Information Security Officers Perceptions of How to Implement Successful Information Security Programs in Health Sciences Center Environments

by

Jessica Klein, B.A., M.A.

A Dissertation

In

Higher Education Administration

Submitted to the Graduate Faculty
of Texas Tech University in
Partial Fulfillment of
the Requirements for
the Degree of

DOCTOR OF EDUCATION

Approved

Dr. Stephanie J. Jones
Chair of Committee

Dr. Justin Louder

Dr. Valerie Paton

Dr. Mark Sheridan
Dean of the Graduate School

December, 2023

TABLE OF CONTENTS

ABSTRACT iv

I. INTRODUCTION 1

Purpose of the Study 9
Research Questions 9
Significance of the Study 10
Summary of Conceptual Framework 11
Summary of Methodology 12
Definition of Terms 13
Assumptions of the Study 14
Limitations to the Study 15
Summary 15
Organization of the Remainder of the Study 16

II. LITERATURE REVIEW 17

Overview of Traditional Higher Education Setting 17
Health Science Centers *21*
Overview of Information Security 23
Information Security Officer 27
Information Security Culture 30
NIST Information Security Framework 32
Information Security in a Healthcare Environment 33
Information Security in an Academic Environment 35
Information Security Compliance Behaviors and Motivations 37
Conceptual Framework of the Study 39
Summary 43

III. METHODOLOGY 44

Restatement of the Purpose of the Study 44
Restatement of the Research Questions 44
Research Design 45
Establishing the Paradigm *45*
Type of Study *48*
Study Setting *51*
Participants *55*
Sampling *56*
Data Collection 57
Data Analysis 62
Trustworthiness of the Study 65
Context of the Study and the Researcher 68
Context of the Study *68*
Context of the Researcher *68*
Summary 72

IV. RESULTS **73**

SUMMARY OF THE RESEARCH DESIGN 74
Data Collection Processes *74*
Data Analysis Processes *79*
STUDY SETTINGS AND PARTICIPANT PROFILES 83
Study Settings *83*
Participant Profiles *86*
FINDINGS 89
Challenges to Implementing an Information Security Program *89*
Information Security Perceived as a roadblock. *89*
End Users lack knowledge. *91*
Better End User Relationships are needed. *93*
Assessing Information Security Compliance *94*
Perception of End User Compliance Behaviors *96*
Best practices for Implementing a Successful Program *98*
SUMMARY 100

V. CONCLUSIONS AND RECOMMENDATIONS **102**

OVERVIEW OF THE STUDY 102
TABLE 1 104
DISCUSSION OF THE FINDINGS 107
Challenges to Implementing an Information Security Program *107*
Assessing Information Security Compliance *111*
Perceptions of End user Compliance Behaviors *113*
Best practices for implementing a successful program *118*
IMPLICATIONS FOR HIGHER EDUCATION PRACTICE 119
RECOMMENDATIONS FOR HIGHER EDUCATION PRACTICE 123
RECOMMENDATIONS FOR FUTURE RESEARCH 126
CONCLUSION 128

REFERENCES **131**

APPENDICES **140**

A. INSTITUTIONAL REVIEW BOARD APPROVAL **140**

B. PARTICIPANT LETTER **142**

C. INFORMATION SHEET **143**

D. INTERVIEW PROTOCOL FOR IN-PERSON INTERVIEWS **145**

ABSTRACT

The purpose of this study was to explore the perceptions and experiences of information security officers about the factors they perceive affect the implementation of information security programs within health science centers. Of specific interest was how these programs are implemented in order to remediate risk to the institution as well as to comply with federal mandates. The study sought to identify information security officers' experiences, perceptions, and processes they used to establish an information security program to ensure compliance in their organizations.

The study was conducted through a social constructive lens as a qualitative, collective case study approach and included information security personnel from accredited health science centers in Texas as participants for this study. The conceptual framework in this study was a values-based approach that examines value conflicts in employees and information security officers.

Data collection for this study included semi-structured interviews, regulatory documents and AV materials, field notes, and the researcher's reflexive journal as data sources. Analysis included coding and theme identification via a comparative analysis and an evaluation of the interpretations to make determinations on analysis and reported the findings.

The findings from the study pertained to the perception information security officers held when they implemented an information security program, and the most recurring theme was the use of security awareness and education for end users. Information security officers emphasized the importance of awareness and discussed

how lack of education and awareness caused end user non-compliance. at their institution.

Implications to higher education were as follows: 1) Emphasis on education and awareness as the most robust strategy did not result in a paradigm shift if the motivations of end users was not considered therefore, non-compliance will continue and the institution will fall back on strict compensating controls perpetuating the perception of information security as a roadblock, 2) Credential theft in higher education persists and can lead to costly data breaches that cyber insurance may not be able to resolve, 3) Institutions that prioritize technical controls over qualitative understanding run the risk of not being able to prevent cyber attacks from threat actors that are becoming more proficient in their methods.

Recommendations for higher education are: 1) higher education and information security personnel need better working relationships and risk management partnerships, 2) Information security should improve program assessments to include qualitative measurements, 3) information security should develop multi-modal awareness to go beyond traditional methods, 4) information security should incorporate more proactive efforts to keep up with frameworks instead of maturing the program via external audits and assessments.

Areas for future research exploration should be conducted in three areas. First, conduct a qualitative collective case study to explore the rationale behind end-users security compliance. Next, information security officers should work to understand how the pandemic restructured the information security landscape. Last, there needs to

be better understanding of the impacts of innovation such as artificial intelligence and corresponding governance within a higher education environment.

CHAPTER I

INTRODUCTION

The use of technology in a higher education environment provided greater access to resources, fluid means of collaboration among researchers, and an outlet to digital communication among end users (Al-Kurdi et al., 2018; Hart, 2015; Rosenbusch, 2020; Tarhini et al., 2019). Information Technology is a division within higher education organizations that was integral to institutional operations as well as provides conduits for distribution of content (Al-Kurdi et al., 2018; Dlamini, 2015; Tarhini et al., 2019) and supported collaboration and authorship (Altbach, 2011; Coffman, 2014). Though technology was used in higher education environments to provide greater access to resources and increase the ability to communicate and collaborate, it also created access to assets housing sensitive data that was not always protected (Coffman, 2014) or managed accordingly to prevent data breaches (Patton, 2015).

According to the National Institute of Standards and Technology ([NIST], 2018), a data breach is defined as the unauthorized copy, retrieval, transmission, use or theft of confidential and protected information by anyone who does not have authority or permission for that data and information. Patton (2015) posited that in higher education organizations, cyberattacks were inevitable. Gardner (2017) found that when it came to colleges and universities, institutions not only had challenges in implementing safeguards to secure data, but they also must combat persistent attempts, including social engineering, of malicious actors to successfully infiltrate those safeguards. Due to the need within higher education environments to share content and

collaborate, data and information that was acquired and accessed using technological services, devices, and infrastructure must be secured.

Information security is a program within organizations that is based on a cybersecurity framework structure that stemmed from U.S. Presidential Executive Order (EO) No.13636, 3 CFR 13636 (2013) to address an increase in cyber intrusions in organizations across the U.S. As identified in this EO, "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront" (p. 11739). In addition, "the cybersecurity framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks" (para 1).

Information security programs "include methodologies to identify and mitigate impacts of the cybersecurity framework and associated information security measure or controls on business confidentiality, and to protect individual privacy and civil liberties" (Executive Order no. 13636, 2013). Information security controls consist of multiple layers of preventative safeguards that are included in an information security program, such as technical controls, administrative controls like security awareness training, and physical controls to safeguard data (Texas Administrative Code [TAC] §202, 2018). According to Huang et al. (2010), despite best efforts, security controls were not always successfully implemented.

Specific guidelines about the architecture of the components of the information security program, and detailed lists of responsibilities for the agency head such as risk management, security awareness, security plan, and implementation of a security

program are outlined in the TAC §202.74 (2018). At an institution of higher education, it was the responsibility of the agency head to "designate an Information Security Officer who has explicit authority and the duty to administer the information security requirements" (Texas Administrative Code [TAC] §202.70, 2018). Information security officers were to implement a program that is aligned with requirements of federal governing entities that have outlined frameworks to minimize risk (EO No. 13636, 2013). Of specific focus in this study was the higher education environment of an Academic Health Science Center (AHSC). These organizations must also have had an information security officer and program implemented within the environment.

An AHSC organization is not only governed by educational agencies, but also by medical regulations such as those stemming from the Health Insurance Portability and Accountability Act (HIPAA) (Davies, 2009; Whiteside & Verma, 2015). Medical campuses have partnerships with local medical care facilities to provide patient care through their clinics and have an integrated approach to academics (Dzau et al., 2010). The clinical side of an AHSC has regulations enforced through the Office of Civil Rights (OCR), national cybersecurity regulations enforced by the Department of Homeland Security (DHS), and the HIPAA Security Rule defined by the U.S. Department of Health and Human Services (HHS) (U.S. Department of Health and Human Services, 2018). With multiple entities regulating information security requirements at AHSCs, the information security officer is required to adhere to and abide by all laws governing the protection of sensitive and confidential data (Texas Administrative Code [TAC] §202, 2018).

Information security compliance within higher education organizations is necessary as the open structure of the academic environment positioned institutions to vulnerability and risk (Hart, 2015; Malavet, 2017; Rezgui & Marks, 2008). With the amount of research and data that colleges and universities collected, higher education was a constant target for hackers (Gardner, 2017; Patton, 2015). In the Verizon 2015 Data Breaches Investigation Report (2015), 65 reported breaches were documented to have occurred in the higher education environment in 2014, listing them as the 9th highest, with data lost among all industries. To understand the gravity of the information in the Verizon report, "A major [data] breach can expose thousands of names and social security numbers, credit card numbers, and other personal data that employees and students turn over to colleges all the time, leaving those affected vulnerable to identity theft" (Gardner, 2017, para 3).

It was the role of the information security department to identify risk, minimize vulnerabilities and potential threats; and implement safeguards within the organization (Texas Administrative Code [TAC] §202, 2015). A threat, according to the TAC §202 (2015), was defined as an event that had the potential to negatively impact the organization, personnel, artifacts, assets, and reputation. A vulnerability was defined as a weakness in an information asset, system, or network that could be exposed and exploited (National Institute of Standards and Technology, 2020). The TAC directed institutions of higher education to implement an information security program and adhere to security safeguards and protocols that minimize risk and potential threats according to what is outlined in TAC §202.74, which was the framework necessary for

implementing a security program within higher education (Texas Administrative Code [TAC] §202, 2015).

Statement of the Problem

Breaches and data loss persisted as threats to security safeguards, especially in higher education when users failed to follow training and failed to behave in ways that secure data (Hart, 2015). Former executive editor for T.H.E. Journal, an online magazine covering educational technology, and now author for another online magazine titled Campus Technology, Hart had numerous years in the field writing about educational technology topics spanning information security best practices, technology in educational environment, and trend analysis of technology in education (Hart, 2015). His work documented findings regarding technology in a higher education setting, and the risk of data breaches that were similar to researchers in the field such as Bialaszewski (2015). Bialaszewski (2015) noted that "there have been many instances of successful breaches of educational data used for assessment of individuals, and with advancing technology one can safely assume there will be more such attempted" (p. 46). Even though some organizations tried to implement security mechanisms to prevent a data breach, Safa et al. (2016) claimed that organizations invested in technology and information security tools, but security breaches and incidents persisted due to the failure of organizations to consider the actions or inactions of employees as the cause for those incidents.

In a study to evaluate security awareness privacy behaviors, Mamanov and Benbunan-Fich (2018) surveyed 400 United States employees that were employed at an online organization that paid employees for completing tasks in what was known as

an online labor market. The research conducted involved a control group presented with generalized computer news stories and a treatment group presented with breach specific news story. After both groups were given the scenarios, both were asked to set a security password and then given a survey of personal questions with an answer choice of allowing them to select the option of not answering if they preferred.

The intent of the study was to understand security behaviors given security threat information or generalized technology information. The findings showed that those that received specific news stories on security threats responded with stronger passwords; however, those same participants with stronger passwords did not show a correlation to revealing more personal information as hypothesized. The reason for the study was due to information security literature that pointed to an increase of security incidents in 2016, that also caused millions of dollars in costs afterwards. Malavet (2017) also presented evidence of costly data breaches within higher education and mentioned that this environment was also susceptible to data breaches due to the openness of the network. Gardner (2017) asserted that higher education was a constant target.

Ki-Aries and Faily (2017) conducted a case study within a security forward organization that was receptive to implementing a new *persona approach* as a framework for security awareness to identify the *human* factor that they claimed needed to be examined as an alternative method to minimize risks within an organization. Ki-Aries and Faily found that organizations relied on technical safeguards to prevent a security incident but failed to consider human actions as important factors to preventing incidents.

Arachchilage and Love (2014) also conducted a study to examine end user behaviors, but this time as a pilot study in the information technology department using 20 participants at Brunel University in London. The study was to see if there was a correlation for end users and social engineering based on the kind of *knowledge* they relied on to prevent security incidents, specifically social engineering. Using a survey approach, Arachilage and Love found that the most vulnerable part of security was personnel who did not have adequate security awareness training to lead them to use preventative behaviors, and that personnel who demonstrated proper *procedural knowledge,* experienced self-efficacy when they were properly informed.

Rezgui and Marks (2008) examined information security in higher education organizations and found that one effective way to minimize risk and protect data was to implement adequate information security awareness training to employees according to their environment. Rezgui and Marks (2008) also stated that security awareness was pivotal to organizational information security overall but particularly in higher education due to the emphasis on information sharing. In state funded higher education environments, an information security officer was expected to implement security awareness as part of the information security plan as advocated by the TAC §202 (2018). Padayachee (2012) stated that user compliance was influenced by a user's perception of security behaviors expected as they were outlined in established policies, and according to Herath and Rao (2009), employees who perceived security as interference may have ignored policies to improve efficiency. Similarly, Boss et al. (2009) also noted that while organizations worked to ensure compliance via policies,

procedures, and system configuration; employee motivation should have also been considered when implementing effective information security.

In a study to examine whether security tools negatively impacted compliance to information security strategies, Hwang and Cha (2018) sought to understand what they defined as techno-stress, which was a non-compliance behavior due to the security tools in place. They surveyed sample populations from 20 organizations in South Korea that were required to adhere to security safeguards regularly but did not have information security as part of their job. Hwang and Cha conducted the study because prior research showed a trend of employees that had difficulty with technology in addition to their daily tasks, and challenges after having learned multiple information technology processes that were put in place for compliance, risk minimization, and data security. The researchers found that another reason for non-compliance of information security safeguards was the security itself.

As evidenced above, researchers have found that there were multiple reasons that are root causes for noncompliance of security safeguards such as lack of understanding for the human element of end user behaviors, employee perceptions of the security protocols, and the security itself. Bialaszewski (2015) discussed breaches in educational environments as a concern to be addressed and mitigated to prevent data loss. Ki-Aries and Faily (2017) emphasized improved methods to security awareness with end users, and Hwang and Cha (2018) identified technology as a stressor to end user compliance. In summary, it was important to explore and understand the person-centered side of information security as it pertained to organizational processes and security implementation (Ki-Aries and Faily, 2017).

Purpose of the Study

The purpose of this collective case study was to explore the perceptions and experiences of information security personnel about the factors they perceived affected the implementation of information security programs within health science centers. Of specific interest in this study was how these programs were implemented to remediate risk to the institution as well as to comply with federal mandates. The intent was to become more informed on best practices used to establish compliance in health science centers, according to the culture of either a clinical or academic environment, while also complying with federal and state mandates of an information security program.

Research Questions

The following research questions guided this study:

1. What do information security personnel in health sciences centers perceive to be the challenges of implementing an information security program in a higher education environment?
2. How do information security officers in health sciences centers assess information security compliance in their organizations?
3. How do information security personnel tasked with implementing components of an information security program in health sciences centers describe end users' security compliance behaviors?
4. What do information security personnel in health sciences centers recommend as best practices for implementing successful information security programs within higher education organizations?

Significance of the Study

The significance of this study is that it offers perspectives of information security personnel as they work to implement a much-needed information security program within higher education (Eyadat, 2015), and specifically an AHSC, as TAC 202 mandates information security programs in all state agencies (Texas Administrative Code [TAC] §202.74, 2015). The study provides insights into the values that were perceived to be significant to information security personnel in aligning with the information security actions of end users as a means for promoting compliance with security safeguards within the organization, while still maintaining the mission of the environment the information security program is implemented into (Hedström, 2011). The study also provides new insight into the significance and success factors of an information security program in a health care environment (Lee et al., 2016) as well as insight into the culture of an organization as it applies to information security (Hedström et al., 2011).

The findings from this study will advance higher education practice in the area of information security compliance and will enable information security personnel to gain an understanding of the perceptions of these personnel of the values that drive end users to act according to compliance or noncompliance regarding prescribed components of an information security program, and position both information security and organizational administration to work towards outcomes that are mutually beneficial (Hedström et al., 2011). Hedström et al. (2011) argued that end user's security behaviors come into conflict with the values embedded in their daily activities against the values assumed when security policies and standards were created and

implemented within an organization therefore, incorporating a values-based model positions the organization to look at compliance from the perspective of where the conflict is happening as opposed to heavy regulation enforcement practices to control end user behaviors. Lack understanding of end user behaviors and values of the environment continue to be the reason for security incidents that occur within organizations (Hedström et al., 2011). In higher education alone, ransomware made up 80% of data security breaches according to the Verizon 2020 Data Breach Investigation Report, and end user errors in healthcare increased from 2019 to 2020 in the number of *confirmed* breaches (Bassett et al., 2020)

Summary of Conceptual Framework

The conceptual framework that is used to frame this study is the values-based model of compliance. The values-based compliance model is described as one where "groups within an organization act based on their different values" (Hedström, et al., 2011, p. 374). Values-based compliance is a model that moves away from traditional regulatory-based compliance models such as policies, procedures, technical configuration, and retribution, and examines reasons for employee behavior regarding information security compliance (Kolkowska et al., 2017).

The model describes behaviors as security actions that are based on concepts that dictate the security actions based on actors. One concept is that security leadership design the rules and organizational employees implement them. The difficulty is that employees may implement these security rules, that have been designed by security leadership and behave only according to what they know and can associate to their

organizational learning so long as value conflict does not occur to interfere with their compliance. (Hedström et al., 2011).

Security behaviors are an "expression of values – values related to their profession" (Hedström et al., 2011, p. 374). Ki-Aries and Faily (2017) mention that some organizations focus a great deal on security awareness to achieve compliance but still fail to examine the human element to end user behavior as it should be examined through the lens of the end user's persona in order to understand the human element to security awareness and risk mitigation in an organization. Kolkowska, et al. (2017) explains that to understand information security compliance of organizational employees, information security professionals need to understand both extrinsic motivations as well as intrinsic motivations or rationalities because the number of incidents continue to rise due to the default information security management style which is that of policies and guidelines that have been established without end user values considerations. According to Safa et al. (2016), hackers target people to create a breach and that is why it is important to understand values that guide behaviors in order to change users' routines (Hedström et al., 2011).

Summary of Methodology

The qualitative collective case study was conducted through the lens of the social constructivist paradigm. The study settings were health science centers located in Texas. The participants were purposefully selected information security personnel at AHSC's who reported to the CIO within the information technology department.

Data for this study was collected through semi-structured interviews, document analysis, website reviews of program maturity and policy documentation, field notes,

and the researcher's reflexive journal. Field notes, reflexive journal, and Excel spreadsheets were used to document the researcher's observations, biases, thoughts, processes, and progress for the duration of the study. Data was analyzed using the constant comparative method as well as open and axial coding to identify themes to answer the research questions that guided the study. To ensure trustworthiness in the conduction of the study, triangulation, member-checking, thick, rich description of the study details and participants' voices, and an audit trail were used.

Definition of Terms

The following definitions are used through this study and are operationalized as follows:

Confidentiality. The security objective of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Texas Administrative Code [TAC] §202, 2018).

Control. A safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources. Controls may include security features, management constraints, personnel security, and security of physical structures, areas, and devices (Texas Administrative Code [TAC] §202, 2018).

Covered Entity. A health care provider, a health plan, or a healthcare clearing house who, in its normal activities, creates, maintains, or transmits PHI (HIPAA Journal, 2018).

Information Security Program. The policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish an information resources security function within an institution of higher education or state agency (Texas Administrative Code [TAC] §202, 2018).

Risk. The effect on the entity's missions, functions, image, reputation, assets, or constituencies considering the probability that a threat will exploit a vulnerability, the safeguards already in place, and the resulting impact (Texas Administrative Code [TAC] §202, 2018).

Standards. Specific mandatory controls that help enforce and support the information security policy (Texas Administrative Code [TAC] §202, 2018).

Assumptions of the Study

Assumptions are the pieces of information that is perceived to be factual but after findings are developed, they may in fact be false (Creswell, 2014). The study was based on the following assumptions:

1. The participants had implemented enough security controls, required in TAC 202, to yield an accurate perception of the maturity of their program.
2. The participants had faced organizational challenges in implementing a security program due to perceptions from end users.
3. The participants had the authority to provide information about their information security program challenges and end user competing values, while still maintaining confidentiality or propriety.
4. The participants were transparent and forthcoming in their responses explaining their perceptions and experiences within their institution.

Limitations to the Study

Limitations to a research study are those portions of the study that the researcher does not have oversight of and cannot manage as part of the study design (Creswell, 2014). Limitations to this study are:

1. Participants were limited to information security personnel from an academic health sciences center environment located within the state of Texas that was guided by the Department of Information Resources.
2. The study focused on information security programs that had information security personnel who reported directly to the CIO.
3. The study did not account for academic health science centers that had such unique environments and implementation of information security programs that this study could not be replicated in any other contexts.

Summary

This qualitative collective study was conducted in the information security landscape in order to gain an understanding of information security programs and end user compliance. The purpose of this collective case study was to explore the perceptions and experiences of information security personnel about the factors they perceived affected the implementation of information security programs within health science centers. Of specific interest in this study was how these programs were implemented to remediate risk to the institution as well as to comply with federal mandates. The intent was to become more informed on best practices used to establish compliance in health science centers, according to the culture of either a clinical or academic environment, while also complying with federal and state mandates of an

information security program. It is through end user compliance that the problem of data protection and end user behaviors can be remedied through the successful implementation of an information security program.

