their organizations, the goal of the study was for IATs to influence security awareness in their organizations, as Edwards (2015) suggested. Additionally, altering budgetary priority so that information security is the first function considered with the implementation of any new IT service. Further, Strauss (2016) reported that laws that are intended to protect student privacy had been amended many times since their creation but still do not contain prescriptive requirements for the prevention of information security breaches as do laws in other industries. This research can aid in advocacy of revisions to federal student privacy laws, funding priorities, organizational structures, and district governance.

Delimitations

Delimitations are characteristics, determined by the researcher that define the boundaries of the study, decided upon during the development of the study plan (Goes & Simon, 2013). The first delimitation was the development of a research question to guide the study. The second delimitation was the identification of a population of subject matter experts responsible for information security in their organizations that have more than 500 employees, and are located in the United States who have scores of 90% or higher on a GIAC.org information security certification exams ("GIAC Advisory Board", n.d.) or identified as a CISO on LinkedIn.com. A third delimitation is a focus on those that have been in their roles for at least two years to experience multiple budget cycles. A final delimitation is that subjects were selected from organizations that do not perform information security in an *at any cost* fashion, implying a lack of budgetary constraints.

Limitations

The limitations in qualitative research are those factors over which the researcher has little control but must be accounted for as the researcher establishes validity (Flick, 2004). The first limitation is the assumed honesty of the participant of the subject in answering screening questions and in interviews. The second limitation is that the limited amount of time allocated for the research study by the time available in the program of study as well as the time available to the researcher. With each interview taking an hour and transcription taking two hours, the resources available to the researcher quickly become exhausted. The third limitation is that of a research protocol and instrument. The validity of this instrument is dependent upon pilot studies of additional subjects, as is suggested by Julious (2005).

Definition of Terms

Attack Surface: The attack surface of an organization is the sum of the different points where an unauthorized user can try to adversely affect the intended operations of the systems of the organization (Manadhata & Wing, 2011). A best practice is to keep the attack surface as small as possible to reduce the opportunities for unauthorized users to exploit system vulnerabilities.

Best Practices for Information Security: A best practice for information security is much like best practices in other industries. These are professional practices that, through use, have proven to be the best method for addressing information security (Carter, Harnett, & McCarthy, 2014). Examples of best practices for information security are to employ a risk-based approach, to patch software regularly, employing backups, employing the least privilege principle, and others that will be covered in chapter 2.

Children's Internet Protection Act: The Children's Internet Protection Act (CIPA), 47 CFR 54.250 was enacted in 2000 to protect minor's activities online at schools and libraries that receive federal E-rate reimbursements for internet costs. The schools that are subject to CIPA must also monitor the online activities of minors and teach digital citizenship, which includes information regarding appropriate online behaviors (Menuey, 2009).

Children's Online Privacy Protection Act: The Children's Online Privacy Protection Act of 1998 (COPPA), 16 CFR 312.1 – 312.12 is intended to police website operators and give parental control over what those operators could collect from their children (Holcomb, 2015). Additionally, children under the age of 13 are not allowed to grant consent for data collection so the parents must give that. Finally, this collected information must not be disclosed to other parties without parental consent.

Family Education Rights Privacy Act: The Family Education Rights Privacy Act of 1974 (FERPA), 34 CFR 99. FERPA has had numerous amendments, but the most relevant aspects for K-12 information security is that the law requires that stewards of student performance data must protect it from accidental disclosure (Strauss, 2016). Additionally, the law requires protections of the release of data from which there is the possibility of the inference of confidential information. Bennett and Brower (2001) wrote that unlike many laws, FERPA is permissive, telling data stewards whom data is releasable to rather than how to protect information from release. There is much criticism of FERPA in that is lacks some of the prescriptive practices, organizational roles, and penalties that more modern privacy and security laws do (Tudor, 2015).

Information Assurance Technologist: The information assurance technologist (IAT) is an individual responsible for the information security of an organization via policies, training, and installation and maintenance of security software and hardware (Abramson, Dawson, & Omar, 2015). This term is also used synonymously with *information assurance manager* or *CISO*. The IAT may be an individual who performs this role as a singular duty or in combination with other responsibilities.

Information Security: Information security is the collection of practices that maintain the confidentiality, integrity, and availability of data for an organization (Van Niekerk & Von Solms, 2013). This term is used synonymously with *cybersecurity* and *information assurance*. For the study, information security is not only the practice of, but also a measurable level that an organization can achieve through its practices, policies, hardware, and software (Brown, 2016).

Information Security Maturity: This is the ability of the organization to defend against information security threats in one of twelve critical domains of information security. Those are identified by Smock (2018) as *application security, service continuity, change and configuration*

management, data security, governance, risk and compliance, endpoint security, identity and access management, mobile security, security analytics, network security, physical security, and *vulnerability management*. An organizations stance on managing security in these twelve domains, combined with the demands from its information security risk tolerance define the strategies needed to improve information security within a district.

Information Security Posture: For this study, information security posture was the organization's capability to address the demand and constraints placed upon it. This posture comprises five elements. The first element is an organizations risk tolerance; next, staff and budget constraints; another is the accepted best practices for security. The final component is the information security culture or the attitudes and knowledge about information security at all levels of the organization.

Information Security Risk Tolerance: The risk tolerance of an organization is its willingness to invest to be able to defend against information security risk. For the study, this tolerance is a combination of the demands of stakeholders, and the amount the organization is able or willing to spend to comply with regulations or laws, best practices, and policies (Barki & Spears, 2010). Economic constraints and staff capabilities moderate demands. Risk tolerance depicts the intersection between limited resources and the demands of those affected by those choices.

K-12 district: This refers to a typical public school operating structure in which a collection of schools across a limited geographical region are responsible for operating and staffing schools serving children beginning in Kindergarten and going through grade twelve. The district is governed by a school board of elected officials and aids in operating services that are shared by individual schools such as centralized transportation services, special education, and

information technology (Dorata & Phillips, 2013). These can also include educational service districts that provide centrally administered services for a collection of smaller districts. For the study, the terms will be interchangeably.

Strategy: In the case of the study, a strategy was a method or plan used to bring about the desired future (Ahmad et al., 2014). These strategies can include prescriptive laws, information security posture, a larger budget or staffing allocation or an allocation strategy that places must-do functions before all others, and demands of stakeholders. The study sought to understand the strategies used by IATs in other industries and apply them for use in K-12 education.

General Overview of the Research Design

The methodology for the study was qualitative exploratory research. The design calls for the use of semi-structured interviews of subject matter experts who are information assurance technologists in other fields. This design suggests the use of semi-structured interviews as a means to explore phenomena that are nascent (Myers & Newman, 2007). The semi-structured interview will become the primary source of data for the study. The use of exploratory research in information assurance allows the exploration of strategies from the subject matter expert perspective. The approach to be used in the study was the identification of the population and sample, use of purposive sampling as recommended by Guest, Mack, MacQueen, Namey, and Woodsong (2005), and the creation and explanation of the instrumentation for the study. The design includes a discussion on validity and reliability and the methods the researcher will employ to ensure both. There is a discussion on ethics and the data collection and analysis methods that conclude the study design.

The data collection plan for the study consisted of presenting thirteen questions to subject matter experts in the field of information security using semi-structured interviews. The questions asked all centered on the research question – What are the strategies needed by K-12

IATs to improve information security in their organizations? Open-ended questions will allow subjects to relate their experiences in their own words (Guba & Lincoln, 1986). The use of probing questions will prompt SME's to give a rich accounting of their lived experience (Whiting, 2008). WebEx video meetings were used, and the entire session was recorded.

The data analysis plan for the study included a transcription of the verbal and non-verbal information from the interviews to synthesize a primary dataset using an online qualitative analysis tool called NVivo (NVivo, n.d.). The next step, as suggested by Yin (2015), is the review of the aggregated information to perform thematic coding that identifies priori themes in the data. The second level of coding, as suggested by Saldana (2011), was axial coding in which major themes are identified. The third level of coding or theoretical coding will analyze the data and seek to identify collections of higher-level themes into which subject answers can be grouped.

Summary of Chapter One

This chapter confirms the importance and significance of identifying the strategies that information assurance technologists can employ to improve information security in their environments. Chapter 1 introduced the importance of understanding these strategies in K-12 institutions and substantiated the fact that strategies in use in other fields are often not present for K-12 IATs to leverage to improve the information security of such organizations. However, as some of these strategies may include aspects of the information security posture of the organization (Ahmad et al., 2014; Barki & Spears, 2010), and the security knowledge of the staff which is cited as a factor by (Brown, 2016; Caldwell, 2013), they may not be present in K-12 organizations. Subject matter expertise must be sought in other organizations that have access to such strategies to gain meaningful data. Presentation of the research question used in the study, propositions, the conceptual framework, assumptions, biases, and the significance of the study

takes place in Chapter 1. With the above components, delimitations of the study, limitations of the study, definitions, and an overview of the research were also provided.

The study intended to learn from subject matter experts that are not employed in K-12 which strategies they employ to improve information security in their organizations. These strategies can be everything from security awareness (Aloul, 2012), local and federal laws (Thaw, 2011), budget allocations (Behara & Huang, 2013), and managing the demands of and expectations internal and external stakeholders. The intent of establishing these strategies for IATs in K-12 is to allow those professionals to advocate for the establishment of those practices, thus improving information security by leveraging them.

While the purpose of the study was to explore the strategies that can be used by IATs to improve information security in a school district, it aligns closely with the problem itself. The problem observed is that the strategies necessary for IATs to improve information security in K-12 environments have not been established (Brown, 2016; Nyachwaya, 2013). In information security, practices from other industries are often transferable. Thus an IAT will be able to apply the finding to their organizations (Kovács et al., 2017).

Chapter 2 will provide a comprehensive review of the literature associated with information security in a K-12 environment. The review will describe the components that make up a good security program by examining industry best practices as described by Okoye (2017). Additionally, laws that affect the information security requirements of K-12 organizations were examined (Bennett & Brower, 2001; Holcomb, 2015; Strauss, 2016). Further, documentation of the expectations of stakeholders is detailed. Chapter 2 also examines the strategies that are in use in other industries such as prescriptive laws, criminal penalties, and funding models that prioritize information security. Finally, the conceptual framework for the study is presented.

Organization of Study

The study contains five chapters that describe the phenomena of insufficient strategies to improve information security in K-12 organizations. Chapter 1 introduces the reader to the phenomena under study and describes the general research design. Chapter 2 presents an exhaustive literature review of the concepts of information security as they pertain to K-12 organizations. Chapter 3 details the research approach and design of the study. Chapter 4 details the results from a series of qualitative interviews of subjects. Chapter 5 interprets the results, presents areas for further study, and provides a conclusion.

CHAPTER TWO

The purpose of this exploration of literature is to explore and understand the strategies that are necessary for IATs to improve the information security of the districts in which they work. Thaw (2011) discovered the demands of IATs from regulations necessitate these strategies. Additionally Brown (2016) discussed the strategies required to implement the information security posture of the organization. Nyachwaya (2013) wrote that accepted best practices for information security in other industries also demonstrated the need for strategies that could be used to implement them within K-12 organizations. Demands for information security are moderated by the information security posture of an organization such as the risk tolerance, demands and constraints, and best practices (Brown, 2016; Nyachwaya, 2013; Thaw, 2011).

Anderson and Choobineh (2008) stated that strategies from early ARPAnet studies on information security had been codified in the NIST guidelines on information security (NIST800-53r4, 2013). This should not be confused with the definition of information security strategies suggested by Park and Ruighaver (2008) who aimed to define ways (strategies) to implement information security technologies. Instead, for the study, strategies are the tools IATs can cite to demonstrate the need to improve information security, as well as the means to fund and implement solutions addressing those obligations and expectations, while the obligations are the justification for doing so. These strategies are listed in table 1.

Table 1

Strategies examined in the study

Strategies
Resource prioritization for information security
Information security policies
A documented risk tolerance

Laws and industry norms that mandate information security practices and consequences
Demands of stakeholders

Ensuring the privacy and security of information had been recognized as a priority in K-12 organizations (Trainor, 2015). Herath and Rao (2009) stated that many forces influenced information security behaviors in organizations and those in school districts that must be explored to synthesize a conceptual framework that encompasses the relevant components. By examining recent literature pertinent to K-12 information security, information security best practices, laws pertinent to student data privacy and security, staffing and economic constraints of K-12 organizations, and law gaps and overlaps, a relevant picture of the literature was developed.

Sources for the literature review included multidisciplinary search engines such as ProQuest Dissertations and Theses Global and Google Scholar. Additional search engines that are specific to information assurance included: IEEE Xplore Digital Library, Science Direct (Elsevier), and the ACM Digital Library. Searches also included Emerald Engineering and SAGE Journals. These are sources available in the Colorado Technical University online library and match those used by Solomon and Chapple (2005) and later Nyachwaya (2013).

Subjects that were searched for are captured in table 2. Those terms include keywords that are specific to information security in the K-12 environment (Trainor, 2015). Additional keywords are specific to school district operating environments and the operations of a district. There are additional terms that were searched for that are not K-12 specific, but do apply to information security in general (Ahmad et al., 2014). These distinctions are used to ensure that the tone of the research, describing the current state of K-12 information security as a contrast to information security in other industries, is kept consistent.

Table 2

Search Terms Used for the Study

K-12 information security keywords	District operating environments	Industry keywords
K-12 information security	School district boards	Information security risk tolerance
K-12 cybersecurity	CAFR	Information security maturity
School district information security	School board behavior	Information security posture
FERPA	School board knowledge	Security behavior intention
COPPA	School district reporting requirements	Information security ethics
CIPA	School district business systems	
Student data privacy	School district as a business	
Student privacy expectations		

This chapter will detail the literature that was reviewed regarding the strategies that are necessary to improve K-12 information security. IT department leadership was forced to evaluate against many regulations, constraints, and demands to prioritize IT department priorities against information security demands (Brown, 2016). In the K-12 environment, these demands are particularly pressing because of the general impression that information assurance practices in K-12 lag behind other industries (Brown, 2016) even though districts possessed sensitive data on students and families. Throughout this chapter, fundamental research will be explored that details the criteria for strategies for information security improvement in a K-12 environment. This chapter contains three sections that will be explored: Previous studies of K-12 information security, information security maturity, and K-12 information security posture.

Previous Studies of K-12 Information Security

A preeminent work on K-12 information security was a quantitative correlational study that sought to discover the potential correlations between the use of preventative measures and

information systems security (ISS) effectiveness, senior management support, organizational size, and the ratio of information security budget to IT budget ratio (Nyachwaya, 2013). Nyachwaya (2013) focused on using an instrument created by Straub (1990) and later used by Kankanhalli, Teo, Tan, & Wei (2003) that centered on the largely subjective assessment of the respondents interpretation of the definition provided and their opinion of effectiveness of the item, based on scaling statements from 1, indicating weak agreement, to 7, indicating strong agreement. By studying the relationships between variable pairs such as preventative measures and information systems security (ISS) effectiveness, and security/IT budget ratio deterrent efforts, the researcher discovered that there are statistically significant relationships between spending on and the taking of precautionary measures and the effectiveness of those measures which matches the findings from similar studies in other industries (Kankanhalli, et al., 2003; Nyachwaya, 2013). This work was positive in that suggested that investing, both financially and culturally, in information security measures, resulted in greater information security in K-12 organizations, regardless of the organizations overall size.

In a subsequent study by Brown (2016) the researcher noted that there was a surprising lack of academic resources regarding K-12 information security, citing the work by previous authors but noting that there was much left to be explored on the topic (Nyachwaya, 2013; Baker, Farrie, & Sciarra, 2014). In his work, Brown (2016) also sought to measure both an objective and subjective level of information security for K-12 organizations in the state of California. Brown contrasted the presence of information security assets in an organization against moderating factors such as policies and upper management support and training to determine a level of information security (Brown, 2016). In his study, Brown (2016) concluded that the only true measures of the effectiveness of an information security program effectiveness

in K-12 were an organizations compliance with policy, information security training, and time spent maintaining security hardware.

Information Security Maturity

Information Security Maturity was defined by Gartner, Inc. as an organizations capability to provide security for its assets as a measured value from one to five on each of twelve major security domains: Vulnerability management, application security, service continuity, change and configuration management, data security, governance risk and compliance, endpoint security, identity and access management, mobile security, security analytics, network security, and physical security (Smock, 2018). The domains of information security are detailed in Figure 1. The domains detailed in the Gartner model are intended to be consistent with all organizations, with the demands for different measures of maturity being specific to the industry of the organization.

It has also been detailed that information security demands in K-12 organizations come from regulatory demands which correspond to governance, risk and compliance, and the organizations own information security posture, comprised of demands and constraints, risk tolerance, and information security best practices (Brown, 2016; Nyachwaya, 2013; Thaw, 2011). While all domains of information security maturity are significant, for the purposes of the study focus was on an organizations maturity in the domain of governance, risk and compliance acknowledging that an organizations risk tolerance is the intersection between its maturity and its posture. The other maturity domains are application security, service continuity, change and configuration management, data security, endpoint security, network security, and physical security the maturity of which are the result of the forces making up the security posture. These forces were both external and internal to the organization and existed regardless of the practitioner's ability to meet the demands that each brought (Nyachwaya, 2013). The forces

individually improved security but together often conflicted and overlapped. This intersection caused the IATs to make decisions on what security could be implemented and what would have to wait as district leaders often did not possess the technical aptitude to contribute to the decision-making process.

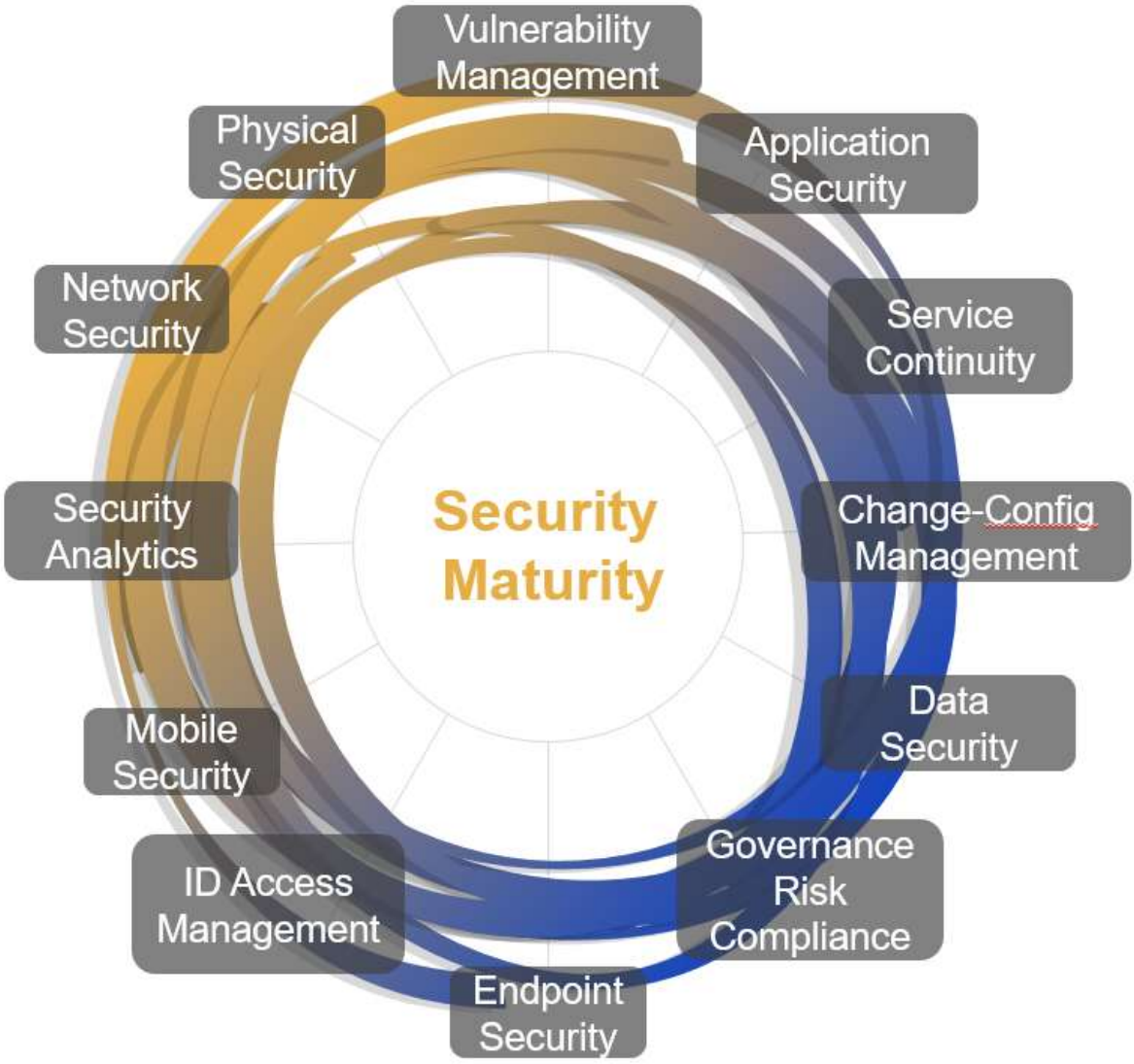

Figure 1. The Gartner model for assessing organizational information security maturity

Information security technical controls were the most easily measured and thus often assume a vital role in the assessment of the information security maturity of an organization

(Brown, 2016). Lacey and Stewart (2012), however stated that the flood of metrics from technical security controls has not resulted in a correlated increase in security program efficacy. Thus measures were often metrics of solved problems rather than performance improvement over time (Lacey & Stewart, 2012). As an example, the reporting on the pieces of blocked malware provided no additional actionable insight and may have contributed to a false sense of greater security (Brown, 2016). As such, information security maturity should be measured as a matter of meeting organizational demands for security in each of the domains.

Governance, Risk, and Compliance

Regulations governing information security in the K-12 space were overwhelmingly vague and often lacked specific implementation guidance as reported by Pusey and Sadera (2011). Laws of significance to K-12 information security are covered in table 3. Ahn, Bivona, and DiScala (2011) found that the Children's Internet Protection Act (Brown, 2016) was the regulation that most directly applied to primary and secondary educational environments. Under CIPA, institutions receiving government funds must block images that are obscene or harmful to minors. Those institutions were most commonly schools and libraries. Batch, Luhtala, and Magi, (2015) reported that the vague language led to over-filtering of internet content which impeded access to educational content by not defining what was considered harmful. Many instructors were troubled by CIPA as an aspect of digital citizenship was learning to navigate an unfiltered world (Batch et al., 2015).

Bennett and Brower (2001) stated in their work that FERPA introduced the concept that all educational information was part of an *educational record* and that employees or third parties involved in the delivery of educational services became *education officials*. FERPA (1974) also described the concept of *directory information*. Directory information was the information used to identify cohorts of students with a common identifier creating directories of interest to military

recruiters, marketers of graduation apparel, and others (Bennett & Brower, 2001). Hild (2017) noted that FERPA grants parents the right to be removed from directory disclosures and that the law prevented disclosures by schools of identifying information related to student grade performance.

In FERPA, the Department of Education stated that organizations should take *reasonable precautions* to prevent a compromise of student data (1974). These reasonable precautions involve making the efforts necessary to protect student data from accidental disclosure to unauthorized parties (Bennett & Brower, 2001). Mader and Smith (2014) reported that this was under the weak threat of a multi-year investigation and the potential loss of federal funding. As of 2014, no educational agency has lost access to federal funding, with the far more real threat having been that of the expense of responding to an investigation (Mader & Smith, 2014).

In 2015, Holcomb wrote that two laws pertained to the protection of student data and student privacy, FERPA, and COPPA. The Family Educational Rights Act, (FERPA) written in 1974 was the preeminent work on student privacy. Schwarz (2017) observed that the ambiguity in FERPA led to misinterpretations that not only were overly broad but have inadvertently shielded criminal acts. As an example, Strauss (2016) reported instances where students' psychological counseling records were shared with school administrators in their role as education officials when they were investigating unrelated matters.

The Children's Online Privacy Protection Act (1998) (COPPA) was aimed at service and software vendors and regulated marketing to children 13 years old or younger as a result of their online activity (Holcomb, 2015). For organizations to comply with COPPA, they must make it a point to have directed parents to consent and privacy sections of any web tools that captured data of children (Hild, 2017). COPPA also incorporated the right for the parent to request deletion of

the data about that student; however, that may conflict with FERPA guidelines that protect access to data for education officials (Mader & Smith, 2014). COPPA targeted operators of commercial websites and not school districts as reported by Stringer (2010).

