A Descriptive Study of Chief Information Security Officers' Roles and Responsibilities in Texas State Government Agencies

By

Sanjuanita Velazquez

Applied Research Project

Sanjuanita v2@gmail.com

Submitted to the Department of Political Science

Texas State Univeristy-San Marcos

In Partial Fulfillment of the Requirements for the Degree

Master's in Public Administration

Spring 2016

Abstract

Research Purpose

The purpose of this research is to describe the responsibilities of Texas Chief Information Security Officers (CISOs). This research should give stake holders, and policy makers a better understanding of Chief Information Security Officers' responsibilities. In addition, it provides information security professionals a landscape of CISOs' responsibilities. A comprehensive review of the literature was used to develop a framework with five descriptive categories: managerial, legal, technical, career development, and information security.

Method

This research via a survey, developed from the conceptual framework, gathered data the responsibilities of CISOs. An open records request was sent to all state offices in Texas. The survey was distributed to 100 CISOs. After carefully sifting through the responses received for the open records request, a total of 100 names of CISOs or titles similar to that were obtained. As a result the survey was administered to a total of 94 potential respondents. A total of 27 individuals responded to the survey, and out of 27 respondents only eleven explicitly identified as Chief Information security Officers.

Results

The results of this survey show that CISOs overwhelmingly support several managerial, legal, and information security responsibilities as extremely important. Extremely important responsibilities include risk management (77%), incident response (77%), information security polices (74%), procurement and contracts (70%), ethics (81%), data security (89%) and network security (70%). Survey results also revealed that respondents alluded to software development as not part of CISO responsibilities (66%).

TABLE OF CONTENTS

Chapter 1: Introduction

Consider the following scenarios

- *So you have decided to apply for a job with the federal government. You have followed all the steps necessary to get your application uploaded to* USAJOBS.GOV. *You even included your social security number to move the process along faster in the event that an agency wants to hire you. Imagine one day that you get a call from your bank, and they tell you that all your information has been stolen. As a result, you now have an enormous amount of debt that does not belong to you and your credit score has taken a hit. You wonder how this could happen. Later, you turn on the TV and see that several federal government webpages have been hacked. This hypothetical scenario is what 18 million federal and non-federal employees are facing. On the morning of June 23, 2015 CNN announced that hackers targeted 18 million Americans who applied to or work for federal jobs. All of the personal information from prospective applicants and current employees was stolen in a breach that affected the main website that manages* USAJOBS.GOV. *This has been the largest breach our federal employees have encountered this century. This situation is often managed by a group of information security officers responsible for maintaining the safety of private information.* (Perez and Prokupecz, 2015)

- *Imagine you get a notification from your information resources division about a scheduled system update. You cautiously follow instructions and make sure the computer is safely shut down after the process is over. Later, your entire organization releases a statement that the computer systems were breached and some of your colleagues might have been affected. It's not until a year later that you get a second W-2 form from a second job that* *you have never been in. You realize that the breach in your office could have contributed to your apparent identity theft. Suddenly the problem you had with the W-2 forms seems so insignificant compared to the other information that could have been stolen. You realize that you have even accessed your bank account on your work computer. You can't stop but to think about the person responsible for your current situation. The Chief Information Security officer is responsible for safeguarding the information at an organization. Unfortunately, in this situation many of the employees wonder what the responsibilities of this CISO are* (Weintraub, 2015 p. 20).

- *Nelson Keen, Deputy Director, leaned back in his leather chair and propped his feet up on the long mahogany table in the conference room. "What do you think about our computer security problem?" he asked Gladys Williams, the organization's chief Information Security officer, or CISO. He was referring to last month's outbreak of a malicious virus on the organization's network. Gladys replied, "I think we have a big problem and we need to put together a real solution, not just a quick one like the last time." To prevent this from happening again all users in the organization were banned from using USB drives. Nelson wasn't convinced: "Can't we just add another thousand dollars to the next training budget?" Gladys shook her head. "You've known for some time now that this organization runs on technology. That's why you hired me as CISO. My staff and I have some ideas to discuss. To start with," Gladys continued, "instead of setting up a computer security solution we need to develop an information security program. We need to review our policies and practices and establish ongoing risk management program." "Sounds expensive," Nelson replied. Gladys answered, "Well, there will be extra expenses for*