Organization of the Remainder of the Study

Chapter II provides a review of literature that covers how information security is perceived within higher education and healthcare context, and compliance issues in a health science center environment. Chapter III provides the methodology and research design that will be used to conduct this study.

CHAPTER II

LITERATURE REVIEW

The purpose of this literature review was to explore the organizational culture of the academic and healthcare environments in health sciences centers, and factors that motivated information security compliance in each. It includes: 1) overview of traditional higher education setting; 2) an introduction to information security and regulatory tenants that make up an information security program and culture; 3) brief description of the National Institute of Standards and Technology (NIST) information security framework; 4) factors to information security compliance behaviors and motivations; and 6) the conceptual framework for the study. The purpose of this collective case study was to explore the perceptions and experiences of information security personnel about the factors they perceived affected the implementation of information security programs within health science centers.

Overview of Traditional Higher Education Setting

Cohen and Kisker (2010) and Altbach et al. (2011) described higher education as an evolving environment that resembled earlier eras of postsecondary education, but that had adapted to societal pressures, geopolitical influences, economic trends, and institutional objectives. Economic funding and spending were examples of those changes to the environment. Some types of higher education institutions were funded through taxes of the surrounding community, and others were funded through appropriations and driven by regulatory standards from external governance or regulatory agencies (Altbach et al., 2011; Cohen & Kisker, 2010).

Higher education administration in order to attain the mission and objectives of the institution were examples of evolution of how an institution operates. Cohen and Kisker (2010) pointed out that internal governance had changed over the years to become more of a shared role where higher education administration modified their own processes to include more faculty in the decision-making processes, and afforded faculty more opportunity for involvement in organizational operations.

While the higher education environment had evolved since earlier eras, so had the administration of higher education. Cohen and Kisker (2010) described higher education administration as operating in two roles that included the bureaucratic role and the institutional structure, while Altbach (2011) described higher education as a model with administration as the top tier of leadership and specific academic departments established to reflect the close ties to the society it serves. Both Cohen and Kisker (2010) and Altbach (2011) described higher education as repositories of knowledge that evolved along with social, political, and economic influences and in turn, administration and organizational structures evolved as well. Technology was an example of a department that had become more integral to higher education, not just for operations but for distribution of knowledge as well as a conduit for academic freedom distribution of content, collaboration, and authorship (Altbach, 2011). With the use of technology, institutions and researchers alike could digitally participate in a virtually connected environment of knowledge sharing, dissemination of information, and online forums to connect institutions and those engaged in scholarship (Altbach, 2011).

Ehrenberg (2012) also referenced an evolving higher education setting. Ehrenberg analyzed data sets of 2,606 organizations that submitted data to the Integrated Postsecondary Education Data System (IPEDS), in search of trends involving tuition, economic impact, and changes in allocation of resources. Among the findings identified were that not only was money being distributed differently from spending trends of the past, but faculty demographics were much different as well in that the number of full time or tenure track faculty was significantly lower.

Tuition increases in public institutions was usually a result of decrease in state funding while an increase in private institutions was due to the perception of the quality of education private institutions offer. Private institution tuition was not regulated the way public institutions were either. Additionally, the economic impact to the communities was different as much of resource allocation was a direct reflection of donors and endowments with predetermined interests. Last, student assistance was different as aid was distributed differently at public versus private institutions due to need and income levels of students thereby driving aid availability (Ehrenberg, 2012). Altbach (2011) mentioned something similar in his description of patterns of higher education reform and change, when he found that while education was historically funded heavily by governments, the shift was placed back on the student more than in prior eras; however, most institutions still focused on serving the needs of the regions they were in.

Further examining the academic setting, there were varied perceptions that made up the culture of higher education interactions of faculty, staff, and administrators that support Bess and Dee's (2012) assertion that culture in higher

education was influenced by behaviors and interactions in the environment. Looking through the lens of relational dynamics, Kuo (2009) sought to better understand relationships between staff and administrators as they developed and evolved in higher education because his argument was that relationships with mutual respect (Spierling & Palmer, 2020), collaboration, and healthy conflict resolution, were derived in the organizational culture and promoted the mission and goals of the institution (Grecmanova et al., 2015). In his study using a sample of 36 staff and administrators from research universities, Kuo explored perceptions according to their construction of professional relationships within their environment and found a set of three relationship patterns that affected collaborations, interactions, and communications. These three relationship patterns were: professional relationships, differential relationships, and fragmentary relationships.

The professional relationship was one based on a collaborative approach to each other's roles where there was a sense of cohesiveness and reciprocated respect. The differential relation was one where there was not always complete alignment between what the staff and administration perceives was the way to carry out duties, projects, and tasks. (Kuo, 2009). The fragmentary relationship was one in which relationships became disconnected and siloed due to administrative, interpersonal, or bureaucratic challenges (Kuo, 2009).

Each type of relationship was rooted in the interactions between administrators and academic staff and influence perceived roles of each within organizational operations. In addition, Kuo (2009) stated that academic staff and administrators "construct their unique cultures through indispensable roles and functions, diverse

perspectives, and dynamic interactions with others," including collegiality (Grecmanova et al., 2015), and interpersonal dynamics (p. 44).

Health Science Centers

The Alliance of Academic Health Centers defined an AHSC as a university with a medical school, health profession program, and affiliation with a hospital or health system (AAMC, 2023). Whiteside and Verma (2015) described the overall objective of an Academic Health Sciences Center (AHSC) as a system to provide patient care and do so through a collaboration of health professionals who also served as educators in a blended academic and clinical environment. AHSC's were comprised of an education and research component while providing patient care and boosting economic impact through collaborative partnerships with local hospitals, clinics, and health service agencies (Davies, 2009; Dzau et al., 2010; Whiteside & Verma, 2015).

According to Ovseiko et al. (2010) William Osler and Abraham Flexner were the primary proponents of establishing an AHSC environment in the United Kingdom after seeing how successful the initiative was in the United States. In 1911, both went before Parliament in the United Kingdom in 1911 to petition for an effort to involve universities to become heavily engaged in healthcare environments. Ovseiko et al. (2010) also noted that the emphasis on innovation was from Osler and Flexner's belief that with novel medical innovation came the opportunity to provide more accessible care to patients and more affordable. Edelman et al., (2017) described the original focus of an AHSC as innovation of medicine due to emphasis on the research component, but that the strategy had since shifted to focus more on a community population-based emphasis on patient care for underserved or disparate.

The shift in focus had yielded a change in organizational models used in an AHSC. While differing models for AHSC's existed, Whiteside and Verma (2015) as well as French et al. (2014) noted that the most widely used framework to architect an AHSC was to define a mission in which the organization aimed to function. Whiteside and Verma (2015) specifically referenced the role of the mission in an AHSC to be similar to that of a traditional higher education setting in that faculty needed to support the mission to promote academic freedom, which was similar to the foundation of traditional higher education. Delaney et al. (2010), Edelman (2017) and French et al. (2014) outlined a three-tiered perspective of categorizing an AHSC mission in that it aligned with standards of clinical care, established types of research discovery, and educated or developed health care professionals.

Similar to Whiteside and Verma (2015), and French et al. (2014), Barrett (2008) also noted that the mission of AHSC, also referred to as an Academic Health Center (AHC) was pivotal to operations and used the University of Florida as a case study to identify practices used to integrate an academic and clinical environment. Barrett (2008) concentrated on dynamic organizational structures (five different models) of an AHSC and worked to understand how academic and clinical settings worked together. In doing so, he found that differing models operated at different levels of integration and regulation; therefore, calling for governance as part of effective integration between academic and clinical activities. One of the academic and clinical activities in an AHS system was managing health related data and Dzau et al. (2010) recommended investing in information technology and informatics, among other items because he claimed that a successful AHSC needed health-care

information technology as a means to manage data and facilitate the distribution of knowledge.

Overview of Information Security

The National Institute of Technology Standards ([NIST], 2018) established that information security was a term that covered the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The NIST established a framework for cybersecurity that was developed at the request of Presidential Executive Order No. 13636, in 2013, to develop a framework alongside industry leaders to reduce and minimize risk of cyber intrusion to organizations that became a more frequent occurrence on a national level (NIST, 2018; Executive Order No. 13636). The emphasis on information security was also evident in Executive Order No. 13800, mandating stricter regulation on critical infrastructure and networks to ensure data protection. The most recent executive order specifically mentioned the use of risk management to mitigate risks, which was a major component of the TAC 202 prescribed information security program. An information security program was described in Executive Order No. 13636, as a program within organizations that was based on a framework to address an increase in cyber intrusions as they occurred from both internal and external threats (Exec.Order No. 13636, 2013).

Cyber intrusions such as malware, phishing, and network penetration via exploit kits were a few examples that constituted persistent external threats to an organization, and while the potential for a cyber intrusion was known, organizations still perceived they were unprepared or did not have a security forward culture to

position information security as a priority fiscally or operationally (Sarrel, 2010; ProserveIT, 2018). Myyry et al. (2009) studied internal threats of non-compliance of information security policies and sought to provide an understanding of lack of adherence due to moral reasoning and values that determined employee actions. Both external and internal threat types were found as root causes identified in a Ponemon Institute study involving 15 countries and global data breaches where researchers found that the top three reasons for data breaches were malicious criminal attacks (cyber intrusion), system glitches, and human error (Ponemon, 2018). Ponemon (2018) is an organization that specialized in studies focusing on privacy and information security on a periodic basis to provide current trend analysis regarding the data protection landscape and cybersecurity.

In studies examining human error, researchers Daugherty and Tajuddin (2018) conducted 55 interviews and 7 focus groups in the United Kingdom (UK) to identify end users' perceptions and data handling/data loss as it pertained to their behaviors and rationale regarding security policies as safeguards within the organization. In the course of their findings, Daugherty and Tajuddin (2018) described employee behavior as an organizational vulnerability that increased risk to protected data due to non-compliance of security safeguards. Posey et al. (2014) conducted a study to understand behaviors of end users to gauge how insiders felt about security threats to the organization and how their actions impacted information security initiatives to curb threats from becoming an exploited incident. The study consisted of 33 interviews of a mix of information security professionals as well as organization end users from multiple companies across the U.S. When asked the question of what they perceived

as the biggest risk to their organization, respondents listed external threat, internet threats and insider threat as their biggest concern (Posey et al., 2014).

To minimize cybersecurity risk and the growing threat landscape, Executive Order 13636 mandated the establishment of a framework to address cyber risk to critical infrastructure and develop a voluntary cybersecurity program "to support the adoption of the cybersecurity framework by owners and operators of critical infrastructure and any other interested entities" (Exec.Order No. 13636, 2013, p. 11741). Those entities included covered entities such as institutions of higher education and state agencies such as health science centers. Texas Administrative Code Rule §202.74 was a rule that defined an information security framework for Texas covered entities and higher education, as it was a framework that was adapted from the National Institute of Standards and Technology and outlined the requirement for institutions of higher education to implement an information security program.

According to §TAC 202.74:

> Each agency shall develop, document, and implement an agency-wide information security program, approved by the agency head under §202.20 of this chapter, that includes protections, based on risk, for all information and information resources owned, leased, or under the custodianship of any department, operating unit, or employee of the agency including outsourced resources to another agency, contractor, or other source (e.g., cloud computing). (Texas Administrative Code, 2018)

An information security program was made up of multiple components. First, the program must include periodic risk assessments that also included general risk

remediation strategies and risk remediation plans for networks, facilities, and information systems. Second, the program must be based on policies, controls, standards, and procedures along with a procedure to plan, implement, evaluate, and document remedial action to address deficiencies in security policies, procedures, and practices. Last, the program must include a process to justify, grant and document any exceptions to specific program requirements (Texas Administrative Code [TAC] §202, 2018).

In order to establish a comprehensive framework that could be utilized in a standardized format, NIST assisted in developing a framework and major components to be used to implement an information security program, to prevent cybersecurity intrusion to execute the intention of the prescribed presidential order (Executive Order No. 13636). NIST (2018) defined framework as a set of guidelines, processes, and standards that can be implemented to address risk within an organization.

There were other security frameworks that information security officers (ISO's) used to implement their security program such as NIST or Control Objectives for Information and Related Technologies (COBIT), but some organizations followed the NIST-based model as it is aligned with federal mandated requirements. While information security programs must implement a legislatively mandated set of controls within an organization in order to be compliant with regulatory mandates (Texas Administrative Code [TAC] §202, 2018), using a NIST-based framework was voluntary and served as a guide for ISO's when implementing an information security program to manage and reduce cybersecurity risk (NIST, 2018). Much like the tenants

of the security program vary according to the framework, so is the information security culture within an organization, especially higher education.

Information Security Officer

The need for an information security officer began to emerge as customer relationships began being automated and organizations began to involve more e-commerce which positioned customers to intersect with security safeguards to mitigate newly introduced risks (Lanz, 2017). Originally, security was not a priority in organizations because the burden fell on the employees, and the Chief Information Security Officer (CISO) was not limited to a technical role but a problem solver and creative thinker with business acumen because they have high visibility, accountability, and agents of change (Alexander & Cummings, 2016). CISO's had to have ability to strategically plan long term and still have agile adaptability to the constant and fast-paced nature of the industry. (Alexander & Cummings, 2016); therefore, cybersecurity did not get priority or financial investment to build out safeguards (Lanz, 2017). The CISO was a liaison within IT that was business contact and had networking skillset, but the role became more executive the greater the need became (Alexander & Cummings, 2016). Responsibilities of the CISO were governance (Karanja, 2017), policy, executive reports, and business continuity (Lanz, 2017).

To further emphasize the importance of the CISO, Karanja (2017) conducted a study examining the responsibilities of the CISO as the defense against data loss, protection of assets, and overall security in an everchanging landscape, was delegated to information technology depending on the environment. Karanja used data sets from

Lexis Nexis to review data from organizations that hired CISO's between 2010 and 2014 and then reviewed a second data set that documented the reporting relationships within the organization. One of the findings was that there was an inconsistent understanding the role of CISO and that many organizations did not know how to clearly define the responsibilities of the person responsible for security within the organization much less find a consistent title for the person with that area of responsibility (Karanja, 2017). In an article supported by the Korn Ferry Institute, a management consulting organization, Alexander and Cummings (2016) pulled together data sources such as surveys from the U.S. State of Cybercrime and Vormetric, a cybersecurity organization, that described the rise of the chief information security officer as a need to address organization issues regarding the protection of data and insider threat.

Persistent threat and risk of being attacked from multiple directions in an organization lead to question not if they will be attacked but when they will be attacked (Karanja, 2017 & Lanz, 2017). The function of cybersecurity to prevent those attacks was no longer something that resided only in IT but impacted all departments of an organization, and the CISO held the corporate function of protecting the enterprise and keep it running (Alexander & Cummings, 2016). The CISO was a data guardian and responsible for technology risk within the enterprise however, there is no panacea to eliminate risks of cyberattacks (Lanz, 2017).

The CISO was not just cybersecurity, but business oriented such as assurance, compliance, technology initiative monitoring, risk assessments, and point of contact with regulatory entities and external third parties (Lanz, 2017). Regardless of their

path to CISO, they all needed a large scope and broad vision to fulfill the job because the CISO had high visibility and accountability in an organization and depending on the organization, may have a distinct reporting line and potential increased vulnerability (Alexander & Cummings, 2016). Depending on the organization, CISO's were placed in different areas, higher education placed them within IT but experts argued that the CISO should report outside of IT and directly to higher ups considering they protect the enterprise data, not just IT (Lanz, 2017).

In 2017, Senate Bill 1910 took effect that outlined responsibilities of the information security officer to be: 1) reports to the agencies executive-level management; 2) has authority for information security for the entire agency; 3) possesses the training and experience required to perform the duties required by department rules; and 4) to the extent feasible, has information security duties as the officer's primary duties. (SB 1910 Sec. 2054.136, 2017).

The information security program at an institution of higher education was under the direction of the information security officer as delegated by the agency head (Texas Administration Code 2018). TAC §202.70 required that the agency head or president of an institution of higher education, designate an information security officer (ISO) with authority for information security at the institution and fulfill the requirements of the position. TAC §202.71 elaborated on four expected duties the ISO was expected to adhere to, and 12 responsibilities that they must carry out (Texas Administration Code 2018). TAC 202 also defined the responsibilities of the information security officer to include an institution-wide risk assessment as well as to develop an information security plan to address all controls and requirements outlined

in the Texas Administrative Code to reduce risk and avoid data exposure or breach. By the TAC definition of resource management, the ISO is required to maintain inventory for the covered entity, track information on all managed assets, and manage risk every asset may pose to the institution.

Information Security Culture

Bess and Dee (2012) defined culture as "the ways of thinking that are prevalent in the organization" (p. 392). An information security culture is comprised of artifacts, value, knowledge and assumptions that guide information security initiatives and operations within an organization (Van Niekerk & Von Solms, 2010; Alhogail & Mirza 2014; Alhogail 2015; DaViega & Martins 2017). DaViega and Martins (2017) conducted a study to identify influences of dominant information security cultures and subcultures within an organization and found that information security culture operated much the same as an organizational culture and subcultures where the subculture was a variation from the dominant culture. Information security dominant and sub-culture was similar to an organizational culture and sub-culture in that the dominant culture is modeled after the process, perceptions and behaviors that emulate leadership, and the sub-culture emulated the lower-level behaviors, processes, and perceptions that were more aligned directly with the employee's daily routine, and tasks (Van Niekerk & Von Solms, 2010; DaViega & Martins 2017).

In a study to evaluate policy compliance among end users, Safa et al. (2016) found that cybersecurity "includes additional dimensions, which extend beyond the formal boundaries of information security, including humans in their personal capacity and society at large" (p. 71). Tang et al. (2015) conducted a study to identify how

information security culture was impacted by perceptions stemming from organizational culture and determined that having shared beliefs and value systems led to behaviors that facilitated "an organization to achieve its objectives in information security management" and that "organizations will have compliant employees if the organization has a coherent culture" (p. 180).

According to Alhogail (2015), there were multiple approaches to information security, but while it was perceived to be a technical issue, it should be a culture change that values compliant human behavior because it was far more effective than relying solely on regulatory compliance. Boss et al. (2009) agreed with Alhogail (2015) about the role of technical considerations and the need for enterprise solutions such as a framework to develop a security-aware culture in an attempt to make information security a responsibility institution-wide, and not just the role of the information security office.

Paulsen and Coulson (2011) found the following:

> That "for users to actively support an information security program, the organization must create a culture where the end users understand threats and guidelines, participate in good habits, make security-minded decisions, and view information security as an integral part of their job instead of just an annoyance" (p. 38).

DaViega and Martins (2017) asserted in their research, that examining and understanding the culture of an organization that the accepted behavior could be understood and rooted in management's vision and strategies of information security.

NIST Information Security Framework

The NIST framework spurred by presidential order 13636, included standards and controls that organizations were expected to implement so as to reduce risk of data breaches and network intrusions from external sources that sought to steal confidential and sensitive data from the institution (NIST, 2018). Of the many components mentioned, risk assessments were part of the NIST framework, mandated by Texas Administrative Code (TAC) 202, and was defined in TAC §202.1 as "identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems" (Texas Administration Code, 2018). TAC also listed risk management as a primary responsibility of the ISO as they were required to implement a program to reduce risk to institutions via initiatives that include insider threats as well as external ones.

TAC §202.1 defined risk management as "a process of aligning information resource risk exposure with the organization's risk tolerance by either accepting, transferring, or mitigating risk exposures" (Texas Administration Code, 2018). According to Grama (2016), risk management is a set of complex activities to identify risks within an organization that the organization then creates an action plan to remediate or minimize risk. In a study by Webb et al. (2014) to propose a more reliable risk management model, they found that one of the deficiencies to current processes was that risk assessment was a costly exercise and challenging to assess, because the number of information assets was far too large, the nature of the security risk is complex and difficult to gauge when trying to determine impact to the

organization. Assets were "resources that an organization uses to fulfill its mission or business objectives" (Murphy, 2015, p. 185). According to Murphy's definition of assets, resources included hardware such as computers, iPads, laptops, and removable media as well as software for a covered entity such as an entire institution. TAC 202 identified the risk assessment mandate to be one that "includes protections based on risk, for all information and information resources owned, leased, or under the custodianship of any department, operating unit, or employee of the institution of higher education including outsourced resources" (Texas Administration Code, Rule §202.1(21), 2018).

Risk management requirements included policies, controls, standards, and procedures in place to reduce institutional risk via risk assessments, to ensure applicable systems were configured to prevent data breaches or loss, and to operate at a level of risk acceptable to the agency head (Texas Administration Code [TAC] §202, 2018). Identifying the level of risk was known as defining the organization's *risk appetite*, and the boundary that determines how much risk the organization is comfortable with (Pareek, 2013). Webb et al. (2014) found that any controls implemented to protect information resources was driven by the level of security risk exposure; however, organizations did not discuss security practices as much as they should have, given the sensitive nature of the topic.

Information Security in a Healthcare Environment

In a health science center, the environment was comprised of a healthcare as well as academic culture and information security in a healthcare environment was governed by the Health Insurance Portability and Accountability Act (HIPAA) (Luna

et al., 2015. The culture of the healthcare setting was compliance-based and was regulated for the protection of confidential information governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Luna et al., 2015). HIPAA was put in place to provide protection to patient health information as well as provide rights for patients to request access to their own patient information (Department of Health and Human Services, 2018). Craig (2017) explained that protected health information "includes demographic information that could reasonably be used to identify an individual" (p. 12).

HIPAA regulation defined the privacy rule and outlined patient privacy and security, and safeguards to protect data known as protected health information (PHI). According to the HIPAA Journal (2018), the security rule was a set of standards to protect information when at rest or in transit according to physical, technical, and administrative safeguards (HIPAA Journal, 2018). Under HIPAA is the security rule that outlined standards to protect electronic protected health information (ePHI). EPHI was the electronic protected health information that was transmitted via the internet. According to the HIPAA Journal (2018), the privacy rule was the standard that provided patient rights to their information and regulated how it was used and how it was disclosed to include employee access and external organizations (HIPAA Journal, 2018). Gantt (2014) further described the privacy rule and explained that there were three purposes for it, which include: 1) The rights of consumers, 2) the quality of healthcare, and 3) the efficiency and effectiveness of healthcare delivery. The privacy rule is in place to protect health related data that is of great value if a security breach occurs.