Outside of the federal arena were laws such as those enacted or by the individual states. Peterson (2016) reported that numerous proposals for such state privacy laws existed. One example was California's Student Online Personal Information Privacy Act (SOPIPA) that prevented the use of student information for marketing purposes (Peterson, 2016). Adams (2016) reported that this had been the model for many of the subsequent state student privacy laws. Both Shear (2015) and Stuart (2005) state that a feature of SOPIPA is that it defined fines explicitly for those who would collect and resell student information for marketing purposes. SOPIPA was the first law to establish such prescriptive penalties.

The regulatory demands on K-12 for information security were old and either tended to be far too broad to reasonably enforced or to have information security consistently implemented to enforce them as reported by Lowenstein (2016). Also, some laws were far too narrow to be used in the context of information security. FERPA (1974) demanded that school districts provide for the privacy of student performance data. State records laws mandate a period which a school must maintain educational records. COPPA insists that parents were provided the opportunity to have given consent and that vendors supported records deletion of minor children on request (1998). Goldberg and Sheikh (2014) stated that all the state laws provided various definitions of Personally Identifiable Information (PII), and educational organizations must ensure that not only they but all of their vendors have complied with these laws. This contradictory and overlapping environment presented challenges for IATs and district legal counsel and required many to err on the side of overwhelming caution when designing security.

Daunted by the resulting cost and complexity, many K-12 organizations chose to accept the risk (Mader & Smith, 2014).

IATs understand that one of the most important obligations for information security is the compliance with law as discovered by Cooke, Dinev, Hart, and Hu (2012). Those obligations were to keep the sensitive data of students, families, and employees secure (Cooke et al., 2012). There were a variety of legal overlaps and grey areas the districts needed to resolve to establish their information security posture.

There were cases where laws such as FERPA supersede the Health Insurance Portability and Privacy Protection Act (HIPAA) regarding the management of Private Health Information (PHI) for students and conflict and contradict according to Strauss in her 2016 work. A district is not a *covered entity* from the perspective of HIPAA rules, and the PHI became a part of the education record according to Strauss (2016) reported that the damage to the student from the release of such information regardless of which law attempted to prevent the release is just as detrimental. The protection of PHI data from release was an obligation that K-12 districts need to meet, but with the non-prescriptive nature of FERPA, student PHI was far more at risk in a school that with a covered medical entity (Strauss, 2016). Still, the data that districts needed to treat with the degree HIPAA mandates is that surrounding employee PHI which the district may have possessed as an administrator of employee health benefits.

Batch et al. (2015) found that CIPA required that schools and libraries protect students from pornography and content that is *harmful* to them. The definition of harmful content was not made clear in the legislation and is the source of much debate and stated by Vicks (2013). Batch (2014) suggested that K-12 organizations need to leverage community input, the input of educators, academic officers, and peer districts to make decisions on blocking but to make those

public and establish an appeals process to accommodate changes. Further, Aukerman and Oh (2013) reported that domain-blocking solutions like OpenDNS might be insufficient and school officials have determined that blocking harmful content required significant labor and tools with many opting for ones that let district officials delegate to parents the ability to individually monitor and block content for their children.

Hartzog and Solove (2014) reported that contracts between the K-12 organization and its third parties must enforce the legal and sociotechnical constraints by which the district is bound. This can be difficult to implement given the legal overlaps identified above. Palmer (2017) also noted that the district may have had to extend its policies to student-owned devices used for academics and is required to ensure CIPA protections are still in place even if the devices are under third-party management.

Table 3

Significant K-12 Laws Pertaining to Information Security

Law Abbreviation	Full Name	Scope
FERPA	Family Education Rights and Privacy Act	Federal: FERPA was created to give families a chance to control who has access to student education records. This law states under what conditions education organizations can share information under the condition of suspension of federal funds.
COPPA	Children's Online Privacy Protection Act	Federal: COPPA was created to protect the privacy of children under 13 years old. The law requires verifiable consent from a parent and website operator responsibilities regarding records keeping, opt-out, and children's protection.

SOPIPA	Student Online Personal Information Privacy Act	California, New Hampshire: SOPIPA requires educational technology companies to delete student information at the request of the district or student, as well as provide for the security of that data.
HIPAA	Health Insurance Portability and Accountability Act	Federal: HIPAA was created to ensure the privacy of electronic health-related information. HIPAA applies to educational records in terms of nurse and psychologist data that may be stored.
CIPA	Children's Internet Protection Act	Federal: CIPA was created to protect children from pornography and harmful content by requiring schools, libraries, and other institutions that receive federal funds to employ content filtering mechanisms or risk the loss of those federal funds.

Information Security Posture

For the study, the concept of K-12 information security posture is the combination of risk tolerance, demands and constraints, and best practice adherence. Ahluwalia, Koong, and Sun (2011) introduced the construct of information security readiness. This measure builds from the observation of staff attitudes towards information security measures. The information security posture of the individual or group, the security level, and their risk level determined the readiness construct (Ahluwalia et al., 2011). The criticality of the data the employee was working with moderated information security readiness, which can then be used to gauge the potential efficacy of information security projects given the organization's acceptance of information security measures (Ahluwalia et al., 2011). Readiness then determined the ability of the organization to create and comply with a set of policies (Brown, 2016).

Ifinedo (2014) posited that the policies and practices of an organization affected overall security posture. The overall security posture is combined though with self-determination theory,

which determines just how much of those policies and practices with which individuals are willing to comply as reported by Cox (2012). Tang and Zhang (2016) concluded that there needs to be more emphasis on an organizations culture, as defined by its norms, practices, and policies, than on technical controls when attempting to create, define, and maintain an information security posture. Johnson (2017) took this a step further by suggesting that information security posture was mostly under the control of the users and their perception of the importance that organizational leadership places on those having abided by those controls. Thus organizational culture towards information security is established not only by policies and procedures but the willingness of the administration, and subsequently, the staff, to follow those stated Lacey (2010). Thus, staff perception of the importance that leadership places on supporting the policies and procedures also influenced the security posture of the organization. Figure 2 details the components of information security posture.

Figure 2. Components of information security posture

The conclusion by Pathari and Sonar (2012) was that establishing an information security posture worked when an organization created a set of security statements based on the value of the security-specific resources. Those statements then determined the strength of the technical or administrative control and the expense that each warranted. (Ekelhart et al., 2016) expanded on this concept by stating that organizations must learn to chain together controls just as an attacker would chain together exploits.

Creating an organizations information security posture occured when an organization combined the Information Security Readiness, with the established policies and procedures, and the information security controls (Brown, 2016; Pathari & Sonar, 2012). This posture can be

thought of as an organizations desire for security of a given asset, in combination with its ability to provide for, and the staff's willingness to take the actions that will ensure that security (Ekelhart et al., 2016). This posture was moderated by the willingness of senior leadership to uphold security practices and impress the expectation upon their direct reports that they were required to do so as well (Pathari & Sonar, 2012).

Each K-12 organization may have experienced a wide variety of demands for the level of information security that is expected of it based on local laws, board directives, and economic constraints. Contrasting these demands were the constraints for meeting those demands. Those constraints were economic factors such as budgets and large licensing costs when students were counted as discovered by Ji, Liu, and Mookerjee (2011). Those constraints were also the staff skills and bandwidth to effectively address and maintain security software and devices as reported by Caldwell (2013) in discussing the skills gap in information security.

Best Practices for Information Security

A key influence of how an individual K-12 organization made decisions on information security was based on the generally accepted best practices for information security. Jauregui (2015) reported that regarding information security, best practices were those that were generally applicable regardless of industry and were threat agnostic. Best practices were a minimum measure of due diligence and due care in the event of a breach and the determination of possible negligence as reported by Dorsey-Lockett (2014). Niemimaa, E. and Niemimaa, M. (2017) said that these practices were one of the principal drivers behind the formation of a security policy suite as well. Figure 3 describes the seven major components of best practices for information security.

Okoye (2017) stated that one of the most critical best practices was the backing up of systems. This practice became far more important as a protection against ransomware as reported

by Goldsborough (2017). This best practice then dictated the creation of a backup policy that created a backup and retention schedule that addressed the importance of the system, the volatility of the data, and the legal requirement for retention. Cherdantseva and Hilton (2013) highlighted that this policy then drove a procedure that described the configuration of backup systems to enforce the policy.

An essential best practice was keeping software in the enterprise up to date (Okoye, 2017). As security vulnerabilities were encountered, manufacturers must release patches so that those vulnerabilities would no longer be vulnerable to be exploited as a result of an attacker taking advantage of a poor patching practice (Okoye, 2017). By creating a patching policy that determined the mechanism by which patches will be identified and authorized, organizations could then implement a procedure that ensured that devices and software remained up to date (Okoye, 2017). Olmstead and Smith (2017) made the statement that the policy and procedure could also serve as a tool for departments to estimate staffing requirements based on the requirements for patching labor.

Jauregui (2015) reported in his work on best practices for information security that encryption was incredibly important. The criteria stated was simple: when encryption was possible, organizations needed to make use of it. As reported by Krisby (2018), encryption should be applied to all stages of the data lifecycle, both while data is at rest and while data was transmitted. Under certain privacy standards, items that could be lost or stolen such as laptops or USB drives were effectively useless if properly encrypted Kirby (2018) reported. This could avoid public notifications of a breach and costly identity theft protection monitoring. Arlitsch and Askey (2015) also pointed out that when indexing sites such as Google consider encryption

mandatory for allowing websites to be listed in its index, organizations should consider it a requirement.

Phishing protection was necessary for the modern enterprise as a security best practice as Campbell noted in 2017. Gupta, Jain, and Tewari (2016) asserted that as a best practice, organizations should be filtering email to flag or remove suspicious links, known bad senders, and other basic criteria that can aid in preventing unsuspecting users from giving out critical information. Edwards (2015) stated that phishing protections must be in combination with user security awareness training to be effective.

Olmstead and Smith (2017) stated that having protections for malware and antivirus had been a best practice since the early days of network computing. This software could act maliciously, in the case of ransomware, or it could serve as a beachhead for other more complicated and malicious software. Focusing on the educational organization, Pye (2016) stated that she felt that viruses and malware posed a more significant threat than in other environments due to the conflicts between bring-your-own-device, low IT funding, and low user security awareness.

Francois (2016) recommended that organizations have a security policy suite as a key information security best practice measure. The idea behind the policy suite is that it set a baseline expectation for the security norms of the organization. These norms established the organization's selection and implementation of controls that helped enforce those policies. Further, the policies can be used to respond to audits and records inquiries that informed the requestor what the district can and cannot supply. Good policies also needed to highlight the requirement for training staff in information security awareness (Mitnick, 2003). Mahmood, Pahnila, and Siponen (2014) warned though that compliance with those policies was not a given

and that policies must be launched with training, monitoring, and cultural initiatives to be effective.

Network defenses were stated to be rapidly evolving but indispensable best practice for information security by Tankard (2016). These defenses could be traditional firewalls, intrusion prevention devices, web application firewalls, honeypots, or any device that insulates assets by way of either obfuscating asset location or inspecting traffic and protecting or preventing malicious traffic from reaching assets (Hong & Hua, 2018). Best practice stated that such devices should exist and that policies should exist around an exception process (Okoye, 2017).

Werosh stated in 2013 that K-12 districts needed to manage third parties that had access to student data to perform service for the K-12 organization. Under FERPA, these third parties became education officials due to the nature of the work performed (1974). Contracts should have declared the third party's responsibility to protect student data as Eichensehr (2017) highlighted. When there was no exchange of funds, the use of zero dollar contracts that contain the same language also accomplished this (Werosh, 2013). These contracts created the legal

framework to ensure that liability rested on the third party, ensuring they are obliged to provide the same protections as the district must.

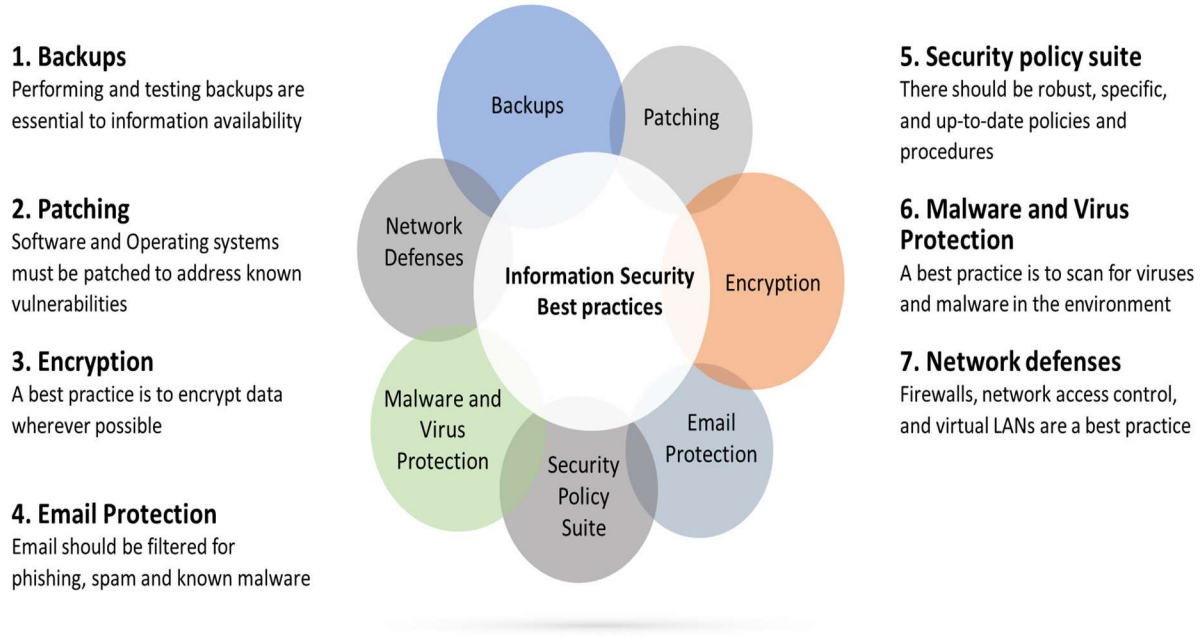

Figure 3. Best practices for information security

Stakeholder Demands

Dorata and Phillips (2013) reported that school board members were often elected volunteers with the responsibility of appointing a superintendent and guided the activity of the school district on behalf of the will of their constituents with no compensation. Adams, McBride, & Moskalski (2015) reported that while both sides worked to improve the district, board members often bend to the will of their constituents. Carruthers and Kay (2017) reported that these officials must make strategic policy decisions regarding Information Technology resources with only the resources at their disposal, usually, those found by searching online, which are often inaccurate or out of context. As a result, board directives may be difficult to implement and

only after considerable effort is expended training them on what measures are reasonable and appropriate.

Gleason and von Gillern (2018) reported that many districts recognized the need for digital citizenship and the shared responsibility around information security. As elected officials, board members may have worked to meet conflicting constituent voices as reported by Asen, Conners, Gumm, Gurke, and Solomon (2013). By working towards the demands of the board, organizations can ensure that they have met the expectations of the citizens. Armarego, Garba, Kenworthy, and Murray (2015) stated that complex and complicated security requirements might become the result, which would have been challenging to implement and maintain. These further consumed information security staff time and other resources. In the end, in the K-12 organization, it was the citizens of the community and the school board that will have had the final say.

Economic Constraints

When examining information security priorities in K-12 districts, one must have considered the economic constraints with which a district must contend (Brown, 2016). Ely and Fermanich (2013) found that student attendance counts, such as the average daily membership (ADM) of a district, determined budget amounts. ADM was a formula provided to districts to measure attendance and then be allocated a portion of the state total for schools as a result. However, Archambault, Bender, and Kennedy (2013) found that as education choice programs continued to expand, the correlation of ADM to district expenses became inaccurate. Baker et al. (2014) reported that by combining this state distribution with revenue received from federal government title programs, special local taxes, interest, bonds, and levies, a total picture of district revenue has emerged.

Of note was that the largest of districts, defined as 25,000 or more students only accounted for 287 districts out of the 13,584 in the United States, or 2.1% (De Brey, Dillow, & Snyder, 2018). The largest portion of districts, 23.7% had only 1,000 to 2,499 students (De Brey, Dillow, & Snyder, 2018). This meant that a large number of districts were too small to have sufficient IT staff to meet their needs. States such as Oregon and Washington addressed this problem through the use of Education Service Districts (ESDs) which allowed many smaller districts to centralize functions and share expensive staff that was difficult to attract and retain (Hill, 2015).

Case (2016) found that school districts spent on average 85% or more of their budgets on salaries. Further, the Council of Greater City Schools (Counsel of Greater City Schools, 2017) found that during the 2015-2016 school year, large districts spent between 1.52% and 2.96% of their annual budgets on core IT, but the definition of the department was loosely defined and rarely encompassed all technology spend. This was in stark contrast to for-profit enterprises. Derksen et al., (2013) reported that in the third year of their annual survey, 95% of organizations had increasing IT budgets as the department continued to demonstrate that was is a component of competitive advantage and cost reduction via process automation. Further, they had found that the IT budget as a percentage of total revenue had moved between 3.5 percent and 4.9% (Derksen et al., 2013). In private industry, IT investment was often a competitive advantage (Pavlou & El Sawy, 2010). Case (2016) reported that in the K-12 environment, IT investment was an indicator of innovation toward efficiency or the creation of more modern classrooms and better and more equitable educational outcomes. Thus Akeju, Aghili, and Butakov (2018) suggested that education leaders work to create changes that demonstrably increase student

learning via technology-aided research by employing student-owned devices if district provided ones were not available.

One of the strategies for improving information security in K-12 organizations was addressing the economic costs. McClain (2016) spoke of the necessity to understand how IT for a K-12 organization differs from that of normal business, in that, the conflict was not between IT and operations groups but between IT and academics. In this clash of priorities, IT leaders would take a second place role every time without having been able to convey the value proposition of information security in the context of providing education (Brown, 2016). Finding IT leadership that can succeed given this intersection was challenging, and McClain (2016) recommended a council to guide IT direction or at the very least, strong collaboration between the Chief Technology Officer and the Chief Academic Officer so that there was free and open communication of the impact of constrained economic resources.

Krueger (2013) stated that the standard Information Technology (IT) governance frameworks such as the IT Information Library (ITIL) were industry based and an attempt to implement them in a school district could provide tangible benefits. McClain (2016) countered this by when he stated that the framework results in two glaring deficiencies. The first was that the frameworks in their most basic sense were too rigid and costly to implement in education (McClain, 2016). The second was that the K-12 organization could not tune variables in its revenue stream to recover increased operating costs and complexity. Cannistraci (2011) wrote that placing technology into the hands of sixth to twelfth graders was one of the most important challenges facing schools today. There was much argument over the efficacy of such moves though. The Substitution, Augmentation, Modification, and Redefinition methodology is critiqued by Akcaoglu, Hamilton, and Rosenberg (2016) for having failed to take into account

the impact that technology distribution will have on existing staff and resources and created an unsustainable learning ecosystem. Davies and West (2014) stated that any such deployment must take into account not only how they will be used, but also the demands they placed on the environment. This proliferation of technology took organizations that had almost no attack surface in placed technology in the hands of those with minimal technology savvy and security awareness (Brown, 2016) resulting in large numbers of vulnerabilities and few methods or resources to address them.

As districts attempted to embrace technology in the classroom, Vandykgibson (2016) wrote that those in K-12 IT found that funds were being shifted to meet that need, but classroom technology was an academic purpose rather than an operational purpose. Ho and Schmidt (2013) discovered that new one-device-per-student ratios meant that many found themselves updating network infrastructure along with the device costs, and in doing so, exhausted management appetite for technology spend without improving. Thus, Tadeja (2015) wrote that the proliferation of student technology in K-12 districts might have negatively impacted the ability of IT to create or maintain security.

Madison (2017) wrote that information security itself came at a cost. Qualified staff was expensive, and because vulnerabilities and exploits evolve, staff required constant training to stay effective. Security devices and software continually evolved and keeping pace with this was costly for large districts. Brecht and Nowey (2013) found that licensing models for security devices often focused on user count rather than knowledge worker or staff member. This created large annual fees because student populations are large and were often a large portion of the annual fee (Madison, 2017).

Leachman and Mai (2014) reported that even many years on, most school districts budgets were less at the time of their report than before the economic depression of 2007 to 2009 in inflation-adjusted dollars. As districts had few mechanisms to replace this lost funding, cuts to staffing and budgets were often the result (Leachman & Mai, 2014). Casey, Dunlap, and Starrett (2014) found that a district would have placed its focus on keeping teachers in front of students, so cuts tended to be absorbed in operational departments, one of those often being IT.

Bernik (2014) discovered that both the costs of cybercrime and the money to prevent it continued to increase as did the profitability for the attacker. Brown (2016) observed that as schools transformed from a transactional, and paper-based methodology, the mechanisms for incorporating the costs of continually aging and depreciating devices were lacking. However, Zhong (2017) discovered that organizations such as the International Society for Technology in Education do not consider factors such as information security posture as being an indication of digital leadership in K-12 education. As such, the proper prioritization of information security was often out of academic reach.

Risk Tolerance

Closely related to economic constraints was the tolerance for risk an organization had. This risk tolerance was the balance between spending on information security and the risk of not doing so (Smock, 2018). This tie was so close that an organization's information security risk tolerance is the amount it is willing to spend on the twelve elements of information security maturity (Smock, 2018). This meant organizations would align investment in an element as an indication of what they had a lower tolerance for the exploitation of a weakness in that element (Rodewald, 2005). This is because the expectation is that increased expenditure results in greater maturity, and thus greater security (Ryan, J. J. & Ryan, D. J., 2006).

IATs also became aware that even heavy investment in information security does not guarantee to be free from breaches. As with many such investments, there were diminishing returns on improved security with increased spend (Anderson & Moore, 2006). Organizations were challenged to determine the appropriate level of information security expenditure to address the growing threat of compromised systems and networks.

Stakeholder Security Expectations

All stakeholders of K-12 information security had inherent expectations that such security exists and was adequate. Anderson, Baskerville, and Kaul (2017) suggested that stakeholders would often have a view and a demand on the information security of an organization that does not account for the difficulties or realities of a given breach. The stakeholder believed that breach prevention is non-negotiable, and the data they are concerned with must not be compromised (Anderson et al., 2017). These expectations often did not reflect the realities of the K-12 organization. Due to constraints on the ability to meet expectations, IATs must have aimed to strike a careful balance between disclosing vulnerabilities to solicit additional resources and compromising security further (Anderson et al., 2017; Nyachwaya, 2013).

As stakeholders, families, and students may be the ones with the most lasting damage from a potential breach. Nyachwaya (2013) stated that Sociotechnical Theory could be used to explain the expectation that security meets the demands of its stakeholders by achieving a fit between the social requirements and the technical capabilities. While this expectation was prevalent in all socio-technical systems, it became particularly relevant in the K-12 space as the privacy and security controls existed largely to protect vulnerable populations (Nyachwaya, 2013). Expectations for security to prevent compromises of student privacy and prevent waste of government funds were high (Hild, 2017; Mader & Smith, 2014). The combination of the

expectations of student and families' expectations, the state and federal Departments of Education (DoE), and the expectations of the employees and leadership of an organization set the stakeholders' expectation for information security. This expectation helped set the priorities for the school district regarding information security.

Hild stated in 2017 that parents and families believed that the protection of their private data should be one of the district's primary priorities. Hild (2017) also told us that parents and families expected that educational organizations privacy and information security protections were advancing at the same rate as private industry. Unfortunately, K-12 information technology capabilities advanced at the speed of legislation, not of industry (Hamel, Laferrière, & Searson, 2013). This juxtaposition of stakeholder expectations and K-12 information security capabilities is one of the key areas of exploration.

As stakeholders, the state and federal DoE expect that schools followed the requirements outlined in applicable federal regulations such as FERPA (United States Department of Education, 2011; Dennen, 2015), CIPA (Batch et al., 2015), COPPA (Holcomb, 2015), and state student privacy laws. In as early as 2011, the United States Department of Education (DoE) gave guidance that recommended that schools only collect social security numbers if it was deemed necessary to their operations (United States Department of Education, 2011). Being that the DoE did not require these numbers for use as identifiers in mandatory reporting, the expectation was that all schools would phase out the collection of social security numbers making districts far less attractive targets for identity thieves. Still, the pace of attacks against K-12 organizations did not lessen (Federal Bureau of Investigation, 2018).

FERPA told us that student performance data that can be tied uniquely back to an individual student must also be protected (1974). Thus, not only must name and address be

hidden from disclosed information, but also demographic identifiers that may have allowed the recipient to deduce the identity of an individual (United States Department of Education, 2011). Dennen (2015) reported the requirement for the protection of individually identifiable performance data is well documented but often misunderstood. As technology continued to become more integral to the task of delivering education, the demands on the educational organization to maintain the privacy of students continued to grow (Dennen, 2015).