> *specific software tools. But the program will be more of change in our attitude about security." In response, "What is your plan, then?" Gladys answered, "we need to initiate a project plan and use our usual systems development and project management approach." "I see," Nelson said. "Bring me the draft plan and budget in two weeks. The audit committee of the board meets in four weeks, and we'll need to report our progress"* (Whitman and Mattrod, 2009 p. 39)

The role of Information security officers has gained prominence in recent years (Goodyear , Nelson, Peterson, & Portillo, 2009). Chief Information security officers (CISOs) safeguard and protect organizational information systems from cybersecurity threats. Cyber security threats are associated with confidential information, data security, and software access to authorized users. In recent years state government cybercrime has become an increasingly complex issue (Goodyear , Nelson, Peterson, & Portillo, 2009). CISOs are under pressure to develop new programs that focus on the use and abuse of technology. In order to assess new threats, CISOs have to work with new aspects of technology that identify threats, develop plans, and react to security breaches. CISOs' responsibilities have evolved dramatically as a result of these new realities.

The increase in cybercrime has brought new challenges to CISOs' daily operations. These challenges include new avenues for cybersecurity threats. The inability to quantify threats questions CISOs' abilities to manage risk within an organization (Burney, 2003). Currently, government CISOs have programs in place to manage risk. For example: Texas State employees enroll in online training that teaches them how to handle, and identify, a network at risk. These programs are developed and managed by CISOs to protect internal network vulnerabilities (Goodyear , Nelson, Peterson, & Portillo, 2009). The focal point of CISOs' evolving responsibilities is to understand all matters involving a breach in information security. Information is a major asset for any organization, and unfortunately a potential liability. Therefore, CISOs' methods of managing information have increasingly become very important. The position of a CISO is no longer driven solely by technical aspects (Cunningham , 2015). CISOs now have to manage information in order to protect the organization. CISOs adhere to government responsibilities that are moving towards information and communication technology. Given the increasing demands on their role and the importance of such a position in public organizations, an in-depth description and understanding of their responsibilities is essential.

As the public sector incorporates information and communication technology, state agencies and local governments are adjusting the ways they communicate their business transactions (MacManus et al., 2013). Though state agencies and local government are not the same entity they incorporate the community outreach in order to understand there stakeholders. Currently, state officials are asking agencies to move towards an E-Government form of communication. CISOs are important because they are responsible for communicating all of an organization's information online. CISOs are accountable for websites and information available outside the organization. As government agencies, businesses, and individuals all depend on technology, there is a need for comprehensible communication (Kaijankoski, 2015). Furthermore, government officials have pressed for more public-private collaboration to increase cybersecurity enforcement. In an attempt to safeguard information, new policies push for legislation that encourages public-private information sharing to combat security issues. Increasingly, CISOs' roles and responsibilities are required to establish good communication avenues for the public and private sectors (Don, 2002). Most of the research about these changes focuses on problems that the federal level encounters while communicating with the public. It is important to point out that state level, and especially the local governments, deserve attention because they are directly involved with the public.

It is important to point out scenarios in which organizations present information security officers and CISOs as two separate positons. For example some CISOs delegates who manages data. However, this research will do its best to identify CISOs in Texas state agencies. CISOs have a broad array of responsibilities that include technical as well as administrative responsibilities.

Technical responsibilities are equally important to administrative ones because as technology is easily incorporated into government systems so do cybersecurity threats. Government organizations that search for CISOs search for individuals who can understand changes in technology. In researching this topic, I used The Texas State Auditor's Office list of job announcements to generalize the technical skills a Chief Information Security Officer needs when applying for a job (Goodyear 2009). Coordinating security programs requires advanced technical skills in order to compete with technology. Though literature that suggests that management is an important part of CISOs' daily operations, there is a need for highly technical workers that serve for an IT position. For this reason, this study examines the responsibilities of Texas Chief Information Security Officers.

The purpose of this research is to describe the responsibilities of Texas CISOs. This study should give state agencies, stake holders, and policy makers a better understanding of Chief Information Security Officers responsibilities. In addition, it provides information security professionals opinions on what daily responsibilities should look like. This ARP uses descriptive categories drawn from Carl Burney and Marilu Goodyear's research. For the purpose of this descriptive research, the categories are: managerial, legal, technical and career development, and information security responsibilities of CISOs. These categories are drawn from the research facilitated by the development of a survey. This survey was distributed to Texas CISOs to understand the importance they accord to each role, and the frequency with which they perform each role.