On the illegal market, the average value of an intact and complete medical record was between $10 and $1,000 (Khan, 2016), but Shameli-Sendi et al. (2016) mentioned that value cannot be measured in monetary value alone. The reason that protected health data was such a lucrative commodity was because of the value of the information to hackers, attackers, and malicious persons. According to Khan (2016), because of the centralized storage of confidential information that was normally used in a healthcare environment, there were privacy concerns that organizations should have been aware of. Luna et al. (2015) "due to the data-rich environment that health information systems (HIS) create, this digital space also creates a breeding ground for criminal activity" (p. 2). Love (2011) noted that secure records were "vital" to the survival of the organization (p. 21).

Information Security in an Academic Environment

Information security compliance within higher education organizations has been necessary as the open structure of the academic environment exposed institutions to vulnerability and risk (Rezgui & Marks, 2008; Hart, 2015; Malavet, 2017). Higher education has had large, open data networks that helped the mission of institutions and operate with transparency, but needed to be defended against intrusion (Gardner, 2017; Hart, 2015). "While the nature of higher education requires openness to the public and a continuous sharing of information, a balance must be maintained to ensure that information assets are not being put at risk or compromised" (Rezgui & Marks, 2008, p. 241). In addition to structure, methods of attack sophistication grew as quickly as technology did, and data used for means such as identity theft were a target (Gardner, 2017). According to Hart (2015), the long-held belief that information

among faculty and collaboration among schools should be widely shared became evident in other components of higher education, and administrative departments began freely and widely sharing information without complying with security safeguards which posed a threat to data protection.

Rezgui and Marks (2008) conducted a study to identify security awareness factors in higher education and found that the culture of higher education organizations operated counter to that of healthcare organizations, where they began by securing everything as much as they can, and then opened up channels as there was a need; academics did the opposite. Hart, (2015) provided recommendations to keep higher education environments safe and in doing so, observed that in higher education "everything is open and only tightened when a breach happens or some kind of mandate" (p. 20). Security measures were categorized according to costs for personnel, infrastructure, and training (Gardner, 2017) but according to Rezgui and Marks (2008) "security objectives cannot be met by technical and procedural protection only; an educated security attitude of employees, management, and external information technology users and partners is also vital to ensure effective information services security" (p. 243).

In the Verizon 2015 Data Breaches Investigation Report 65 reported breaches were documented to have occurred in the higher education environment as reported for the 2014 year, listing them as the 9th highest in the report with data actually lost among all industries. As recent as 2018, both the Ponemon Institute and researchers Doherty and Tajuddin (2018), found a continued threat persistent in organizations. Doherty and Tajuddin found that security incidents and attacks continued while in an

international study of over 15 countries, the 2018 Ponemon Cost of a Data Breach Study (Ponemon, 2018), found that not only did the cost of a breach increase for yet another year but that the average cost was 3.86 million. According to Malavet (2017), there was much discussion in higher education about data breaches and costs associated with recovery, but there was no discussion about more secure methods at much lower costs. According to Rezgui and Marks (2008), universities were highly unsecured due to the requirement of having an open network and an infrastructure created to meet the needs of multiple types of end users, and to facilitate sharing large amounts of research data.

Information Security Compliance Behaviors and Motivations

Security compliance behaviors and motivations had been presumed to be influenced by technical controls or regulatory factors that the security program is based on but did not always consider the human element or motivations of end users (Boss, Kirsch, Angermeier, Shingler & Boss, 2009; Padayachee, 2012; Safa, Von Solms, & Furnell, 2016). Kayworth and Whitten (2010) found that "security managers are faced with the complex challenge of meeting multiple compliance requirements from a growing array of federal, state, and industry standards" (p. 165). Implementing a security program to prevent the increasing need to avoid security threats had resulted in the increased use of forced compliance based on "tighter information security policies and technical obligations" (Lee, Lee, & Kim, 2016). In order to ensure data is protected, the institutional information security program under the direction of the ISO, needed to implement security standards, policies, and activities as safeguards and protocols (Texas Administration Code, 2018). Herath and Rao (2009) asserted that

there needed to be consideration on the human side of security due to the fact that employees actually perceived an increase in security conformity as interference, which lead employees to disregard security best practices in an attempt to continue performing their jobs. Boss et al. (2009) examined compliance behaviors as policy driven and stated that personnel subscribed to the idea that they can choose to subscribe to or modify their behavior to comply with or not, and the result could have been disadvantageous to the institution because non-compliance would have caused risk to the institution.

A theme in the literature was interpreting and understanding the behaviors of information processing that end users engaged in to determine compliance and perception. Hwang and Cha (2018) studied potential threats to employee non-compliance and concluded that employees faced "complexity, overload, and uncertainty" every day, and security brought about stress (p. 283). Mananov and Benbunam-Fich (2018), researched privacy behaviors and identified how relying on technology too much lead to risky end-user behaviors that persisted because of life pressures that forced end users to make split second decisions that were not based on cognition, but fear. It was these kinds of interactions central to business operations that Ki-Aries and Faily (2017) mentioned are important to study regarding security awareness.

Another behavior that has impacted end users and information security compliance was described by Hwang and Cha (2018) as "techno stress" and was defined as the increased level of stress induced by the use of technology that can lead to various negative outcomes. Techno-stress is a negative outcome that impacted the

user's self-efficacy or confidence in their own abilities, which was a concept seen throughout the literature as a variable that could have been a reason for failing to be more security compliant (Mananov & Benbunam-Fich (2018). Hwang and Cha (2018) also asserted that literature regarding this issue did not include an analysis or examination of the technological aspects of information security and how it impacted employees.

Also noted in the review of the literature related to compliance regarding information security processes, was an emphasis on values and decision making. According to Hedström et al. (2011), in their study about values-based compliance as a viable model for information security within an organization, they found that end users and managers alike operated and conducted daily processes based on values. Those values were not always the same among end users and managers, but those values dictated their decisions when choosing to comply with security safeguards. However, Safa et al. (2016) found that some employees that had a strong bond to their organization and did not tend to deviate from security policies because of their internal commitment to the organization that resulted in compliance.

Conceptual Framework of the Study

The conceptual framework for this study involved a values-based model that examined the information security culture as defined by end users and implemented by information security personnel in an AHSC environment. Security researchers have different definitions and interpretations of values-based compliance and even more variations of the term *value*. Myyry et al. (2009) defined values as "goals and motivations that are guiding principles in people's lives" (p.128) and Kolkowska et al.

(2017) defined values as rationalities. Hedström et al. (2011) defined values-compliance as a model that groups in an organization act based on different values and that "changing peoples' daily practice is best addressed through an understanding of the values that guide their behaviors" (p. 374).

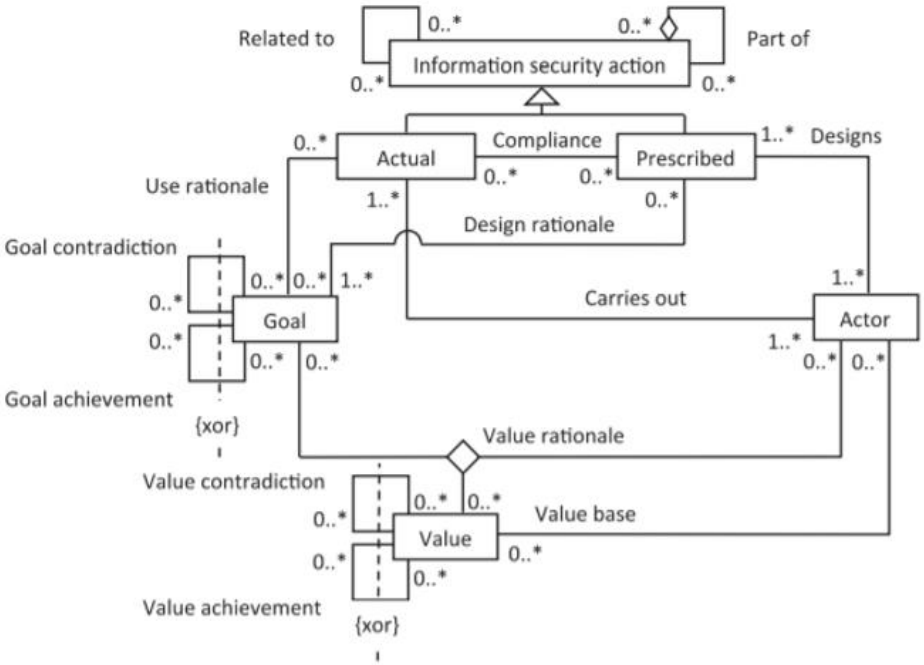
In a study by Myyry et al. (2009), researchers sought to understand moral reasoning and values as a means of information security compliance behavior, using a new framework that was based on Kohlberg's Theory of Cognitive Development and Schwartz' Theory of Motivational Types of Values. Myyry et al. (2009) explored compliance through understanding value priorities but also included moral reasoning as a parallel factor to understanding motivation to comply with information security policies. The study was conducted in Finland and included a total of 250 potential respondents. The study participants were comprised of two different sample populations and were surveyed using a previously vetted 12-question instrument called the *Defining Issues Test,* to assess the Theory of Cognitive Development portion of the framework. One group was clerical employees in a technical organization and the second was a group of master's students that had work experience in Finland. All participants were given the test, and 163 responded.

Among the findings, Myyry et al. (2009) found that not only are there multiple value types that guided compliance behaviors, but values were displayed through behaviors that were also considered "self-presentation" of the person and lead to understanding the person's identity (p. 129). In justifying employee behavior, the researchers concluded that moral reasoning intertwined with values to lead a person to

make judgments about whether compliance behaviors were justified according to either personal or professional values.

Kolkowska et al. (2017) introduced the values-based compliance framework, analysis of values, and described the need for the model as being that research existed to sufficiently examine the motivations behind employee compliance behaviors but not enough to examine the rationale extrinsic and intrinsic to understand the values behind information security policies that were implemented. The values-based model is shown in Figure 1.

Figure 1
Values Based Compliance Model



Reprinted from *Value conflicts for Information security management. (p. 375),* by Hedström et al. (2011). Copyright 2011 by Karin Hedström et al.

Kolkowska et al. (2017) argued that failure to examine employee values (rationalities) in the development of policies and information security programs caused values conflict scenarios where the employee felt forced to choose between the

goals of the organization (extrinsic motivation) or their values (intrinsic motivation). Kolkowska et al. (2017) claimed that employees operated under a command-and-control approach to information security policies which means that they had to execute and comply with information security policies and regulations that had been prescribed to them and in doing so, they carried the burden to rationalize compliance behaviors in the organization as opposed to information security management considering and analyzing values in the development of policies and security program.

Kayworth and Whitten (2010) also found the need to prioritize values and claimed that security values needed to mesh with the values of the organization. They stated that cultural conflict occurred when the values of the end users clashed with the values of the organization, and it was a values conflict that lead an individual to act in a manner that was inconsistent with security policies. Herath and Rao (2009) mentioned that while policies tried to establish best practices, employees did not perceive them as requirements and in turn violated or disregarded them leaving organizations to experienced difficulty enforcing them.

"User violations of information security policies and regulations within healthcare organizations are not always best managed through a control-based compliance model" (Hedström et al., 2011, p. 374). One of the potential causes for an end user's security violation behavior was that a user made a compliance decision based on the perceived value of the information that the end user was handling (Doherty & Tajuddin, 2018). Compliance decisions stemmed from the idea that "attitudinal and behavioural features have a socio-cultural and human dimension that

need to be analyzed and understood to ensure full users' commitment and adherence to IS security regulations" (Rezgui & Marks, 2008, p. 242).

Summary

The literature presented in this chapter began with a description of the higher education environment and included a concentrated view of a health science center so that differences between the two were presented. The chapter also included information regarding an introduction to an information security program based on frameworks introduced by government legislation, and information security in higher education as well as a health science center. To understand information security and end user behaviors, this chapter also introduced information on end user motivation, higher education culture, and research on end user motivations that resulted in some of the user behaviors observed within higher education as it intersected with an information security program. While the chapter described some of the perceived factors to implementing an information security program in a health sciences center, there was not much discussion on how the culture of an information security environment or intrinsic values of the end user influence compliance of information security safeguards.

CHAPTER III

METHODOLOGY

Chapter III presents the methodology and research design of the study. The chapter will include the following sections: 1) restatement of the purpose of the study; 2) restatement of the research questions; 3) research design; 4) data collection; 5) data analysis; 6) trustworthiness of the study; and 7) context of the study and the researcher.

Restatement of the Purpose of the Study

The purpose of this collective case study was to explore the perceptions and experiences of information security personnel about the factors they perceived affected the implementation of information security programs within health science centers. Of specific interest in this study was how these programs were implemented to remediate risk to the institution as well as to comply with federal mandates. The intent was to become more informed on best practices used to establish compliance in health science centers, according to the culture of either a clinical or academic environment, while also complying with federal and state mandates of an information security program.

Restatement of the Research Questions

The following research questions guided this study:

1. What did information security personnel in health sciences centers perceive to be the challenges of implementing an information security program in a higher education environment?

2. How did information security personnel in health sciences centers assess information security compliance in their organizations?
3. How did information security personnel tasked with implementing components of an information security program in health sciences centers describe end users' security compliance behaviors?
4. What did information security personnel in health sciences centers recommend as best practices for implementing successful information security programs within higher education organizations?

Research Design

Establishing the Paradigm

Qualitative research was defined by Denzin and Lincoln (2011) as an intersecting process that was rooted in multiple theoretical perspectives that focused on research methods to provide an interpretation to the researcher. Denzin and Lincoln also mentioned that in order for the researcher to adequately study something, he needed to participate in research that occurred in the natural setting of the phenomenon in order to develop an understanding of how that phenomenon was defined by the people in that setting that assigned meaning to it (Creswell & Poth, 2018; Denzin & Lincoln, 2011; Patton, 2015), as well as to develop a robust comprehension of things as seen from the root of the phenomena (Joubish et al., 2011; Ospina, 2004). Qualitative research was also described as a method that enabled the researcher to examine a social problem with greater depth that occurred in the natural setting (Creswell 2014; Creswell & Poth, 2018).

Creswell and Poth (2018) described qualitative research similar to Denzin and Lincoln (2011) as an interpretive process that relies on the use of practices to make the world "visible" to the researcher (p. 7). The researcher was the primary data collection instrument; therefore, "the quality of the research depends heavily on the qualities of that human being" (Joubish et al, 2011, p. 2084). Also noted by Creswell and Poth (2018) was the idea that while the qualitative researcher interprets the meanings people bring to the phenomenon, the nature of qualitative inquiry allows the researcher to make inferences that promote further inquiry and rich interpretations of the meanings derived from the natural setting. In order to guide the inquiry, the researcher needed to determine the view or set of beliefs also known as the paradigm, through which the inquiry was to be conducted (Creswell & Poth, 2018). A paradigm, according to Patton (2015), was a world view that is inherent to the researcher that is used to develop the study framework.

There are several main paradigms or ways of thinking embedded in qualitative research, including positivist, postpositivist, pragmatist, and constructivist (Creswell & Poth, 2018). Positivism was defined as research that seeks more causal relationships and trends (Patton, 2015). Post positivism was defined as the research method that is more scientific in nature and focused on a cause-and-effect approach where research methods are logically related (Patton, 2015). Pragmatist view was defined as research that focused more on the results of the research and relied on multiple means of data collection as opposed to subscribing to one model. (Creswell & Poth, 2018).

Social constructivism was defined as research to understand the world in which individuals participate and is more subjective in nature as the researcher relies on the

view of the participants (Patton, 2015). Creswell (2014) and Lincoln and Guba (1985) described social construction as being based on experiences to develop meanings of a phenomenon and is generally created through the interactions of the participants to do so. Because it focused on the participants' views, it was considered subjective; however, the goal was to develop rich understanding (Creswell, 2014). Lincoln and Guba (1985) expanded on social construction in their discussion of *realities* and provided an overview of four basic realities which were: objective, perceived, constructed, and created.

Lincoln and Guba (1985) developed the four categories of realities and defined each of them based on what was constructed, and experienced. The objective reality was described as a reality that could be attained and known, and when it was experienced, it became known to exist. Perceived reality was also attainable but not to the full and finite sense because there were so many perceptions in the construction, that a full and complete understanding was non-existent. A constructed reality was one in which it was an endless construction and only existed in the realm of the person constructing that reality. The created reality was the idea that no certain reality existed until the person experiencing it brought it into fruition (Lincoln & Guba, 1985).

This study was conducted through a social constructive lens as it included information security personnel's perceptions and experiences as well as those of the researcher about factors perceived to affect the implementation of information security programs within health science centers. The social constructivist approach to the study allowed for deep understanding of the practices that had been implemented based on the perceived understanding of end user behaviors as experienced by the information

security officer (Barker, 2019; Pieters 2011). The information security officer perceptions and experiences were integral to understanding the environment of the AHSC in which they implemented best practices.

Type of Study

Qualitative research had various types of inquiry design, and of the multiple approaches to conduct the study, there were five designs that are most often used: narrative, phenomenology, grounded theory, ethnography, and case study (Creswell 2014; Creswell & Poth, 2018). A narrative research design was defined as an approach that is reliant on the lived experiences as told and retold by the participant who has lived the experience or phenomena, and that has an embedded story (Patton, 2015) of the phenomena that is rich in context (Creswell, 2014; Creswell & Poth, 2018).

Phenomenology was a research design that aimed to understand the nature or meaning of everyday experiences (Patton, 2015). It has a philosophical and psychological root where the researcher describes the phenomenon through the individual's description of those experiences, and all the participants share the commonality of having experienced the same phenomenon (Creswell, 2014; Creswell & Poth, 2018). Grounded theory research was also considered a phenomenon but unlike narrative or phenomenology, the design "is meant to build theory rather than test theory" (Patton, 2015, p. 110). Grounded theory design was where the researcher refines multiple stages of data collection and develops a general abstract theory of a process, action, or interaction based on the views of participants (Patton, 2015). It was a theory where the participants would all have experienced the phenomenon, but they

were not necessarily part of the same cultural phenomenon or located in the same location (Creswell, 2014).

Creswell and Poth (2018) described an ethnographic study as one that looks at shared patterns among an entire "culture-sharing group" (p. 90) and is the study of a group of people who interact with each other to establish a culture (Patton, 2015). Creswell (2014) described ethnography as an anthropological inquiry with focus on shared patterns of behavior, actions of a cultural group in their natural setting over prolonged time.

The final research design is case study. There were variations on what experts defined as what constituted a case and how a case study was defined (Crowe et al., 2011; Denzin & Lincoln, 2011). Creswell and Poth (2018) defined a case study as:

> A type of design that may be an object of study as well as a product of the inquiry and is an approach where the investigator explores a contemporary bounded system or multiple, over time, through detailed data collection with multiple sources of information. (p. 96)

A common definition of a case study involved framing a phenomenon, sometimes complex, to focus on the context in which it occurred (Creswell, 2014; Creswell & Poth 2018; Crowe et al., 2011; Patton, 2015), but the unit of analysis or artifacts that were used in the data collection was decided by the researcher (Denzin & Lincoln 2011). A few of the multiple units of case analysis included programs, individual participants, groups of people, documents, time, and patterns during data collection units (Creswell 2014; Creswell & Poth 2018; Patton 2015). Lincoln and Guba (1985) as well as Creswell and Poth (2018), mentioned five approaches to a case

study design which were: 1) identify if the case study is going to be the most effective design to address the issue or problem the researcher is attempting to examine; 2) figure out the purpose of the study by providing context so that the researcher can determine the most appropriate type of case that is necessary; 3) develop a formal set of procedures or processes that are most relevant and reliable as data sources and data collection; 4) determine how the researcher will be analyzing the data; and 5) document all components of the case study in a way that it is written for the audience it is intended.

Creswell and Poth (2018) identified three specific types of case studies: 1) instrumental, 2) intrinsic, and 3) collective. Each relied on an issue or concern but differed in the construction of the design. Instrumental case study was limited to a concern and relies on only one case to further examine the issue more in depth (Crowe et al., 2011). An intrinsic case study is one in which the issue was unique and warranted more in-depth examination and did not include other cases due to how unique the phenomenon was (Crowe et al., 2011).

A collective case study is one in which the issue was explored through using multiple cases that have the same issue or concern as the bounded unit of analysis (Creswell & Poth, 2018; Crowe et al., 2011). Creswell and Poth (2018) mentioned that a collective case study is used to identify one issue or concern and illustrate it through multiple cases to develop a "broader appreciation" (Crowe et al., 2011, p. 2), and offer a broad understanding to explanatory research of the multiple cases examined for the phenomenon being focused on (Crowe et al., 2011). According to Creswell and Poth

(2018), a collective case study could be classified as intrinsic or instrumental depending on the issue or phenomenon itself.

This study was conducted using a collective case study approach to yield more descriptive interpretations of information security, and the units of analysis was the information security officers leading information security programs at Health Science Centers. A collective case study approach was especially useful as interpretations of information security evolved as data collection progressed (Crowe et al., 2011).

Study Setting

The study setting according to Creswell (2014) is the site or sites in which the study was conducted. The sites for this study were institutions that have a Health Sciences Center (AHSC) designation through the state of Texas as a fully accredited center in good standing with accrediting agencies. In addition, the study settings were chosen based on the Information Technology Department having an Information Security Office who reported to the CIO.

The profiles of the nine institutions that met the inclusion criteria are listed below. Pseudonyms were used to protect the identities of the participants and the institutions.

AHSC – A was an AHSC in southern Texas that has a School of Nursing, School of Pharmacy, and Biomedical Sciences. The information technology department did not advertise their organizational chart, but their information security program seemed to be partially based on the NIST framework. It also looked as though the IT department was decentralized in nature meaning some of their personnel are shared external to the IT department. The Information Security Officer resided in

another city but served in the same role on the host campus. Their policies were similar to the AHSC policies as the parent campus as well.

AHSC – D was an AHSC located in central Texas but only housed a School of Pharmacy. As of academic year 2020, the total enrollment for the school was 236 total students. For this institution, it deferred to the organizational chart and reporting line for IT and information security for the main campus in the system. The institution also relied on the same policy structure as the main campus institution, so the only visible policy was that of the acceptable use policy made available to the general population.

AHSC – H was an AHSC located in central Texas. The AHSC had a School of Medicine, School of Nursing, School of Biomedical Informatics, School of Dentistry, and School of Public Health. This school had teaching partnerships with 3 hospitals within the city. They had over 4300 students enrolled and offered 13 graduate degrees as of 2017. In reviewing their information technology department, the CIO was part of the president's executive council and reported directly to the president. Further review of the site showed that only the leadership for Information Technology was centralized but the structure was decentralized to have IT mini departments and representation at each of the schools. This institution also had a chief information security officer, but the reporting structure was not clear. Additionally, the only policy information listed was a policy exception request site but no publicly available policies to determine framework used or followed.