Mayeh, Mishra, and Ramayah (2016) cited that K-12 organizations are businesses as well as educational institutions and had the same demands on back-end business systems as any other similarly-sized enterprise. Educational institutions had all the information assets that similar sized private enterprises had, yet are dependent on their culture in defense of these assets as detailed by Da Veiga and Eloff (2010). These organizations may have had payroll for thousands of staff and financial systems that controlled the movement of millions of dollars. Employees entrusted the district with social security numbers, and bank account information as an employee of another organization would be (Da Veiga & Eloff, 2010). Bloch, Issa, and Peterson (2015) reported that larger K-12 organization leaders were expected to produce a Comprehensive Annual Final Report (CAFR) that required leadership attestation of the accuracy of results. Thus, ensuring the information security of the environment became essential to performing that attestation and leaders demanded the integrity of their information systems to make such assertions (Bloch et al., 2015).

Staff Constraints

Hightower, Lowry, Posey, and Roberts (2014) pointed out that technical staff wanted to provide adequate protection for the resources under their care but given the economic constraints above were unable to. Rogers (1975) proposed a theory of protection motivation (PMT) based on fear appeals and attitude change. The PMT was the theoretical foundation for those responsible

for the protection of information assets in K-12 organizations as the fear rhetoric of organizational damages, but also of harm to the students, families, and staff that could result. Burns, Lowry, Posey, and Roberts (2017) reported that this conflict between the want to protect and other organizational constraints led to frustration and stress on behalf of staff members.

Hechter and Vermette (2013) observed that budgets were one of the most significant technology constraints in education. While the skill level of staff may have been perfectly adequate for the tasks required, the number of IT staffers were insufficient for the amount of work to be performed. Lancaster and Topper (2013) report that this may be related to the drive that many K-12 organizations had to achieve a higher computer to student ratio. Additionally, Allen (2008) had observed that K-12 organizations often lacked operational maturity and pushed business domain expertise for complex system usage such as use of enterprise resource planning systems into the IT department rather than developing expertise and maturity in the functional department where the skill is needed. This drive further diminished budgets, diluted the focus of IT staff, and exhausts board appetite for technology spending which meant security tasks might not get addressed as a result.

Gap Identified in the Body of Knowledge

After a review of the literature, it was apparent that research in the K-12 information security area with a focus on the practitioner lens was lacking. Research to date focused on quantitative analysis of survey instruments to assess information security readiness and capabilities of an organization (Brown, 2016; Nyachwaya, 2013). There are works in other industry spaces that focus on the strategies to be used to improve information security, but those assume a funding model that can absorb the costs of providing information security as a cost of doing business rendering cost only somewhat important (Ahmad et al., 2014). This was not consistent with the realities of a K-12 environment.

K-12 organizations, just like all organizations in the United States, needed to own the responsibility for the protection of their information from foreign adversaries as that was out of scope for the responsibility of the government (Sanger, 2018). Additionally, even domestic adversaries are not deterred by the possibility of criminal prosecution, and seemed to contradict general deterrence theory and protection motivation theory as such criminals viewed the crimes requiring greater skill and having larger impact as having the greater merit rather than the fear of more significant punishment (Aurigemma & Panko, 2012; Baskerville et al., 2013). According to Sanger, the only effective deterrence is denial (2018) thus K-12 organizations needed to understand and implement effective information security strategies to deny their adversaries access in the first place.

Boser and Levenson (2014) found that district technology funding tended to remain flat, yet Mayes, Natividad, and Spector (2015) found that more was being asked of K-12 IT staff regarding classroom technology and security protections, while there was less staff actually to perform the work. This indicates a need for an understanding of strategies to prevent unnecessary expenditures of constrained resources. In preserving those constrained resources, IAT's in K-12 need to understand the strategies that are successfully employed in other industries as those strategies, with some exceptions, could then be applied to K-12 (Kovács et al., 2017). This will allow IAT's in K-12 to apply resources towards creating similar strategies in their organizations. Further, Mattord and Whitman (2011) reported that such strategies could set expectations for information security in a cost-benefit format.

Research thus far has overlooked the opportunity to understand the perspective of those IATs responsible for information security, satisfying stakeholders, and complying with regulations in K-12 organizations. This research will focus on learning what the strategies are

that those practitioners can leverage by exploring information security strategies in other organizations and applying lessons from these counterparts in other industries (Anderson & Choobineh, 2008). This study is a valuable contribution to the body of knowledge for K-12 administration and governance because it addresses opportunities for further study indicated by Nyachwaya (2013). Additionally, the study advances knowledge of Doctors of Science who focus in Information Assurance, by studying a broad collection of industries and proving the applicability of findings to a single industry where strategies are lacking. Further, researchers will be better able to understand better how critical security needs are addressed and what combination of addressing organizational constraints and addressing stakeholder demands will result in information security being improved.

There is a contribution to the body of knowledge for information security as the gap presents an opportunity to understand how information security is addressed in the face of and absence of regulation or profit-motive. Additionally, there is a contribution to the body of knowledge for sociotechnical systems in understanding how an IAT, when faced with more demands than resources, leverages strategies to address those demands, and what risks are accepted. This may lead to better systems of governance, more effective school board engagement, funding models more properly aligned to the organizational priorities, and possibly even better, industry-specific legislation.

Methods

Myers and Newman (2007) stated that qualitative interviews are a powerful research tool for information systems research. This power stemmed largely from granting the researcher the insight of the individual rather than a set of descriptive statistics about a result set as reported by Edmondson and McManus (2007) who elaborate that nascent fields of study lend themselves to qualitative, exploratory methods. Albrechtsen and Hovden (2009) went past simple information

systems and applied Myers and Newman's guidance to information security research. Given the valuable insight gained in these studies, the methodology used was the qualitative interview.

Ten information assurance practitioners who are members of the GIAC advisory board listserv ("GIAC Advisory Board", n.d.) or identified as a CISO on LinkedIn.com were interviewed to understand their organization's information security strategies. The interview will also seek to understand the subjects view regarding what information security obligations have been completed and are meeting expectations. The interviews will ask what strategies that those who are engaged in information assurance roles employ in their organizations to improve information security. Mason (2002) wrote that using these interviews is a reliable way to infer applicability to other domains after employing transferability verification. By using interviews with IATs, understanding the needed strategies to improve information security in a school district should become apparent.

Conceptual Framework

The illustration of the conceptual framework for the strategies for improving information security in K-12 school districts is in Figure 4 below. Morrow (2005) stated that the conceptual framework is a useful guide for the study that can demonstrate to the researcher and the reader the path that will be followed through the literature. Jabareen (2009) stated that this network of linked topics charts the path of discovery for the researcher.

Mattord and Whitman (2011) recommended that the conceptual framework for the study detail the stakeholders that have expectations of and are affected by the information security demands of the K-12 organization. Additionally, the framework accounts for the forces affecting information security decisions within the K-12 organization. Those forces are moderated by organizational obligations and constraints (Ahluwalia et al., 2011). Where forces and constraints intersect, there are the strategies needed to improve information security in a school district.

The first significant element of the scope of the dissertation was the information security posture. A significant force was the economic factors, both regarding the school district budget and the cost of the technical controls in question, as stated by Holland (2016). The economic factor is so significant that some authors defined information security posture as risk tolerance, is the amount the organization spends on addressing the twelve components of information security maturity (Smock, 2018).

In continuing to examine security posture beyond the economic components, Smedinghoff (2005) reported that one of the forces contributing to posture was the current laws both at the federal and state level. Another force, as reported by Wynn (2017) was the organizational security posture, including the cultures readiness for security, staffing skills and willingness to comply with preexisting policies and controls, and risk tolerance. Another element of scope was the best practices for information security (Jauregui, 2015). Basic best practices, such as the need for information security awareness training, may meet resistance in the K-12 environment as reported by Michael (1998). A very significant constraint was the economic one where a district could only afford some of the information security solutions it desired (Brown, 2016).

The organizational security maturity overlapped with the information security posture. These measures included legal obligations such as HIPAA versus FERPA (Strauss, 2016) that require the district to make decisions on where on the spectrum of risk its decision-making can fall. Security maturity was also constrained by staffing levels and staff skills both of which may be insufficient to address the level of security desired. This combines with the willingness of the organization to invest in security improvement (Smock, 2018).

Where the forces affecting information security maturity and the organizational security posture overlap, are the strategies for improving K-12 information security. Behara and Huang (2013) reported IATs made decisions based on best practices, staff levels and skills, budgets, legal compliance, and stakeholder expectations (Ji et al., 2011). Ahmad, Chang, Lim, and Maynard (2010) stated that inevitably, there was a requirement for more information security demands and obligations than the IT department could provide with a limited budget.

By examining information security maturity and the organizational security posture along with stakeholder expectations (Mattord & Whitman, 2011), the study will provide a comprehensive understanding of the strategies necessary for IATs to improve information security in K-12 districts. By understanding these factors, the hope is that the strategies necessary to implement and maintain due diligence information security controls can be understood, communicated and conveyed by IATs to district administrators for assistance in implementing those strategies. Additionally, the hope is to demonstrate the need for future privacy and security legislation to ensure these strategies are implemented (Brown, 2016). This will allow individual states to address persistent gaps in the information technologists ability to perform necessary due diligence.

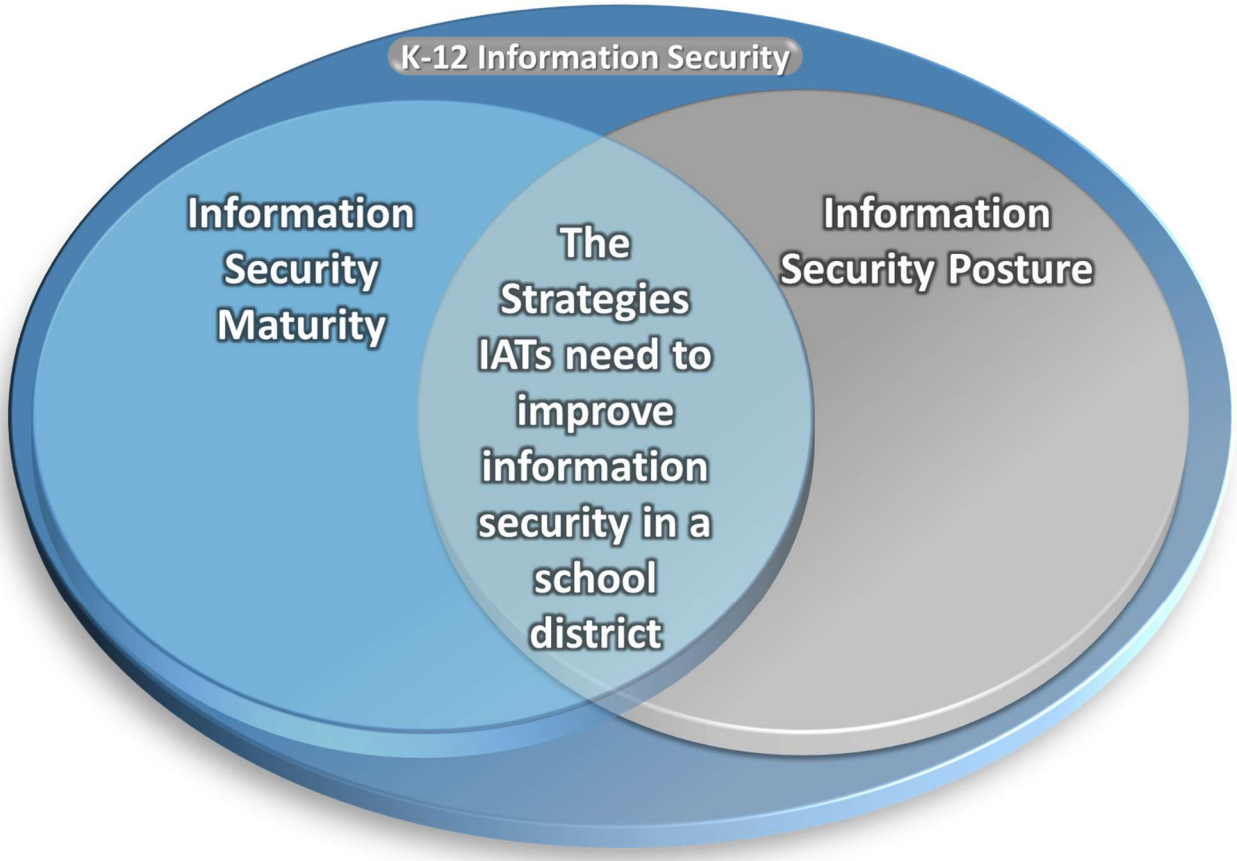

Figure 4. The conceptual framework for the strategies needed by IATs for improving information security in a school district

Summary of Literature Review

This chapter examined literature that describes the forces that affect K-12 information security demands, organizational obligations and constraints for security, and the resulting strategies necessary for the improvement of information security in a school district. Considering the forces affecting information security demands by reviewing the literature about regulations such as FERPA (1974), COPPA (Hild, 2017), and CIPA (Batch et al., 2015), the readiness of the organization for information security, and the requirements of stakeholders both internal and external, a greater understanding can be had of what is expected of the K-12 organization IATs.

By reviewing past works detailing best practices for information security, knowledge of the expectations for rational and reasonable precautions as they pertain to information security become understood. As a result of the review of the literature surrounding organizational obligations and constraints, the impacts of intersecting and overlapping laws are understood as well as the impact of economic constraints and the demand to invest funds where student impact is most significant.

This review has identified a gap in the literature. While much is known about the state of information security in K-12 organizations (Nyachwaya, 2013; Brown, 2016), a gap exists in documenting how IATs, faced with insufficient resources to meet demands, could inform leadership about the requirements for strategies that will improve information security. This gap will document what IATs need in the absence of strict laws and in an industry that often eschewed commercial concepts like best practice (McClain, 2016). The result of this work could include new regulation of compliance frameworks that oblige districts to comply or face penalties, not the least of which is negative media attention.

In the following chapter, the study will be discussed. Information detailing the justification for the use of a phenomenological study methodology and the qualitative interview methods will be detailed. An in-depth examination of the method to select the subjects and analyze the data will be also be presented. Finally, the research design will be discussed and how the research was conducted in a way that is ethically sound while preserving trustworthiness of the discoveries will be presented.

CHAPTER THREE

The problem the study examined was that since the proliferation of student information systems, information security best practices have not been followed in K-12 education because the strategies IATs need to improve information security practices in a school district have not been established (Brown, 2016; Nyachwaya, 2013). Functions such as attendance, academic progress tracking for students and payroll, and human resources systems had become core to how a district does business (Ely & Fermanich, 2013). IATs in school districts have not been able to maintain the expected level of information security because the strategies to improve information security in a school district have not been established as they have in other industries (Nyachwaya, 2013). The purpose of the qualitative exploratory study was to explore the strategies IATs need to be able to improve information security in a school district. The information in Chapter 3 will build upon the selected qualitative research tradition and explain its choice for discovering information that does not already exist in the literature. Chapter 3 will also tell how qualitative exploratory research was used and describe the population and the sample for the research. Also, in Chapter 3 is information on the sampling procedure and the instrumentation that was used. Chapter 3 continues with a description of how information for the study was analyzed and synthesized. Chapter 3 concludes with discussions on instrumentation and validity will conclude the chapter which will discuss the protocol and instrument used with subjects for the acquisition of data for the study.

Research Tradition

A methodology is used in research to ensure the quality of the results of a research effort and determine if the results will integrate with the results of other initiatives (Lee & Markus, 1999). Information security researchers may seek to understand elements that are highly technical but can also be very relevant to the human aspect of those technical issues (Niekerk &

Solms, 2010). Given this, information security has many methodologies that may fit. For the study of the human aspects of information systems, Myers (1997) suggests the use of the qualitative methodology.

The qualitative exploratory approach was used for the study. Qualitative studies in information systems could be used for investigating the actions and choices of subjects in a particular situation, given sociotechnical and political constraints (Kaplan & Maxwell, 2005). Qualitative explorations seek to understand the human aspects of phenomena (Seale, 1998). Some of these explorations use research techniques in which the researcher becomes the instrument, but must also maintain neutrality, as Poggenpoel and Myburgh (2003) reported.

The qualitative methodology was appropriate for the study because of how nascent the area of research into K-12 information security strategies is, as well as granting the opportunity to understand the phenomena in an organizational setting (Kaplan & Maxwell, 2005). The quantitative methodology was not be used for the study because the quantitative approach relies upon structured surveys and statistical analysis of responses, as Parylo (2012) wrote. The mixed methods methodology was not be used for the study because it combines the statistical analyses of a quantitative approach with the features of the qualitative approach (Parylo, 2012) which was not appropriate for the study.

A research design was used to integrate the components of the study, ensuring that the researcher addressed the research problem in a way that was adequate (Denzin & Lincoln, 2011). This design becomes the template the researcher will use across multiple subjects to ensure that a consistent set of questions is asked of the subjects - this template aided in establishing the validity of the study because each subject is given a similar treatment. The design, as Maxwell

(2012) suggests, is not a standalone, one-time process, but rather an iterative one that is revisited and refined through the proposal process.

Based on the selection of the qualitative methodology, an exploratory design approach was used as it is intended for problems that have not been studied thoroughly. Qualitative exploratory designs are used when the research is intended to discover new information and leave room for further research (Sandhursen, 2000). The exploration of a qualitative phenomenon may require less mathematical rigor than statistical methods require, yet allowing a rigorous study of phenomena that largely defy mathematical descriptions (Singh, 2015).

An exploratory qualitative approach is appropriate for the study because it focused on subjects lived experiences which will allow the discovery of common themes amongst the subjects that can then be correlated into a list of strategies (Denzin & Lincoln, 2011). The researcher considered three design options: ethnography, case study, and phenomenology. The case study design was not used for the study because the case study aims to create a detailed analysis of an occurrence or individuals. The ethnography design was not used in the study because ethnography focuses on groups of people that share a similar culture, language, or behaviors, and would not lend itself to answering the research question. The exploratory design was used in the study because it is used to explore the questions under study and create room for further study (Singh, 2015).

Research Question

The research question is the guiding question to be addressed in a study and that the study must support addressing this question (Law, 2004). As such, establishing the research question is the first step in any study (Law, 2004). This research question guides the researcher in the acquisition of supporting literature as well as the collection of data from subjects for later analysis (Mason, 2002).

The study was concerned with the strategies that can be used by IATs to improve information security practices in a school district. The study explored what strategies are being used by IATs in other fields that can then be applied to information security programs in K-12 education. The research question to be addressed is: What are the strategies that IATs can use to improve information security within a school district?

Research Design

A research design is used to integrate the components of the study, ensuring that the researcher will address the research problem in a way that is adequate (Denzin & Lincoln, 2011). This design becomes the template the researcher will use across multiple subjects to ensure a consistent set of questions is asked of the subjects - this template aids in establishing the validity of the study because each subject is given a similar treatment. The exploratory phenomenological research design is most appropriate because it seeks to describe the lived experience of the participants (Lewis, 2015).

Population and Sample

The population in a research study is defined by Henry (1990) as all of the elements or units that meet a given definition, which is the larger group that the researcher wishes to study. These experts were solicited from the Global Information Assurance Certification (GIAC) Advisory Board, a collection of individuals who have scored 90% or higher when attempting to pass SANS certified information security professional exams ("GIAC Advisory Board", n.d.) or as CISO on LinkedIn.com. The estimated size of the population is 14,000. This population is appropriate because Borg, Gall, and Gall (2007) created the idea of the accessible population, which is made up of the individuals that could be reasonably included in a sample.

A sample is a subset of the population (Guest et al., 2005). The sample size is used to allow the researcher to make reasonable inferences about the entire population as interviewing

all members of populations is often not feasible or necessary (Mason, 2010). Further, sample sizes researched indicate sample sizes for phenomenology made use of samples of as few as seven and as many as eighty-nine (Mason, 2010). Researchers highlighted a critical lack of justification for sample sizes in information systems research and suggested that saturation was reached with a sample of 30 (Cardon et al., 2013). Concerning the nature of the instrument, the study sought a sample size of 10. The sample size is appropriate because Lucas (2018) and Jackson (2017) conducted similar qualitative, explorative studies in which both used samples of 10 subject matter experts, reporting that subject matter expertise increased the amount of information available to the researcher and thus reduced the need for a larger sample size.

Sampling Procedure

A sampling procedure is used to restrict the researcher to study the group size necessary to elicit useful results (Guest et al., 2005). For the study, purposive sampling was used to identify the sample out of the population. The goal of the sample size in purposive sampling is to reach saturation or the point at which the answers are similar, and no new data is gathered from additional interviews (Mason, 2010). Purposive sampling allows the researcher to select a sample size based on the resources available and determined by the size required to achieve saturation (Guest et al., 2005). Purposive sampling is appropriate for the study because of the resource constraints in terms of time, because saturation can be achieved by thirty, fewer subjects can be used with higher subject matter expertise, and data review and analysis was performed following data collection (Cardon et al., 2013; Grover, Jette, & Keck, 2003; Guest et al., 2005).

Before participants are chosen, a letter was sent to GIAC.org asking for permission to make use of their distribution list to solicit participants as these site letters are vital in ensuring ethical standards (Sales & Folkman, 2000). Data collection, in the form of recorded WebEx interviews, will identify the subjects via a pseudonym allowing anonymity in all places except

the file where that number is associated directly with the subjects name (Ramos, 1989). Between the use of identifiers and the fact that the data collected is the property of the researcher only, and only used for the study, subject confidentiality is achieved (Dogra, Giordano, O'Reilly, & Taylor, 2007). Finally, Braunschweiger and Goodman (2007) tell us that all participants must have the right to withdraw from the study at any time for any reason.

After the permission to use the site is received via letter, and following the approval from the institutional review board (IRB), participants were solicited from the GIAC Advisory Board mailing list and a LinkedIn.com search of persons matching the string CISO. Those responding were selected based on being an information assurance leader in an organization with an information security practice at least 3 years old, that have successfully performed in their roles for a minimum of 2 years at organizations with a total staff size of 500 employees or higher that are not in a K-12 educational field, in the United States. The first set of criteria will ensure that staff work for an information security program that has had a chance to become established, with leaders that have gone through at least one budget cycle. The organizational size restrictions ensure that the company is large enough to have dedicated IT staff. The restriction on the United States ensures that the organizations are obligated to follow the same set of laws as the target population.

Qualified potential subjects were contacted by email requesting a sixty-minute time slot for a WebEx video interview. The informed consent will request the permission of the subjects to record video. The consent included the name of the researcher and the sponsoring institution, the purpose the study aimed to achieve, the benefits of the study for the participant, clear indication of the level and type of involvement in the study by the participant, a reminder that the participant can withdraw at any time, and finally, contact information for the researcher

(Sarantakos, 2012). When the interview time is set, an informed consent form (see Appendix A) was sent, and the interview will not proceed without having received it signed by the participant as well as keeping a copy for themselves (Corti, Backhouse, & Day, 2000).

Instrumentation

In qualitative studies, the researcher is an implicit part of the research as stated by Chenail (2011) and must take care to collect data that is free from bias to acquire valid data that can be verified as reliable. Qualitative researchers must take great care not to influence those who are being interviewed (Guba & Lincoln, 1986). Hence, the qualitative researchers make use of open-ended questions so that subjects may gather the experiences of the subjects without inserting bias.

During the data collection process, a WebEx video recording was used to capture data from the remote interviews as a parallel product to Skype per the suggestion of Brown, Lo Iacono, and Symonds (2016). The data collection will entail conducting an interview that includes thirteen questions and probing questions (see Appendix C). Based on the number of questions, the interview is expected to take sixty minutes. Participants were sent the list of questions ahead of time so that any data gathering necessary on the subject's part can be completed.

The WebEx video meeting recording feature was the primary data collection tool of the interview. A timer will also be used in addition to a field notebook so that the researcher can make notes based on time in the interview when any statements of interest as well as the time in the interview during which it may occur (Whiting, 2008). This field notebook was used to highlight specific answers as well as capture non-verbal cues.

Semi-structured, open-ended questions were used to prompt each subject on their experiences on the information security strategy elements. This interview is the best tool to

examine phenomena without influencing it (Brinkmann, 2014). The use of the probing questions is used to gain additional insight from the interviewee's experiences (Whiting, 2008). There were one or more probing questions for each interview question in the study.

The researcher collected handwritten notes in a field journal. These notes will detail the body language of the participant and the tone of voice during the interview. Additionally, ambient noise and conversations were noted. Also notable is non-verbal cues such as the subject checking a cell phone or watch as well as sighs, pauses, smiles, laughs, and others that would indicate a feeling experienced by the subject that was not apparent in a transcription of the response.

Protections were taken to ensure that the video recordings of the interviews are accessible only to the researcher and only for the requisite time before being destroyed. Labeling the information from the subjects was used to highlight essential topics or terms for analysis (Casey, Houghton, Murphy, & Shaw, 2013). Labels could be useful as an approach to credibility as they can be used with peers to see if they would use the same labels given the research (Graneheim & Lundman, 2004). The researcher will aim to evaluate each interview separately for appropriate labels and justify the path taken to arrive at each label.