Chapter 2: Literature Review

Chapter Purpose

This chapter reviews the scholarly literature on the responsibilities of information security officers in the public sector. The information from this section will provide in-depth information on the responsibilities of current Chief Information Security Officers (CISOs) in Texas. This chapter ends with a conceptual framework that lays out the roles and responsibilities of CISOs.

Managerial

CISOs have a broad array of duties that are managerial in nature. CISOs must often articulate technical issues to a non-technical leadership within their organization (Goodyear, 2015). This is why managerial skills are a key component of any organization with a technical staff. Because CISOs provide assistance in matters that involve information technology, it is important to identify non-technical responsibilities.

Management helps articulate technical information in practical ways (Burney, 2003). Management also ensures that members in an organization understand how technology is secured by the technical staff. Though these definitions encompass the importance of CISOs, Micheal Whitman and Herbert Mattord (2011) further state, “management skills include those necessary to obtain the effective acquisition, allocation, and utilization of human efforts and physical resources to accomplish a goal” (p. 167).

Organizations are increasingly moving towards concerns over information and communication technology. CISOs are included in many important decisions in an organization to ensure that this technology is managed accordingly (Burney, 2003). CISOs management of information abides by the needs of an organization in efforts to enforce security policies. Though CISOs manage technical issues, they use different skills to communicate important components of managerial responsibilities. The most important components of CISOs' managerial responsibilities are risk management, planning, incident response, and budgeting. These responsibilities are important to address because they are concerned with the confidentially, integrity, and availability of data within an organization (Goodyear, 2009). Though it is difficult to successfully quantify the threats to an organization, it is important to try and manage any type of risk to information security. Responsibilities like risk management ensures that all projects and programs address information security in timely manner.

Risk Management

Risk management assesses and establishes appropriate levels of protection for all information systems. Risk management is the process of identifying risks that are present in an organizations' information assets and infrastructure (Whitman and Mattord, 2011). Also, risk management determines risk and controls by identifying vulnerabilities. Protection of information assets and security requires the ability to quantify vulnerabilities (Goodyear, 2015). The ability to combine technical and managerial functions are currently the number one responsibilities of any organization. CISOs are required to understand the risk to information security and undertake important responsibilities that encompass risk management. Scholars have pointed out some important risk management responsibilities while working with information assets and security vulnerabilities. These include:

- *Ensuring that all security safeguards are cost effective.*
- *Manage damage if the information is lost, improperly accessed or improperly modified.*

- *Conducing periodic risk analyses to maintain proper protection of information.*
- *Evaluating the risk.*
- *Determining what is a control option that is cost effective to the organization.*

Despite this information, there remains a gap between knowledge of cybercrime and the needs for prevention. According to Caruson *et al*., (2012), public officials with little understanding of dangerous cybercrime activities face an escalating problem that is getting more complex. Therefore, CISOs are under pressure to manage risk accordingly and cost effectively. Organizations at the state level, especially at larger agencies, have more vulnerabilities because they deal with a broader scope of cybersecurity. This does not mean that small organizations are not a target for criminal activity. Caruson, *et al*., point out that non-IT officials underestimate the likelihood of major internal threats, and therefore call for better understanding of risk management (Caruson et al., 2012). Risk management allocates vulnerabilities and assesses threats. However, there is tension between how much money organizations are willing to spend on managing risk and the organizations' allocation of funds.

Budget

Budgeting is where CISOs manage their ability to allocate funds where they are needed for projects and technology (Goodyear, 2009). It is understood that budget constraints may hinder the possibility to protect information security. Budgeting is the distribution of funds that are needed in order to designate, plan, and protect information security. Formulating a budget applicable for an entire organization is a difficult task in every organization (Goodyear, 2009).

It is understood that cybersecurity preparedness is expensive in nature. As cyber threats become more sophisticated so does technology. Sophisticated technology is not cheap, and CISOs who work in the public always take budgets into consideration. According to Caruson *et al*., (2012) during budgetary shortfalls it is especially difficult to ask for new equipment (p. 3). As a result, CISOs' need for better equipment or manpower to secure the systems of the organization requires a good reputation for protection. Scholars agree that in order to ask for money for cyber threats CISOs must convince upper management that the money is going to be well spent. Fitzgerald and Krause (2007) suggest that "given the complex nature of the budgetary processes for public sector organizations, it is difficult to secure a defined position the agency's budget" (p. 96). Budgets can be premeditated, and if there have been few threats to the agency, public officials might not think they need to allocate money for cybersecurity. Consequently, Scholars agree that this is a problem because the organization might not be ready for a breach (Fitzgerald and Krause, 2007; Caruson *et al*., 2012; Goodyear *et al*., 2009)

CISOs must deal with allocating the money given to the organization to protect information technology. Unfortunately, sophisticated cyber threats require expensive technology, and this becomes a problem because budgets are predetermined. In order to work towards the protection of an agency's information security it is necessary to understand it is expensive to protect against cyber-attacks.