AHSC – L was an AHSC located in northern Texas. It was comprised of the Graduate School of Biomedical Sciences, School of Health Professions, School of Medicine, School of Nursing, and School of Pharmacy. As of 2020, it had an

estimated combined student enrollment at the AHSC of 1, 713 students pursuing education in the medical profession. Examining the IT component in the organizational chart, the institution had a vice president of IT & CIO that reported to the executive vice president for finance & operations and an information security officer that reported to the CIO. Searching through the institution website, the only policy posted publicly was their acceptable use policy and information security policies were protected by authentication.

AHSC -M was an AHSC in central Texas. The AHSC had a School of Medicine, School of Nursing, School of Dentistry, School of Pharmacy, and School of Public Health. They had multiple Texas campuses throughout the central region of the state. The information technology was a centralized department and had a chief information security officer that reported directly to the CIO. According to their organizational chart, the IT department reported to the operations vice president and chief of staff. In reviewing the information security website, the program seemed to be based on an open-ended policy framework, and all their policies were posted in a public web page allowing for external persons to view them.

AHSC – R was an AHSC also located in northern Texas and was also part of a university system. As of 2020, it was made up of the School of Health Professions, School of Medicine, School of Nursing, School of Pharmacy, and the Graduate School of Biomedical Sciences. For this institution, it deferred to the organizational chart and reporting line for IT and information security for the main campus in the system. The approximate enrollment was 358 students enrolled as of 2020. The institution also

relied on the same policy structure as the main campus institution, so the only visible policy was that of the acceptable use policy made available to the general population.

AHSC–S was located in central Texas and had a School of Medicine, School of Nursing, School of Dentistry, Graduate School of Biomedical Sciences, School of Health Professions, and was a member of university collaborative to offer a PhD in translational science. The information security officer at this institution reported directly to the chief information officer and the information security framework was not NIST-based. It was not determined if the information technology department was centralized or decentralized. In reviewing their website, the staff of the information security group was published along with directory information to contact each of them. Their policies were listed for viewing but only if you had an account with the institution to access them.

AHSC – T was an AHSC located in east Texas and had an approximate student population of over 10,000 students each year. The AHSC portion of the campus consisted of a school of Community and Rural Health as well as a School of Medical Biological Sciences. In reviewing the organizational chart, the school had an information security department that was separate from the information technology department and both reported directly to the executive vice president. In terms of policy information, the only publicly available policy was their acceptable use policy that was accessible by doing a general search of their website.

AHSC–U was located in central Texas and had a School of Osteopathic Medicine, Graduate School of Biomedical Sciences, School of Public Health, School of Health Professions, College of Pharmacy, and School of Medicine. It had an

information security department that reported to the CIO and had implemented an information security program aligned with HIPAA and TAC regulatory requirements. In reviewing their website, very little information about the department was publicly available and policies and policy framework was NIST 800-53 and 800-171, which aligned with the criteria of the study participation.

Participants

The participants for this study were currently employed, full-time information security personnel at each of the study institutions. The position of information security officer is an office that was outlined in the Texas Administrative Code (TAC) §202.71 as required by all state agencies and was expected to adhere to responsibilities as outlined by the information security standards for institutions of higher education. TAC §202.71 outlined the role of the information security officer and described the 12 responsibilities of the office to ensure information security within the institution of higher education that included responsibilities to develop an information security program (TAC, 2018). As mentioned in TAC 202, the ISO is designated by the agency head, and is expected to carry out the duties of implementing an information security program to minimize risk to the institution, implement an information security awareness program, develop a risk management program and conduct a risk assessment, develop an annual information security plan, report all security plans and status of the state of security to the agency head and executive leadership, to name a few responsibilities (TAC 2018, Executive Order no. 13636, NIST, 2018).

Participants of this study included information security officers personnel from the information security team at the AHSC campus that had been delegated to

implement, operate, monitor, and/or investigate any of the information security components as TAC 202 provided authority. Due to the complexity of each information security program, the researcher planned to schedule follow up interviews with personnel tasked with information security program components if additional discussion about compliance and/or privacy issues were needed, but that plan was not necessary after all.

Sampling

Qualitative sampling as described by Patton (2015) was often smaller in size but still rich in content. Patton (2015) mentioned that sample size can be a starting point and adjusted based on the fieldwork as inquiry deepened. While sample size was important to consider, so was the type of sampling the researcher chose to use. Within qualitative research, there were different types of sampling techniques used. For this study, purposeful sampling was used for participant selection. As described by Creswell and Poth (2018), purposeful sampling with case studies allows for the researcher to "select cases that show different perspectives on the problem" (p. 100).

Purposeful sampling was aimed at ensuring the sample was aligned with the overall purpose of the study, interview questions, and assurance that the types of data selected had more depth as compared to quantitative sampling methods. Creswell and Poth (2018) further defined purposeful sampling, with maximum variation, as a method used as criteria that the researcher predetermines to increase chances of finding different perspectives, which was the goal of qualitative research. Maximum variation was described as the method of selecting a varied sampling based on specific

criteria that would yield a wide range of responses from participants to reflect an accurate depiction of the population (Creswell & Poth, 2018).

The study used purposeful sampling with maximum variation to yield as diverse of a participant pool as possible, and to ensure those who were selected to participate were the most informed to address the study's research questions (Creswell & Poth, 2018; Patton, 2015). Sampling for the study focused on those fulfilling the role of information security officers at health science centers in Texas in hopes that the researcher would identify perceptions and factors that made up a successful implementation of an information security program in a blended healthcare and academic environment. The two environments had competing cultural characteristics, and staff at each environment accessed, stored, and manipulated different types of data that was classified as sensitive and protected. The researcher sought information to identify if those competing environments and handling of data types were values that information security officers used when developing and implementing an information security program.

Data Collection

Creswell and Poth (2018) defined data collection as a series of activities that the researcher engages in to gather information that is used to answer research questions that have been established in the study. Data collection was an involved process that also included anticipating ethical issues such as privacy, welfare, and avoiding harm; and are practiced explaining the purpose of the study, and even sought permission from the institutional review board to ensure the study was guided by ethical practices (Creswell & Poth, 2018). It was a process of considering permissions,

sample, sample size, recording information, and handling issues that arose. Patton (2015) pointed out that data collection takes place as either a one-time or a longitudinal approach depending on the objective of the data, and whether it needed multiple points of contact over a longer period of time or a single interaction via single interview or single site visit.

Data collection methods most used in qualitative studies included interviews, observations, documents and audiovisual (AV) materials, field notes, and reflexive journaling (as means to provide rich description and depth of meaning for the phenomenon that the study was trying to understand or interpret) (Creswell, 2014; Creswell & Poth, 2018; Patton, 2015). Creswell (2014) mentioned that the use of interviews was helpful for when the participant cannot be observed but can still provide information to be considered by the researcher. Interviews were structured according to a one-on-one interaction, group, or even web based (Creswell & Poth, 2018; Patton, 2015), and could be unstructured, structured, or semi-structured (Patton, 2015).

Unstructured interviews are free from specific questions, are based on open-ended questions, and questions are often developed through the flow of the conversation (Creswell, 2014; Patton, 2015). The structured interview was more specific in the types of questions asked as they were the same for all participants and allowed much less room for open-ended responses, with the questions being "carefully-worded" (Patton, 2015, p 439). Semi-structured interviews are a combination of the structured and unstructured interview question formats to allow for

the interview to be more conversational, but also allow for more granular inquiry as the conversation progresses (Patton, 2015).

Interviews were developed according to an interview protocol that had questions as the core of the protocol, which were used to guide the exchange (Creswell & Poth 2018). According to Creswell (2014) and Creswell and Poth (2018), interviews could be conducted using various mediums including face-to-face, telephone, and video conferencing as a means to collect information from the participants. Creswell (2014) and Creswell & Poth (2018) mentioned that during the preparation to conduct interviews, the researcher should use an interview protocol to record answers, document notes, and consider using audio or video to record the interviews.

The semi-structured interview protocol outlined expectations and explanation that the participant could have chosen to withdraw from the study at any time (Creswell, 2014). The semi-structured interview began with questions involving basic demographic data and continued into questions about the factors that were considered when developing the information security program.

Patton (2015) classified observations as participant and non-participant, while Creswell and Poth (2018) defined observations as a participant as the observer type, and complete observer observations. Participant observer was where the researcher is actively engaged with the people, whereas participant as observer positioned the researcher as disengaged but still at the study site (Creswell & Poth, 2018). Non-participant observation was where the researcher is not engaged and observing from a distance away but still able to record and document the activity taking place with the people being studied (Creswell & Poth, 2018). Complete observation was when the

researcher is disengaged completely from the study field of activity and is not seen or engaged with the people being observed during the study (Creswell, 2014). Denzin and Lincoln's (2011) research on observations stated that in the context of technology, the tool served as a conduit to capture the "reality" (p. 472). Observations included online behavior, compliance with mandated information security standards as outlined in information security program, and online security awareness behaviors.

Documents and AV materials are another data source used in qualitative research. Documents consist of any kind of material, written, visual, or digital, that the researcher could analyze (Creswell & Poth, 2018). AV materials include items that ae technical in nature and could include pictures, sounds, online materials, website items, and any item created by the participant themselves (Creswell & Poth 2018). Patton (2015) stated that documentation as a data collection tool offered insight into programs, processes, and concepts. Creswell and Poth (2014) and Patton (2015) mentioned that researchers could collect documents that went beyond typical observations to include public documents or private ones.

Field notes are also used in the data collection process. Field notes are used to document the researcher's observations during interviews and included descriptions of the study settings as well as observations about the participants (Creswell & Poth, 2018). Field notes are detailed and tend to be chronological in nature, as well as factual and descriptive (Creswell & Poth, 2018). In addition, reflexive journaling is used in qualitative research to help manage the subjective lens of the researcher about items observed and documented (Korstjens & Moser, 2018) throughout the conduction of the study.

For this study, semi-structured interviews, documents and AV materials, field notes, and the researcher's reflexive journal were used as data sources. Documents included information security policies and information technology policies that were posted on public facing websites of the study institutions as well as those outlining the major tenants of the information security program, the type of information security framework they utilized to align security standards, organizational charts guiding the authority and reporting line of the department, pieces of legislation or regulations outside of the security framework that guided the formation of the information security program, and website information about the description, mission, vision, and composition of the department.

Recruitment of participants for this study include an introductory email script that outlined the specific details of the study as well as an Information Sheet that provided specific study details. The researcher conducted a follow-up phone call to acclimate prospective participants to the study. After participation had been agreed upon, the researcher utilized purposeful sampling to select the participants. Once participants were selected, semi-structured interviews were scheduled at a time and place that was convenient for the participants.

According to Creswell and Poth (2018), researchers often collect data in the environment that participants experience the problem. Because information security is a digitally mediated environment, the researcher needed to rely on the non-verbal intricacies of online communication and the institutions best practices that were allowable, to be consistent with confidentiality and integrity of protected data that was shared or accessed during this study. Also, the study setting was digitally mediated to

ensure integrity of communication methods as well as technical mechanisms in places that were approved by the institution such as email, digital repositories, and file sharing applications. The study also included campus artifacts that were in plain sight that signal evidence of security awareness communications, reminders, messages, or protocols in place that the researcher would normally see when at the interview location. In lieu of a physical campus visit, the researcher requested copies of artifacts from the participant institution.

Data Analysis

Data analysis is defined as a multi-step process of organizing, categorizing, interpreting, and representing data to make sense of it (Creswell, 2014; Creswell & Poth, 2018; Patton, 2015). Creswell (2014) also described data analysis as the dissecting of the information collected, sorting through all that was collected, and extracting the data that is helpful and relevant while recognizing that not all of the data collected will be used. Creswell (2014); and Creswell and Poth, (2018) listed data analysis steps as: 1) organizing and preparing data for analysis (Creswell, 2014; Creswell & Poth, 2018); 2) reading and reviewing all of the data; 3) coding all of the data and organizing it into segmented pieces of information (Creswell & Poth, 2018); 4) using a coding process to generate description of the information to categorized into themes and categories; 5) identifying the description and how themes will be presented; and 6) interpreting the findings or results.

A constant comparative analysis according to Patton (2015) is a process of "systematically making comparisons to generate explanations" (p. 590). Patton also described the comparative analysis as a process of developing units to compare to each

other and through the categorization, coding the units of information together to generate common traits, characteristics, or trends. In order to develop the units of categorization, Creswell and Poth (2018) discussed the use of open coding, axial coding and selective coding. Open coding is the beginning of separating all of the data into categories. Axial coding is when the researcher determines one overarching theme or category and then provides supplemental categories whereas, selective coding is where the concepts intersect (Creswell & Poth 2018).

According to Creswell (2014), coding is the process of organizing data by chunks and writing category words associated to those chunks (p.198). The researcher coded the raw data and used open coding to identify themes across all of the data types that were collected and based on the data themes, the researcher created a themes crosswalk and included findings found in comparing documents from each of the identified institutions. The researcher identified commonalities such as similarities in language that pointed to a compliance-driven, values-based, or more undefined culture. Creswell and Poth (2018) mentioned that coding "is central to qualitative research and involves making sense of the text collected from interviews, observations, and documents" (p. 190).

For the purpose of the study, the researcher separated all data into an organized hierarchy of digital files and created a spreadsheet to document analysis. The researcher then categorized the information and stored it in a secure central repository that was only accessed by the researcher and protected the integrity of the data. Due to the proprietary nature of raw data that could have poses risk to participant institutions, the data was secured via encrypted laptop and no additional copies made.

The next stage of data analysis that the researcher conducted was review each of the transcripts and code them to identify themes in best practices that information security officers perceived to promote successful implementation of an information security program. The study included document review to identify which technical framework they were based on to understand how they were rooted. The researcher categorized those themes and looked for similarities during the comparative analysis.

The next step of analysis was to compare themes across data types and identify if there were any contradicting themes that did not align with each other (Creswell, 2014; Creswell & Poth, 2018). By cross-referencing themes and categories, the researcher developed a robust narrative of recurring concepts and best practices among security personnel. According to Creswell (2014), a description is a rendering of information about people, places, or events in a setting. For the information security setting, the researcher was looking for themes among the healthcare and academic environment that were prevalent in the blended health science center environment as addressed by the information security personnel in the implementation of their information security program.

Last, the researcher evaluated the interpretations from the analysis and themes that emerged and made determinations as to how they were interpreted and reported in the findings section of the study. Creswell (2014) defines this step as "making an interpretation and could involve meaning derived from comparing findings with literature or theories" (p. 200). In line with the social constructivist approach, the researcher worked to determine how security personnel constructed meaning of their programs and how staff perceived the program based on their own realities of

information security. Descriptive narratives create multiple levels of meanings toward information security, assisting the information security officer in successfully implementing a comprehensive security program that leads to end-user compliance.

Trustworthiness of the Study

A means to establish trustworthiness of the study is to demonstrate the equivalent of validity, which is defined as methods that the researcher uses "to demonstrate the accuracy of their findings" (Creswell, 2014, p. 250). The major tenants of trustworthiness are described by Lincoln and Guba (1985) as internal validity, external validity, reliability, and objectivity. Trustworthiness is more recently described by Creswell and Poth (2018) as credibility, transferability, dependability, and confirmability after Lincoln and Guba's original adaptation to the newer terms.

Internal validity, also known as credibility, is how accurately the researcher captured the participants' perceptions, context, and responses in relation to the researcher's understanding of the phenomenon (Lincoln & Guba, 1985). Strategies that can be used to establish credibility and that were used in this study included triangulation, member checking, and peer debriefing. Triangulation is described as the use of multiple data sources to compare or confirm the evidence that has been gathered (Creswell & Poth, 2018; Patton, 2015). Member checking is described as a process of sharing findings and their interpretations with the participants, seeking their feedback on what has been presented (Creswell & Poth, 2018). It also includes checking in with participants during their interviews to confirm the researcher's understanding as well as having them review their transcribed interview for accuracy. This was done both verbally and through email by the researcher to ensure that they

had captured and interpreted the responses of the participants accurately. Peer debriefing is defined as a review process, by someone other than the researcher, who reads the study, poses inquiries, and identifies if the study was one that others could subscribe to as well (Creswell & Poth, 2018).

External validity or transferability is defined as how accurate the researcher captured the case that was used so that it could be replicated with other cases reliably (Lincoln & Guba, 1985). The researcher identified a sample group that was bound by security frameworks that all academic health sciences centers in the state of Texas are bound to implement to be compliant with governing agencies. A strategy used to ensure transferability in this study was the use of thick, rich descriptions of the context of the research. To ensure transferability, the researcher provided thick, rich descriptions of the context, experiences, and detailed accounts of the study (Creswell, 2014; Korstjens & Moser, 2017).

Dependability is described as the process used to see if the study is traceable. In order to ensure dependability, the researcher sought an external audit of the data when the researcher followed up with participants to confirm correctness of information captured against transcriptions. The researcher also kept a record of processes used to ensure each interview was conducted the same for each participant and the researcher, documented responses based on the same research questions and used the same interview method for each participant to ensure accurate results of the study.

Confirmability is defined as the data used to develop logically sound and reasonable conclusions that can be verified as having factual support (Patton,

2015). The information confirmed was compared against the researchers reflexive journal to ensure any biases were not included in the data confirmed by participants and responses were also compared to other participant responses to identify if they were similar among information security personnel so that trends can be identified and captured in the excel spreadsheet. Lincoln and Guba (1985) recommend the strategy of reflexivity to ensure confirmability. Reflexivity in this study included the use of the researcher's reflexive journal as well as included the context of the researcher. These are important strategies to include because, as the primary instrument of data collection (Merriam & Tisdell, 2015), it is necessary for researchers to first consider and then set aside their own experiences and biases. The use of a reflexive journal allowed for the documentation of thoughts and musings of the researcher throughout the conduction of the study (Lincoln & Guba, 1985; Merriam & Tisdell, 2015). To serve as a bias check, the researcher journaled initial perceptions, interpretations, and thoughts through the duration of the study. The inclusion of the context of the researcher within the study allowed for the reader to develop an understanding of the lens through which the researcher conducted the study (Creswell & Poth, 2018). The context of the researcher involved a sense of self-reflection to identify any biases that emerged or prohibited the researcher from conducting a fair and objective study (Creswell & Poth, 2018). To reiterate, to establish reliability and confirmability, the researcher engaged in triangulation, member checking, and thick description, as an approach to create a reliable study that can be replicated in the future.

Context of the Study and the Researcher

Context of the Study

In order to expand the scope of research among the information security industry to include more human-centered, values-based, and behavior focused observations and analysis, the study was geared towards perceptions and experiences that lead to implementation of security programs in AHSC's in the state of Texas. The context of the study was set in Texas due to governance of the Texas Administrative Code that is applied to all state agencies. The requirements outlined in TAC 202 for the role of the information security officer as well as the purpose and scope for the information security program are consistent throughout the state of Texas and are measured by the same metric by the Department of Information Resources. The Department of Information Resources requires the biennial submission of the information security plan with maturity levels for each of the major security control families for all state agencies.

Context of the Researcher

As the researcher for this study, interest in the topic was rooted in personal observations from my role in information security assurance. It was an anecdotal interest in the challenges that stem from implementing an information security program in a blended environment where there are competing cultural contexts due to dichotomous value sets in each setting that the security program is implemented. The researcher's personal curiosity led to an interest in exploring factors that promoted a successful integration of a security program in a blended environment such as an AHSC and also understand the motivations and efforts of the information security

officer to be mindful of those unique settings to ensure success. While serving in information security, the researcher observed challenges to implementation and end user compliance, that mostly stemmed from staff who perceived that safeguards should not apply to them or that are frustrated with the security mechanism and requirement they perceived as an impediment to the staff person carrying out their duties. It is because of this personal observation that I sought to understand more about the context of staff who felt frustrated or challenged the security safeguard to have more insights as to how to meet the needs of the institution as well as the staff members trying to conduct operations.

Additionally, because of my role in information security assurance, I needed to be mindful of the trust that came with interviewing other professionals in the field. I needed to ensure that after collecting data explained from a technical perspective, I fully explained from the non-technical perspective if it was to be included within the findings of the study and available to lay persons not familiar with the intricacies of implementing an information security program.

Last, because I am currently employed in the information security environment, as an industry professional, I have a blended background that intertwines faculty experience with information technology (IT) roles, over a span of 20 years. My IT experience started as a fluke in middle school and was not apparent again until my first year of college. In middle school, I took a technology class as a recommendation from a counselor because they were introducing a new class. I was highly successful in it, acing exams that were technical for others but came easy to me. Though the class was easy, I did not pursue an interest in technology until I started college and

became a graphic artist for the university program office as part of the work-study program.

After serving as a graphic artist, I later became a multimedia specialist for the university IT department as a means of paying for school. Even after those multimedia years, I still did not pursue an interest in technology, it was simply how I paid tuition. At the same university, as a graduate student, I also worked as a teaching assistant as to build my higher education administration experience, however, after graduation, I moved back to my hometown and began working as a multimedia developer in a health care agency because that field had a better job outlook than higher education at the time.

I spent a year as a multimedia developer before starting a job as an adjunct instructor at my local community college and thrived in that environment, moving up the ranks over the course of the next few years. Ironically, my success at the community college was due to my experience with IT which led to serving on IT committees, quickly befriending the IT professionals at my campus, and being active in IT initiatives campus wide. Having all the signs pointing me back to IT, I still did not pursue a career in the industry as I enjoyed being in the classroom and connecting with students. It was not until I left the community college environment that I was hired as an IT analyst supporting the academic faculty. Having served in an academic setting for much of my professional career, I had served in the technical construction of course delivery systems, taught in both the community college and university environment, and served in an administrative role of technology regulation in an academic setting with a clinical influence.

At my role in higher education, I had served in the academic analyst role for 4 years before being offered a temporary role under the information security officer. It was known that I was in the doctoral program so the idea was to have me work for 3 months under information security to write all the departmental policies and then resume duties supporting academics. That temporary 3-month role turned into a permanent hire for IT Assurance and Strategic Planning. It turned out that I was the only person that enjoyed reading legislation, translating technical requirements into action items to keep our division compliant, and identifying technical gaps based on regulatory standards from government agencies.