The process for ensuring that participants are not harmed includes delivery of informed consent and ensuring that participants are aware they could leave the study at any time. Additionally, if it is determined that company consent is also needed by the IRB, this consent was acquired as well. Finally, the records of the interviews and all interactions are being kept in private folders on Google Drive that only the researcher can access.

Validity

Validity is the measure of the degree that the research makes use of methods and procedures that ensure a high degree of research quality and rigor (Borg et al., 2007). Validity is

vital for a qualitative study because it demonstrates that the researcher has performed the diligence of demonstrating the rigor of the study in the absence of overarching scientific rules that would declare such validity (Whittemore, Chase, & Mandle, 2001). Internal validity focuses on the design and methodology of the study and aims to prove it is free from error and eliminate other possible explanations for the findings (Leung, 2015). Internal validity was established by using purposive sampling, which is appropriate for qualitative exploratory studies (Leech & Onwuegbuzie, 2007; Leung, 2015). Validity will also be determined through the use of triangulation, member checking, the use of rich and thick descriptive language for describing participant interactions, being detailed and forthright regarding researcher bias, and detailing outlier information (Creswell, 2009).

Dependability is the ability of the researcher's results to be repeatable and consistent (Guba & Lincoln, 1986). Dependability is essential for a qualitative study because the reality in a social setting is that the conditions are continually changing. For the study, dependability was addressed by doing data triangulation (Leech & Onwuegbuzie, 2007). Specifically, by verifying individual viewpoints against others (Shenton, 2004). Participants will only have a few options for valid thematic answers for the majority of the questions in the instrument. By verifying that the subject answers fit into these themes, triangulation is achieved.

Credibility is also referred to as internal validity and is related to the believability of the results to a participant of the research (Guba & Lincoln, 1986). Credibility is essential for a qualitative study because the participants are the only ones that can reliably understand the phenomena (Cutcliffe & McKenna, 1999). For the study, credibility was addressed by doing member checking by consulting with the survey participants on the validity of the conclusions (Birt, Cavers, Campbell, Scott, & Walter, 2016).

Transferability is the ability of the research to be generalized or transferred to other contexts (Guba & Lincoln, 1986). Transferability is vital for a qualitative study because it adds the ability for other researchers to apply the study observations to future work (Morrow, 2005). For the study, transferability was addressed by doing performing a thick description of the research context such as the social and cultural contexts that are present during data collection that provides a full understanding of the research setting (Guba & Lincoln, 1986).

Confirmability is the property achieved after credibility, transferability, and dependability are established (Guba & Lincoln, 1986). Confirmability is essential for a qualitative study because it confirms the decisions and interpretations of the study (Moules, Norris, Nowell, & White, 2017). For the study, confirmability was addressed by maintaining detailed notes regarding the development of themes creating an audit trail (Moules et al., 2017).

Reliability

Reliability relates to the ability of a measuring instrument to deliver consistent results across different researchers and studies (Gibbs, 2008). Reliability refers to the extent of the consistency of the researcher's instrument so that others may arrive at similar conclusions proving accuracy and repeatability. However, since the researcher is the instrument, external forms of verification may be needed to ensure reliability (Guba & Lincoln, 1986).

Reliability is the consistency that a researcher's instrument will make the same measurement (Guba & Lincoln, 1986). Triangulation improves the reliability of collected data by attempting to reach the same conclusion by different modes or using different researchers (Moules et al., 2017). The reliability of the collected data obtained by asking open-ended questions increases by making use of triangulation by using data from different sources to construct a robust justification for identified themes (Creswell, 1996).

Conducting member checking enhances the reliability and validity of the data collection process (Moules et al., 2017). After reviewing the interview data, interviewees were sent a draft of the strategies identified via the initial interviews to ensure that they agree with the themes and subthemes identified. Researchers use member checking to validate study findings through the eyes of those who experience the phenomena (Birt et al., 2016). Member checking can be used as a basis to establish a more collaborative and ethical approach to establishing consistency (Harvey, 2015). The transcribed interview was reviewed, as well as the level one coding results using previous research as a guide (Guba & Lincoln, 1986). An email was sent ahead of a phone call during which the subject was asked to confirm that they agree with the transcription for the answers for each of the questions that were asked as well as the themes identified.

Using triangulation contributes to reliability by allowing researchers to acquire more than one proof (Flick, 2004). Through triangulation, the researcher will identify categories and themes using multiple resources in an attempt to confirm those identified via the research - this process aids in interpreting the data and establishing the reliability of the results (Golafshani, 2003). Triangulation is a data analysis technique used in qualitative case studies to confirm the reliability of the observations of the researcher (Golafshani, 2003). Triangulation is the process of using multiple sources of data as a check to ensure that the researcher has arrived at results that can be considered reliable (Flick, 2004). For the study, data triangulation was accomplished by examining frameworks such as the NIST 800-53 revision 4 (NIST800-53r4, 2013), HIPAA (Strauss, 2016) Sarbanes-Oxley (Sarbanes, 2002) to confirm that the strategies suggested by those IATs in non-education industries to confirm the strategies that each of these legal mandates provides IATs in other industries (Golafshani, 2003).

A pilot study was conducted by identifying two subjects (Julious, 2005). This pilot study was used with the intent of refining data collection methods and strategies (Barrett, Mayan, Morse, Olson, & Spiers, 2002). By performing this pilot study, barriers to recruitment can be discovered and mitigated as well as refinements can be made of the data collection methods, thus aiding in establishing reliability (Barrett et al., 2002). The pilot study was conducted in a way that looks identical to the research study by contacting participants using WebEx with video, asking the thirteen questions (Appendix C), and then later performing member checking to verify the results.

Data Collection

Yin (2015) stated that the research question is drives the data collection process that was needed to acquire the data required for the study. The research question is: What are the strategies needed by IATs need to improve information security in school districts? The data collection method chosen to acquire data for the study is the semi-structured interviews. According to Huberman and Miles (1994), the semi-structured interview will provide reliable data from subject matter experts with first-hand knowledge of the phenomena under study as well as observations of the environment and other unspoken observations. Semi-structured interviews encourage participants to relate their lived experiences regarding the phenomena under study and prompt subjects to elaborate, giving the researcher details about their experience (Yin, 2015).

An email was used to communicate with the GIAC Advisory board to solicit participants. Additionally, messages were sent to members of linkedin.com that have the title of CISO. Participants will reply individually, signaling their willingness to participate and coordinate their availability for a WebEx interview. Volunteer eligibility will also be determined via this email. After vetting, email communication was used until the WebEx with video interview.

Ten participants from the GIAC Advisory Board or LinkedIn.com that match the criteria were interviewed. Two participants were used to pilot-test the interview and an additional ten for the actual interview itself. The interview protocol is outlined in Appendix D. All participants were asked thirteen open-ended questions regarding the strategies employed to implement or advocate for information security in their organizations during the semi-structured interviews. The plan is to conduct the interviews via WebEx using video at a time convenient for the subject. The exact time for each interview was determined following the eligibility survey.

The semi-structured interview will include the following general steps as suggested by Austin and Sutton (2015), and Yin (2015): (a) establish rapport with each participant; (b) introduce the study, speak of its purpose, define vernacular used in the study, and describe the study constraints; (c) review the signed consent agreement form to be used that each participant should have returned to the researcher before the interview time; (d) make use of the interview protocol (see Appendix C) ensuring that all questions are asked in the intended format; (e) engage probing techniques such as the silent probe, overt encouragement, requests for elaboration, requests for clarification, and verbal reflection; (f) thank the participant for their time and effort; (g) confirm the participant will be available to verify the transcript of the study.

Interviews were recorded using WebEx with video. A personal journal was used during the interview to capture non-verbal communication such as sighs, eye-rolls, and pauses that may be significant but unspoken, as suggested by Ryan, Coughlan, and Cronin (2009). The journal will also detail the setting such and the subject dress and background, including attentiveness, to create a think description of the subject interview environment (Guba & Lincoln, 1986). This data was assimilated to create a complete picture of the subject and their environment (Guba & Lincoln, 1986).

Following the completion of the interviews, the recorded information was transcribed into Microsoft Word using the Webex playback process. This playback was converted into an audio file and uploaded to NVivo for transcription. Next, the transcribed file was carefully checked against the playback to ensure proper interpretation of the words of the participants as well as allow for the addition of other non-verbal information. This process will involve a careful, verbatim recording of the entire conversation, as recommended by Davidson (2009) to ensure quality and trustworthiness. The transcriptions were passed back to the subjects as a part of member checking (Birt et al., 2016; Harvey, 2015).

The collected data to be stored includes the WebEx recordings of the interviews, all email correspondence, the cross-reference file of subject numbers to identifying information (Flick, 2004), and the field journal which will contain notes of the non-verbal aspects of the interviews, the transcripts of those interviews as well as the subsequent coding that takes place. These data sources will be stored for five years on Google Drive in an account created specifically for the study. For the sake of security, any collaboration involving this data will involve a short-term share of the file with the recipient. Zhou (2014) stated that the use of sharing in a Google account would prevent re-sharing of information if properly configured. Additionally, information that cross-references subjects to unique identifiers will not be kept.

In summary, data collection will take place using recorded WebEx interviews. Those interviews were transcribed into Microsoft Word along with any non-verbal information. The transcriptions and other collected notes will then be entered into Nvivo that for identification of coding opportunities and thematic elements as suggested by Alabri and Hilal (2013). The data is stored in Google Drive with access restricted to ensure that only the researcher will have access to it outside of times that collaboration is necessary.

Data Analysis

An exploratory quantitative methodology was chosen for the study because the focus of the research is to categorize and code to identify and interpret themes (Berg & Lune, 2004). Qualitative data analysis methods allow for the discovery of conceptual themes and relationships (Suter, 2011). The conceptual analysis starts with the emergence of themes from the data (Suter, 2011). The analysis of relational or content data looks to construct semantic relationships using units of themes (Bell & Bryman, 2015). Thematic units are collections of similar themes identified from the qualitative data that can be aggregated to a high-level. The data analysis process involved identifying themes from transcripts, the researcher's field journal, and other sources of qualitative data (Thomas & Harden, 2008).

The analysis of qualitative data follows a five-step approach, as outlined by Dey (2003). The first step is the organization of the data, followed by a review of the data, classification, and synthesis. In exploratory analysis, analysis includes (a) aggregating the data from interviews, (b) organizing the data by participant, (c) coding the data in level one coding using ten priori codes from the literature review (Yin, 2011), (d) level two coding identified by Saldana (2011) as axial coding, major themes from the previous step are identified, and (e) where level three coding or theoretical coding (i.e. combining or separating of the identified groups and subgroups to establish data relationships) (Saldana, 2011). The final step may be iterative. After this process, the resulting themed categories are the findings of the study.

The coding rules that were used to map textual units into data terms that include during open coding are (a) laws, (b) economic constraints, (c) security posture, (d) user security awareness, (e) expectations from customers, (f) capabilities of the technology staff, (g) expectations of stakeholders, (h) government oversight, (i) fines, and (j) security posture. These phase one coding rules were used to derive the initial categorization of data that were used in the

subsequent phases of data analysis (Priest, Roberts, & Woods, 2002). This process will then add additional categories until all data elements are captured.

In phase two coding, called axial coding, similar categories from the first phase are joined together to create themes (Priest et al., 2002). Axial coding is the process of collecting the labels from within each interview question and grouping similar ones into a single label (Priest et al., 2002; Yin, 2011). These themes prepare the researcher for the third phase of coding.

In the third phase, or selective coding, groups of themes are collected across interview questions (Priest et al., 2002). The process is to select one or two categories to which all other categories are related. The results of this step, even though iterative, are the outcome of the study (Priest et al., 2002; Yin, 2011). The third phase identified the high-level strategies that IATs can use to improve information security in school districts.

Nvivo is the tool that was used to conduct data analysis in the study. The Nvivo suite of tools provides the ability to perform the stages of data analysis within the tool. Additionally, Nvivo provides the ability to perform analysis that may be more difficult if performed manually, such as the counting of instances of a word or phrase, and the identification of themes within the data surrounding different subjects. The addition of visual presentation tools will also save labor in producing such presentations for the study.

Ethical Considerations

The ethical principles that were applied during the study include that of informed consent (see Appendix A), having a safe interview environment, and explain to each subject that they have the right to terminate the interview at any time for any reason as Braunschweiger and Goodman (2007) stated is a necessity. The informed consent was provided to the subject at the time the interview appointment was set, and cannot proceed until it has been received signed in return.

The ethical principles contained in the Belmont Report protocol are focused on the ethical protection of human subjects (Sims, 2010). The report states that vulnerable populations must be protected and efforts to seek consent must be made so that subjects are not exploited (Braunschweiger & Goodman, 2007). Autonomy, benefice, and justice are principles contained in the *Belmont Report* and must be followed as part of the protocol for the protection of human subjects (Sims, 2010).

The study ensured that no harm comes to its participants due to participation in the study (O'Neill, 2003). As a part of protecting subjects, researcher subjects must be informed of the risks and benefits via the informed consent form (see Appendix A). This form (a) describes the purpose of the study, (b) the involvement required of participants, (c) the procedures for participation, (d) the potential benefits of the research, (e) the potential risks to the subject, (f) any compensation, (g) the subjects right to confidentiality, (h) the fact that participation is voluntary, (i) that the subject may withdraw from the study at any time and for any reason (Corti et al., 2000).

Biases could occur due to preexisting interest, knowledge, or interest in the topic of the study (Noble & Smith, 2015). Potential bias was mitigated through the use of an interview process that makes use of open-ended questions that do not lead the subject. This interview process will focus on the response of the subjects, use of a field notebook for non-verbal observations, performing triangulation and member checking to ensure that the findings of the researcher match the experiences of the participants (Noble & Smith, 2015).

Summary of Chapter Three

The research design of the study was an exploratory qualitative design which provides insight as to the subjects lived experiences regarding the strategies to improve information security in their respective organizations (Lewis, 2015). This approach is appropriate for the

study as the study of information security in school districts is nascent. Further, this will provide insight from those subjects who have implemented or leveraged these strategies to improve information security.

Data were collected from 10 participants who are members of a GIAC.org email listserv or LinkedIn.com CISOs. The participants on the listserv are restricted to those information security professionals who have obtained a score of 90% or higher on one of the GIAC information security certification exams or are designated security leaders of their organizations. This purposive sampling will allow the research to narrow the selection criteria further by seeking out those who are responsible for information security in their organization, who have successfully performed their roles for three years. Semi-structured interview questions were used to allow the researcher to inquire without leading the subject.

The analysis of data will follow an approach given by Dey (2003), Saldana (2011), and Yin (2011). The analysis will transcribe the interviews and rich descriptions of the non-verbal elements to arrive at coding and themes that were the findings of the study. These themes will be aggregated and presented in Chapter 4.

CHAPTER FOUR

The purpose of the qualitative exploratory study was to explore the strategies that IATs need to be able to improve information security in a school district. Accomplishing this is done via semi-structured qualitative interviews with information security subject matter experts in fields other than education to learn the strategies they use. By learning these, K-12 IATs can then aim to implement such strategies in their organizations or begin advocacy for those strategies to be made available to them.

Chapter 4 will begin with an overview of the demographics of the participants of the study. The chapter will continue with a presentation of the data collected from the ten subject matter expert subjects. Chapter 4 then moves into the presentation and discussion of the findings from the study. The chapter will then conclude with a summary.

Participant Demographics

Ten subjects participated in the study providing answers to the thirteen questions of the interview protocol. These subjects were identified as subject matter experts in information security and as security leaders for their respective organizations. The pilot study engaged two additional security leaders who aided in the adjustment of the interview questions so that the flow of the interview made more sense and questions did not ask information that participants would often volunteer in previous answers. The questions (Appendix B) were altered to reflect the input received from these security leaders. The final version of the questions are listed in Appendix C. The pilot study participants were both males, with one in the field of healthcare and one in the field of higher education.

The selection criteria for the participants of the study included that each respondent was (a) a member of the GIAC advisory board or a CISO on LinkedIn.com and that (b) the subject is

employed at an organization with greater than 500 employees and has been so for at least one budget cycle, and (c) are not in the industries of K-12 education of national security. A total of 10 SME's were selected to participate in the study from across the United States, and all were male participants. The research participants are designated by the identifiers P1 through P10 in the study. Six of the subjects (60%) are identified by the role of Chief Information Security Officer (CISO), with two (20%) having a role of Vice President (VP) or higher, one (10%) had the role of Information Security Manager, and one (10%) had the role of Information Security Officer (ISO). The determination of security team coverage is by the number of dedicated security staff, divided by the total number of IT staff. Four subjects (40%) led teams with 1-2% coverage, three subjects (30%) led teams with 3-4% coverage, one (10%) had 9% coverage, and two (20%) had 15% or higher coverage.

All of the subjects met the criteria for participation in the study with each participant meeting or exceeding the number of years required to be at their current employer. Four of the subjects (40%) had been with their organizations for 2 years or less, two subjects (20%) had been with their organizations for three years, three subjects (30%) had been with their organization four years, and one subject (10%) had been with their organization for seven years.

Table 4.

Research Participants, Industry, Gender, Years at Organization, and Coverage

Participant	Industry	Gender	Years at Organization	Security Team Coverage
P1	Government	Male	4	4%
P2	Healthcare	Male	3	1%
P3	Manufacturing	Male	2	4%
P4	Government	Male	4	2%
P5	Retail	Male	3	2%
P6	Technology	Male	4	2%
P7	Healthcare/Higher Ed	Male	2	9%

P8	Government Contractor	Male	5	3%
P9	Healthcare	Male	2	22%
P10	Advertising	Female	2	50%

Presentation of the Data

The study aims to learn from SME's in industries other than K-12 education of the strategies that they use to improve information security in their organizations so that IATs in K-12 education can apply them in their organizations. Chosen subjects were from LinkedIn and the GIAC advisory board. Subjects that volunteered were asked to select a 60-minute time slot. The data collection took place in the form of recordings of semi-structured interviews using WebEx and subsequent transcription.

A pilot study was conducted using two subjects. This study was conducted via WebEx at a time at which the subjects indicated that they had 60 minutes or more available. The thirteen questions contained in Appendix A given to the subjects resulted in some changes. The pilot study resulted in the refinement of several sub-questions and ensured that answers to the instrument could fit within a 60-minute timeframe. The updated instrument is contained in Appendix C and also in table 5.

Table 5.

Interview questions for the study

Interview Questions
1. What is your organizations annual budget?
a. What has been your experience with budget changes of the last 3 years?
b. What are your experiences with using these changes to benefit your security posture?
2. What is your organizations annual IT budget?
a) Can you tell me the staff size of IT?
b) Can you tell me the staff size of information security?
3. What is your organization's annual information security budget?
a) Is this sufficient to meet your stakeholder expectations or how much more would be necessary to meet those expectations?

b) Can you tell me about your experiences attempting to get additional budget to support information security?

4. Can you describe what regulations affect you and how you address those?

a) What are your experiences with new regulations like GDPR?

5. Can you please describe who your stakeholders are and what are their information security expectations?

a) What are your experiences with expectations that are not met with those stakeholders?

b) Can you describe any unrealistic expectations that you are asked to fulfill?

6. Can you describe your experiences with your organization's information security posture and culture?

a) What methods have you used to attempt to influence this? Would you describe these as successful?

b) Can you describe your strategies for attempting to improve your information security posture and culture?

7. Can you tell me what the largest security concerns are for your organization?

a) What concerns are more recent versus more persistent over time?

8. What security frameworks or best practice frameworks do you employ?

a) What are some of the experiences you have trying to support these frameworks?

9. How would you describe the general IT staff level of knowledge on information security?

a) What about the larger user population?

b) How does this compare to the information security staff?

10. Can you describe your experiences with external or internal auditors as they relate to information security?

a) What has been your experiences with auditor finding remediation expectations?

b) Can you describe a time when you had to push back on audit findings?

11. Does your security team manage information security basics like firewalls and virus scanning or is that delegated to other organizations?

12. What have your experiences been with cloud hosting services in regards to information security?

a) Do you anticipate a change in your cloud posture in the next 12 months?

b) How has this affected your security posture as an organization?

c) What is your organizational position on managed security services?

13. Other than mentioned in response to the above, are there strategies in your organization that are essential to the level of information security you provide?

a) Have there been strategies that were not effective in improving your information security posture?

The data analysis for the study consisted of loading the transcriptions of each of the ten subject's interviews into nVivo qualitative analysis software by QSR international. From the answers given, six major themes emerged for the strategies that are used by IAT's in other

industries to improve the information security of their organizations. Table 6 captures those major themes.

Table 6.

The Major Themes Identified in the Study

Themes
The Need for Laws, Regulations, and Standards
The Need for Staffing and Funding
The Need for a Culture of Security
The Need for Frameworks
Augmenting Security Teams
Auditors

The Need for Laws and Regulations

Ten out of ten subjects (100%) cited the need to be compliant with one or more laws or regulations as a key strategy they used to influence the information security posture of the organization. None of the laws, regulations, or standards were listed by all of the subjects, though. Each subject had a different combination of depending on the industry sectors they operated in, the business model, and the specifics of their organization. For instance, eight out of ten respondents (80%) stated that HIPAA had a significant impact on their information security decisions. However, three respondents are in the field of healthcare or health research.

All the participants cited one or more laws, regulations, or standards that they were required to comply with or meet. These laws could be in the United States, such as HIPAA or

Sarbanes-Oxley, or other countries such as the European Union's General Data Protection Regulation (GDPR). Table 7 lists the laws and the frequencies of their mention in the data.

Table 7.

Respondents Affected by Laws, Regulations, and Standards

Laws, Standards and Regulations	Number of Respondents	Instances of Mention
HIPAA	8/10	43
CJIS	2/10	5
Sarbanes-Oxley	5/10	16
GDPR	4/10	17
FISMA	1/10	2
PCI-DSS	7/10	40
FERPA	1/10	2
Other state Privacy Laws	4/10	17

Responses to question 4: *Can you describe what regulations affect you and how you address those?*

All respondents (100%) listed at least one and often several regulations to which they must comply with and demonstrate that compliance. Respondents stated that the need to meet the requirements of these laws drove the requests for funding and staffing but also had significant impacts on the organization's culture of security. Participant 2 stated, "HIPAA is the 800-pound gorilla here, it is the foundation of everything we do with information systems at [my organization]. If we don't comply, it is not only a violation of that law but also that of the trust that our patients and board places in us."

There were frequent mentions of other laws. Five subjects cited Sarbanes-Oxley. Those subjects were either directly publicly traded companies or owned by publicly traded companies. Subjects referred to the fact that many of the laws insist that organizations apply a common-sense approach to information security. Participant 5 proclaims that "All of these laws are saying

the same thing, right? Don't do anything stupid, and we are going to hold you accountable for the level of stupid you bring to the table."

Seven of the respondents (70%) stated that they are concerned with the emerging California Consumer Privacy Act of 2018 that will also create stringent demands for information security teams that operate in the state or house data of the citizens of the state. Participant 4 shared his analysis, "the CCPA is California's answer to GDPR and is almost as strict." Participant 5 stated that "the California law will really start to force some behavior change" in terms of organizations cloud adoptions.

Figure 5. The questions that determined the need for laws and regulations

The Need for Staffing and Funding

Ten out of ten respondents (100%) indicated that they had information security team sizes of four or more persons. There was a large variance in team structures. Three out of ten (30%) indicated that functions related to information security that are generally tasks for the larger IT department, such as virus scan finding remediation, and firewalls monitoring, were handled within the information security team. The remaining seven out of ten (70%) indicated that they engaged a hybrid responsibility model in which the security team held functions that were strategic while more mundane and tactical work was delegated to other groups or outsourced. Figure 6 details the questions which demonstrated the need for staffing and funding.

Responses to question 1, 2, and 3: *What is your organizations annual budget? What is your organizations annual IT budget? What is your organization's annual information security budget?*

Ten out of ten (100%) participants in the study indicated that proper funding and staffing of the information security team was a requirement for the information security of their organizations. Four out of ten (40%) said that their staffing and funding level determination is by predetermined staff size and was not variable based on workload or demand. Three out of the ten reported that their team sizes were determined based on the workload and the regulator demand. The remaining three (30%) indicated that staff sizes in their organizations were not variable and that workload and expectation management is used as well as operational expenditures to obtain third-party assistance from Managed Security Service Providers (MSSP).

Participant 7 expressed the importance of properly funding an information security organization, "most organizations don't understand the value of a well-funded, well-sized security team." Participant 10 stated that "Gartner recommends budgets between 5 to 6 percent of the IT budget." Participant 6 justified these by stating "[information] security is really quality assurance for IT, we use the lenses of confidentiality, integrity, and availability to do so but you need to be staffed to check the output from all of IT."