As the new lead for assurance and strategic planning, I was tasked with building out a completely new IT division and with it came all things compliance, audit, and strategic planning related. Later, my success with legislation, regulatory controls, and technical standards led to me also becoming the institutional Electronic Information Resource (EIR) Coordinator and placed me again entrenched with the academic side to ensure all our technologies met electronic information resource accessibility regulations. Thereafter, I had a dichotomous role and served as the subject matter expert on all of the technical policies and compliance initiatives for IT and information security. To further complicate my responsibilities, my compliance role was also split among the academic environment as well as the clinical environment because our institution is a health science center and operated in both regulatory realms.

In the higher education role, I had an opportunity to explore security concepts and process to understand them with greater detail compared to those staff members

that encountered information security that was based on safeguards and protocols prescribed to them. My career path has always included an academic focus with a brief employment in a healthcare setting serving in an IT capacity, and through a culmination of multiple career roles, I found myself in a hybrid environment that combined both academic and healthcare, with me serving in an IT role.

From the standpoint of a security professional, I have had the opportunity to spend greater amounts of time researching and learning about the intricate and robust layers comprising information security programs. This experience provided insight about how an information security program functioned within an organization that most people do not get to experience outside of technical controls placed on their systems or training they received as part of the information security awareness and training campaign.

Summary

This qualitative study was a collective case study and the primary people interviewed included information security personnel or chief information security officers within the health science center environment within the state of Texas. Data collection was conducted by the researcher via semi-structured interviews, and document analysis, of institutions participating. Data was analyzed using open coding to construct themes and categories among all data sources to be interpreted and utilized to develop a final set of findings at the conclusion of the study.

CHAPTERI IV

RESULTS

Chapter IV presents the results of the study. The following topics were addressed: 1) summary of the research design, 2) overview of the study institutions and participant profiles, and 3) the findings of the study. The purpose of this study was to explore the perceptions and experiences of information security personnel (e.g., information security officers and those reporting to them) about the factors they perceived affected the implementation of information security programs within health science centers.

The following research questions guided this study:

1. What do information security personnel in health sciences centers perceive to be the challenges of implementing an information security program in a higher education environment?
2. How do information security personnel in health sciences centers assess information security compliance in their organizations?
3. How do information security personnel tasked with implementing components of an information security program in health sciences centers describe end users' security compliance behaviors?
4. What do information security personnel in health sciences centers recommend as best practices for implementing successful information security programs within higher education organizations?

Summary of the Research Design

This qualitative collective case study was conducted through the lens of the social constructivist paradigm, which allowed the researcher to establish a thorough understanding of how information security programs were implemented based on the perceptions of those authorized to do so in a blended academic and clinical environment. In a blended environment, business operations and regulatory compliance are priorities for an institution, but often come into conflict with end users regarding an information security program and user behaviors. Hedström et al. (2011) argued that end user's security behaviors come into conflict with the values embedded in their daily activities against the values assumed when security policies and standards were implemented within an organization; therefore, incorporating a values-based model that positions the organization to look at compliance from where the conflict was happening as opposed to controlling behaviors using heavy regulation enforcement. Prior to conducting this study, approval was sought from Texas Tech University's Human Research Protection Program, which was granted (see Appendix A). No further approval for human subjects research was needed from the study institutions.

Data Collection Processes

Data collection processes used in this study included semi-structured interviews, institutional documents, field notes, and the researcher's reflexive journal. Much of the data was also captured into Microsoft Excel spreadsheets for data analysis purposes. The first step in the data collection process was the recruitment of participants. A primary list of prospective participants was created in Microsoft Excel

with directory information as it was available. The initial inclusion criteria to participate in this study were that participants were information security officers who were employed at a health science center in the state of Texas. Contact information for each information security officer was collected from their respective institutional website and entered into a spreadsheet for tracking purposes. Some of the institutional websites only listed a department email address, which was not directly connected to the targeted population, which made recruitment more difficult.

Initial recruitment was done via email. The initial contact list included 10 potential participants who were sent an email script (see Appendix B) that included introductory information about the study as well as an Information Sheet that contained additional study details (see Appendix C). This initial email was sent out in early September 2021, with a two-week window to respond, and it yielded only one response.

After two weeks a second round of recruitment emails were sent in late September 2021 to all 10 of the original participants identified, with potential participants afforded another two weeks to respond. This second round of recruitment did not yield any responses, so recruitment efforts evolved to include phone calls. Additionally, the decision was made to recruit other information security personnel who were involved in information security program implementation. Recruitment continued with six phone calls made to each of the offices that had phone numbers listed on their departmental website, and emails sent to support personnel. Phone messages were left with four information security officers who had not responded to the prior two inquiries noted, with two of them responding affirmatively to the request

to participate in the study. The emails to support personnel included the same information as was used in initial recruitment efforts of information security officers, which resulted in five additional potential participants.

After confirmation with the responding potential participants that they were willing to participate in the study, semi-structured online interviews were scheduled with each of them through email, and a second copy of the Information Sheet was provided. After all of the recruitment efforts outlined above, the final number of participants who participated in the study was seven and included three information security officers and four others who had roles in implementing information security.

All semi-structured interviews were conducted virtually through Zoom video conferencing due to the COVID-19 pandemic. At the beginning of each interview, the interview protocol (see Appendix D) was reviewed with each participant, and they were advised that they could skip any questions they did not want to answer, and they could stop the interview at any point. Information for how the data was going to be used was reviewed, and steps taken to protect their privacy were discussed. Protection of privacy included the use of pseudonyms in place of institution name as well as participant's actual name. Each participant was asked if they would be willing to review their interview transcript once transcribed, of which they all agreed. The participants were asked if their interview could be audio and video recorded to ensure accuracy of the interview transcripts, and they all agreed.

Each interview followed a semi-structured format, which included the introduction to the study, overview of the purpose of the study, interview questions that were asked of all of the participants, and a conclusion section. Each participant

was asked if they had any questions prior to beginning each interview. Once all questions were answered, the interview began. During each interview, participants were afforded opportunities to converse freely and allowed to ask questions as the interview progressed (Patton, 2015). During each of the interviews, the researcher took field notes to document her observations (Creswell & Poth, 2018). All but one participant had their video on for the duration of their interview, as they had been working from home the day of the interview and preferred not to be on camera. A reflexive journal was used by the researcher throughout the conduction of the study to document her thoughts and to help maintain any potential biases due to her knowledge of the field under study (Creswell & Poth, 2018). Member checking was conducted during each interview as follow-up questions were asked of participants to not only verify their response, but to probe for additional information (Creswell, 2014). The interviews lasted between 30 minutes and one hour.

At the end of each interview, a summary of next steps for the data was again discussed as well as confirmation that participants would be willing to review their interview transcripts to ensure their accuracy, of which they all agreed.

After the interview was concluded, the automatic transcript from Zoom was downloaded and reviewed for accuracy. Several of the transcripts had errors because the Zoom transcription service did not accurately capture the speech of the participant, which made some of the automated transcripts unusable in their original form. For those interviews that the Zoom transcript were unusable, the audio files of the interview were downloaded and then transcribed by the researcher using Microsoft Word.

To check the accuracy of the participants' responses to the interview questions, a copy of the interview transcript was compared to the Zoom audio recording, and edits were made to correct inaccurate information in the transcripts. Inaccuracies that needed to be corrected included language that was incorrectly translated if the participant had an accent or pronunciation that was difficult to decipher by the software. Once the interview transcripts were reviewed for accuracy, they were sent via email to each of the participants for review, which is a form of member checking (Creswell, 2014). Each participant was requested to confirm the accuracy of their transcript, and to offer any corrections or clarifications needed. All but three participants responded with confirmation, clarification, or their own observations after reviewing their transcript for accuracy. Transcripts were stored in a research repository folder on the researcher's password protected laptop. Each participant had their own folder that was named using their pseudonym. Also included in the folders were artifacts documents specific to the institution of the participant.

The second data source in the study was publicly available policy documents, security awareness documents, and organizational charts that supported the information security program at the study institutions. During the interviews, some of the participants referenced those artifacts and mentioned that those items were integrated into the organizational software package and were proprietary information. Other institutional documents such as publicly available policy documents and some security awareness documents that should have been available on public facing departmental websites related to security awareness were limited in presence. On many of the study institutions' webpages, items that were available were the

institution's organizational charts in the Factbook section of their website, and the Acceptable Use Policy. For some of the study institutions, there was a link to the information security website.

The last two data sources used in the study were field notes and the researcher's reflexive journal. Field notes were captured during each of the participant's interviews and were not captured in a digital format but instead kept in a physical journal where notes were jotted down as the interviews progressed (Creswell, 2014). Notes included observations about the interview medium, participant's non-verbal nuances, and observations about the interview itself. In addition, a reflexive journal was used to capture rich description of nuances of the participant, references to activities that were familiar to the researcher that participants referenced, mannerisms that participants used to emphasize certain responses, and description of the rapport between the participant and the researcher. In addition, the researcher reflected on her thoughts and observations in general after each interview, to document any of her biases due to her knowledge of the topic. This data source was used to keep the lens of the researcher in balance with the data collected (Creswell, 2014). The reflexive journal was also not in digital format and instead a physical journal alongside fieldnotes.

Data Analysis Processes

To begin the data analysis process, all data sources were organized and transcribed using Microsoft Word or the automatic transcription in Zoom. Once all interviews, field notes, and reflexive journal were transcribed, they were read through multiple times to ensure familiarity with the data. After this step, the interview

transcripts, field notes, and reflexive journal entries were imported into a Microsoft Excel workbook in order to more easily organize all of the data by research question and then by participant. Each participant's pseudonym was noted on a separate worksheet tab in the workbook. In the worksheets, the top row headings were interview question, participant pseudonym, response trends, associated research question, and discussion points. Each row beneath the heading had an individual interview question and each participant's response. In a second Excel workbook, the same data were categorized according to interview questions tied to each of the four research questions. In Column A was the research question and each column next to it were the interview questions. Each row had all participants responses in the same cell per question. For example, if interview question three was relevant to research question two, it was mapped together.

The next piece of categorization was to take the interview questions that were mapped to each research question and put them together in a separate spreadsheet to visually provide another layer of categorization of the participants' responses. Doing this in a spreadsheet made it visually helpful to organize and compare responses from each participant across columns. Separating responses according to interview questions and participants were the first steps in organizing and categorizing the data to prepare it for analysis.

Analysis of the data occurred through the constant comparative method of analysis as well as open and axial coding. The constant comparative analysis is a process of "systematically making comparisons to generate explanations" (Patton, 2015, p. 590). Interviews were compared to each other as they were conducted as well

as during the transcription process (Creswell & Poth, 2018). In addition, they were read through multiple times to gain further familiarity with the data. All data collected through interviews, field notes, study settings' documents, and reflexive journal were compared to the data previously collected. Comparing the data allowed for similarities and differences within the data to emerge and to be documented (Merriam, 2009). These multiple data sources were triangulated as part of ensuring the trustworthiness of the findings of the study (Lincoln & Guba, 1985; Patton, 2015), which enabled the cross-checking of the information gathered (Merriam, 2009).

After the constant comparison of the data sources, coding processes were applied. Open coding and axial coding were conducted through Microsoft Excel. According to Creswell (2014), coding was defined as the process of organizing data by chunks and writing category words associated to those chunks (p. 198). After the data were compared at multiple levels, it was coded using open coding to identify themes across the data sources. Significant pieces of data were color coded (Merriam, 2009), documenting common keywords and phrases in the Microsoft Excel spreadsheet. A themes crosswalk was created and included findings identified in comparing documents from each of the study institutions and responses from participants. Themes and similarities such as key phrases, industry terms, and similar descriptions used in participant responses and observed during the comparative analysis were documented in the Excel spreadsheet.

The next step in the coding process was axial coding. Axial coding helped the researcher determine overarching themes or categories and then provides supplemental categories (Creswell & Poth 2018). Using axial coding, commonalities and differences

in responses were found that demonstrated trends in end user compliance and information security culture at each study institution. Data were then combined into specific categories using axial coding (Saldaña, 2009). Frequency counts were made of the number of times topics were identified through open and axial coding within the data sources. Categories were developed and redeveloped as repetition emerged. From there, the researcher was able to synthesize data into themes with key phrases supporting each theme (Saldaña, 2009).

By cross-referencing themes and categories to identify recurring concepts, best practices among security officers became evident. According to Creswell (2014), a description was defined as a rendering of information about people, places, or events in a setting. For the information security setting, themes emerged that were prevalent in the blended health science center environment as addressed by the information security officer in the implementation of their information security program.

Last, interpretations from the analysis and themes that emerged as well as determinations as to how commonalities were interpreted and reported in the findings section of the study were evaluated and documented. In alignment with the social constructivist approach, the objective was to determine how security officers construct meaning of their programs and how staff perceived the program based on their own realities of information security. The descriptive narratives created multiple levels of meanings toward information security, assisting the information security officer in successfully implementing a comprehensive security program that led to end-user compliance.

Study Settings and Participant Profiles

Study Settings

The sites for this study were institutions that had a Health Sciences Center (AHSC) designation through the state of Texas as a fully accredited center in good standing with accrediting agencies. In addition, the study settings were chosen based on the Information Technology Department having an Information Security Officer who reports to the CIO. The institutions that fell within the interview pool according to their Pseudonyms were:

AHSC – A was an AHSC in southern Texas that has a School of Nursing, School of Pharmacy, and Biomedical Sciences. The information technology department did not advertise their organizational chart, but their information security program seemed to be partially based on the NIST framework. It also looked as though the IT department was decentralized in nature meaning some of their personnel were shared external to the IT department. The Information Security Officer resided in another city but served in the same role on the host campus. Their policies were similar to the AHSC policies as the parent campus as well.

AHSC – D was an AHSC located in central Texas but only housed a School of Pharmacy. As of the academic year 2020, the total enrollment for the school was 236 total students. For this institution, it deferred to the organizational chart and reporting line for IT and information security for the main campus in the system. The institution also relied on the same policy structure as the main campus institution, so the only visible policy was that of the acceptable use policy made available to the general population.

AHSC – H was an AHSC located in central Texas. The AHSC had a School of Medicine, School of Nursing, School of Biomedical Informatics, School of Dentistry, and School of Public Health. This school had teaching partnerships with 3 hospitals within the city. They had over 4300 students enrolled and offer 13 graduate degrees as of 2017. In reviewing their information technology department, the CIO was part of the president's executive council and reported directly to the president. Further review of the site showed that only the leadership for Information Technology was centralized but the structure was decentralized to have IT mini departments and representation at each of the schools. This institution also had a chief information security officer, but the reporting structure was not clear. Additionally, the only policy information listed was a policy exception request site but no publicly available policies to determine framework used or followed.

AHSC – L was an AHSC located in northern Texas. It was comprised of the Graduate School of Biomedical Sciences, School of Health Professions, School of Medicine, School of Nursing, and School of Pharmacy. As of 2020, it had an estimated combined student enrollment at the AHSC of 1,713 students pursuing education in the medical profession. Examining the IT component in the organizational chart, the institution had a vice president of IT & CIO that reported to the executive vice president for finance & operations and an information security officer that reported to the CIO. Searching through the institution website, the only policy posted publicly was their acceptable use policy and information security policies were protected by authentication.

AHSC -M was an AHSC in central Texas. The AHSC had a School of Medicine, School of Nursing, School of Dentistry, School of Pharmacy, and School of Public Health. They had multiple Texas campuses throughout the central region of the state. The information technology was a centralized department and had a chief information security officer that reported directly to the CIO. According to their organizational chart, the IT department reported to the operations vice president and chief of staff. In reviewing the information security website, the program seemed to be based on an open-ended policy framework, and all their policies were posted in a public web page allowing for external persons to view them.

AHSC – R was an AHSC also located in northern Texas and was also part of a university system. As of 2020, it was made up of the School of Health Professions, School of Medicine, School of Nursing, School of Pharmacy, and the Graduate School of Biomedical Sciences. For this institution, it deferred to the organizational chart and reporting line for IT and information security for the main campus in the system. The approximate enrollment was 358 students enrolled as of 2020. The institution also relied on the same policy structure as the main campus institution, so the only visible policy was that of the acceptable use policy made available to the general population.

AHSC–S was located in central Texas and had a School of Medicine, School of Nursing, School of Dentistry, Graduate School of Biomedical Sciences, School of Health Professions, and was a member of university collaborative to offer a PhD in translational science. The information security officer at this institution reported directly to the chief information officer and the information security framework was not NIST-based. It was not determined if the information technology department was

centralized or decentralized. In reviewing their website, the staff of the information security group was published along with directory information to contact each of them. Their policies were listed for viewing but only if someone had an account with the institution to access them.

AHSC – T was an AHSC located in east Texas and had an approximate student population of over 10,000 students each year. The AHSC portion of the campus consisted of a school of Community and Rural Health as well as a School of Medical Biological Sciences. In reviewing the organizational chart, the school had an information security department that was separate from the information technology department, and both reported directly to the executive vice president. In terms of policy information, the only publicly available policy was their acceptable use policy that was accessible by doing a general search of their website.

AHSC–U was located in central Texas and had a School of Osteopathic Medicine, Graduate School of Biomedical Sciences, School of Public Health, School of Health Professions, College of Pharmacy, and School of Medicine. It had an information security department that reported to the CIO and had implemented an information security program aligned with HIPAA and TAC regulatory requirements. In reviewing their website, very little information about the department was not publicly available but policies and policy framework was NIST 800-53 and 800-171, which aligned with the criteria of the study participation.

Participant Profiles

Participants for the study were currently employed, full-time information security officers at AHSC's who reported to the CIO within the information

technology department at the time of the study. The information security officer position was outlined in the Texas Administrative Code (TAC) §202.71 and required to be in place at all state agencies.

Joseph was an Associate Vice President for Information Security and also had a title of Information Security Officer at AHSC- R at the time of the study. They were in the role for a little over two years and reported directly to the CIO who reported directly to the President. Joseph described IT within the institution as primarily centralized but acknowledged some minor decentralized units.

Eddie was an Assistant Vice President of Information Security and Information Security Officer at AHSC - L. They were in the role for three years and reported directly to the CIO. Eddie described IT as centralized but mentioned that the CIO had an executive management council that was referred to as the executive management team.

Samuel was an Associate Managing Director of Project Management and IT Assurance at AHSC - R. They were in the role for 9 months and served in Project Management for a few years when they expanded their title to include IT Assurance as part of their role. They reported directly to the CIO and described their division as centralized in nature.

Steven was an Associate Vice President of Information Security and had a working title of Chief Information Security Officer at AHSC - A. He had been in that role beginning in 2006 and reported to the Senior Vice President of General Counsel. They built the structure of their department to be 90 percent centralized with a few pockets of decentralized areas.

Isaac was an Enterprise Security Analyst and was in that role for a year and 10 months at AHSC - R. They reported directly to the Associate Managing Director for Information Security and described the IT Department as Centralized as it operated within the organization but decentralized in regard to distribution of work internal to IT.

Carl was a Chief Information Officer and Vice President for Information Technology and served as the Information Resource Manager at AHSC - L. They were in their position since December of 2017 and reported to the Chief Financial Officer. They mentioned that until a reorganization, they reported directly to the President but later to the Chief Financial Officer instead. They described their IT department as a hybrid model where some of the clinics had their own IT personnel that they worked closely with to ensure they were included in collaborative efforts across the institution. The environments AHSC – L on the academic and clinical side were different and functioned in an educational technology role within the individual school. When clarified, it was a reference to e-learning as opposed to IT.

Angela was an Associate Managing Director of Information Security and was in that position for a year at AHSC - R. They reported to the Assistant Vice President of Information Security and Information Security Office at their institution and described their IT department as a hybrid. It was mostly centralized but categorized it as 80% centralized and 20 percent decentralized.

Findings

Challenges to Implementing an Information Security Program

Research question one sought to understand what information security personnel in health sciences centers perceived to be challenges to implementing an information security program in a higher education environment. The analysis of the data produced three themes to answer this research question: 1) information security was seen as roadblock to operations and impeded business, 2) end users lacked knowledge of the role of information security, and 3) better relationships were needed between information security and end users.

Information Security Perceived as a roadblock.

All participants identified challenges related to the implementation of information security programs at their institutions. A common challenge discussed was that end users perceived information security as a roadblock to operations and impeded business within the organization. Carl, Joseph, Angela, and Isaac mentioned that end users perceived information security protocols were a nuisance and inconvenient, and when new initiatives were introduced into the environment, end users complained and pushed back. Some examples were shared by some of the participants. Carl (Chief Information Officer) mentioned that the complaining and push back was in part due to "every year more and more regulations come on." His point of reference was regulatory controls that were pushed down from governing agencies requiring more requirements and updates to control frameworks. Carl also communicated that "all of those things and of course all of the agreements, contractually, or by the business associates' agreements have to be evaluated and

managed so there is some manpower involved." Eddie (Vice President of information security and information security officer) pointed out that he perceived that "people just want to do their job, and they want the easiest pathway."

Isaac (Enterprise Security Analyst) and Angela (Associate Managing Director) both discussed the importance of balancing inconvenience and not affecting production considering all the layers of security need to be implemented. Angela specifically mentioned patching software and equipment as an example of a security initiative that was necessary to mitigate vulnerabilities in order to protect the institution but would be perceived as an interruption by end users. Isaac noted that "they could have as many security layers as they want but if that affects production in the school, in the healthcare then that's the hardest part of it."

When asked about challenges, Joseph agreed that information security was perceived as a roadblock, but that support was an education process for them to combat that perception. He specifically discussed a security incident that had taken place in their city that had helped the information security team educate end users and combat the perception of security being a roadblock. It allowed Joseph to request and receive funding for improved security, create awareness, and "have conversations he hadn't had previously." Eddie echoed the idea of balance but mentioned that he not only relied on his team to work with end users, but he engaged other technical teams within the institution to assist in troubleshooting when end users experienced technical issues.

Steven (Associate Vice President of Information Security) mentioned that due to the way he experienced pushback, he made every effort to test all new processes

and safeguards to minimize the chance of failure while also saturating end users with information about new efforts that may impact them. He mentioned that he did not want to introduce something that impacted his end users in a negative way if it did not have to, so they worked to minimize the impact by using the testing phase of development.

Another example of security perceived as a roadblock was the Research Department. Steven mentioned that it had always been a challenge working with that group and how they worked to go around security mostly regarding storage and enterprise-wide solutions because of cost, or lack of proper planning. Eddie pointed out, "They'll kick off their research and find out they're generating terabytes of storage and when they try to store it on an institutional server, there is a cost associated with that and to sidestep costs, researchers will buy their own off the shelf server. The risk of going that route was that if there is drive failure, there is a chance that all those years of research are lost because the server is not on the institutional network and not backed up periodically and not secured as well as enterprise equipment". Eddie continued that at his institution, he highlighted the importance of data handling because "it's institutional data until they publish it."

End Users lack knowledge.

The second most common response was the effort of getting information to end users regarding security safeguards or the perception that end users lacked knowledge of what information security was trying to do to secure data and the institution. Samuel pointed out the importance of getting everyone involved and getting their feedback so that security understood their "portion" in whatever

responses they provided back after information security sent them information. Eddie created a group of information security "champions" that served as the liaison between information security and their departments with the intent of "providing education" in order to "foster goodwill and get people on board" because to Eddie, it was important to build collaboration rooted in good communication. Joseph mentioned that he had used local instances of security incidents as a way of communicating the importance of security at his institution and in doing so, the perception of security had improved.

When discussing information that needed to be disseminated, Carl referenced the use of frameworks and development of policy that governed the information security processes and program at the institution. When frameworks were updated, policies should have changed, and annual audits were used to keep up with language modifications that would reside in policies aligned with updated frameworks.

Eddie specifically mentioned security awareness and advised that "the way you start to overcome (the challenge of phishing and security awareness) was just to work diligently with them." Samuel mentioned feedback and specifically noted that "they don't sit on any committees, it would just be when we send whatever we send to the end user if they have any responses."

This finding supported the argument Arachchilage and Love (2014) made when they found that "most computer users have a lack of security awareness" (p.305). Information security personnel mentioned that a lot of users were not informed or educated and that was why they emphasized education and awareness. In order to ensure robust training, many of the respondents referenced the Knowbe4 application to deliver training and phishing campaigns to test their users, as well as

educate them on a regular basis. Samuel referred to it as "pestering" as an effective form of compliance. Angela described her effort as "if you explain to them the reason behind it, most of the time they agree and they understand." Steven mentioned "they're unaware of policies for programs and then there's an occasion where they just don't care. They're aware of it but they're just like I'm gonna go do this anyway."

Better End User Relationships are needed.

The last challenge that came up more than once regarding end user support of information security protocols was that prior to the current information security officer taking on the role of the information security officer, they needed to improve the culture of the information security office because end users perceived the information security officer and their team as unapproachable and too authoritarian in implementing an information security program. Carl observed that what had "driven largely the success that we have of implementing security within our institution now compared to what it was before, is how critical it is for your ISO and your security team to be approachable by anybody and…and to really step back and listen." Carl also mentioned understanding the mindset and "that everybody else has a job to do too." For the ISO to step into the role of the information security officer, they needed to improve the culture of the information security office.

Carl further explained that in order to establish a collaborative partnership and end user support, they needed to change the culture of how information security was perceived at the institution and in doing so, the shift resulted in personnel changes and increased engagement with stakeholders at multiple levels. Joseph asserted that information security was difficult "because a lot of people that control budgets, which

control the business side of the organization, are faculty that are education based. It was really an education process for them and what you're trying to do and trying to overcome some of the perceptions that they have of security being a roadblock rather than being a partner and making sure their successful in what they're doing." Steven pointed out that "faculty can be difficult from time to time. You know, the masses for the business side of the house, of the typical end user. They never push back on anything but once you involve faculty in it, there's a lot of pushback there." Contrary to this sentiment, Samuel countered that the institution is pretty aware of the criticality of some of the things we are rolling out so wholistically I would say it is well received."

Assessing Information Security Compliance

The second question sought to see how information security officers in health sciences centers assessed information security compliance in their organizations. The findings resulted in three themes: 1) compliance was based on the behaviors of the end users, 2) Knowbe4 was a common platform to provide awareness training and used metrics to gauge compliance, and 3) information security officers supplemented compliance and compliance methods with individualized reports and assessments that were unique to their institution in order to gauge compliance and health of the information security program they are implementing.

The consensus of how information security officers assessed compliance was mostly based on the behaviors of the end user and whether they were successfully passing phishing campaigns sent out from the information security office and/or whether or not they were completing assigned security awareness trainings. This

finding was consistent with the argument Hedström et al. (2011) made when they stated that end user's security behaviors came into conflict with the values embedded in their daily activities against the values assumed when security policies and standards were created and implemented within an organization. Eddie claimed that "it's very important to have the participation of your people that work in your institution. In this case the faculty, staff, and students."

Joseph, Angela, Samuel, and Isaac disclosed they actively used "Knowbe4" as the platform that distributed phishing campaigns and provided trainings, and that this task was a contentious effort to get some end users to complete. To support the security awareness effort described in TAC 202, process custodians that provided awareness and training, relied on metrics pulled from knowbe4 that documented completion counts, phishing failure numbers and overall risk score to the institution if the phishing campaigns were legitimate attacks. In addition to Knowbe4, Eddie included the use of Proofpoint as a product in his program that provided metrics as well.

While the majority of respondents mentioned metrics related to security awareness and training, other types of assessments used included incident reports that were sent to the state when an incident occurred, and feedback from executives, students, administrators, consumer surveys regarding perceived approachability of the information security team as the result of a healthier information security culture. An example of state metrics used was described by Eddie as an external assessment conducted over the TAC 202, 42 controls that each state entity was required to adhere to. It was an external assessment that occurred every two years with results reported

back to the state pertaining to maturity levels of each control as it was implemented in the institution. For Eddie to gauge success of his program, he relied on metrics that revealed gaps in controls that he needed to remediate. Steven addressed assessments differently and instead consolidated all the required frameworks into one called HiTrust. It was a method where all of the requirements in HIPAA, PCI, FERPA, TAC 202, and any other frameworks they needed to comply with were in one large framework so instead of measuring compliance per each individual framework, they looked at one framework and measured compliance per a large list of requirements.

Perception of End User Compliance Behaviors

The third question sought to identify how information security officers and personnel tasked with implementing components of an information security program in health sciences centers described end users' security compliance behaviors. After analyzing the responses, most of the responses again revolved around the end user's lack of education and awareness as a means of justifying their non-compliant behaviors. To combat this, information security officers mentioned that they tailored their security awareness to their unique audiences.

Eddie and Steven had similar avenues for creating awareness and distributing information to end users which was through the use of security committees and "champions." Each found that by building collaborative groups, they were able to educate on solutions to security issues and explained why those solutions were the best solutions. Steven was adamant in clarifying that his committees were not approval committees but advisory committees that assisted him in finding the best solution with the least impact to end users and organizational business. The result of these efforts

was that security solutions and awareness was better received, and end users were more compliant because they finally understood the context surrounding why something was implemented or necessary.

One of the objectives of this study was to identify compliance according to either a clinical or academic environment and one of the institutions was particularly mindful of that concept. They noted that the audiences in a health sciences center had roles that spanned the academic and clinical environments, therefore the efforts to protect the different kinds of data would be slightly different in each environment and conversations around compliance with those security protocols was going to differ.

Respondents also mentioned other perceptions as reasons for end user non-compliance such as arrogance, complacency, and inconvenience or disruption to the operations as competing elements to what they needed to do. Angela mentioned "Sometimes you have users that um…for instance, the security awareness training…they hate it, and they will leave it until the end, until they start getting that email that says the people that have not finished this training, they will…a list of these people will be sent to executive management. Then you immediately see all those percentages of those people going up with people finishing their training. Unfortunately, that's human nature." This perception was aligned with the statement by Hedström et al. (2011) which advocated for incorporating a values-based model that helped the organization look at compliance from the perspective of where the conflict was happening as opposed to heavy regulation enforcement to control end user behaviors. To this point, Angela mentioned the need to use fear appeals to combat end user non-compliance. "The fear of losing your position or getting

reprimanded, or having a consequence that will affect your income, I think that's what makes them do something."

Best practices for Implementing a Successful Program

Similar to multiple information security frameworks, literature had not shown mutually agreed upon best practices to implementing a program. The last question in the study was to identify what information security officers in health sciences centers recommend as best practices for implementing successful information security programs within higher education organizations. When asked about the most successful strategies to implementing an information security program, the majority of the responses revolved around security awareness, education, and information made available to end users. Respondents felt it was important to ensure that initiatives introduced in the institution needed to be communicated with transparency, advantages described, and guidance on why complying with security protocols was important. Joseph described it from a "monitoring and control perspective" and mentioned that they provided constant communication to executive leadership as well as to the state, information on "any kind of incidents." Similarly, Eddie had a manager that spent half the work week communicating with his champions group important information about information security, and those individuals communicated back to their respective department where they served as the point of contact for information security issues as a first line of support, prior to escalating more technical issues to the information security group.

While most respondents advocated transparency and saturating end users with information, there was not much security awareness information on the information

security websites that promoted awareness at each of the institutions. The websites were sparse in offering that information, and any other policy documentation was protected by authentication controls. Looking at institutional websites, only one institution had a small piece of security awareness on it and that was a threat meter that tracked the severity of risk of attack to the institution. As of the last view of the site, the level was at a minimal elevated level and lower risk level.

Another theme that surfaced as an effective strategy was support from executive management and collaboration with end users. Carl, Eddie, and Steven mentioned how their seat at the executive table was beneficial for them to generate support regarding information security efforts, serving as a conduit for conversing about threats to the organization, the need for contentious security measures, and providing current state of security updates to institutional stakeholders. Engagement with end users seemed to be a priority for Eddie when he they mentioned the use of "champions" throughout many of his responses during the interview. Carl and Steven emphasized that the purpose of this effort was to provide a role for them to serve as subject matter expert on security related issues that go back to their departments and advocated for security while also bringing back concerns, inquiries, and feedback back to the information security group for consideration as they work to implement components of the information security program. Steven described it as "focused on security and how we can better manage our program and the controls around the specific technology that they support." Steven also mentioned that they valued the fact that "they have the attention of the President's executive committee and meets with them twice a year."

Summary

The use of a qualitative, collective case study conducted in academic health sciences centers in Texas yielded some interesting findings regarding how information security officers perceived implementing an information security program. The most recurring theme that emerged in many of the research questions was the use of security awareness and education for end users. While information security officers emphasized the importance of awareness, there did not seem to be a robust repository of resources readily available on the information security websites to promote awareness and education.

According to information security officers, challenges, best practices, and reasons for end user non-compliance, all revolved around the education of the end users at their institution. Not all information security officers agreed on how to combat those challenges but all of them relied on the same software application to deliver training and phishing to gauge the success of their efforts as well as work towards risk reduction at their institution.

Some perceptions varied due to the role the respondent had in implementing the piece of the security program they were responsible for. For example, not all the respondents were in a supervisory or management position and therefore did not have as much engagement with end users as other respondents did. Due to the difference in responsibility, some participants had a limited context in which to base their responses. The common thread among all of the participants was focused on education and awareness regardless of the role they had in implementing an information security program. Because of the heavy emphasis on security awareness, implementing a

program had potential to lead to risky environments and technically deficient information security infrastructure. Additionally, programs with such a pointed approach could have also positioned institutions for further ramifications if regulatory controls were not implemented within an information security program in a satisfactory fashion for external assessors. Additional ramifications of these findings are discussed further in Implications to Higher Education.

CHAPTER V

CONCLUSIONS AND RECOMMENDATIONS

Chapter V presents the conclusion of the study. Topics covered include: 1) an overview of the study and the findings, 2) implications and recommendations for higher education, 3) recommendations for future research, and 4) conclusion.

Overview of the Study

Information security within academic health science centers was important in establishing a security program and culture that balanced the open structure of the academic environment alongside a clinical setting. This need for an open structure created vulnerability for these centers. In 2015 higher education organizations were ranked 9th as a target for attack for cybersecurity incidents (Verizon, 2015). Higher education had consistently been targeted because of the types of data that were collected, processed, and stored within the higher education environment (Ulven & Wangen, 2021). In 2022 higher education was still a target and "Top patterns listed were: threatened both education and healthcare environments included system intrusion, basic web application attacks, and miscellaneous errors." (Verizon, 2022).

Ulven and Wangen (2021) mentioned that it was the responsibility of information security departments to implement measures to secure the environment, but as Hart (2015) claimed, users did not always follow the training they received or behaved in ways to secure data to prevent incidents and safeguards failed to consider human actions (Ki-Aries & Faily, 2017), which demonstrated a persistent risk to the organization (Ulgen & Wangen, 2021).

The purpose of this collective case study was to explore the perceptions and experiences of information security personnel about the factors they perceived affected the implementation of information security programs within health science centers. Of specific interest in this study was how these programs were implemented to remediate risk to the institution as well as to comply with federal mandates. The intent was to become more informed on best practices used to establish compliance in health science centers, according to the culture of either a clinical or academic environment, while also complying with federal and state mandates of an information security program.

This qualitative collective case study was conducted through the lens of the constructivist paradigm to answer the following research questions:

1. What did information security personnel in health sciences centers perceive to be the challenges of implementing an information security program in a higher education environment?
2. How did information security personnel in health sciences centers assess information security compliance in their organizations?
3. How did information security personnel tasked with implementing components of an information security program in health sciences centers describe end users' security compliance behaviors?
4. What did information security personnel in health sciences centers recommend as best practices for implementing successful information security programs within higher education organizations?

The study settings were institutions that were accredited AHSC's in the state of Texas and had an information security program implemented by information security personnel according to multiple regulatory frameworks. Each institution was composed of one or more of the following: A School of Nursing, School of Pharmacy, School of Medicine, School of Medical Sciences, School of Dentistry, School of Public Health, School of Health Professions, School of Community and Rural Health, and School of Osteopathic Medicine. Each AHSC was associated with a medical center and had a varied number of students enrolled depending on the program.

There were seven participants in this study who met the inclusion criteria to participate, which included whether or not they were tasked with implementing different components of an information security program in a health sciences center within the state of Texas, and whether or not they served in a management or program support role to implement various components of information security frameworks into their environment. Table 1 provides a summary of their profiles.

Table 1

Participant Profiles

Participant	Role	Framework	Reporting To	Study Setting
Eddie	Management	TAC 202, NIST 800-53	Chief Information Officer	AHSC - L
Carl	Program Support	HIPAA, FERPA, TAC 202	Chief Financial Officer	AHSC - L
Joseph	Management	HIPAA, FERPA, PCI, TAC 202	Chief Information Officer	AHSC - R
Angela	Management	NIST 800-53	Information Security Personnel	AHSC - R
Steven	Management	HiTrust	General Counsel	AHSC - A
Samuel	Program Support	NIST 800-53	Chief Information Officer	AHSC - R

Table 1, Continued

Isaac	Program Support	Unknown	Information Security Personnel	AHSC - L

The conceptual framework that framed this study was a values-based compliance model that was described as one where "groups within an organization act based on their different values" (Hedström, et al., 2011, p. 374) and examined the reasons for employee behavior regarding information security compliance that dictated their security actions rooted in intrinsic and extrinsic motivation. According to the values -based model, security behaviors were an "expression of values – values related to their profession" (Hedström et al., 2011, p. 374), and in terms of compliance, organizations did not focus on the human element of end user behaviors or their persona to understand security awareness and risk mitigation (Ki-Aries and Faily, 2017).

The findings for this study were derived using the values-based model as it pertained to value conflict, development of information security "rules", security behaviors perceived to express employee values, and extrinsic and intrinsic motivations. In terms of value conflict, the participants acknowledged conflict of prioritizing processes to support the business over implementing security protocols that disrupt some of those processes. Not everyone in the organization was motivated to subscribe to prescriptive information security because it contradicted other organizational values such as seamless operations, financial health, and academic success.

The model was also used to further understand the findings regarding the development of security rules and behaviors as explained through the lens of values based compliance regarding employee values that emerged during the study. One example of this behavior that was perceived to demonstrate value conflict was the mention of behaviors observed in the research department. The perception from participants was that the priority for researchers was centered on collecting large amounts of data throughout the course of their work. However, in an effort to minimize technology costs, security of the data was lower on the list of priorities that drove the research plan. Researchers' behaviors were perceived to be far different than behaviors of other employees and end users in the institution, which led to non-compliance of security rules that governed data protection and asset management.

The model was also used to explain the findings as they pertained to extrinsic and intrinsic motivations. One of the findings was how employees responded to security awareness training according to the value system they held. For example, if an employee demonstrated a positive perception of security when they were included in discussions and participated as "champions" for their department, it was because they had intrinsic motivations met of being an integral part of the organization. Those same "champions" were positioned to combat extrinsic motivations from employees that were aligned with the culture of the organization more than the protocols from information security because they were not privy to the same "insider" information champions were. Overall, the model was used to frame the findings into the scope of the values-based model to understand any similarities or contradictions to any of the

tenants of the model. Each of the tenants served as a baseline to understand the findings and categories that emerged.

Discussion of the Findings

Challenges to Implementing an Information Security Program

The first research question explored what information security personnel in health sciences centers perceived to be challenges of implementing an information security program in a higher education environment. The themes that addressed this question were: 1) information security was perceived as a roadblock, 2) end users lacked knowledge, and 3) relationships between information security and end users needed to exist for the program to be successful. The most persistent finding was participants perceived information security as a roadblock to security operations, impeded business, and was a leading cause for non-compliance. Carl pointed out that the roadblock perception was mostly attributed to more and more regulations that needed to be implemented annually, and the effort was a nuisance every time something new was introduced. This was not a new finding as it had been documented in the previous literature.

Rezgui and Marks (2008) found that new regulations coupled with the emphasis on new technologies to secure the environment were often not effective and seldom considered the human element of end users, which was also found in the research of Boss et al. (2009), Padayachee (2012), and Safa et al. (2016). The reason this finding was impactful was that cybersecurity is heavily regulated and governed to reduce risk to the organization to protect data, end users, and the institution itself. If end users perceived regulation to be a burden, they continued to behave in a manner

that increased risk and positioned information security personnel to heavily rely on technical controls over non-technical controls which in turn made end users feel as though the technical controls were restrictive to operations.

The effect of too much emphasis on technical controls as a roadblock leading to non-compliant behavior was originally cited by Herath and Rao (2009) and Hwang and Cha (2018), when they found that employees perceived security as an interference and therefore disregarded best practices especially with those that had limited access to sensitive data because they perceived compliance to be superfluous to their role in the organization. Not all participants agreed with literature about why security was a roadblock as security personnel had varied experiences with end users which in turn led to different perceptions. For example, Eddie's perception was contradictory to Herath and Rao's finding and believed that end users did not have difficulty with the safeguards but instead they did not know how to incorporate the safeguards into operations and often pushed back because of it.

To remedy this scenario, Eddie's team alongside the helpdesk would assist in developing a way to implement and practice safeguards in a way the end user could understand and comply with. Eddie's perspective and actions were important because it moved away from the idea that the difficulty was the control itself but instead how to incorporate it into the users daily operations. This perspective favored the end user as unique use cases instead of assuming the control could be implemented in exactly the same method for everyone. It proved that not all solutions are easily merged into the organization's operations. It confirmed the effect Rezgui and Marks (2008) discussed regarding the human element of the end user.

The other reason the finding about regulations was impactful is because the NIST framework which is the main framework that Texas Administrative Code Chapter 202 (TAC 202) is rooted in, is currently being updated to the NIST 2.0 framework. The NIST framework which was created as a response to U.S. Presidential Executive Order (EO) No.13636, 3 CFR 13636 (2013) to address an increase in cyber intrusions in organizations across the U.S. will include a revised set of requirements in every section and will also include a new section on governance. The governance section will involve more emphasis and accountability on the processes, procedures, policies, and assurance within an organization regarding security (National Institute of Standards and Technology, 2023). The new framework is currently in revision and soliciting final comments from impacted audiences (National Institute of Standards and Technology, 2023). If end users are struggling to comply with current program requirements and have pushed back, these non-compliant behaviors will continue when the revised version of the NIST framework is published, and information security personnel begin implementing components to update their program to be compliant.

The decisions to push back and disregard security advice was described by Kolkowska, et. al (2017) as "rationalities" and according to the values-based model described by Hedström, et al. (2011), groups in an organization needed to understand values that guided users behaviors. Employees were overwhelmed with technical controls, security regulations, and constant safeguards so much so that they viewed security as an impediment to their daily routines. Findings from this study proved that the competing values between information security personnel and end users were

consistent as those mentioned by Kolkowska, et.al (2017) and it also proved Alhogail (2015), that information security should be a culture change that values compliant human behavior because it is far more effective than relying solely on regulatory compliance. This is an important finding because when new safeguards are introduced, information security personnel have the opportunity to focus on continuing communication and collaboration with end users to build a strong support of compliance behaviors while facilitating organizational operations.

Culture as a value is also in alignment with Tang et al. (2015) that stated when information security officers and personnel involved in supporting an information security program are in alignment with the culture and values of the organization, there is a culture of conversation, collaboration, and success. The participants consistently mentioned how their programs improved when the information security office became more approachable, receptive to feedback, open to collaboration, and transparent. For example, Eddie mentioned that "it is very important to have the participation of your people". Paulsen and Coulson (2011) stated that an organization needed to create a healthy culture so that they could view information security as important and a relevant part of their role in order to support it and that was what participants did. A few participants noted that in order to improve the culture, they changed information security leadership to persons that were better suited to being approachable and problem solving as opposed to rigid and closed off to conversation. The decision to change information security management signaled that the organization is cognizant of the value of a healthy security department that works with mutual respect, consideration for end user engagement, and continuous improvement.

Assessing Information Security Compliance

The second research question sought to understand how information security officers in health sciences centers assessed information security compliance in their organizations. The findings were categorized into one main finding and one small acknowledgment among participants. Compliance was mostly focused on the behaviors of the end users, but a small number of participants mentioned assessments from external assessors using maturity models against their program to gauge compliance of their overall program. This requirement was defined in the Texas Administrative Code 202 to conduct risk assessments on a periodic basis and report findings to the Department of Information Resources (Texas Administrative Code [TAC] §202.75, 2021). These were normally in the form of individualized reports and assessments that included audit reports, incident reports, vulnerability reports, and other metrics requested by governing entities.