Table 8 lists the subjects by industry, the information security budget as a percentage of the overall IT budget, the information security team size, and the information security team size as a percentage of IT budget. Note that participant 8 was only taking into account the centralized information security team for which they were responsible, stating individual contracts may "focus purely on security-related efforts then you might have, you know, 10 or 20 [security] people on that contract."

Table 8.

Infosec team size comparison to IT by budget and staff

Subject	Industry	Infosec budget as a percentage IT	Team size	IT staff size	Infosec team size as a percentage of IT
P1	Government	4.67%	6	170	3.53%
P2	Healthcare	7.20%	6	380	1.58%
P3	Technology	10.00%	5	130	3.85%
P4	Government	3.25%	5	240	2.08%
P5	Retail	3.50%	5	200	2.50%
P6	Technology	7.00%	4	200	2.00%
P7	Higher Education	9.09%	50	550	9.09%
P8	Contracting	1.49%	27	800	3.38%
P9	Healthcare	5.49%	88	400	22.00%
P10	Advertising	5.00%	10	20	50.00%

Figure 6. The questions that determined the need for staffing and funding

The Need for a Culture of Security

Nine out of ten (90%) of participants indicated that a strong culture of security was imperative to their ability to deliver adequate security. An element of this culture was the need for senior leadership support. Five out of ten (50%) of participants indicated that support from the CIO or higher was essential to the role. Participant 10 said it was so crucial, "that I wouldn't

have taken the role without leadership support." Participant 3 observed that, "the organization has a strong security culture, and that is only because it began at the top." Figure 7 details the questions that determined the need for a culture of security.

Ten out of ten (100%) of participants made mention of the importance of end-user training and engagement as being essential to the level of information security they provide. Participant 10 stated that "getting someone to sit for an hour is really difficult, so I ensure training that is concise and to the point, 20 to 25 minutes maximum." Table 9 describes the techniques that the participants described using when performing end-user training.

Table 9.

End User Training Methods and Frequency

End User Training Method	Number of Participants Using Method
Mandatory Annual Training CBT	10
End-User Training Presentations	8
Phishing Simulations	6
Steering Committees	3
Newsletters	3
Brown Bags	2
Spot Awards	2

Seven out of ten participants (70%) cited that policies and procedures that the user community is well informed of, that are up to date, and cover a wide breadth of business scenarios are essential to the level of information security they provide in their organizations. Five out of ten (50%) stated that their policies needed major revisions upon them assuming their role. All of those five also cited the need for annual changes. All ten (100%) of those in the previous paragraph that emphasized the importance of end-user training also cited that training on organizational information security policies as an essential part of their end-user training.

Responses to question 5: *Can you please describe who your stakeholders are and what are their information security expectations?*

Participants indicated that stakeholders were vital in the level of information security they provided but that all had multiple groups with different expectations from information security. Participant 7 responded, "I've got constituency across the entire organization, so I've got the board of directors, I've got executive management, I've got hospital management, I've got management of the physician practices, and they're all have different expectations." Participant 8 stated that his stakeholders are "anybody who has an interest in IT, which is literally everybody in the company." Table 10 contains a listing of the stakeholders listed by participants.

Table 10

Stakeholders Listed and Frequency

Stakeholders	Frequency
Senior Leadership or Board	10/10
Employees	7/10
Customers	5/10
Stockholders	4/10
Citizens	4/10
The Government or Regulatory bodies	4/10
Subsidiary Leadership	2/10
Third parties	2/10

Responses to question 6: *Can you describe your experiences with organizations information security posture and culture?*

The importance of the information security posture and culture, and an IAT's role is shaping said posture and culture was evident in the responses to question 6. Participant 1 cited his *human firewall* program in which gamified incentives promote security practices. Participant 2 stated that "data is a great ally. The ship has sailed on using fear to scare [users] into

complying." Participant 4 stated that not having a culture of information security is "a steep hill to climb in terms of having to build it first," as he stated it was a prerequisite to all other technical work so that IATs are viewed as enabling organizational goals, not impeding them.

Responses to question 7: *Can you tell me what the largest security concerns are for your organization?*

The most widespread information security concerns varied widely among subjects. The most significant number, four out of the ten subjects, were concerned with compromised user accounts (40%). Also, participants 3, 5, 7, and 10 were concerned with items categorized as overall security management and governance with participant 6 stating that because of the business model of his organization, his users are "effectively independent consultants. [Because of this] the biggest challenge and risk is what they are doing with data while at a client site." Participant 10 states that "we have over a billion records [that can uniquely identify a consumer] so that is probably the one thing that could happen that would probably bankrupt this company." Table 11 details the concerns of the participants.

Table 11.

Concerns About Information Security Threats and Frequency

Concern	Frequency
Compromised User Accounts	4
Overall Security Management and Governance	4
Third Party Risk	3
Data Inventory and Control	2
Rogue devices	2
Breach of Data	2
Intellectual Property Theft	1
Artificial Intelligence Threats	1

Responses to question 9: *How would you describe the general IT staff level of knowledge on information security?*

Question 9 and its probing subquestions were asked to understand how common knowledge about information security is within the participant's organization to aid in building a picture of the information security culture and posture. Participant 6 responded that his information security team "is the best I've ever had the opportunity to lead." Participant 1 stated that, in regards to the larger user population, "I have everything from landscapers to doctors so I would expect to have a large user population that never thinks about information security." Table 12 details some of the comments on the level of information security awareness that the participants gave about different user populations in their organizations.

Table 12

Participant Observations on the Level of Security Awareness by Population

Participant	IT	User Population	Infosec team
p1	Above average	Low	All Over the Board
p2	Very Aware	Middle of the Range	Highly Skilled
p3	Pretty Good	Low to Knowledgeable	Half and Half
p4	Pretty Keen	Low	Very Good
p5	Moderate	Getting Better	Good
p6	Medium	Functional	Best Team of His Career
p7	Improving	More Aware Than Most	High
p8	Really Good	Reluctantly Knowledgeable	Most are Good but Some are Building
p9	Dramatically Improved	Good	The Best of the Best
p10	Basic	Very General	Good

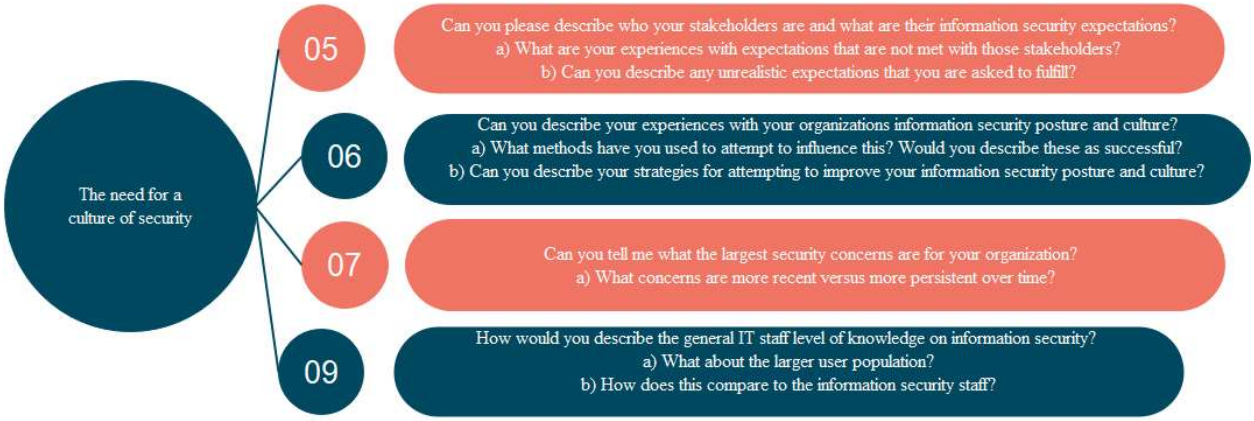

*Figure 7.*The questions which determined the need for a culture of security

The Use of Frameworks

Responses to question 8: *What security frameworks or best practice frameworks do you employ?*

Nine out of the 10 (90%) of the respondents responded that their organizations made use of a security framework such as the National Institute of Standards and Technology Cyber Security Framework (NIST-CSF), the Center for Internet Security (CIS) Top 20, HiTrust, or ISO-27001. This use of frameworks is in response to the laws, regulations, or standards that they must comply with, in addition to requirements placed on them by stakeholders. These frameworks are sometimes industry-specific, but all contain a set of security controls and measures that organizations can use to assess their ability to identify, protect, detect, respond to, and recover from threats. Table 13 lists the frameworks used by respondents and their frequency.

Table 13.

Frameworks Used by Respondents

Framework	Respondents
NIST CSF	9/9
CIS Top 20	6/9

ISO-27001	3/9
HiTrust	3/9
PCI-DSS	7/9

Due to the complex nature of frameworks, seven respondents (70%) indicated that they had internally created "cross-walks" that connected the controls from the frameworks they use to their compliance obligations. These spreadsheets are matrices of the regulatory obligations and the framework controls. The result of these crosswalks is the demonstration of meeting several compliance obligations with a single control. Subject 5, who had expended considerable effort on producing such cross-walks stated that crosswalks aid in "the cycle of information security by allowing you to swap out frameworks, and mine performs additional calculations for reporting." These reports can then be used as vehicles for communicating summaries of the status and needs of information security.

Additionally, respondents indicated that the implementation of the framework and the associated controls is a long-term process taking years, and requires iterations to increase the level of information security maturity effectively. Participant 6 stated in regards to implementing controls "I think a lot of organizations would find that they probably implement somewhere around 5 to 10 percent of those controls per year and through that process, they systematically are increasing their overall security capability and security maturity." Figure 8 displays the question from the instrument that led to determining the need for the use of a framework.

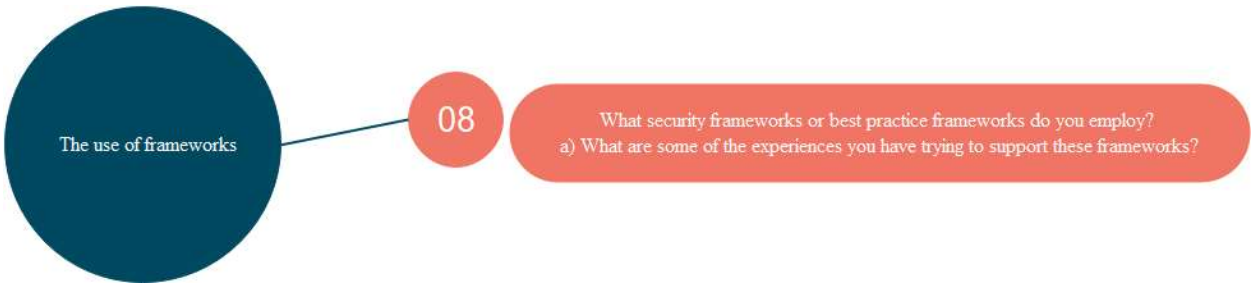

Figure 8. The questions which determined the requirement for the use of frameworks

Augmenting Security Teams

Participants indicated that there are duties that cross functional lines between information security and IT teams. As such, opportunities arise for an organization to engage an information security team that consists of strategic resources and to leverage other teams for tactical work. Additionally, Managed Security Service Providers (MSSP) can be employed to provide additional services that would otherwise require security team staff to deliver. Figure 9 shows the questions in the instrument that helped determine the need to augment security teams.

Five of the ten participants (50%) stated that they currently use MSSPs to augment the capabilities of their security teams today. Four indicated that they were open to the use of MSSPs but did not use them now and were able to perform the functions requested of an MSSP in-house for less money. One participant said they were not using MSSPs, nor were they open to doing so.

Six out of the ten participants (60%) shared that they operate information security departments that do not centralize all functions that involve security and instead engage other departments to perform that work. Four participants out of ten (40%) said they all centralize functions. One participant stated that the only reason they could centralize was due to substantial investment in high-end antivirus software, which keeps manual intervention to a minimum. Two participants stated that they centralize the function but dispatch other teams to remediate low-

level issues. One participant (10%) uses their MSSP for monitoring so that they are free to address the remediation activities.

Table 14

Options Used to Augment Information Security Teams Capabilities

Participant	Use of MSSPs	Security Tasks Kept Within the Security Team Only
P1	Yes but only basic after-hours monitoring	No, Shared with Desktop and IT
P2	Open to it, but not using them	Yes, Centralized in Infosec. May Deputize Other Teams as Necessary
P3	Open to it, but not using them	No, Duties Shared with Service Desk and Infrastructure
P4	Open to it, but not using them	No, Duties Shared with Desktop and Network
P5	Open to it for SOC, but RFP proved that it should be done in-house	Yes, but only because of use of a High-End Virus Product
P6	No, in-house SOC	No, functions are federated throughout the enterprise
P7	Yes but limited use-cases	No, Desktop Engineering for AV and firewalls are co-owned with Network
P8	Yes, for monitoring and first-level triage	Security function by monitored by the MSSP
P9	Yes, for after-hours SOC	No, Shared with Desktop and IT
P10	Yes, wherever they can add value	Yes, Security receives all alerts and dispatches other teams to remediate

Responses to question 11: *Does your security team manage information security basics like firewalls and virus scanning or is that delegated to other organizations?*

Participant 10 responded that, since the formation of her organization was the result of a high profile breach, information security "must be done right. I just can't trust any other team to do it." In contrast, participant 7 stated that "we are a force multiplier, we don't hunt down every alert, but if we see the same thing fire off across 20 or 30 machines we will investigate it. Otherwise, we distribute that work." Participant 1 lamented about the limitations of a smaller

team when he said, “we try to trust our technology as much as possible, and there is a lot of stuff we just don’t have turned on because we don’t have the ability to respond to it if we did.”

Responses to question 12c: *What is your organizational position on managed security services?*

Participant 9 responded, “I use them very judiciously. I mean I signed an agreement with a SOC provider to do after hours support for our SOC, there's certain parts of it that I'm probably going to be outsourcing, for example on third party assurance.” Participant 10 stated, “I'm a huge proponent. I think they expand my team. They create subject matter experts to the place where I don't have to pay them because the skills gap is so big, if I can leverage other organizations to become like an extension of my security team then I think that's an extreme value to myself.” Participant 1 stated that his feelings towards MSSPs are that they facilitate situational awareness and that he did not, “see a time when we're not going to, at least in the near future, where we're not going to rely on the managed services provider to at least help us.”

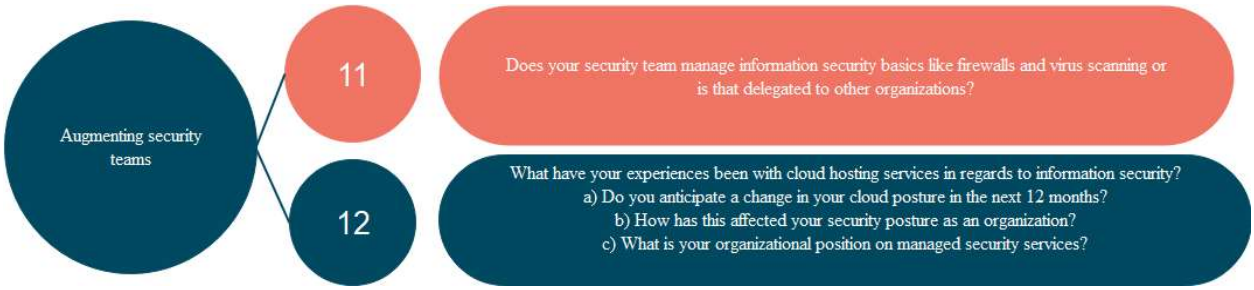

Figure 9. The questions contributing to the finding of the need to augment security teams

Auditors

Internal and external auditors can be used by organizations to examine the efficacy of a security program and act as a third party to examine how controls are implemented and monitored. Eight of the ten participants (80%) expressed a sentiment that indicated that auditors were a positive contributor to improving security posture and culture. One out of ten (10%) of

participants stated that auditors engagements should be limited to confine findings to an actionable, beneficial set of deficiencies. One out of ten (10%) participants stated that auditors need to understand the business benefit of the controls they demand and only insist on those that benefit the business as a whole. Table 15 describes audit sentiment and remediation expectations.

Table 15

Auditor Sentiment and Remediation Expectations

Participant	Sentiment	Remediation Expectations
P1	Auditors are used to drive the infosec roadmap	Findings remediated over the year as a project
P2	Auditors are encouraged to examine areas of known deficiencies	We set those timelines
P3	Use mock audits and limit scope to avoid surprises	We set those timelines
P4	Has internal auditors that are welcome visitors	Usually no findings to remediate that are not already planned work
P5	Internal auditors are a great partner team	Usually no findings to remediate that are not already planned work
P6	Auditors need to demand controls that have business benefit	Findings need to evaluate risk against business need
P7	Auditors aid in interpreting compliance obligations	We negotiate the content of the letter to management
P8	Auditors are encouraged to examine areas of known deficiencies	Thorough audit reports drive funding and staffing
P9	Auditors are used to drive the infosec roadmap	We set those timelines
P10	Auditors challenge infosec to demonstrate viable controls	We negotiate the content of the letter to management

Responses to question 10: *Can you describe your experiences with external or internal auditors as they relate to information security?*

Participant 7, when asked about their experiences with internal and external auditors stated, “I love them both…They help me make it rain [money].” Subject 3 aimed to ensure that the initiating auditing projects establish the “scope the engagement and put some thought into what they're doing and what you want out of this. I think that you can be successful with most auditors. Ideally you want to have a mock audit before to now that you're prepared. And it's not terribly difficult to execute on, and that'll save you a lot of money. If and when you do that and make it a lot more efficient.” Figure 10 shows the question and subquestions from the instrument that led to the determination of the need for auditors.

Figure 10. The questions contributing to the finding of the need to engage auditors

Miscellaneous

Responses to question 13: *Other than mentioned in response to the above, are there strategies in your organization that are essential to the level of information security you provide?*

As the final question of the interview, participants were asked to reflect on the answers they have given to the other twelve questions and see if there was anything that they would personally recommend as strategies for consideration. Two of the ten (20%) stated the importance of engaging the user community of an organization in the information security process. An additional two out of ten (20%) stressed the importance of being secure by assessment and refinement, not just checking the boxes in a compliance framework. Another two out of ten (20%) stressed the importance of engaging the organization's leadership board so that

factoring cybersecurity into significant decisions is a common practice. Table 16 summarizes these responses.

Table 16.

Responses to the Question Prompting for Additional Strategies

Participant	Response
P1	Security is a shared responsibility so turn your end users into security advocates
P2	Treat all data as though it is Protected Health Information
P3	Conduct frequent maturity assessments
P4	Strive to create a workforce engaged in security
P5	Use caution in on-boarding new third parties
P6	Engage infosec staff in leadership development programs
P7	Get cybersecurity representation on the board
P8	Don't be lazy (don’t just check boxes)
P9	Employ intentional and clear communications with the board
P10	Don't use the security framework to merely check boxes

Presentation and Discussion of Findings

The qualitative exploratory study used semi-structured interviews to learn the strategies used by Information Assurance Technologists that are leaders in their organization’s cybersecurity departments to understand the strategies they leverage to improve information security in their organizations. The interviews were recorded via WebEx meetings and transcribed using NVivo transcribe. The transcriptions were then manually verified and edited before being confirmed via member checking. The interviews resulted in a large amount of data that was then reviewed to familiarize the researcher with the data and unique perspective of each of the participants before coding began.

Importing the transcript of each of the interviews into NVivo version12 for analysis was the next step. Because of the unique perspectives and industry differences, automated identification of themes was unsuccessful and resulted in the researcher engaging in manual

techniques. Using NVivo, priori codes were identified in each transcript. Codes were created for each technique that SMEs indicated was used to improve the level of information security in their organizations.

After a review of these codes, a collection of themes emerged during phases two and three of coding. Some themes applied only to the individual participant. Iterations at level three coding combined themes across multiple participants and revealed six strategies employed by the SMEs in which categorization of all of the perspectives, advice, experiences, and observations of the participants fit. A summary of the themes is in table 17.

Table 17.

Themes That Emerged from the Study and Their Frequency of Occurrence

Themes	Frequency
Laws and regulations	91
The need for staffing and funding	88
The need for a culture of security	84
Frameworks	65
Augmenting security teams	45
Auditors	33

One of the most prevalent themes identified in the study was that the security leaders in the study all cited the strategy of leveraging prescriptive laws and regulations provide for the information security of their organizations. The need for laws was the foundation for establishing the need for the information security program. Those participants operating under the presence of such laws often lost sight of them as a strategy aiding in the establishment of information security goals and the protection of the organization's assets. This strategy creates a demand for information security that is then addressed by additional strategies. No participant was not beholden to some information security law.

The next most prevalent theme was the need for a strategy that provides adequate staffing and funding of the information security team. All participants had teams of multiple people, the exact size of which was either built on a formulaic ratio of information security staff or budget to that of the IT department staff or budget or was constructed based on a sum of the estimates of hours necessary to properly secure the organization. Emphasis was clear that larger team ratios, when compared to IT, are far more capable, and that teams would need to be initially larger to build the security practice in an organization than they would be for sustaining operations and that planning should encompass this.

The third most prevalent theme was that security leaders employ a strategy that creates and promotes a culture of security. Many axial themes comprised this. Examples are user engagement in and awareness of information security, stakeholder expectations, and the need for robust and up-to-date information security policies and procedures. Participants spoke of using this strategy as a critical element in establishing a level of information security for an organization as the rigor of all other items was determined by an organizations security culture.

The fourth theme to emerge from the study was the use of frameworks as a strategy to address the organization's compliance obligations. Nine of the respondents cited the use of a framework as a key strategic element in the provision of information security in their organization, and many mentioned more than one framework that they were obligated or chose to follow. Many subjects created a matrix or crosswalk that demonstrated a compliance obligation, and the controls and the frameworks they used that ensure the addressing of compliance burdens. Participants stated that these frameworks are not singularly responsible for the level of information security they provide but the source of reporting on the efficacy of

information security and the basis of the documentation that demonstrates current capabilities and future planned capabilities.

The fifth theme was the strategy of augmenting information security teams. This augmentation can take place with the use of outsourcing vendors, by dividing up lower level security tasks among different departments, or by centralizing all security intake functions but then dispatching frontline and mundane tasks to more generalist work teams. Participants also emphasized the need for proper tooling and investments to ensure minimization of the number of actionable tasks.

The final theme to emerge was the strategy of engaging internal or external auditors to assess the information security program. Participants emphasized that this is not a punitive step but one where a different perspective both evaluates the compliance obligations but also the needs of the security program to address those obligations. Participants expressed that using auditors as an additional, objective subject matter expert on the information security needs to the organization is a valuable and beneficial strategy to improve the level of information security in an organization.

Summary of Chapter Four

The study produced involved ten subject matter experts, information security leaders in industries other than K-12 education. Those SMEs were then asked 13 questions in qualitative semi-structured interviews. The data resulting from those interviews were analyzed until six major themes emerged. Those themes were the need for laws, regulations, and standards, the need for staffing and funding, the need for a culture of security, the need for frameworks, augmenting security teams, and the need for auditors.

The findings from the research suggest that there are six strategies that K-12 information Assurance Technologists should be advocating for to improve the level of information security in their organizations. By advocating for more prescriptive laws mandating information security obligations, IATs will have a clear foundation for expected behaviors and expenditures. That foundation can then be used to justify the requests in the remaining six themes.

By establishing strategies for staffing and funding, organizational leaders are placed in a position to consciously acknowledge risk and fund or staff appropriately. Subjects in the study stated that they either built these strategies on the workload in the information security group, as a pure percentage of IT staff or funding or using a fixed headcount. Subjects indicated that by establishing a baseline funding or staffing strategy, changes to baseline tasks could then easily dictate changes to the budget or staffing.

By creating a culture of security, IATs can reduce the demands on limited information security resources by engaging all staff in information security as a shared responsibility. The participants provided data that suggests that such a culture consists of leadership support, end-user training, firm but enforceable policies and procedures, and the engagement of stakeholders on matters of security. Participants indicated that providing gamified learning experiences and involving and informing at all levels is most important in creating this culture, but that efforts to improve information security would not work at all without senior leadership support.

All of the participants in the study mentioned had at least one framework they used to ensure that controls address laws, regulations, and standards that their organization must comply. Those participants then often created a cross-reference of one or more frameworks against the requirements in the laws, regulations, and standards they must comply. These later became the basis of roadmaps, and future budget asks.

The size of the information security departments varied significantly between participants, but nearly all expressed the need for more resources than they currently had. To address this, participants augmented teams either by using outsourced MSSPs or by delegating some information security duties to other departments. Augmenting allows constrained departments to provide the capabilities in addressing more tactical and mundane work without impacting strategic capacity.

All participants cited the use of and presence of auditors as a crucial strategy in providing information security for their organizations. Auditors give an impartial view into the deficiencies of a security organization and the recommendations to address those. Additionally, auditors were leveraged by the participants to highlight areas that the participants wanted to fund and focus on tackling.

These six themes resulted in a list of strategies that K-12 IATs can then advocate for or use to improve the information security of their organizations. While some are strategies that can be employed today, others may require laws to be advocated for and passed. A discussion on these findings also creates a layered approach for the building of a robust information security program detailed in chapter 5.

Chapter 5 contains a discussion on the conclusions based on the findings in the study as well as recommendations that result from the research. Chapter 5 will guide the reader through the findings and conclusions from the study, recommendations, and suggestions for future research. The chapter will conclude with a summary of the contribution to the body of knowledge.

CHAPTER FIVE

The problem that the study examined is that a lack of information assurance strategies in K-12 organizations has led the level of information security in said organizations lagging behind that of other industries. For this study, strategies encompass prescriptive laws, information security posture, a budget allocation plan that prioritizes security needs, and the demands of stakeholders. IATs not having access to these strategies has led to a level of information security in K-12 organizations that subjects the K-12 organization to a great deal of risk.

The purpose statement of the study is to explore the strategies information assurance technologists need to improve information security in a K-12 organization. These strategies may seem self-evident to the IATs within other industries. No substantive research showed information security strategies that exist in other industries are universally present in K-12 organizations. The presence of information security strategies allows other industries to achieve a higher level of information security. The senior leaders in K-12 organizations have had little exposure to those strategies given that K-12 leaders typically rise through the ranks of education, and may not have work experiences in which these strategies were present and proven effective.

The methodology for the study was qualitative exploratory research. The design called for the use of a thirteen question semi-structured interview with information security leaders from industries other than K-12 education. This design was selected because qualitative studies of information security strategies applicable to K-12 education are a nascent phenomenon — this methodology allowed for subject matter experts to relay their insights on strategies used in their organizations — further, the researcher to make use of probing subquestions to prompt additional data.

One of the first limitations of the study was the assumption of participant honesty. Subject matter experts may have been inclined to emphasize the positive aspects of their security programs and neglect to mention the negative. The second limitation is the amount of time allocated for the researcher to conduct the research, which is limited by the program of study. The third limitation is that of the instrument itself, the validity of which was determined by a pilot study. There was an additional assumption that the IAT participant was aware of or had influence or ownership of such strategies.

The primary ethical concern of the study was the protection of the participants. The subjects received the informed consent contained in Appendix A to ensure that they were aware of their rights under the study. Steps were also taken to ensure the anonymity of the subjects of the study so that answers they gave could not be attributed to them as individuals, or reveal vulnerabilities in their organizations. Further, subject matter expert answers were edited to change elements that would uniquely identify an organization to more generic responses contained in brackets. Additionally, questions were asked in a fashion that emphasized the learnings the participant had achieved rather than a focus on mistakes of shortcomings of their specific organizations.

Following this introduction, chapter 5 will explore the findings and conclusions. The limitations of the study will be explored, followed by implications for practice by IATs and K-12 organizational leaders and stakeholders and the implications of the study and the recommendations for future research. Finally, chapter 5 concludes with a review of the chapter.

Findings and Conclusions

This qualitative exploratory study was designed to aid the investigation of the lived experiences of information security leaders in industries other than K-12 education and understand what strategies those leaders leverage to improve information security in their

organizations. The target population for this study was subject matter experts that were either on the GIAC advisory board or those who listed a title of CISO on LinkedIn.com, indicating that they were leaders of information security programs at their organizations. As information security becomes essential in all industries, it is necessary that IATs apply the strategies that have worked to promote information security in industries where compliance with privacy and security laws are more enforced and regulated.

The research consisted of qualitative interviews via WebEx, and subjects were asked a series of thirteen questions that were designed to understand the strategies and posture of the participant's organization. Subjects answered questions in interviews that ranged from as little as forty minutes to over two hours. Nvivo was used to transcribe the interviews for analysis, which identified several themes through manual review and iterative coding efforts.

In the interviews, it was clear that there was not a universal understanding of what the term *strategies* meant when participants answered questions about them in the pilot study. The researcher informed participants that strategies are viewed as resourcing prioritization that recognizes the necessity of information security spending, the establishment of information security policies, a documented risk tolerance, access to laws and industry norms that mandate certain security practices and consequences for non-compliance as a matter of due care and due diligence, and the demands of stakeholders (Smock, 2018). Following this clarification, the mindset of the participants focused on the study's intent to uncover high-level components, not specific technologies or tactics.

The study's research indicated that six overarching strategies IATs in industries other than K-12 education use to further information security in their organizations. The first strategy is the need for laws, regulations, and standards. The second is the need for appropriate staffing

and funding. The third is the need for a culture of security. The fourth strategy that emerged is the need for frameworks to define security practice. The fifth strategy is that of augmenting security teams. The final strategy is to make use of internal and external auditors to further the goals of a security department.

Another essential result of the study was that the participants relayed their experiences in the form of advising an apprentice. The participants recognized the nascent area of the field of study and tailored responses to aid the advancement of K-12 information security practices. The K-12 IAT may have networking opportunities in the K-12 arena, but an opportunity outside of professional organizations is rare due to time to or funding.

Theme 1: The Need for Prescriptive Laws, Regulations, and Standards

The first theme to emerge from the study is the need for prescriptive laws, regulations, standards, or industry norms. All participants stated that they must comply with one or more laws addressing the participant's obligation for information security. Subjects often correlated their practices to the mandated requirements of laws or regulations. Participant two stated that the information security law that is specific their industry was the key driver for their entire information security program. Other participants felt that legal compliance is so pervasive in the work that they needed prompting through the use of probing subquestions to reflect on the impact such laws and regulations have on their information security programs.

Participants 4 and 10 reflected on how the governance of their organizations by various laws and how information security groups found such intersections challenging to navigate. Participants stated they make use of crosswalks to highlight where compliance with a component of one regulation also simultaneously addressed compliance with a requirement of a different law, reducing the overall burden on IATs. Some of these laws reflected a compliance burden that could result in criminal prosecution if not met (Sarbanes, 2002; Overly, 2018). As such, IATs

were free to design programs consisting of administrative and technical controls and the funding to implement them. Those programs then had the support of organizational leadership as a cost of running the organization, according to participant 9.

Previous research stated that one of the most important considerations of an IAT is to ensure their organization's compliance with the law (Cooke, et al., 2012). That research was confirmed in the study as all ten participants stated the importance of legal compliance as a primary driver in their security programs. Additionally, in cases of weak and out of date laws, such as FERPA (Mader & Smith, 2014) the study was able to prove that IATs in industries with prescriptive laws such a HIPAA, viewed the law as a critical driver for their organization's security posture.

In practice, the K-12 IAT may not be immediately empowered to create new laws. The need for better laws is certainly a good area for activism in replacing and updating laws such as FERPA which are out of date and do not prescribe the requirements for K-12 school district compliance. A possible interim step is the voluntary establishment of a generally accepted set of industry norms. In creating these, obligations to meet these norms become the standard for due care and a minimum obligation of the K-12 organization. Later legislation can then subsequently cite those norms as requirements for compliance.

Theme 2: Engage in Appropriate Staffing and Funding for Information Security

Participant 7 emphasized the need for an appropriately sized security team after observing that a small yet very talented team cannot overcome the constraint of a lack of financial and staffing resources. The lowest team size was 4, and the largest was 88. There did not appear to be a correlation with the staff size of IT.

Participant 9 emphasized the need for appropriate staffing by indicating that an information security team cannot be too large. Due to change saturation (Drago & Geisler,

1997), or the overwhelming of an organization with the implementation of too many changes too rapidly. Participant 9 advised that security leaders must carefully monitor the organization to observe the amount of change absorption that can take place at any given time. The subject went on to state that attempting to execute too much change would result in a lack of support for security efforts, and that lack of support would prove fatal for the program. Participant 7 suggested that IATs were a form of quality assurance for IT and that larger the number of IT staff and the higher the complexity of that staff's work, the larger the demand for IATs to maintain appropriate security.

The research showed that participants referenced proper allocation of resources such as budgets, both capital expense and operational, as well as human resources to be critical to the level of information security they offered their organizations. Participants indicated that initiating a program required more significant resource support than when an information security program is well established and operating normally.

A report from previous research stated that information security comes at a cost (Madison, 2017), which the study confirms. Participant 9 also emphasized a sizing guideline for information security from Gartner in terms of budgeting paraphrasing the recommendation of between 5 to 6 percent of IT department budgets. Budgets of the participants ranged from 1.49% to 10% of IT budgets, with six of the respondents reporting that their budget is 5% or more of the overall IT budget. Those who were under 5% of the IT budget rely on augmenting security teams as covered in theme 5.

IAT's should begin the practice of using other strategies listed below to build cases to justify investment in information security programs in K-12 education. Further, if their organization is too small to implement such recommendations, the IAT could consider forming a

co-operative, non-profit, or other consortia body manage information security for a variety of nearby districts. Finally, the IAT should monitor and report on organizational statistics over time so that senior leadership is kept aware of the threat landscape and understands the need for sustained information security sustaining support.

Theme 3: Foster a Culture of Security

Nyachwaya (2013) indicated that security to IT budget ratios only had a moderate impact on information security effectiveness. This study confirmed his assertion in that participants stated that in addition to being adequately resourced, a culture of security was also necessary to improve overall security. Participant 4 stated that "you can't spend your way out of bad practice." A culture of security is typically where, from the top of the organization downward, individuals are expected to perform their tasks in a way that supports the security goals of the organization. This view is opposed to the classical view of information security being an IT function and the responsibility of an IAT. By creating a culture of security, the number of overall information security incidents is lessened, allowing IATs to focus on strategic improvements to information security posture and maturity rather than remediating issues introduced by careless or uninformed constituents (Jauregui, 2015). This study confirmed Nyachwaya's (2013) finding by revealing that investment is only a part of the necessary components for information security.

Participant 4 stated that a pre-existing culture of security was the only way their program was able to operate in such a large organization with such a small team size. Participant 7 stated that in their new hire orientation, their information security culture manifested in the form of each of the presenting managers referencing how new hires could perform tasks relative to those managers areas in a secure way. Both spoke of how their respective organizations had recovered from a highly publicized breach before adopting such practices, but that breach had predated them.

The act of building a culture of security is mostly the creation of an educated senior leadership and the IAT leader building relationships and trust with other departments according to participant 9. Participant 2 also suggested several ways to promote security such as gamification and the dedication of a security team member to communications. All participants indicated that security training is vitally important. Participants also stated that there is a need for constant retraining to be sure that learned information security practices continue to be a part of everyday operations. All of the participants stated that one of their primary stakeholders was the Board or senior leadership. A board or leadership official could be a force that impedes IAT progress in improving information security (Armarego, et al., 2015). This finding agrees with the literature which found that consideration for the culture must take place when determining security posture and that information security posture is mainly under control of the users. Thus training, and leadership by example were essential (Tang & Zhang, 2016; Johnson, 2017; Lacey, 2010).

Previous research highlighted the requirement for a robust security policy suite (Francois, 2016) that covers a wide range of business scenarios and is endorsed and followed by senior leadership. The research confirmed the requirement for policies. This set of policies should frequently be and should be a part of each employee's onboarding and annual mandatory training according to Participant 4. Participant 10 promoted the idea that a policy suite was going to have many exceptions and that those exceptions merely needed to be appropriately recorded when those exceptions occur to feedback into annual policy updates.

It is the stakeholders who influence posture and must be the IAT must influence those stakeholders to act securely. The study also confirmed that IATs would need to influence and inform to create policies that are meaningful and enforceable (Armarego, et al., 2015). Many

practices can be adopted by the K-12 IAT to implement a culture of security, but the study participants recommended end-user education and communication with senior leadership as the key elements. A robust policy suite is also required to promote this culture. Participant 2 stated that a primary function member for a member of their team was to communicate with all levels of the organization. The IAT should focus on communicating with leadership, parents and families, and the student population about the implications of the information security decisions they make every day.

Theme 4: Implement and Follow a Security Framework

A theme that emerged from the study is the use of security frameworks as a strategy to improve information security. Information security frameworks such as NIST CSF or the CIS Top 20 are a codified set of strategies and best practices for that organizations can implement and follow to create a formal and proactive security practice that meets their requirements for security event prevention and remediation. These frameworks were cited by study nine of the participants as being an essential strategy for their security program. Participant 2 stated that the use of the CIS framework in their organization allows leadership and IATs to develop a common vernacular around what work needs prioritization, when it will be complete, as well as the degree of risk being accepted by the organization as a result of such prioritization.

The study seems to contradict previous research, which only makes passing reference to the use of a security framework (Brown, 2016). Participant 5 indicated that security frameworks and the administration and documentation of their compliance with those frameworks were the bulk of their organization's information security program and the guiding driver for the work performed by IATs in that organization. Participant 1 indicated that their organization measures itself on eight frameworks. By the IAT communicating what the organization was complying

with and where there were gaps in compliance, leaders can make informed decisions about funding to address such gaps.

Theme 5: Augment Security Teams

The fifth theme to emerge from the study is the idea that the security team in some organizations was not staffed sufficiently to be able to address enough of the work involving information security to meet standards of due care. One of the themes that emerge in the study is that of engaging in a outsource partner such as an MSSP. Five of the participants said that they make use of an external MSSP for some amount of tactical work, freeing IATs to perform more critical tasks. The practice of augmenting information security teams agrees with the literature. The option of outsourcing is only mentioned briefly in previous research (Brown, 2016).

Other literature did not distinguish from work that was performed by IATs or by other groups in the organization. This finding disagrees with the literature in that six of the study participants stated that they augment their IATs with other teams. Participant 7 emphasized that their team could be far more effective by handling newer incident types or implementing more advanced controls. Security teams should plan a steady migration of rote tasks for either security automation or less constrained teams to manage on behalf of the IATs to address this constraint.

Theme 6: Leverage the Use of Auditors

Eight of the study participants expressed that they welcomed auditors internal or external to their organizations due to the ability to leverage audit findings to justify current spending or future requests for information assurance investment. Participants mentioned that auditors were mostly responsible for the ability to give an external voice to departmental concerns. Participants also said that auditors offered a form of quality check for the controls the IATs have implemented, granting additional sets of eyes and different perspectives on control efficacy. Both of these resulted in higher security in IATs organizations.

Theme six seems to agree with the literature by extension as common strategies and security postures did not call explicitly for the use of auditors as a critical strategy. The literature does reference the use of security frameworks, however, and specifically, NIST 800-53 lists audit accountability as one of its eighteen families of controls (NIST800-53r4, 2013). While not explicitly calling upon IATs to leverage auditors as a strategy, it does recommend that IATs develop policies and procedures around audits and how to collect and preserve auditable elements for inspection.

Conclusions

The study found six strategies that could be used by IATs to improve information security in a school district by examining strategies leveraged in organizations not involved with K-12 education. The strategies are broader categories that contain many practices and recommendations by the participants, and that exist in the literature. By highlighting these strategies specifically, IATs in K-12 education can set goals for themselves and their team to move the organizational security program forward while improving student and staff safety and privacy and protecting the organization from harm.

By listing the findings of the study in order of frequency of occurrence, they align so that one strategy supports each subsequent strategy. As an example, the strategy of prescriptive laws and regulations could serve as a foundation. With this prerequisite in place, engaging in appropriate staffing and funding strategies could then be addressed because one would not know what level of both is appropriate. Without knowing what the law would require, the IAT would be unable to understand what the requirements are on the security program. The frequency could order the strategies participants identified them. In the study, laws and regulations were mentioned 91 times. The strategies of appropriate staffing and funding and the need for a culture of security were mentioned 88 and 84 times respectively and could occupy the same level. The

strategy of making use of a framework was mentioned 65 times and would hold the next level up. Augmenting security teams would be an appropriate next level as the augmentation may not be determinable without the earlier layers. Finally, the strategy to leverage auditors would be of little use without a structured security practice established in the previous five strategies. Figure 11 captures the layering of these strategies to form a pyramid of K-12 information security strategies.

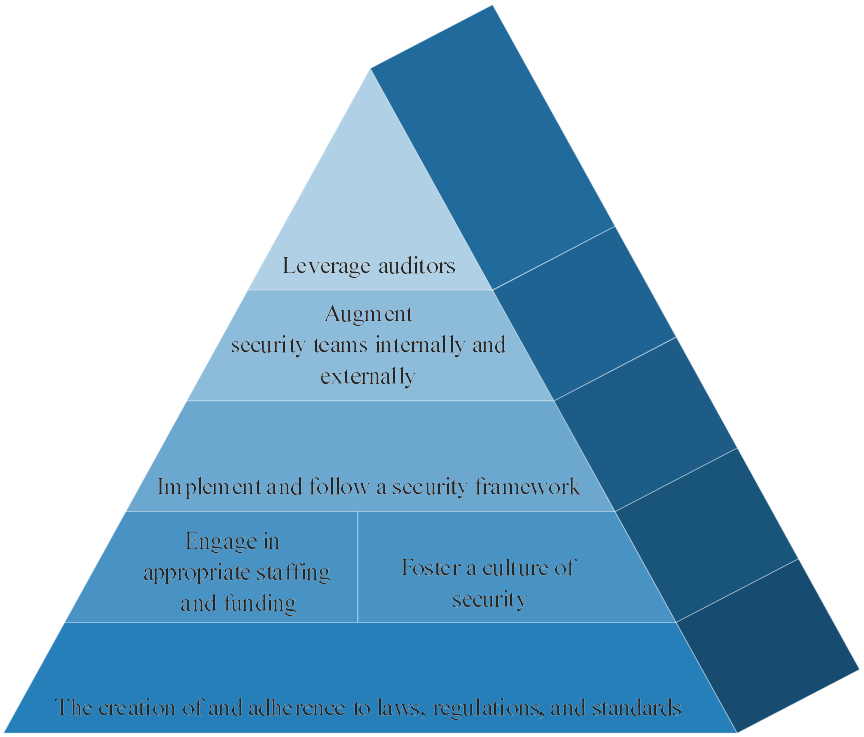

Figure 11. The strategies needed by IATs in a K-12 school district to improve information security

Limitations of the Study

Asking IATs about how they provide security could create a vulnerability in that should their identity become known, others may know where the strengths and weaknesses of the organizational information assurance measures. The IATs in the study were forthcoming about their environments and professional experiences. The participants were open to discussions

regarding vendors and systems used as well as external partners. All were willing to share where they hoped to improve, but also, all participants had a significant number of strengths to explore as well. The answers were uninhibited, which is attributable to the researcher assuring participants of their anonymity and communicating that replacement of specific names, or places that might identify a participant with generic terms in brackets will take place.

The IATs recruitment was via purposive sampling on profiles maintained publicly. The participants consisted of twelve total subjects, with two becoming a pilot group that served to refine the questions used for interviews. Another set of limitations were those of time for the researcher in the program of study. This time constraint was challenging for recruitment of participants of the subjects and finding mutually acceptable times for interviews with such busy individuals. The limitations did not seem to impact the study. Each of the 10 participants was willing and able to submit to the interview.

There were four critical assumptions about the study. The first assumption is that subjects were truthful in their stated qualifications. This assumption was proven reasonable after some subjects recused themselves during the qualification process because they did not meet the specified qualifications. There is also an assumption that 10 participants would be sufficient to reach saturation. It is possible that the inclusion of additional subjects might reveal more data specific to the industry the participant operates in, but at the strategy level, ten participants proved more than adequate to reach saturation. Another assumption was that the participants performed in environments where security was not key to their business model, thus forcing prioritization and complex, risk-based decision making by IATs on information assurance tasks. All participants acknowledged that information security was ancillary to their organization's primary mission and as such, the IAT was not granted unlimited resources to solve their

problems, thus requiring the use of strategies to fund and prioritize work. The final assumption was that the strategies that IATs in other industries use could extrapolate from the industry of the IAT and applied in the realm of the K-12 IAT. The resulting strategies demonstrate that this assumption was fair and reasonable again at the strategy level.

The research question set the delimiters of the study. While the participants did not universally understand the term *strategies*, a brief definition of the term at the beginning of the interview was used to get participants operating from the same frame of reference. Another delimiter of the study was the qualifications for participants such as being from an organization with higher than 500 employees and being a CISO or a GIAC Advisory Board member. These delimitations may have limited the number of responses because CISOs are often very busy and often unavailable for non-work related appointments. Participants rarely had to cancel, but meetings were scheduled usually weeks in advance. A delimitation that the participant had to have been in their role for two years did cause two potential participants to drop out as study participant candidates. This delimitation was that IATs in the study are in a job market that may make locating candidates with two years in their roles challenging.

Implications for Practice

In K-12 organizations, there is ample awareness of the threat posed by ineffective or absent information security measures. Due to a lack of strategies in the K-12 space to implement and maintain information security, IATs are often unable to create appropriate levels of security for their organization. This exploratory study sought to understand the strategies used by IATs in other industries for application in K-12 education. The results of this research address the central research question by revealing the strategies that IATs in sectors other than K-12 use to influence the information security of their organizations. By engaging in qualitative interviews, strategies

that the participants may have otherwise taken for granted emerged in addition to those that the participants acknowledged as being key to their level of information security.

The first finding was that IATs need to have access to prescriptive and comprehensive laws, regulations, and industry norms that require a level of information security. Largely the creation of a new law is outside the scope of IATs. However, there is the possibility of advocacy for such laws to replace the outdated and weakly defined laws currently in place. In the scope of the IAT is the creation of an industry norm in the absence of a prescriptive law which will create a standard of due diligence for districts to embrace or be held accountable by their constituents. Creation of these norms can serve as the basis for future laws. Such laws can ensure that information security in K-12 is a mandated requirement of the operations of the district. New markets will open for those that can audit and implement controls to meet such requirements as well as cooperatives and not-for-profit entities that allow smaller districts to establish a reasonable level of security.

The second finding was that IATs need a strategy that allows them to engage in appropriate staffing and funding. Participants often indicated that the role of the IAT is to inform organizational leaders of the state of information security and recommend goals for appropriate advancement of the program. By telling organizational leaders, they are made aware of the current state of information security and become accountable for the decisions made about enacting or ignoring the IATs recommendations. This finding means the IAT will have to develop skill in informing the leadership of quantifiable risks and make reasonable, documented recommendations for staffing and funding to avert those risks while keeping a balanced view of the organizational goals about those risks.

The third finding was that IATs need to employ strategies that foster a culture of security. Participants suggested that ensuring staff understands that security is not just the job of the IAT, but everyone in the organization is critically important. Doing so results in less overall tactical work for the IAT — thus finding three means that IATs need to engage in constant training and communication with the user population and senior leadership. This training and communication must not only convey how to perform tasks securely but how to effectively avoid situations that create additional work burden on constricted resources. Many suggested actively employing gamification and other learning and teaching techniques to ensure that those who may otherwise not demonstrate a great deal of interest in the subject of information security stay engaged. This culture of information security will be a challenging necessity for K-12 IATs in that information security will likely be a small team or even an ancillary duty of an employee. However, the very task that would aid that constrained resource, education to facilitate a security culture, is itself time-consuming and will require the support of senior leadership according to participants. The IAT may have to look for outsourced or augmented methods of accomplishing this work in some cases.

The fourth finding was that IATs in K-12 education need to employ a strategy of selecting and implementing a security framework. Participants recommended the use of a framework such as those offered by NIST of CIS as a critical strategy to measure the current state of information security as well as aid in setting a future direction for the information security program. Participants suggested that they may be bound to more than one framework but use a matrix to ensure that controls map to frameworks and legal obligations. Of significance to the K-12 IAT is the use of a framework that gives them the ability to leverage a generally accepted standard for information security practices. This strategy provides the IAT with the

ability to impress upon all stakeholders the importance of information security but also to benchmark the organization against the frameworks to recommended practices.

The need to augment information security teams internally and externally is the fifth strategy that emerged from the study for K-12 IATs to follow. Participants in many organizations suggested that tasks that may be security related but can follow a simple remediation process could be moved to teams such as desktop support, freeing the IAT to focus on more strategic security goals that can have a more substantial and more lasting impact. Participants also suggested finding ways to leverage managed security services offered by third parties that can handle the proactive monitoring and filtering of security events. Implications for the K-12 IAT are that tools, such as a reliable anti-virus platform, must be selected that allow technical but non-security professionals to remediate more basic issues. Also, IATs may need to campaign for an increase in operational expense budgets to allow for the use of managed security services as opposed to direct labor. Finally, IATs must examine policy structures that allow for third parties to access sensitive data and for support staff to reimage machines after the failure of early remediation efforts.