The importance of this type of metrics is that it holds information security personnel accountable just as much as end users and it provides a structure of what information security personnel are expected to implement according to an outlined set of requirements defined by the state (TAC 202). While this set of metrics is helpful to establish a maturity level for participants' programs, these assessments do not provide incentives for maturing or recourse for failing to mature. State assessments simply serve as informative in nature for information security personnel can use to benchmark or to strategize their program within their institution. Maturity levels also do not account for understanding information security rationalities behind what type implemented and how safeguards are prioritized over others, rather it is a measure of

whether or not requirements at each level are met. While rationality information may be presented in the interview and conversations with assessors, it is not documented in the final results of the program assessment.

These metrics can also be an additional set of reporting on top of specific requirements that pertain uniquely to the academic health science centers (AHSC). The state uses the NIST framework for governance and assurance but does not consider other frameworks that are relevant for AHSC's such as HIPAA or even PCI for patient accounts. Those frameworks are an additional audit set and much like the end users they serve, information security personnel can also experience value conflicts when trying to prioritize one framework over another to ensure compliance with each. The burden to meet requirements in each relevant framework can even impact the overall risk strategy and risk appetite in the institution.

Participants mentioned another type of metrics to assess individual end users through an automated software platform Knowbe4 which enabled information security personnel to provide information such as awareness training and provided access to a wide range of reports that can be sent to state officials, auditors, or even institutional leadership to support risk reporting that information security officers build into their strategy to safeguard the institution. These metrics can be large depending on the number of end users at the institution and can provide a high-level view of performance of the institution as a whole which support the effort to minimize risk and implement safeguards to protect the institution from attacks such as the ones that were the top reasons the Ponemon Institute reported as the reasons for data breaches (Ponemon, 2018). Daugherty and Tajuddin (2018) also described end user behavior as

a vulnerability to an organization for failing to comply with security safeguards. This is consistent with findings from the 2022 Verizon Data Breach Investigation report (Verizon, 2022), that stated "The human element continues to drive breaches." While Knowbe4 is a good source of education and awareness, it cannot make decisions on behalf of the end user if a legitimate phishing attack were to occur.

Security awareness and education as an assessment delivered through Knowbe4 is beneficial for tracking things like the number of incidents that have happened during phishing campaigns, the number of end users that have or have not been compliant with training, or the number of times an end user has fallen for phishing schemes, but it does not provide insight regarding the intrinsic motivations of end users as described by Kolkowska et. al (2017). Metrics in the Knowbe4 assessments are limited to phishing campaigns information security personnel create but do not capture the rationalities that led to incidents that take place in the institution and does not capture contextual information for the number of vulnerabilities found in the periodic scans. Knowbe4 is a tool that provides immediate reports but not to the level of understanding about why rationality conflicts exist within each end user or where those values are derived from.

Perceptions of End user Compliance Behaviors

The third research question explored how information security personnel tasked with implementing components of an information security program in health sciences centers describe end users' security compliance behaviors. There were two main categories to describe behaviors: 1) end users lacked education and awareness, and their lack of understanding security protocols was perceived as a means of

justifying their non-compliance behaviors, and 2) efforts to secure data within academic health sciences centers varied according to audiences with different data access roles.

Initially, end users were described as needing much help to understand security initiatives that were introduced to the institution. However, according to Huang et al. (2010), despite best efforts, security controls are not always successfully implemented. These security initiatives included prescribed security behaviors that participants described as being built into institutional policies and procedures and introduced via security awareness and training as a safeguard for the institution. When asked about the reason for non-compliance, most participants mentioned that security training was perceived as a nuisance, inconvenience, and interruption, and end users did not understand the required education.

This perception is important to consider because it highlights the value conflict between information security personnel and end users in how security awareness is received. Information security personnel advocate for training as a reliable means of preventing incidents but end users still lack motivation to even complete training. The disadvantage to difference in perception is that end users can skew training metrics due to lack of effort. For example, if an end user is hesitant to complete the training, they may rush through the education material simply to complete it but not with the goal of completing the training for comprehension and learning how to prevent security incidents.

Information security personnel still emphasized training and awareness as effective and as proof that education was helpful, Mamanov and Benbunan-Fich

(2018) found that when given more information, users were more responsive to the security requirements they were asked to follow. Many of the participants in this study said that they saturated their audience whenever possible because the perception was that end users preferred to see improved workflows, how information security protected the institution, and information that helped secure the home environment as well. This perception was supported by Arachchilage and Love (2014) when they found that personnel demonstrating proper *procedural knowledge,* experienced self-efficacy when they were properly informed. This is an important concept because when end users have knowledge and information available to them and are trained properly, they are more confident of behaving in a manner that is more secure and aligned with best practices. These compliant behaviors also make for a risk averse environment so the organization can continue to function according to business operations and organizational objectives.

The disadvantage to the manner in which security awareness is delivered is that it can also be information overload for some end users. There needs to be a balance between assessment and education so that end users have an opportunity to establish their own rationalities and perception of how to internalize the information and incorporate it into their daily practices. This is particularly important to those end higher education because Rezgui and Marks (2008) stated that security awareness was pivotal to organizational information security overall but particularly in higher education due to the emphasis on information sharing. This is an important practice because in a higher education environment, knowledge sharing is an intrinsic value

that is highly regarded so when information security personnel understand this, it is easier for them to align with the business operations.

The second behavior as perceived by participants was described as efforts to secure data that varied according to audiences and different data access roles. To adapt to the unique environments of their institution, participants mentioned that they supplemented compliance methods based on the audiences. One audience group mentioned consistently was the research department and their challenge to safeguard research data. The research group as a challenging audience is importance because participants must incorporate data loss prevention strategies that are not always well received by the institution because it was perceived to stifle academic research and collaboration. This was an impactful finding because higher education research is a funding source to keep operations running and lack of research can prove to hamper academic innovation. The role of information security personnel is challenging because TAC 202 requires data protection but in research departments, that effort needs to be a collaborative effort and that is not always the case according to participants.

An additional challenge to information security was that participants noted the difficulty of providing access for environments with distinctly different access roles. Audiences in health sciences centers had roles that span both academic and clinical environments, therefore the efforts to protect different classifications of data slightly differed in each environment. Rezgui and Marks (2008), argued that universities were highly unsecure due to an open network and infrastructure to meet the needs of multiple types of end users and facilitate sharing large amounts of data.

This finding is proven to persist as a problem for both higher education as well as the healthcare environment because it was mentioned in multiple Verizon Data Breach Reports ranging from 2015 to 2022. As recent as 2022, researchers calculated "this year 82% of breaches involved the human element." (Verizon, 2022), The values conflict taking place in this challenge is that the higher education and clinical environments compete for how open or regulated the environment functions however, faculty that operate in both environments cannot operate in both environments without adapting to the safeguards unique to each. This behavior causes end users to prove the perception that security is a roadblock to operations. These safeguards are integral to demonstrate compliance with the components of an information security program required by the state as well as requirements for competing frameworks.

It is also important to note that separating the two environments requires implementation of technical safeguards and access controls and according to Ki-Aries and Faily (2017), relying too heavily on technical safeguards detracts from focusing on the person. This proves the assertion by Hwang and Cha (2018) studied regarding non-compliance that employees face "complexity, overload, and uncertainty" every day, and security brings about stress (p. 283). This means that security can be a perpetuating cycle for the AHSC environment due to the need for heavy technical controls to align with multiple governing frameworks resulting in a challenge for end users that are forced to navigate each environment according to different security behaviors. This also means that the rationalities will continue to be in conflict as the goals and values needed to function in each environment will differ between patient car and academia.

Best practices for implementing a successful program

The last research question sought to understand what information security personnel in health sciences centers recommended as best practices for implementing successful information security programs within higher education organizations. The two most common responses that were identified included: 1) Security awareness efforts, education, and accessibility of information for end users, and 2) Support of executive management and collaboration with end users. According to Rezgui and Marks (2008) "security objectives cannot be met by technical and procedural protection only; an educated security attitude of employees, management, and external information technology users and partners was also vital to ensure effective information services security" (p.243).

Respondents felt it was important to ensure initiatives introduced in the institution were communicated with transparency, a focus on operations, and guidance on why complying with security protocols was important. This finding is consistent with the argument Rezgui and Marks (2008) made when they found that the best way to minimize risk was to provide security awareness training. However, this finding revealed that not all participants implemented awareness in a manner that was easily accessible to audiences. TAC 202 mentioned policies as one component to an information security program and in the capacity of security awareness, there was not much security awareness information on information security websites that promoted awareness at each of the institutions. This was inconsistent with remarks on transparency and guidance and seemed to contradict one of the main assertions information security personnel tried to make. This finding demonstrated efforts to

preserve confidentiality, which is a primary objective for the information security office.

The second practice for a successful program was the need for support from executive management that needed to have top-down buy in to incorporate a collaborative problem/solution approach with operational objectives, security posture, and end user support in mind. This finding was presented by Kuo (2009) to describe the impact of relationships at various levels of the institution and how it impacted respect, collaboration, and conflict resolution. All of the participants agreed that collaboration was important and facilitated a successful information security program. Some participants mentioned that they "have a seat at the executive table" but other participants mentioned that they had to rely on the chain of command to communicate or escalate security concerns or risks to the institution. This finding is indicative of the perspective of information security personnel that value the opportunity to have a voice in the organization. It also demonstrates the importance of communicating information that is most beneficial and informative for institutional leadership to make informed decisions when developing the risk posture for the institution and enables them to model appropriate security behaviors as described by Van Niekerk and Von Solms (2010).

Implications for Higher Education Practice

The findings from this study presented several implications for information security personnel in academic health science centers. The first implication for academic health science centers was that emphasis on education and awareness as the first and persistent strategy in order to implement a program did not support a

paradigm shift if the motivations of end user compliance were not thoroughly studied and end user behavior understood. Hedström et al. (2011), argued that lack of end user behaviors continued to be the reason for security incidents in organizations. Myyry et al. (2009) found that not only were there multiple value types that guided compliance behaviors, but values were displayed through behaviors that were also considered "self-presentation" (p. 129), and that moral reasoning intertwined with values lead a person to make judgments about compliance behaviors. None of those concepts were mentioned in the responses of participants therefore demonstrating that rationalities and the human element are not considered when implementing a security awareness component of the overall information security program. The result is that higher education will continue to be a target and will continue to have a high number of security incidents taking place which in turn introduces more risks to the institution.

According to the 2022 Verizon Data Breach Investigation report, "The human element continues to drive breaches. This year 82% of breaches involved the human element" (Verizon, 2022). In the context of an academic health science center where end users had access to data that was required to be safeguarded by significantly more regulatory controls than a traditional higher education environment, the risk of end users being the leading cause of an incident was still unresolved and rationalities that guided their behaviors and motivations to comply were left unexplored and left out of consideration when implementing a security program and regulatory controls. Given that cyber threat persists, security controls, regulations, and updated frameworks continued to be necessary and therefore, end users will continue to view information as a roadblock.

Credentials theft was among the top type of data lost in a data breach and enabled malicious threat actors access to servers as well as web applications housing confidential data (Verizon, 2022). This could result in compromised patient data, research data, student data, financial data for both students and patients, and proprietary data accessed by higher education administration. For higher education, this kind of exposure would not only result in data held hostage and susceptible to ransomware, potential loss of future funding for research projects, and an increased need for cyber insurance as well as potential increase in cyber insurance premiums, if not secured in the environment. Because an academic health sciences center is a blended environment of a healthcare environment and academic environment, the implication is that it is more attractive to malicious threat actors.

Multiple participants in the study mentioned the research department was a constant challenge to secure due to their lack of adequate planning for technology when applying for grants. If credentials were lost and access to servers was gained by a malicious threat actor, the institution would stand to lose data integrity, data availability, and data confidentiality of research awarded under whatever grant the institution had received, including federally funded grants. Additionally, a breach could result in fines from governing entities, legislative bodies, educational accreditors, and federal regulators according to the type of data lost. For example, losing Health Insurance Portability and Accountability Act (HIPAA) data could yield different penalties and sanctions as losing academic data. The Office of Civil Rights now has the right to seek criminal penalties for data loss involving HIPAA information. Above all else, data loss could also result in serious reputational damage

to the institution and the university system, crippling future recruitment, research opportunities, state funding, and even accreditation in extreme cases.

In alignment with Boss et al. (2009); Padayachee, (2012); Safa et al. (2016) the reliance on technical controls over human error, the institution could rely on products to secure the environment over education and sometimes equipment is costly therefore, the organization sought other means of protection. To secure the environment, organizations turned to cyber insurance as a layer of protection, but it had become more stringent and often harder to acquire. Cyber insurance companies are implementing protocols to ensure that organizations are doing due diligence to secure the environment prior to insuring the institution. If found to be negligent, the institution could stand to be financially responsible for any breaches, which could potentially bankrupt the institution.

Verizon (2022) pointed out that malicious threat actors have become more sophisticated and so have the tools used to infiltrate an organization therefore, the payout sought was financially lucrative. Threat actors do not pursue small ransomware amounts that could be easily paid out, instead they seek larger amounts of financial compensation to account for the investment they've made to infiltrate an organization. Hacking efforts are not only expensive but are time consuming as well.

Verizon (2022) noted that one of the most frequently used types of attacks was a denial-of-service attack. In a DoS attack, technical controls were compromised. In the study, information security personnel emphasized technical controls alongside awareness however, if an attack on technical controls took place as an advanced

persistent threat, it would take far longer to track down the source of the attack as opposed to remediating the attack.

Recommendations for Higher Education Practice

The study findings are a good baseline to a few recommendations for higher education that should be considered. The first recommendation is that higher education staff and information security personnel should work together to establish better working relationships and risk management partnerships at multiple levels to establish mutual respect and appreciation for the roles of all involved in implementing an information security program. Hedström et al. (2011) defined the values-based compliance model as one where "groups within an organization act based on their different values." This recommendation would be an opportunity to explore differing values and establish an understanding of how those groups operate within the organization. Grecmanova et al. (2015) and Spierling and Palmer (2020) established the importance of higher education relationships as they pertained to respect, healthy conflict resolution, and promotion of the mission and goals of the institution. Eddie, Joseph, and Steven all pointed out that when they stepped into the role of information security officer, they worked a great deal to change the culture and perception of the Information Security Office left by the previous officer so that end users were more comfortable approaching information security personnel.

According to the definition by Kuo (2009), fragmentary relationships were those that were disconnected, and siloed due to administrative, interpersonal, or bureaucratic challenges. Information security was perceived as a roadblock therefore the state of some relationships in higher education was fragmented between

information security and end users and in some cases, between information security and institutional administration. The challenge was rooted from the origination of information security as a lower priority and served in a technical capacity (Alexander & Cummings, 2016), but had since evolved to a more involved role within the institution.

Participants Eddie and Steven both mentioned that they had executive support, but that relationships were not consistent among all of the information security personnel that participated. Continued support from executive management is needed to correct the fragmented relationships that some institutions experience.

The second recommendation is to improve assessments to include more qualitative methods that address more of the "human" side end user compliance. This recommendation supports the basis behind values-based compliance model that looks to incorporate other reasons for employee behavior that is outside the scope of traditional regulatory-based compliance (Kolkowska et al., 2017). This recommendation also satisfies the argument that Hedstrom et al. makes when stating that there is a lack of understanding of end user behaviors and values of the environment that continues to lead to security incidents. Eddie pointed out more than once during his interview that "it's very important to have the participation of your people that work in your institution. In this case the faculty, staff, and students." Eddie's response was an example of the importance of understanding the end user audience in order to garner participation, collaboration, and compliance. According to the values-based model, it was important to facilitate understanding of the rationalization behind end user behaviors regarding security protocols. Quantitative

metrics pulled from security awareness only demonstrated if compliance took place but did not offer insight into the decision making of those being assessed.

The third recommendation is to develop a multi-modal security awareness program that goes beyond the traditional education and awareness methods and include a qualitive component to complement technical, and administrative controls that are heavily used in initial safeguards in an information security program. The multi modal approach supports the concept Kolkowska et al. (2017) in the values-based model to fully understand both extrinsic motivations as well as intrinsic motivations and rationalities. This recommendation includes a formal education program as part of the onboarding process and awareness initiatives to supplement automated trainings. Qualitative efforts include panel discussions, interviews, focus groups, and concentrated conversations that present threat information, risk avoidance information, and extensive engagement with end users. This recommendation in alignment with a finding in the study by Mamanov and Benbunan-Fich (2018) that provided threat information to end users and proved a positive correlation to improved security behaviors when given threat information.

The last recommendation for higher education practice is to keep up with frameworks and industry advances as they are updated to be more proactive about advances that first adopters pursue and may inadvertently introduce risk to the institution. This includes continuing education and awareness regarding implementation of information security controls to include additional forms of communication and engagement, network segmentation, more concentrated effort to understand motivations of end users and how they rationalize security controls,

increased communication and education on policies that impact departments, and collaborative efforts to improve and develop organizational process that support the objectives of the institution as well as information security requirements. The motivation behind this recommendation is to address the argument Kolkowska et al. (2017) makes to justify the need for the values-based model that combats the information security management style based primarily on policies and guidelines that have been established without end user values considerations. This recommendation is in pursuit of the multiple layers of safeguards described in the Texas Administrative Code §202 (TAC, 2018). The justification for additional forms of communication and engagement is meant to address the finding from Huang et al. (2010) that security controls are not always successfully implemented.

Recommendations for Future Research

Given the limited literature about the rationale behind end user behaviors as they pertain to information security compliance, there is significantly more research needed in this area. There is value to fully understanding the motivations of end users that go beyond organizational behavioral theories and seek more comprehension of how values rationale is carried out in the actions and decision making of end users. It would be useful to conduct a qualitative collective case study to understand how end users followed their motivation for compliance based on their value prioritization and judgment.

A second area or future research could be mixed methods study understanding how the pandemic restructured the information security landscape to account for a significantly higher number of remote employees. The pandemic positioned higher

education to adapt over a short period of time to continue teaching and learning and in doing so, efforts to secure the environment grew as the scope of the connectivity perimeter grew. The study could look to understand the perceptions of information security personnel as they restructured processes and procedures to maintain business continuity while securing the institutions to minimize the number of incidents encountered during the pandemic. Information security personnel now account for assets within and outside of their immediate network. Additionally, due to the increase of personnel working remotely, their behaviors change as well. The behaviors and precautions faculty and staff normally take while in the workplace environment are not consistent with the precautions taken in their home environment. Research could benefit from exploring how information security officers are adapting to the remote nature of securing an academic health science center post pandemic and newer cybersecurity threats.

The third area of future research is based on innovation such as artificial intelligence software and the impact to information security in a blended academic health science center (AHSC) environments when used without comprehensive understanding of security focused rationalization that drives behaviors needed in the institution. A mixed methods case study could look at rationalities and perceptions about how to implement governance around AI while also examining the regulatory controls that become part of updated frameworks that information security personnel incorporate into the security program. Innovation has specifically prompted an interest in artificial intelligence that could position both early adopters as well as malicious threat actors to use AI whether it be generative AI or sentient being to expose and

infiltrate environments with high value protected data however, AI is till unregulated and lacks mature governance protocols. AI can be researched further from an anthropological perspective to understand it's impact to the culture of an AHSC environment. To ensure a foundation of information security to control AI, information security leadership would need to understand pending legislation and framework updates to incorporate policy text into the administration of information security within their institution that govern security behaviors because the reality is that you can govern the asset owners but not the technological assets themselves.

Conclusion

Chapter V presented the conclusion and discussion of the findings that resulted from the study. The main sections included: 1) an overview of the study and the findings, 2) Implications and recommendations for higher education, 3) recommendations for future research, and 4) Conclusion. The main findings for the first research question were: 1) Information Security is perceived as a roadblock, 2) End users lack knowledge and 3) There need to be better relationships between information security and end users. The main findings for the second research question were: 1) Information security compliance is based on behaviors of the end users, 2) Knowbe4 was the most common platform to provide metrics and provide awareness training, and 3) Information security personnel supplement compliance methods with individualized reports and assessments unique to their institution. The main finding for the third research question was that a lack of education and awareness is why users are non-compliant therefore information security personnel tailor their security awareness to their audiences. The main findings for the fourth research question were categorized

as : 1) Security awareness efforts, education, and accessibility of information for end users, and 2) Support of executive management and collaboration with end users. Security awareness, education, and availability.

The implications to higher education were: 1) emphasis on education and awareness as a strategy did not result in a paradigm shift if rationalities were not considered in the awareness and education, and 2) Human error persists and the institution is required to fall back on more compensating controls resulting on continued perception that information security is a roadblock.

The recommendations to higher education are: 1) Higher education staff and information security personnel need better working relationships and risk management partnerships, 2) Improved assessments need to include qualitative measurements to account for the human element of end users, 3) Information security officers need to develop multi-modal awareness to go beyond traditional security methods, and 4) Information security personnel need to incorporate more proactive efforts to keep up with frameworks to avoid a reactive approach to changes.

Recommendations for future research include: 1) Explore the rationale behind end users security compliance, 2) Seek to understand how broadly the pandemic has restructured the information security landscape, and 3) Explore the impacts of innovation such as artificial intelligence as an unregulated novelty with little to no governance required around it yet.

The overarching consensus was that information security officers rely heavily on a partnership with their end users, leadership, and industry standards to implement an information security program. The most visible component to do so is via security

awareness and education in an effort to continuously inform end users and prevent incidents as best as possible. Information security personnel emphasize the need for an improved culture and perception of information security within their environment and support to secure their institution and rely on a variety of metrics and benchmarks to gauge the maturity of their program for continuous improvement.

Many of the information security personnel recognize the different methods available to garner end user compliance and acknowledge that users have different motivations when following information security advice. Information security personnel also acknowledged the uniqueness of an academic health sciences center as it differentiates from a traditional higher education environment in that the regulatory controls and cybersecurity frameworks are far more stringent and require strict adherence to controls in order to secure positive external assessments and good status for the institution.

Overall, there seemed to be a healthy balance of basic understanding of the motivations of end users in regards to information security in the academic health science environment but there is still a need for improved understanding of rationale that leads to compliant or non-compliant behaviors. Information security personnel seemed to have cultivated more positive working partnerships than some of them inherited but they recognize the importance of communication and collaboration to ensure their efforts align with and support the mission and objectives of the business. Each of the participants noted that there is still much room for improvement within their institutions, but they also acknowledged that they have the tools and support to continue moving forward with their end users.

REFERENCES

Alexander, A., & Cummings, J. (2016). The rise of the chief information security officer. *People + Strategy, 39*(1)*,* 10-13.

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49,* 567-575.

Alhogail, A., Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology. 24*(2)*,* 540 – 549.