Engaging auditors to tell the story of the state of the information security program was the final identified strategy. The participants recommended that IATs make use of auditing to examine the information security program from an impartial perspective. While districts make use of auditors in the preparation of financial statements, participants recommend that audits expand to examine the controls in information security. The engagement of auditors allows the IAT to leverage another professional opinion to influence senior leadership of the direction of the program. Engaging auditors require that the IAT is familiar with what controls are in place, and

how effective those controls are in comparison to the intended information security maturity and posture of the organization.

A limitation to consider is that of the school district, and subsequently, IT department size. Smaller IT departments may have no staff to dedicate to information security. IATs in those scenarios should look to leverage educational service districts, or examine the possibility of leveraging intergovernmental agreements to pool and share resources. Additionally, smaller districts can look to transfer risk to managed service providers to host sensitive data and manage the systems that house such data. Leveraging state and federal resources for information security can also help smaller districts achieve parity with larger ones.

Implications of Study and Recommendations for Future Research

The lived experiences of IATs in fields other than K-12 education in this study demonstrate that there are strategies in use at other organizations that are necessary to improve information security in a school district. A link is possible between the ability to improve information security in the organization where the participant is employed, and the presence of these strategies. The participants also clearly outlined the need for the continual effort to reaffirm the existence and use of these strategies in their organizations. The compliance with laws, promoting awareness of security and its importance, the use of roadmaps to guide the organization on multi-year change efforts so that information security can improve at a pace the organization can absorb, and others suggest that security must be a continual operational and strategic practice, not a one-time project.

The findings of this qualitative exploratory study contribute to the body of knowledge by answering the question: What are the strategies that IATs need to improve information security in a K-12 school district. The study's findings fill gaps in the knowledge of the field of information security, information technology, and in K-12 school district leadership. The study's

findings are particularly valuable to districts struggling with new and increasing stakeholder demands for student privacy. Also, the findings from the study can aid in helping school districts begin to align investments in information security with the organizational changes necessary to make such investments demonstrate return in the form of improved levels of information security for their organizations. The strategies identified are the building blocks for an information security program. Participants stated that the use of the strategies in their organizations and conveyed their importance the strategies play in improving information security.

A recommendation for future research is a case study in which the recommended strategies are put into place in a K-12 district with an assessment of the information security program efficacy done before and afterward. This assessment can be using the subjective assessment that Nyachwaya (2013) used in previous studies. By performing this study, a researcher can prove the ability of the identified strategies to improve information security in a K-12 district. Such a study may have different results depending on the size of the district, so this could have variations depending upon the size of the district. This study could act as a research basis for the creation of a prescriptive law or set of laws to enforce K-12 information security.

Another recommendation is to conduct a future study in which the researcher identifies another industry with information security practices that are relatively unmandated similar K-12 education and applying the same strategies in that industry. Doing so will demonstrate the transferability of these strategies not only to K-12 education but to all industries with nascent information security practices. Similarly, a before and after study of information security program efficacy could also be conducted to measure the degree of improvement such an application of strategies produces. This analysis could result in a series of recommendations that

apply to all industries lacking regulation but with sensitive information assets that need protection.

A final recommendation for a possible future study would be to identify organizations within K-12 education with highly effective information security programs and via qualitative interviews, determine if such strategies exist within those organizations and if there is any variation from the strategies identified by this study. This recommendation will be able to identify highly effective information security programs and perform analysis of their strategies to determine if there is anything exclusive to K-12 information security that would not have been gathered by interviewing the IATs from other industries. The result would be even more robust recommendations for the improvement of K-12 information security.

Recommendation 1

Recommendation one is to begin the development of an industry norm for information security practices in K-12 districts. Smaller districts may have trouble living up to the standards established in this norm which could lead to non-profit co-operatives, intergovernmental agreements for multiple districts to fund staff members or private companies that specialize in K-12 information security. By establishing the norm, moving the industry towards compliance with it, and establishing mechanisms so that districts of all sizes could comply, these norms could form the basis of prescriptive laws which demand the protection of K-12 information assets.

Recommendation 2

State Departments of Education should establish a self-assessment questionnaire similar to that used by the PCI-DSS for organizations to annually assess and report on their information protection capabilities. These departments should report on this data in much the same way they do with other school district organizational metrics. In doing so, stakeholders become informed of the level of information security provided to them. Additionally, this recommendation would

hold district leaders publicly accountable for the level of information security they offer and force them to be on record for the choices they make with both student and business data. Constituents can monitor this score and petition to speak during public testimony about their demand for appropriate levels of security in their district.

Recommendation 3

Recommendation three is to create requirements for information security training in coursework for school administrators such as the university level masters programs required to obtain the license required for principals. Since it is rare that a school district superintendent was not a principal first, this will aid in creating a top-level awareness of information security. Further, since all principals in the system will receive this training, it will foster a culture of security by creating a mid-level awareness. Those principals can then influence compliance and mentor those above them without the information security training as well as hold their teaching staff accountable for the privacy implications of educational applications they opt to use in the classroom.

Recommendation 4

IATs in K-12 information security should stay abreast of the information being published by existing advocacy groups with an emerging information security focus. Groups such as the Council of School Networking and the Council of the Great City Schools offer research on peer districts and basic, high-level steps to improve and promote information security, and statistical data. Through these groups, IATs can be in contact with other IATs to discuss resource sharing, and tools and techniques specific to K-12 that can improve the level of security. Information learned from these groups can be used in improving the information security posture of the organization as well as advocating for funding to improve information security maturity.

Other groups such as the multi-state information sharing and analysis center (MS-ISAC) can give free threat intelligence and access to a wealth of no or low-cost resources that are for the exclusive use of U.S. state, local, territorial and tribal governmental agencies. MS-ISAC also offers low-cost services such as network monitoring, consulting, and managed security services. By leveraging these, the IAT and effectively augment the capabilities of their information security team.

Recommendation 5

K-12 school districts should begin an evaluation of the information technology department budgetary requirements. This budget analysis should involve a zero-based budgeting approach, evaluating the requirements, and associating a cost for each department activity and contract until all requirements are determined and communicated to leadership. In doing so, K-12 leadership can receive a cost for information technology activates that include security and if they are unwilling or unable to fund at the requested level, be given choices as to which initiatives do or do not get funded. Following this recommendation, the annual budget will contain the design for appropriate information security measures, or leaders have to make the conscious choice to accept the risk of not doing so.

Recommendation 6

School districts, either on their own or through some of the resource sharing methods described in recommendation 1, should begin the use of annual audits to discover holes in the organization's information security capabilities. After discovering those deficiencies, the auditor, working together with the IATs responsible for the district should jointly develop a plan for remediating those findings that is specific, measurable, achievable, reasonable and timely (SMART). District funding and priorities need to support achieving that remediation plan, or

alterations must be approved and made and to give new timelines for when milestones are achievable.

Recommendation 7

School districts receiving federal E-rate funding are required to be providing students with training in digital citizenship, which involves positive engagement in with digital technologies. A recommendation from this study is that training for the adults in the K-12 district for information security awareness is carried out via that same office responsible for digital citizenship education. IAT's can place focus during cybersecurity awareness month in October of each year. By ensuring the education of both students and staff in secure ways to access and use information, information security incidents can be lessened, leaving more room for IATs to work on improving overall information security posture and maturity for the organization.

Recommendation 8

School districts respond to the voiced concerns of their constituents. Due to public transparency rules, school board meetings are often open to the public, and most have the opportunity to address the board as a concerned citizen. Constituents with a concern regarding K-12 information security should request time to address the board either publicly during meetings or privately by meeting with their board member. While a district cannot be transparent about the controls that are in place, a high-level accounting of the information security efforts or redacted copies of security audits could be made public to drive the organization towards resolving long-term information security deficiencies.

Recommendation 9

The instrument in this study intentionally steered away from topics involving privacy because organizations can have information security without privacy, but organizations cannot have privacy without information security. The two are closely related, and a goal for

information security in a K-12 district is to preserve student data privacy. A recommendation for further study is to examine the mechanisms IATs employ to ensure the privacy of student data and transparency of whom confidential student data sharing takes place with and for what reason. While those responsible for privacy may exist outside of IT, ensuring privacy is not possible without the IAT.

REFERENCES

Abramson, J., Dawson, M., & Omar, M. (2015). Understanding the methods behind cyber terrorism. In *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1539-1549). IGI Global.

Adams, H., McBride, L. L., & Moskalski, M. D. (2015). Access to Information: Perspectives of a Superintendent and a School Board Member. *Knowledge Quest*, *44*(1), 49-53.

Adams, H. R. (2016). Choose privacy week educate your students (and yourself) about privacy. *Knowledge Quest*, *44*(4), 30-33.

Ahluwalia, P., Koong, K. S., & Sun, J. (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems, 111*(4), 570-588.

Ahmad, A., Chang, S., Lim, J. S., & Maynard, S. B. (2010, July). Embedding information security culture emerging concerns and challenges. In *PACIS* (p. 43).

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 357-370.

Ahn, J., Bivona, L. K., & DiScala, J. (2011). Social media access in K-12 schools: Intractable policy controversies in an evolving world. *Proceedings of the Association for Information Science and Technology*, *48*(1), 1-10.

Ajredini, A., Ebibi, M., Fetaji, M., & Fetaji, B. (2013, June). Devising a model of electronic School Management System based on web services for secondary schools in Macedonia. In *Proceedings of the ITI 2013 35th International Conference on Information Technology Interfaces* (pp. 187-192). IEEE.

Akcaoglu, M., Hamilton, E., & Rosenberg, J. (2016). The Substitution Augmentation Modification Redefinition (SAMR) Model: A critical review and suggestions for its use. *Techtrends: Linking Research & Practice to Improve Learning*, *60*(5), 433-441.

Akeju, O., Aghili, S., & Butakov, S. (2018). Main factors and good practices for managing BYOD and IoT risks in a K-12 environment. *International Journal of Internet of Things and Cyber-Assurance*, *1*(1), 22-39.

Alabri, S. S., & Hilal, A. H. (2013). Using NVivo for data analysis in qualitative research. *International Interdisciplinary Journal of Education*, *2*(2), 181-186.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476-490.

Allen, L. E. (2008). Where good ERP implementations go bad: A case for continuity. *Business Process Management Journal*, *14*(3), 327-337.

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, *3*(3), 176-183.

Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. Journal of Management Information Systems, 34(4), 1082-1112.

Anderson, E. E., & Choobineh, J. (2008). Enterprise information security strategies. *Computers & Security*, *27*(1-2), 22-29.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610-613.

Archambault, L., Bender, S., & Kennedy, K. (2013). Cyber-Truancy: Addressing issues of attendance in the Digital Age. *Journal of Research on Technology In Education*, *46*(1), 1-28.

Arlitsch, K., & Askey, D. (2015). Heeding the Signals: Applying web best practices when Google recommends. *Journal of Library Administration*, *55*(1), 49-59.

Armarego, J., Garba, A. B., Kenworthy, W., & Murray, D. (2015). Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. *Journal of Information privacy and security*, *11*(1), 38-54.

Asen, R., Conners, P., Gumm, E., Gurke, D., & Solomon, R. (2013). Research evidence and school board deliberations: Lessons from three Wisconsin school districts. *Educational Policy*, *27*(1), 33-63.

Aukerman, R. A., & Oh, J. (2013). Freedom of speech and censorship in the internet. *International Journal of Management & Information Systems (Online), 17*(4), 251.

Aurigemma, S., & Panko, R. (2012, January). A composite framework for behavioral compliance with information security policies. In *2012 45th Hawaii International Conference on System Sciences* (pp. 3248-3257). IEEE.

Austin, Z., & Sutton, J. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian journal of hospital pharmacy*, *68*(3), 226.

Baker, B. D., Farrie, D., & Sciarra, D. G. (2014). Is school funding fair? A national report card. *Education Law Center*.

Barki, H., & Spears, J. L. (2010). User participation in information systems security risk management. *MIS quarterly*, 503-522.

Barrett, M., Mayan, M., Morse, J. M., Olson, K., & Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International journal of qualitative methods*, *1*(2), 13-22.

Baskerville, R., Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., & Warkentin, M. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101.

Batch, K. R. (2014). *Fencing Out Knowledge: Impacts of the Children's Internet Protection Act 10 Years Later*. Office for Information Technology Policy, American Library Association.

Batch, K. R., Luhtala, M., & Magi, T. (2015). Filtering beyond CIPA: Consequences of and Alternatives to overfiltering in Schools. *Knowledge Quest*, *44*(1), 60-66.

Behara, R. S., & Huang, C. D. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics*, *141*(1), 255-268.

Bell, E., & Bryman, A. (2015). *Business research methods*. Oxford University Press, USA.

Bennett, A., & Brower, A. (2001). 'That's not what FERPA Says!': The Tenth Circuit Court gives dangerous breadth to FERPA in its confusing and contradictory Falvo V. Owasso Independent School District decision. *Brigham Young University Education & Law Journal*, *2001*(2), 327.

Berg, B. L., & Lune, H. (2004). *Qualitative research methods for the social sciences* (Vol. 5). Boston, MA: Pearson

Bernard, J., Burke, B. L., Cole, S. L., Dharmar, M., Hall-Barrow, J., McSwain, S. D., … & Yeager, B. (2017). American Telemedicine Association operating procedures for pediatric telehealth. *Telemedicine and e-Health*, *23*(9), 699-706.

Bernik, I. (2014). Cybercrime: The cost of investments into protection. *Varstvoslovje: Journal of Criminal Justice & Security*, *16*(2), 105-116.

Birt, L., Cavers, D., Campbell, C., Scott, S., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation?. *Qualitative Health Research*, *26*(13), 1802-1811.

Bloch, R., Issa, H., & Peterson, A. (2015). The DATA act. *The CPA Journal, 85*(6), 36-42.

Borg, W. R., Gall, J. P., & Gall, M. D. (2007). Educational research: An introduction' eighth edition Boston: Pearson Education.

Boser, U., & Levenson, N. (2014). *The promise of education information systems* [Ebook]. The Center for American Progress District Management Council. Retrieved from https://files.eric.ed.gov/fulltext/ED561090.pdf

Braunschweiger, P., & Goodman, K. W. (2007). The CITI program: An international online resource for education in human subjects protection and the responsible conduct of research. *Academic Medicine*, *82*(9), 861-864.

Brecht, M., & Nowey, T. (2013). A closer look at information security costs. In *The Economics of Information Security and Privacy* (pp. 3-24). Springer, Berlin, Heidelberg.

Brinkmann, S. (2014). Interview. In *Encyclopedia of critical psychology* (pp. 1008-1010). Springer New York.

Brown, B. R. (2016). *Measuring the level of security in the K-12 IT environment in southern California* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10125690).

Brown, D. H., Lo Iacono, V., & Symonds, P. (2016). Skype as a tool for qualitative research interviews. *Sociological Research Online*, *21*(2), 1-15.

Burns, A. J., Lowry, P. B., Posey, C., & Roberts, T. L. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209.

Butavicius, M., Jerram, C., McCormac, A., Parsons, K., & Pattinson, M. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, 165-176.Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, *2013*(7), 5-10.

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, *2013*(7), 5-10.

Campbell, C. (2017). *Exploring future solutions to counter social engineering attacks: A Delphi study* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10285134).

Cannistraci, L. (2011). The value of instructional technology in a K-12 district. *Distance Learning, 8*(1), 9-16. Retrieved from ProQuest.

Cardon, P., Fontenot, R., Marshall, B., & Poddar, A. (2013). Does sample size matter in qualitative research?: A review of qualitative interviews in IS research. *The Journal of Computer Information Systems, 54*(1), 11-22.

Carruthers, L., & Kay, R. (2017). Examining school board leaders' use of online resources to inform decision-making. *Canadian Journal of Learning & Technology*, *43*(1), 1-25.

Carter, A., Harnett, K., & McCarthy, C. (2014). *A summary of cybersecurity best practices* (No. DOT HS 812 075).

Case, A. (2016). *Major general fund expenditures impact on student achievement* (Order No. 10242409). (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (1865331082)

Casey, D., Houghton, C., Murphy, K., & Shaw, D. (2013). Rigour in qualitative case-study research. *Nurse researcher*, *20*(4).

Casey, P., Dunlap, K., & Starrett, T. M. (2014). Superintendent response to the financial downturn. *Journal of Education and Learning*, *3*(1), 34-39.

Chenail, R. J. (2011). Interviewing the investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research. *The qualitative report*, *16*(1), 255-262.

Cherdantseva, Y., & Hilton, J. (2013, September). A reference model of information assurance & security. In *Availability, reliability and security (ares), 2013 eighth international conference on* (pp. 546-555). IEEE.

Children's Online Privacy Protection Act (COPPA). (1998). 16 CFR § 312

Choraś, M., Churchill, A., Kozik, R., & Yautsiukhin, A. (2016). Are we doing all the right things to counter cybercrime?. In *Combatting Cybercrime and Cyberterrorism* (pp. 279-294). Springer, Cham.

Cooke, D., Dinev, T., Hart, P., & Hu, Q. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

Corti, L., Backhouse, G., & Day, A. (2000, December). Confidentiality and informed consent: Issues for consideration in the preservation of and provision of access to qualitative data archives. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 1, No. 3).

Counsel of Greater City Schools. (2017). *Managing for results in America's Great City Schools* [Ebook]. Retrieved from https://www.cgcs.org/cms/lib/DC00001581/Centricity/Domain/87/Managing%20for%20Results%202015.pdf

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, *28*(5), 1849-1858.

Creswell, J. W. (1996). Research design. *Qualitative and Quantitative Approach. Thousand Oaks: SagePublications*.

Creswell, J. W. (2009). Research design, Qualitative, Quantitative, and Mixing Approaches.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *Mis Quarterly*, 673-687.

Cutcliffe, J. R., & McKenna, H. P. (1999). Establishing the credibility of qualitative research findings: The plot thickens. *Journal of advanced nursing*, *30*(2), 374-380.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196-207.

Davidson, C. (2009). Transcription: Imperatives for qualitative research. *International Journal of Qualitative Methods*, *8*(2), 35-52.

Davies, R. S., & West, R. E. (2014). Technology integration in schools. In *Handbook of research on educational communications and technology* (pp. 841-853). Springer, New York, NY.

De Brey, C., Dillow, S. A., & Snyder, T. D. (2018). Digest of Education Statistics 2017, NCES 2017-094. *National Center for Education Statistics*.

Dennen, V. P. (2015). Technology transience and learner data. *Quarterly Review of Distance Education*, *16*(2), 45-60.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2011). *The SAGE handbook of qualitative research*. Sage.

Derksen, B., Huang, Z., Luftman, J., Rigoni, E. H., Santana, M., & Zadeh, H. S. (2013). Key information technology and management issues 2012-2013: An international study. *Journal of Information Technology, 28*(4), 354-366.

Dey, I. (2003). *Qualitative data analysis: A user friendly guide for social scientists*. Routledge.

Dogra, N., Giordano, J., O'Reilly, M., & Taylor, H. (2007). Confidentiality and autonomy: The challenge (s) of offering research participants a choice of disclosing their identity. *Qualitative health research*, *17*(2), 264-275.

Dorata, N. T., & Phillips, C. R. (2013). School district boards, audit committees, and budget oversight. *CPA Journal*, *83*(3), 18-23.

Dorsey-Lockett, K. (2014). *Examining the correlation between organizational security climate and demographic variables and the self-efficacy of information security of local government employees: A quantitative study* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3614238)

Drago, W., & Geisler, E. (1997). Business process re-engineering: Lessons from the past. *Industrial Management & Data Systems, 97*(8), 297-303.

Edmondson, A. C., & McManus, S. E. (2007). Methodological fit in management field research. *Academy of management review*, *32*(4), 1246-1264.

Edwards, K. (2015). *Examining the security awareness, information privacy, and the security behaviors of home computer users* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10029813)

Edwards, M. M. (2018). *Identifying factors contributing towards information security maturity in an organization*. Available from ProQuest Dissertations & Theses Global. (Order No. 10746212).

Eichensehr, K. E. (2017). Public-Private Cybersecurity. *Texas Law Review*, *95*(3), 467-538.

Ekelhart, A., Grill, B., Kiesling, E., Strauss, C., & Stummer, C. (2016). Selecting security control portfolios: A multi-objective simulation-optimization approach. *EURO Journal on Decision Processes, 4*(1-2), 85-117.

Ely, T. L., & Fermanich, M. L. (2013). Learning to count: School finance formula count methods and attendance-related student outcomes. *Journal of Education Finance*, *38*(4), 343-369.

Family Educational Rights and Privacy Act (FERPA). (1974). 20 U.S.C. § 1232g

Federal Bureau of Investigation. (2018). *Education technologies: Data collection and unsecured systems could pose risks to students*. Retrieved from https://www.ic3.gov/media/2018/180913.aspx

Flick, U. (2004). Triangulation in qualitative research. *A companion to qualitative research*, *3*, 178-183.

Francois, M. T. (2016). *A quantitative study on the relationship of information security policy awareness, enforcement, and maintenance to information security program effectiveness* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10252444).

GIAC Advisory Board. (n.d.). Retrieved from https://www.giac.org/certified-professionals/advisory-board

Gibbs, G. R. (2008). *Analysing qualitative data*. Sage.

Gleason, B., & von Gillern, S. (2018). Digital citizenship with social media: Participatory practices of teaching and learning in secondary education. *Journal of Educational Technology & Society*, *21*(1), 200-212.

Goes, J., & Simon, M. K. (2013). Assumption, limitations, delimitations, and scope of the study.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report*, *8*(4), 597-606

Goldberg, K., & Sheikh, K. A. (2014). Schools and digital education technologies. *NJ Law.*, 23.

Goldsborough, R. (2017). The increasing threat of ransomware. *Teacher Librarian*, *45*(1), 61.

Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse education today*, *24*(2), 105-112.

Grover, L., Jette, D. U., & Keck, C. P. (2003). A qualitative study of clinical decision making in recommending discharge placement from the acute care setting. *Physical Therapy*, *83*(3), 224-236.

Guba, E. G., & Lincoln, Y. S. (1986). But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New directions for program evaluation*, *1986*(30), 73-84.

Guest, G., Mack, N., MacQueen, K. M., Namey, E., & Woodsong, C. (2005). Qualitative research methods: A data collectors field guide.

Gupta, B. B., Jain, A. K., & Tewari, A. (2016). Recent survey of various defense mechanisms against phishing attacks. *Journal of Information Privacy & Security, 12*(1), 3-13.

Hambright, G., & Diamantes, T. (2004). Definitions, benefits, and barriers of K-12 educational strategic planning. *Journal of Instructional Psychology*, *31*(3), 233–239.

Hamel, C., Laferrière, T., & Searson, M. (2013). Barriers to successful implementation of technology integration in educational settings: A case study. *Journal of Computer Assisted Learning*, *29*(5), 463-473.

Hartzog, W., & Solove, D. (2014). *The FTC and privacy and security duties for the cloud*. GWU Law School. Retrieved from https://ssrn.com/abstract=2424998

Harvey, L. (2015). Beyond member-checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education*, *38*(1), 23-38.

Hechter, R. P., & Vermette, L. A. (2013). Technology integration in K-12 science classrooms: An analysis of barriers and implications. *Themes in Science and Technology Education*, *6*(2), 73-90.

Henry, G. T. (1990). *Practical sampling* (Vol. 21). Sage.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Hightower, R. T., Lowry, P. B., Posey, C., & Roberts, T. L. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & management*, *51*(5), 551-567.

Hild, K. A. (2017). *Leave me alone: Protecting children's privacy in the digital age* (Order No. 10274455). Available from ProQuest Dissertations & Theses Global. (1897514225)

Hill, P. T. (2015). States could do more for rural education. *Uncovering the productivity promise of rural education*, *4*.

Ho, C., & Schmidt, M. (2013, October). It doesn't “just work”: Lessons learned from a mass deployment of iPad tablets pilot project. In *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education* (pp. 959-967). Association for the Advancement of Computing in Education (AACE).

Holcomb, C. (2015). Navigating student data privacy laws. *Risk Management*, *62*(7), 14.

Holland, S. E. (2016). Making the grade five tips for school district audits. *The CPA Journal, 86*(4), 36-37.

Hong, J., & Hua, Y. (2018, March). Research on network defense strategy based on honey pot technology. In *IOP Conference Series: Materials Science and Engineering* (Vol. 322, No. 5, p. 052033). IOP Publishing.

Huberman, A. M., & Miles, M. B. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69-79.

Jabareen, Y. (2009). Building a conceptual framework: philosophy, definitions, and procedure. *International Journal of qualitative methods*, *8*(4), 49-62.

Jackson, C. S. (2017). *Cybersecurity policy: Exploring leadership strategies that influence insider compliance.* Available from ProQuest Dissertations & Theses Global. (Order No. 10623113).

Jauregui, E. (2015). *Analyzing corporate cyber security best practices* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 1587608).