Al-Kurdi, O., El-Haddadeh, R., Eldabi, T. (2018). Knowledge sharing in higher education institutions: A systematic review. *Journal of Enterprise Information Management, 3*(2), 226-246.

Altbach, P.G., Gumport, P.J., Berdahl, R.O. (2011) American higher education in the twenty-first century: Social, political, and economic challenges. In P.G. Altbach, P.J. Gumport, & R.O. Berdahl (Eds.), *The Contexts of American Higher Education* (3rd ed., pp. 2-11).

Altbach, P.G., Gumport, P.J., Berdahl, R.O. (2011) American higher education in the twenty-first century: Social, political, and economic challenges. In P.G. Altbach, P.J. Gumport, & R.O. Berdahl (Eds.), *Patterns of Higher Education Development* (3rd ed., pp. 16-36).

Amaio, T. E. (2009). *Exploring and examining the business value of information security: Corporate Executives Perceptions,* (Dissertation).

Arachchilage, N.A.G., Love, S. (2014) Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, (38).* 301-312.

Association of American Medical Colleges (2023). About AAHCI. https://aamc.org/career-development/affinity-groups/alliance-and-aahci/about-aahci

Barker, J. (2019) The human nature of cybersecurity. *Educause Review. Spring 2019.* 11-17.

Barrett, D.J. (2008). The evolving organizational structure of academic health centers: The case of the university of Florida. *Academic Medicine. 83(*9). 804- 808.

Bassett, G.C., Hylender, D., Langlois, P., Pinto, A., Widup, S. (2020) Verizon. The 2020 Verizon data breach investigation report. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Bess, J. L., & Dee, J. R. (2012) *Understanding college and university organization: Theories for effective policy and practice.* (Volume 1) Sterling, VA: Stylus Publishing.

Bialaszewski, D. (2015). Information security in education: Are we continually improving? *Issues in Informing Science and Information Technology. 12,* 45-54.

Boss, S. R, Kirsch, L. J., Angermeier, I., Shingler, R.A., & Boss, R.W. (2009). If someone is watching, I'll do what I'm asked: Manditoriness, control, and information security. *European Journal of Information Systems. 18,* 151-164.

Cervone, H. F. (2016). Information doesn't always want to be free: An overview of regulations affecting information security. *Digital Library Perspectives, 32*(2), 68-72.

Coffman, D. (2014, September). Managing data protection in higher education. *Risk Management Magazine.* https://www.rmmagazine.com/articles/article/2014/09/01/-Managing-Data-Protection-in-Higher-Education-

Cohen, A.M., & Kisker, C.B. (2010). *The shaping of American higher education: Emergence and growth of the contemporary system*. (2nd edition). Jossey-Bass.

Craig, D. J. (2017). Ensuring compliance with the HIPAA security rule: Think twice when e-mailing protected health information. *Nurse Practitioner, 42*(6)*,* 12-14.

Creswell, J. W. (2014) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. (4th edition) SAGE Publications.

Creswell, J. W., & Poth, C. N. (2018) *Qualitative Inquiry & Research Design: Choosing Among Five Approaches.* (4th edition) SAGE Publications.

Crowe, S., Creswell, K., Robertson, A., Huby, G., Avery, & Sheikh, A. (2011) The case study approach. *BMC Medical Research Methodology, 11*(100)*,* 1471-2288.

Da Veiga, A., Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security, 70,* 72-94.

Dance, S. (2014). Hacking incidents prompt universities to rethink balance between openness, security. *The Network Journal.* https://tnj.com/hacking-incidents-prompt-universities-to-rethink-balance-openness-security/

Davies, S.M., (2009). Introducing academic health science centres. *British Journal of Healthcare Management 15*(4).

Delaney, B., Moxham, J., Lechler, R. (2010). Academic health sciences centres: An opportunity to improve services, teaching, and research. *British Journal of General Practice, 60*(579), 719-720.

Denzin, N. K., & Lincoln, Y. S., (2011). *The SAGE Handbook of Qualitative Research* (4th edition) SAGE Publications, Inc.

DeVore, S. D., & Figlioli, K. (2010). Lessons premier hospitals learned about implementing electronic health records. *Health Affairs, 29*(4), 664-667.

Dlamini, R.S., (2015). The role of the strategic and adaptive chief information officer in higher education. *Educational information technology 20,* 113-140.

Doherty, N. F., Tajuddin, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. *Information Technology & People, 31*(2), 348 – 367.

Dzau, V. J., Ackerly, D. C., Sutton-Wallace, P., Merson, M. H., Williams, R. S., Krishnan, K. R., Califf, R. M., (2010). The role of academic health science systems in the transformation of medicine. *Viewpoint, 375,* 949-953.

Edelman, A., Taylor, J., Ovseiko, P.V., Topp, S. (2017). The role of academic health centres in building equitable health systems: A systematic review protocol. *BMJ Open, 7*(5). 1-6.

Ehrenberg, R.G. (2012). American higher education. *Journal of Economic Perspectives, 26*(1). 193-216.

Eyadat, M. S. (2015). Higher education administrators roles in fortification of information security program. *Journal of Academic Administration in Higher Education, Fall 2015 11*(2). 61-68.

Exec. Order No. 13636, 3 C.F.R. 11739-11744 (2013). – Improving critical infrastructure cybersecurity. /12/executive-order-improving-critical-infrastructure-cybersecurity.

French, C.E., Ferlie, E., Fulop, N.J. (2014) The international spread of academic health science centres: A scoping review and the case of policy transfer to England. *Health Policy, 117,* 382-391.

Gantt, G. (2014). Hacking healthcare: authentication security in the age of meaningful use. *Journal of Law and Health, 27,* 232-259.

Gardner, L. (2017). Keeping up with the growing threat to data security. *The Chronicle of Higher Education.*

Grama, J. (2016) Risk management basics. *Educause Review.*

Grecmanová, H., Dopita, M., Cabanová, V. (2015). Communication in the academic environment and its influence on organizational climate of universities. *Media, Culture and Public Relations, 6*(2), 119-127.

Hart, M. (2015). Data security in higher ed: A moving target. *Campus Technology.*

Hedström, K. Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems, 20,* 373-384.

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

HIPAA Journal (2018). *HIPAA compliance checklist.* HIPAA Journal https://www.hipaajournal.com/hipaa-compliance-checklist/

Hoeijmakers, M., Harting, J., & Jansen, M. (2013). Academic collaborative centre Limburg: A platform for knowledge transfer and exchange in public health policy, research and practice? *Health Policy* 111, 175 – 183.

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology, 29*(3), 221-232.

Hwang, I., & Cha, O. (2018) Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior, 81,* 282-293.

Joubish, M. F., Khurram, M. A., Ahmed, A., Fatima, S. T., & Haider, K. (2011). Paradigms and characteristics of a good qualitative research. *World Applied Sciences Journal, 12*(1), 2018 – 2087.

Karanja, E., Rosso, M. (2017). The chief information security officer: An exploratory study. *Journal of International Technology and Information Management, 26*(2), 23-47.

Korstjens, I., & Moser, A., (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice, 24*(1), 120-124.https://doi.org/10.1080/1314788.2017.1375092

Kayworth, T., Whitten, D. (2010) Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive, 9*(3), 163 – 175.

Khan, S. I., Hoque, A. S. M. L. (2016) Digital health data: A comprehensive review of privacy and security risks and some recommendations. *Computer Science Journal of Moldova, 24*(2), 273-292.

Ki-Aries, D. & Faily, S. (2017) Persona-centered information security awareness. *Computers & Security, 70,* 663-674.

Kolkowska, E., Karlsson, F., Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method. *Journal of Strategic Information Systems, 26,* 39-57.

Kuo, H. (2009). Understanding relationships between academic staff and administrators: An organizational culture perspective. *Journal of Higher Education Policy and Management, 31*(1), 43-54.

Lanz, J. (2017). The chief information security officer: The new cfo of information security. *The CPA Journal, June 2017* 52-57.

Lee, C., Lee, C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security, 59* 60-70.

Lincoln, Y.S., & Guba, E.G. (1985). *Naturalistic inquiry*. (Vol. 75). Sage Publications, Inc.

Love, V. D. (2011). IT security strategy: Is your healthcare organization doing everything it can to protect patient information? *Journal of Health Care Compliance,* 21-64.

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C.S. (2015). Cyber threats to health information systems: A systematic review. *Technology and Health Care, 24,* 1-9.

Malavet, J. N. (2017). *Cybersecurity in higher education: Accuracy of resources utilized by information technology departments to prevent data breaches.* (Dissertation). Retrieved from ProQuest dissertations and theses. (UMI no. 10682256).

Mamanov, S., & Benbunam-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior, 83,* 32-44.

McHaney, R., Cronan, T.P., & Douglas, D.E. (2016). Academic integrity: Information systems education perspective. *Journal of Information Systems Education, 27*(3), 153 – 158. https://search-proquest-com.lib-e2.lib.ttu.edu/docview/1928986196?accountid=7098

Merriam, S.B. (2009). *Qualitative research: A guide to design and implementation.* Jossey-Bass.

Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative research: A guide to design and implementation, 4th Edition* (4 edition). John Wiley & Sons.

Milfort, K., & Grama, J. (2015) This magic moment: Reflections on cybersecurity. *Educause Review.*

Murphy, G. B. (2015). Understanding the risk management process. *SSCP (ISC)^2 Systems Security Certified Practitioner Official Study Guide* (pp. 185). Indianapolis, Indiana: John Wiley & Sons.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*. *18*, 126-139.

NIST (2018). *NIST Cybersecurity Framework (CSF) Reference Tool*. Cybersecurity Framework. https://www.nist.gov/cyberframework/nist-cybersecurity-framework-csf-reference-tool

National Institute of Standards and Technology (2023). NIST cybersecurity framework 2.0 concept paper: Potential significant updates to the cybersecurity framework. https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

National Institute of Standards and Technology (2023) Glossary. https://csrc.nist.gov/glossary/

Ospina, S. (2004). Qualitative Research. *Encyclopedia of Leadership.* SAGE Publishing.

Ovseiko, P. V., Davies, S. M., & Buchan, A. M. (2010). Organizational models of emerging academic health science centers in England. *Academic Medicine, 85(*8*),* 1282 – 1289.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31,* 673-680.

Pareek, M. (2013). What is your risk appetite? *ISACA Journal,* (4) p.12-15.

Patton, M. (2015) Battling data breaches. *Community College Journal, August/September.*

Patton, M. Q. (2015) *Qualitative Research & Evaluation Methods*. (4th Edition) SAGE Publishing.

Paulsen, C., & Coulson, T. (2011). Beyond awareness: Using business intelligence to create a culture of information security. *Communications of the IIMA, 11*(3), 35-55.

Pieters, W. (2011). The (social) construction of information security. *The Information Society*. 27, 326-335.

Ponemon Institute (2018). *2018 cost of a data breach study: global overview*. Security Intelligence. https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/

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

ProserveIT (2018). Cybersecurity 101: your end-users are the first line of defense. *CIO*. https://www.cio.com/article/3274587/it-industry/cybersecurity-101-your-ene-users-are-the-first-line-of-defense.html.

Relating to state agency information security plans, information technology employees, and online and mobile applications, Senate Bill 1910, 2017-2018, (2015). https://legiscan.com/TX/text/SB1910/id/1624439.

Rezgui, Y. & Marks, A. (2008) Information security awareness in higher education: An exploratory study. *Computers & Security, 27,* 241-253.

Rosenbusch, K. (2020). Technology intervention: Rethinking the role of education and faculty in the transformative digital environment. *Advances in Developing Human Resources, 22(1).* 87-101.

Safa, N. S., Von Solms, R., Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

Saldana, J. (2009). *The coding manual for qualitative researchers.* Sage Publications.

Sarrel, M. D. (2010). The biggest security threats right now. e*week.* https://www.eweek.com/security/the-biggest-security-threats-right-now/

Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M., (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security, 57,*14-30.

Slade, C.P., Hull, J.M., Azziz, R., Levin, S., Caughman, G. B., Hefner, D.S., James, S. (2017). Health system creation and integration at a health sciences university: A five-year follow-up. *Journal of Healthcare Management, 62*(6), 386-402.

Šolić, K. & llakovac, V. (2009). Security perception of a portable pc user (the difference between medical doctors and engineers): A pilot study. *Medicinski Glasnik, 6*(2), 261-264.

Spierling, K. & Palmer, J. (2020). The time for teamwork is now. *Inside Higher Ed,* Retrieved April 20, 2021, from https://www.insidehighered.com/advice/2020/11/06/professor-and-administrator-provide-advice-effectively-working-teams-opinion

Tang, M., Li, M. G., & Zhang (2015). The impacts of organizational culture on information security culture: A case study. *Information Technology Management, 17,* 179-186

Tarhini, A., Tarhini, J., & Tarhini, A. (2019). Information technology adoption and implementation in higher education: A case study in Lebanon. *International Journal of Educational Management, 33*(7), 1466-1482.

Texas Administrative Code (2018). *Information Security standards for Institutions of Higher Education.*

Ulven, J.B. & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13(39).* 1-40. https://doi.org/10.3390/fi13020039

U.S. Department of Health and Human Services. (2018). *Health information privacy:* Covered entities and business associates. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

U.S. Department of Health and Human Services (2018). *The Security Rule.* Health Information Privacy. https://www.hhs.gov/hipaa/for-professionals/security/index.html

U.S. Department of Homeland Security. (May 15, 2018). *U.S. Department of Homeland Security Cybersecurity Strategy.*

Van Niekerk, J. F., Von Solms, R. (2010) Information security culture: A management perspective. *Computers & Security, 29,* 476 – 486.

Verizon (2015). 2015 Data breach investigation report. Retrieved from https://www.verizon.com/about/news/verizon-2015-data-breach-investigations-report#report

Verizon (2022). 2022 Data breach investigation report. https://www.verizon.com/business/resources/Te01/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

Webb, J., Ahmad, A., Maynard, S.B., Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security, 44,* 1-15.

Whiteside, C., & Verma, S. (2015). Universal Lessons for Academic Health Science Centers – Recognizing the Value of Integration. *The Evolution of the Academic Health Center,* 39 – 46

APPENDICES

APPENDIX A

INSTITUTIONAL REVIEW BOARD APPROVAL

TEXAS TECH UNIVERSITY
Human Research Protection Program

Jul 19, 2021 10:13:05 AM CDT

Stephanie Jones
Educational Psychology Leaders

Re: IRB2021-526 Information Security Officers Perceptions of How to Implement Successful Information Security Programs in Health Sciences Center Environments

Findings: *All the best with your study!*

Dear Dr. Stephanie Jones, Jessica Klein:

A Texas Tech University IRB reviewer has approved the proposal referenced above within the limited review category of:
Category 2.(iii). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording) if at least one of the following criteria is met:
The information obtained is recorded by the investigator in such a manner that the identity of the human subjects can readily be ascertained, directly or through identifiers linked to the subjects, and an IRB conducts a limited IRB review to make the determination required by §46.111(a)(7).

The determination was made on July 19, 2021. Annual review is not required, and no expiration date will be listed on your letter.

The research must follow Texas Tech University's Operating Procedures, the Belmont Report, and 45 CFR 46. If changes to the approved protocol occur, a **Modification Submission** must be reviewed and approved by the IRB before implementation. Please be aware that changes to the research protocol may prevent the research from qualifying for exempt review and require submission of a new IRB application or other materials to the Texas Tech University IRB.

A goal of the IRB is to prevent negative occurrences during any research study. However, despite our best intent, unforeseen circumstances or events may arise during the research. If a deviation, unanticipated problem or adverse event happens during your research, please notify the Texas Tech University, Human Research Protection Program as soon as possible (45 CFR 46). We will ask for a complete explanation of the event and for you to submit an **Incident Submission** in Cayuse IRB.

Your study may be selected for a Post-Approval Monitoring (PAM). You will be notified if your study has been chosen for a PAM. A PAM investigator may request to observe your data collection procedures, including the consent process.

Once your research is complete and no identifiable data remains, please use a **Closure Submission** to archive this study. IRBs that remain active are subject to audit by the IRB.

ORIGINAL SIGNATURE
AVAILABLE UPON REQUEST

Martin Binks, Ph.D.
Chair, Texas Tech University Institutional Review Board
Director, Nutrition & Metabolic Health Initiative (NMHI)
Professor, Department of Nutritional Sciences, College of Human Sciences

Human Research Protection Program
357 Administration Building
Lubbock, Texas 79409-1075
T 806.742.2064
www.hrpp.ttu.edu

APPENDIX B

PARTICIPANT LETTER

Dear Information Security Officer,

I hope this email finds you well. My name is Jessica Klein, and I am a doctoral student at Texas Tech University in the Higher Education Administration program. For my dissertation, I am conducting research on Information Security Officers' perceptions of how to implement successful information security programs in health sciences center environments.

I am reaching out for your assistance in conducting this research. For this study, I am looking for Information Security Officers who are responsible for implementing an information security program at a Texas Health Sciences Center. Attached is an information sheet that provides more details about this research study. If you agree to participate in the study, you will be asked to take part in a 60 minute semi-structured interview via video conferencing on a date and time that best fits your schedule. Your participation in the study is completely voluntary, and you can stop participating in the study at any point.

If you are willing to participate in this study or have any questions, please contact me at Jessica.Klein@ttu.edu or XXX–XXX–XXX. You may also contact Dr. Stephanie J. Jones at stephanie.j.jones@ttu.edu. If you have any questions about your rights as a human subject in research you may contact the Human Research Protection Program at Texas Tech University. Their phone number is (806)-742-2064 and their email is hrpp@ttu.edu.

I am truly grateful for your time and consideration in helping me conduct this research. I look forward to hearing from you soon.

Thank you,

Jessica Klein
Higher Education Administration Doctoral Student
College of Education
Texas Tech University

APPENDIX C

INFORMATION SHEET

What is this research studying?
The title of this study is "Information Security Officers Perceptions of Implementing Successful Information Security Programs in Health Sciences Centers." This study is to being conducted to explore the perceptions and experiences of information security officers about the factors they perceive affect the implementation of information security programs within health sciences centers as an effort to become more informed on best practices in establishing compliance in these environments.

What would I do if I participate?
In this study, you will be asked to participate in an interview that will be held virtually through web conferencing software that will be audio recorded with your permission.

How long will participation take?
We are asking for 60 minutes of your time for the interview as well as 15 minutes to review your transcribed interview to ensure your thoughts were captured accurately.

Can I quit if I become uncomfortable?
Yes, absolutely. Dr. Stephanie J. Jones and Texas Tech University's Institutional Review Board have reviewed this research project and think you can participate comfortably. However, you can skip parts of the research you are not comfortable with and stop at any time. You will keep all the benefits of participating even if you stop. Participating is your choice.

How are you protecting privacy?
Your name will not be linked to any material in reports, publications or presentations. No one other than the researchers associated with this project will have access to the raw data. All related documentation will be stored in the researcher's locked office and on a password protected computer.

What will happen to my data?
Your information collected as part of the research, even if identifiers are removed, will not be used or distributed for future research studies.

What are the benefits and risks of participating in this research?
There are no anticipated risks to your participation in this research and the benefits are that you will be contributing to a body of knowledge that is still relatively unresearched in the industry landscape of higher education and information security. We appreciate your time and effort with this research study.

I have some questions about this study. Who can I ask?
The study is being run by Dr. Stephanie Jones and Jessica Klein from the Doctor of Education Higher Education Administration program at Texas Tech University. If you have questions, you can call Jessica Klein at XXX-XXX-XXXX or email her at Jessica.Klein@ttu.edu. You may also contact Dr. Jones at stephanie.j.jones@ttu.edu.

Texas Tech University also has a Board that protects the rights of people who participate in research. You can contact them at 806-742-2064 or hrpp@ttu.edu.

APPENDIX D

INTERVIEW PROTOCOL FOR IN-PERSON INTERVIEWS

Interview Protocol Project: Information Security Officers perceptions of Factors to Successful Security Program Implementation to promote Compliant Security Behaviors.

Date of Interview: _____

Time of Interview: _____

Place of Interview: _____

Interviewer: _____

Interviewee: _____

Pseudonym: _____

Thank you so much for agreeing to meet with me this afternoon. Your participation is greatly appreciated. Your participation today will assist me in gathering information regarding information security officer perceptions as they pertain to factors contributing to successful implementation of an information security program to promote compliant behaviors among end users. All of your responses will be kept anonymous and no identifying characteristics of information will be disclosed. With your permission, I will tape record your responses so that I can transcribe the interview later. This interview will only take 45 minutes of your time and be limited to this specific topic area.

Again, your participation is voluntary and if for some reason, you do not wish to answer any of the questions, you are free to skip it. If for some reason, you wish to exit the interview, we can stop the interview process at any time.

1. What is your official title?
2. How long have you served in your role?
3. Who do you report to?
4. How would you describe the configuration of your Information Technology Department as they support the institution?
5. How would you describe the configuration of your Information Security Department as they support the institution?
6. How do you incorporate TAC 202 requirements into your operations?
7. What security framework do you follow? NIST? Cobit? ISO? Other?
    a. Why did you select that framework?
8. In submitting your security plan to DIR, what were some areas of your program that could yield more efforts to improve maturity levels that end users could support?
9. What factors do you consider most when looking for strategies to implement your security program?
10. What is your perception of how security safeguards are received at your institution?
11. What are your biggest challenges as you implement tenants of your security plan?
    a. How did you overcome those challenges?
12. What do you perceive is the reason for end user non-compliance of information security advice?

13. What strategies do you perceive work best when getting end users to comply with security safeguards?
    a. What made those strategies effective?
    b. How did you measure the success of this strategy?
14. What are the program implementation strategies approved through your immediate supervisor?
15. What role does the CIO play in governing your information security program?
16. What is your experience with end users and your role as an information security officer?
17. What perceptions do you hold about introducing information security Processes?
18. What have been some challenges to following Information Security requirements as you carry out your duties at your institution?
19. What feedback have you received from end users that have played a role in your architecture of an information security program?
20. What do you perceive as important to end users in order to motivate them to comply with security advice (prescriptive protocol)?
21. Are there any additional details you would like included in this documentation?

Thank you for taking the time to participate in this interview with me. As mentioned above, your information will be deidentified for the purposes of this study and I am obligated to maintain ethical standards when handling this information and

maintaining confidentiality with you, the interviewer. If at a later time, I need more information to clarify your responses, are you available for a follow up? __Y __N

Thank you so much for your time.