Ji, Y., Liu, D., & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support Systems*, *52*(1), 95-107.

Johnson, D. P. (2017). *How attitude toward the behavior, subjective norm, and perceived behavioral control affects information security behavior intention.* Walden University. Retrieved from http://scholarworks.waldenu.edu/dissertations

Julious, S. A. (2005). Sample size of 12 per group rule of thumb for a pilot study. *Pharmaceutical Statistics: The Journal of Applied Statistics in the Pharmaceutical Industry*, *4*(4), 287-291.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International journal of information management*, *23*(2), 139-154.

Kaplan, B., & Maxwell, J. A. (2005). Qualitative research methods for evaluating computer information systems. In *Evaluating the organizational impact of healthcare information systems* (pp. 30-55). Springer, New York, NY.

Kirby, S. (2018). Legal requirements of notification of breaches: An overview. *ISSA Journal*, *16*(2), 29-34.

Kongnso, F. J. (2015). *Best practices to minimize data security breaches for increased business performance* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3739769).

Kovács, L., Nemeslaki, A., Orbók, A., & Szabó, A. (2017). Structuration theory and strategic alignment in information security management: Introduction of a comprehensive research approach and program1. *AARMS*, 5.

Krisby, R. M. (2018). Health care held ransom: modifications to data breach security & the future of health care privacy protection. *Health Matrix: Journal of Law-Medicine*, *28*365-401.

Krueger, K. R. (2013). 6 Tips for smart IT in 2014: From building robust networks to collaborating with other departments to fund new projects, here's what you need to do to keep innovating in the new year. *THE Journal (Technological Horizons in Education)*, *40*(12), 9.

Laboy, J., Schaffer, H. E., Stein, S., & Ware, J. (2013). Improving K-12 pedagogy via a cloud designed for education. *International Journal of Information Management*, *33*(1), 235-241.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), 4-13.

Lacey, D., & Stewart, G. (2012). Death by a thousand facts. *Information Management & Computer Security, 20*(1), 29-38.

Lancaster, S., & Topper, A. (2013). Common challenges and experiences of school districts that are implementing one-to-one computing initiatives. *Computers in the Schools*, *30*(4), 346-358.

Law, R. (2004). From research topic to research question: A challenging process. *Nurse Researcher*, *11*(4), 54-66.

Leachman, M., & Mai, C. (2014). Most states still funding schools less than before the recession. *Center on Budget and Policy Priorities*, *16*.

Lee, A. S., & Markus, M. L. (1999). Special issue on intensive research in information systems: Using qualitative, interpretive, and case methods to study Information Technology: Foreward. *MIS quarterly*, 35-38.

Leech, N. L., & Onwuegbuzie, A. J. (2007). Validity and qualitative research: An oxymoron? *Quality and Quantity, 41*(2), 233-249. doi:http://dx.doi.org.proxy.cecybrary.com/10.1007/s11135-006-9000-3

Lestch, C. (2015). Cybersecurity in K-12 education: Schools face increased risk of cyber attacks. *Retrieved from http://fedscoop. com/cybersecurity-in-k-12-education-schools-around-the-country-face-risk-of-cyber-attacks*.

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of family medicine and primary care*, *4*(3), 324.

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice*, *16*(4), 473-475.

Lowenstein, H. (2016). The great wall of FERPA: Surmounting a law's barrier to assurance of learning. *Journal of Legal Studies Education*, *33*(1), 129-164.

Lucas, M. L. (2018). *Exploring the strategies cybersecurity managers recommend for implementing or transitioning to the cloud.* Available from ProQuest Dissertations & Theses Global. (Order No. 10843999).

Mader, J., & Smith, B. (2014). Protecting students' online privacy--By law. *Science Teacher*, *81*(9), 8.

Madison, J. J. (2017). *Challenges with funding of information security projects per threat perceptions: A qualitative case study* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10256844).

Mahmood, M. A., Pahnila, S., & Siponen, M. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), 217-224.

Manadhata, P. K., & Wing, J. M. (2011). An attack surface metric. *IEEE Transactions on Software Engineering*, *37*(3), 371-386.

Mason, J. (2002). *Qualitative researching*. Sage.

Mason, M. (2010, August). Sample size and saturation in PhD studies using qualitative interviews. In *Forum qualitative Sozialforschung/Forum: qualitative social research* (Vol. 11, No. 3).

Mattord, H. J., & Whitman, M. E. (2011). *Principles of information security*. Cengage Learning.

Maxwell, J. A. (2012). *Qualitative research design: An interactive approach* (Vol. 41). Sage publications.

Mayeh, M., Mishra, A., & Ramayah, T. (2016). The role of absorptive capacity, communication and trust in ERP adoption. *Journal of Systems and Software*, *119*, 58-69.

Mayes, R., Natividad, G., & Spector, J. M. (2015). Challenges for educational technologists in the 21st century. *Education Sciences*, *5*(3), 221-237.

McClain, D. J. (2016). *Building an effective IT decision-making structure in K–12 education* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10125140).

McLaughlin, K. L. (2011). Cyber attack! Is a counter attack warranted? *Information Security Journal: A Global Perspective*, *20*(1), 58-64.

Mehra, B. (2002). Bias in qualitative research: Voices from an online classroom. *The Qualitative Report*, *7*(1), 1-19.

Menuey, B. P. (2009). CIPA: A brief history. *Computers in the Schools*, *26*(1), 40-47.

Michael, S. O. (1998). Best practices in information technology (IT) management: Insights from K-12 schools' technology audits. *International Journal of Educational Management*, *12*(6), 277-288.

Mitnick, K. D. (2003). Best practice: Are you the weak link?. *Harvard Business Review*, *81*(4), 18-18.

Morrow, S. L. (2005). Quality and trustworthiness in qualitative research in counseling psychology. *Journal of counseling psychology*, *52*(2), 250.

Moules, N. J., Norris, J. M., Nowell, L. S., & White, D. E. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*(1), 1609406917733847.

Myers, M. D. (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, *21*(2), 241-242.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2-26.

Niekerk, J. F., & Solms, R. (2010, September). Research Methodologies in Information Security research: The road ahead. In *25th IFIP TC 11 International Information Security Conference (SEC)/Held as Part of World Computer Congress (WCC)* (pp. 215-216). Springer.

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems, 26*(1), 1-20.

NIST800-53r4. (2013). National Institute of Standards and Technology. Special Publication on security and privacy controls for Federal information systems and organizations. U.S. Dept. of Commerce.

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, ebnurs-2015.

NVivo. (n.d.). Retrieved from https://www.qsrinternational.com/nvivo/nvivo-products

Nyachwaya, S. (2013). Information Security Management Practices of K-12 School Districts. *ProQuest LLC*.

Okoye, S. I. (2017). *Strategies to minimize the effects of information security threats on business performance* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10606454).

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. *Pew Research Center*, *26*.

O'Neill, O. (2003). Some limits of informed consent. *Journal of medical ethics*, *29*(1), 4-7.

Overly, M. R. (2018). Is California's consumer privacy act of 2018 going to be GDPR version 2? *CSO (Online)*

Palmer, D. S. (2017). *A look into the planning processes of bring your own device programs in K-12 schools.* Available from ProQuest Dissertations & Theses Global. (Order No. 10666724).

Park, S., & Ruighaver, T. (2008, January). Strategic approach to information security in organizations. In *Information Science and Security, 2008. ICISS. International Conference on* (pp. 26-31). IEEE.

Parylo, O. (2012). Qualitative, quantitative, or mixed methods: An analysis of research design in articles on principal professional development (1998–2008). *International Journal of Multiple Research Approaches*, *6*(3), 297-313.

Pathari, V., & Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security, 20*(4), 264-280.

Pavlou, P. A., & El Sawy, O. A. (2010). The "third hand": IT-enabled competitive advantage in turbulence through improvisational capabilities. *Information systems research*, *21*(3), 443-471.

Peterson, D. (2016). Edtech and student privacy: California law as a model. *Berkeley Technology Law Journal*, *31*961-995.

Poggenpoel, M., & Myburgh, C. (2003). The researcher as research instrument in educational research: a possible threat to trustworthiness? *Education*, *124*(2).

Priest, H., Roberts, P., & Woods, L. (2002). An overview of three different approaches to the interpretation of qualitative data. Part 1: Theoretical issues. *Nurse Researcher (through 2013)*, *10*(1), 43.

Pusey, P., & Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education*, *28*(2), 82-85.

Pye, K. (2016). *Teaching cybersecurity in K-12 schools* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10155676)

Ramos, M. C. (1989). Some ethical implications of qualitative research. *Research in Nursing & Health*, *12*(1), 57-63.

Renaud, K. (2016). How smaller businesses struggle with security advice. *Computer Fraud & Security*, *2016*(8), 10-18.

Rodewald, G. (2005, September). Aligning information security investments with a firm's risk tolerance. In *Proceedings of the 2nd annual conference on Information security curriculum development* (pp. 139-141). ACM.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93-114.

Ryan, F., Coughlan, M., & Cronin, P. (2009). Interviewing in qualitative research: The one-to-one interview. *International Journal of Therapy and Rehabilitation*, *16*(6), 309-314.

Ryan, J. J., & Ryan, D. J. (2006). Expected benefits of information security investments. *Computers & Security*, *25*(8), 579-588.

Saldana, J. (2011). *Fundamentals of qualitative research*. OUP USA.

Sales, B. D., & Folkman, S. E. (2000). *Ethics in research with human participants*. American Psychological Association.

Sandhursen, R. L. (2000). Marketing (3rd Ed). New York, New York: Barron's Business Review Books.

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age*. Crown.

Sarantakos, S. (2012). *Social research*. Macmillan International Higher Education.

Sarbanes, P. (2002, July). Sarbanes-Oxley act of 2002. In *The Public Company Accounting Reform and Investor Protection Act. Washington DC: US Congress*.

Schwarz, C. C. (2017). Are student-athletes alleged of sex-crimes granted educational privacy protections? FERPA's misinterpretation by academic institutions. *Ohio State Journal of Criminal Law*, *14*(2), 809-829.

Seale, C. (1998). Qualitative interviewing. *Researching society and culture*, 202-216.

Shear, B. (2015). Ed tech must embrace stronger student privacy laws. *THE Journal (Technological Horizons In Education)*, *42*(3), 6.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information*, *22*(2), 63-75.

Sims, J. M. (2010). A brief review of the Belmont report. *Dimensions of critical care nursing*, *29*(4), 173-174.

Singh, K. D. (2015). Creating your own qualitative research approach: Selecting, integrating and operationalizing philosophy, methodology and methods. *Vision*, *19*(2), 132-146.

Smedinghoff, T. J. (2005). Trends in the law of information security. *Intellectual Property & Technology Law Journal*, *17*(1), 1-5.

Smock, B. (2018). *K-12 Cybersecurity Discussion: Increasing Resilience is a Collective Responsibility*. Presentation, Orlando, FL.

Solomon, M. G., & Chapple, M. (2005). *Information security illuminated*. Jones & Bartlett Learning.

Straub, D. W., Jr. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276.

Strauss, L. J. (2016). HIPAA versus FERPA. *Journal of Health Care Compliance*, *18*(6), 37-38.

Stringer, J. (2010). Protecting K-12 students' personally identifiable information: What data is at risk and what you can do about it. *SOPHOS. Retrieved from http://www.mgcwallace.com/wp-content/uploads/sophos-protecting-personally-identifiable-information-k12-wpna.*

Stuart, S. P. (2005). A local distinction: State education privacy laws for public school children. *W. Va. L. Rev.*, *108*, 361.

Suter, W. N. (2011). *Introduction to educational research: A critical thinking approach*. SAGE publications.

Tadeja, C. (2015). *An enquiry into California school district superintendents: Their role in creating, promoting and sustaining a digital-age learning culture* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3671784).

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5-8.

Tang, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, *17*(2), 179-186.

Thaw, D. B. (2011). *Characterizing, classifying, and understanding information security laws and regulations: Considerations for policymakers and organizations protecting sensitive information assets* Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3473927).

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC medical research methodology*, *8*(1), 45.

Trainor, S. (2015). Student data privacy is cloudy today, clearer tomorrow. *Phi Delta Kappan*, *96*(5), 13-18.

Tudor, J. (2015). Legal implications of using digital technology in public schools: Effects on privacy. *JL & Educ.*, *44*, 287.

United States Department of Education. (2011). *Questions and answers for school districts and parents* [Ebook]. Washington, D.C. Retrieved from https://www2.ed.gov/about/offices/list/ocr/docs/qa-201101.pdf

Vandykgibson, J. L. (2016). *K-12 educational technology implementations: A Delphi study* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10146105).

Van Niekerk, J., & Von Solms, R. (2013). From information security to cyber security. C*omputers & Security*, *38*, 97-102.

Vicks, M. E. (2013). *An examination of internet filtering and safety policy trends and issues in South Carolina's K–12 public schools* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3588586).

Werosh, K. R. (2013). *Faculty and administrator knowledge of the family educational rights and privacy act at select U.S. complementary and alternative healthcare educational institutions* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3589259)

Whiting, L. S. (2008). Semi-structured interviews: Guidance for novice researchers. *Nursing Standard*, *22*(23).

Whittemore, R., Chase, S. K., & Mandle, C. L. (2001). Validity in qualitative research. *Qualitative health research*, *11*(4), 522-537.

Wynn, C. L. (2017). *Examining the relationship of business operations and the information security culture in the United States*. (Doctoral dissertation). Available from Retrieved from ProQuest Dissertations & Theses Global. (Order No. 10257795).

Yin, R. K. (2011). *Applications of case study research*. Sage.

Yin, R. K. (2015). *Qualitative research from start to finish*. Guilford Publications.

Zhong, L. (2017). Indicators of digital leadership in the context of K-12 education. *Journal of Educational Technology Development and Exchange (JETDE)*, *10*(1), 3.

Zhou, J. (2014, June). On the security of cloud data storage and sharing. In *Proceedings of the 2nd international workshop on Security in cloud computing* (pp. 1-2). ACM.

APPENDIX A

Informed Consent

Title of Study: The Strategies Information Assurance Technologists Need To Improve Information Security Practices In An School District

Investigator: Travis Paakki

Contact Number: []

Purpose of the Study

You are invited to participate in a research study. The purpose of this study is to explore the strategies that have been successfully employed by information assurance technologists in other industries so that those can be advocated for and brought into K-12 school districts to address acknowledged gaps in information security.

Participants

You are being asked to participate in the study because as a member of the GIAC advisory group who works at an organization with over 500 employees with an established information security program, or you were identified on LinkedIn.com as a security leader with similar organizational characteristics, you are identified as a subject matter expert. By inquiring as to your experiences with several strategy elements, a picture of which elements can be applied to and advocated for in K-12 education will emerge.

Procedures

If you volunteer to participate in this study, you will be asked to do the following: Participate in a recorded sixty minute semi-structured, thirteen question interview via WebEx with video. Additionally, you will be asked to confirm a transscript of that interview within a week of having given the interview. A key will be kept offline that associates names and organizations to subject identifiers to protect this data from a possible compromise.

Benefits of Participation

There may/may not be direct benefits to you as a participant in this study. However, we hope to learn what strategies can be employed in K-12 education to improve the information security of those organizations. As such the participants may be responsible for the passing of regualtions and guidelines

that mandate or recommend minimal staffing or funding levels to achieve the identified strategies. The end result will be a safer internet, and better protected vulnerable populations, as well as a deterrance of potential adversaries.

Risks of Participation

There are risks involved in all research studies. This study is estimated to involve minimal risk. An example of this risk is through the inadvertant release of identifying information, adversary knowledge of your defenses could become known. To mitigate this, records of your identity will only be in the hands of the researcher in a offline document. Further, information that could uniquely identify your organization will be changed into ratios and percentages to make identification unlikely.

Cost/Compensation

This will be no financial cost to you to participate in this study. The study will take sixty minutes for the initial interview and an additional sixty minutes to verify the transcript. You will not be compensated for your time aside from a $15 Starbucks gift card. *Colorado Technical University will not provide compensation or free medical care for an unanticipated injury sustained as a result of participating in this research study.*

Contact Information

If you have any questions or concerns about the study, you may contact Travis Paakki at []@student.ctuonline.edu or []. Additionally you may contact Dr. James Webb at []@coloradotech.edu. For questions regard the rights of research subjects, any complaints or comments regarding the manner in which the study is being conducted, you may contact Colorado Technical University – Doctoral Programs at [].

Voluntary Participation

Your participation in this study is voluntary. You may refuse to participate in this study or in any part of this study. You may withdraw at any time without prejudice. You are encouraged to ask questions about this study at the beginning or at any time during the research study.

Confidentiality

Recorded WebEx interviews will be stored in a Google drive account owned solely by the investigator. Written notes and transcripts will also be digitized and transferred to that same storage location. The records will be kept for a period of one year after the dissertation publication at which time the recordings will be destroyed. The transcripts will be kept as long as the researcher can protect the confidentiality of the information.

Participant Consent

I have read the above information and agree to participate in this study. I am at least 18 years of age. A copy of this form has been given to me.

_____ _____

Signature of Participant Date

_____

Participant Name (Please Print)

APPENDIX B

Original Interview Questions

1. What is your organizations annual budget?
    a. What has been your experience with budget changes of the last 3 years?
    b. What are your experiences with using these changes to benefit your security posture?
2. What is you organizations annual IT budget?
    a) Can you tell me the staff size of IT?
    b) Can you tell me the staff size of information security?
3. What is your organizations annual information security budget?
    a. Is this sufficient to meet your stakeholder expectations?
    b. How much more would be necessary to meet those expectations?
    c. Can you tell me about your experiences attempting to get additional budget to support information security?
4. Can you describe what regulations affect you and how you address those?
    a) What are your experiences with regulations or requirements that you are unsure you address the requirements of?
    b) What are your experiences with industry standards such as PCI that you must maintain compliance with?
5. Can you please describe who your stakeholders are and what are their information security expectations?
    a. What are your experiences with expectations that are not met with those stakeholders?

b. Can you describe any unrealistic expectations that you are asked to fulfill?

6. Can you describe your experiences with organizations information security posture and culture?
    a) What methods have you used to attempt to influence this? Would you describe these as successful?
    b) Can you describe your strategies for attempting to improve your information security posture and culture?
7. Can you describe your experiences with any legal gaps or overlaps that you must contend with when providing information security to your organization?
    a) What have been your experiences in addressing legal gaps?
    b) What have been your experiences in addressing legal overlaps?
8. What security frameworks or best practice frameworks do you employ?
    a) What are some of the experiences you have trying to support these frameworks?
    b) What strategies do you use to implement controls?
9. How would you describe the general IT staff level of knowledge on information security?
    a) What about the larger user population?
    b) What strategies do you use to improve this level?
10. Can you describe your experiences with external or internal auditors as they relate to information security?
    a) What has been your experiences with auditor finding remediation expectations?
    b) Can you describe a time when you had to push back on those findings?

11. What are you organizations stance on IT basics such as virus scanning, threat management gateways, and next generation firewalls?
    a) What have been your experiences in trying to implement these?
    b) How has this stance affected your organizations information security posture?
12. What have your experiences been with cloud services in regards to information security?
    a) Do you anticipate a change in your cloud posture in the next 12 months?
    b) How has this affected your security posture as an organization?
    c) Can you describe your organizations view on managed security services?
13. What are the strategies in your organization that are essential to the level of information security you provide?
    a) What strategies would you like to make use of in the future?
    b) Have there been strategies that were not effective in improving your information security posture?

APPENDIX C

Interview Questions Following Pilot Study

1. What is your organizations annual budget?
    a. What has been your experience with budget changes of the last 3 years?
    b. What are your experiences with using these changes to benefit your security posture?
2. What is you organizations annual IT budget?
    a. Can you tell me the staff size of IT?
    b. Can you tell me the staff size of information security?
3. What is your organizations annual information security budget?
    a. Is this sufficient to meet your stakeholder expectations?
    b. How much more would be necessary to meet those expectations?
    c. Can you tell me about your experiences attempting to get additional budget to support information security?
4. Can you describe what regulations affect you and how you address those?
    a. What are your experiences with regulations or requirements that you are unsure you address the requirements of?
    b. What are your experiences with industry standards such as PCI that you must maintain compliance with?
5. Can you please describe who your stakeholders are and what are their information security expectations?
    a. What are your experiences with expectations that are not met with those stakeholders?
    b. Can you describe any unrealistic expectations that you are asked to fulfill?

6. Can you describe your experiences with organizations information security posture and culture?
    a. What methods have you used to attempt to influence this? Would you describe these as successful?
    b. Can you describe your strategies for attempting to improve your information security posture and culture?
7. Can you tell me what the largest security concerns are for your organization?
    a. What concerns are more recent?
    b. What concerns are persistent over time?
8. What security frameworks or best practice frameworks do you employ?
    a. What are some of the experiences you have trying to support these frameworks?
    b. What strategies do you use to implement controls?
9. How would you describe the general IT staff level of knowledge on information security?
    a. What about the larger user population?
    b. How does this compare to the information security staff?
10. Can you describe your experiences with external or internal auditors as they relate to information security?
    a. What has been your experiences with auditor finding remediation expectations?
    b. Can you describe a time when you had to push back on audit findings?
11. What is your organizations stance on IT basics such as virus scanning, threat management gateways, and next generation firewalls?
    a. What have been your experiences in trying to implement these?

b. How has this stance affected your organizations information security posture?

12. What have your experiences been with cloud services in regards to information security?
    a. Do you anticipate a change in your cloud posture in the next 12 months?
    b. How has this affected your security posture as an organization?
13. Other than mentioned in response to the above, are there strategies in your organization that are essential to the level of information security you provide?
    a. What strategies would you like to make use of in the future?
    b. Have there been strategies that were not effective in improving your information security posture?

APPENDIX D

Interview Protocol

1. Explain the purpose of the study.
2. Assure participant confidentiality and have the participant sign the informed consent agreement form.
3. Ensure that this is still a good time and that the participant has sixty uninterrupted minutes for the interview.
4. Record the subject's number on the top of the interview field notes.
5. Encourage participants to open up about their experiences.
6. Monitor participant body language to minimize influencing subject answers.
7. Precisely record participant responses and annotate any non-verbal responses.
8. WebEx record and assign a chronological number to each interview.
9. Ask interview questions in order and ask follow-on questions for clarification (see Appendix C).

    Interview and follow-on questions:

    1. What is your organizations annual budget?
        c. What has been your experience with budget changes of the last 3 years?
        d. What are your experiences with using these changes to benefit your security posture?
    2. What is you organizations annual IT budget?
        c. Can you tell me the staff size of IT?
        d. Can you tell me the staff size of information security?

3. What is your organizations annual information security budget?
    d. Is this sufficient to meet your stakeholder expectations?
    e. How much more would be necessary to meet those expectations?
    f. Can you tell me about your experiences attempting to get additional budget to support information security?
4. Can you describe what regulations affect you and how you address those?
    c. What are your experiences with regulations or requirements that you are unsure you address the requirements of?
    d. What are your experiences with industry standards such as PCI that you must maintain compliance with?
5. Can you please describe who your stakeholders are and what are their information security expectations?
    c. What are your experiences with expectations that are not met with those stakeholders?
    d. Can you describe any unrealistic expectations that you are asked to fulfill?
6. Can you describe your experiences with organizations information security posture and culture?
    c. What methods have you used to attempt to influence this? Would you describe these as successful?
    d. Can you describe your strategies for attempting to improve your information security posture and culture?
7. Can you tell me what the largest security concerns are for your organization?
    c. What concerns are more recent?

d. What concerns are persistent over time?

8. What security frameworks or best practice frameworks do you employ?
    c. What are some of the experiences you have trying to support these frameworks?
    d. What strategies do you use to implement controls?
9. How would you describe the general IT staff level of knowledge on information security?
    c. What about the larger user population?
    d. How does this compare to the information security staff?
10. Can you describe your experiences with external or internal auditors as they relate to information security?
    c. What has been your experiences with auditor finding remediation expectations?
    d. Can you describe a time when you had to push back on audit findings?
11. What is your organizations stance on IT basics such as virus scanning, threat management gateways, and next generation firewalls?
    c. What have been your experiences in trying to implement these?
    d. How has this stance affected your organizations information security posture?
12. What have your experiences been with cloud services in regards to information security?
    c. Do you anticipate a change in your cloud posture in the next 12 months?
    d. How has this affected your security posture as an organization?
13. Other than mentioned in response to the above, are there strategies in your organization that are essential to the level of information security you provide?
    c. What strategies would you like to make use of in the future?

Have there been strategies that were not effective in improving your information security posture?

10. Thank each subject for his or her participation in the study at the end of the interview.
11. Inform participants that a transcript of their interview will be made available to them when transcription is complete, and ensure participants understand they will have a final opportunity to clarify or add to responses.