Incident response planning

This responsibility is crucial for CISOs' managerial skills because it uses the quantified analysis of vulnerabilities and plans for future disasters. This proactive ability to respond to threats is continually pushing CISOs into executive roles within organizations. Incident response planning is the process of reacting to an attack that is immediate or escalating in nature (Whitman and

Mattrod 2011). Preventative measures also encompass planning for future attacks and is part of incident response planning. This means incident response planning formulates preventative measure and plans for possible threats to information assets and infrastructure (MacManus *et al*., 2013). There is a need to develop a preventative plan to address the protection of an organization's confidentiality, integrity, and availability of information technology (Goodyear, 2015). CISOs work closely with the IR team to plan for incidents, and this requires the ability to effectively manage a team of planners whose goal is to respond to an incident (Whitten, 2008).

There is considerable agreement among scholars that cyber threats are on the rise due to more sophisticated technology (Goodyear et al., 2015; MacManus et al., 2013; Whitman and Mattrod, 2011; Goodyear et al., 2009; Whitten, 2008). In a survey conducted in order to find the number of cyber-attacks the Florida state government had in a year, MacManus *et al*., (2013) found that out of 67 counties 92% of the county officials acknowledged that their agencies are less able to handle a major cybersecurity breach caused by terrorist-related incident (p. 461). This points to the importance of planning for a possible breach in a state government.

Though this study was conducted in another state, other scholars recognized that each organization should take steps to develop an incident response plan that is adaptable to their needs (Coronado and Wong, 2014). Managing this responsibility to prevent a threat from happening entails developing an effective risk management plan to share with other departments, and to coordinate emergency responses (Whitten, 2008).

Telecommunication

Telecommunication "is the transmission of data from one point to another for the purpose of communication" (White, 2007, p. 75); this enables data to be transmitted across organizational grounds. Public sector information security professionals need to manage telecommunication devices. These telecommunication devices assure interconnection between organizations. CISOs work closely with information resources departments in order to ensure that secure forms of communication are acquired. Because this telecommunication is an important part of CISOs' growing responsibilities it is important to define different aspects of telecommunication.

Laws

Laws are the rules that mandate or forbid certain behaviors (Whitman and Mattrod, 2011). Laws that are relevant to information security help CISOs compensate for wrongs committed within an organization. Also, laws help state government formulate policies that are applicable to public organizations (Powner, 2014). Since laws set a bar on behavioral standards, they are the best approach to information security. CISOs' behaviors are influenced by the laws that govern information security (Whitman and Mattrod, 2011).

Compared to the private sector, public sector CISOs are governed by information security statues, "although the private sector CISO do have to address regulatory requirements, public sector information security programs are derived from various statues passed by concerned legislators who are attempting to correct identified problems that have resulted in the compromise of citizen information or loss of taxpayer dollars" (Fitzgerald and Krause, 2007, p. 92). CISOs use laws to help the public recognize how the government is using funds in regards to information technology. Furthermore, evidence suggests that state governments mirror federal government formal regulations in order to correct problems within their regulatory programs. Whitman states, "The United States has been a leader in the development and implementation of information security rules to prevent misuse and exploitation of information technology" (Whiteman and Mattrod, 2011).

The Federal Information Security Management Act (FISMA) is one legislative piece that was implemented to control agency assets. Though this required federal agencies to develop, document, and implement an agency-wide information security program, scholars agree that state entities have operated while trying to mirror federal agencies. State agencies created CISOs positions in order to manage information security programs like the federal agencies do, and with the intent to protect citizen information and prevent loss of taxpayer money (Fitzgerald and Krause, 2007).

As a result, laws can establish a requirement for permissible behavior within federal agencies (Powner, 2014). State entities use these federal identities to regulate and modify programs within their organizations. CISOs are responsible for recognizing how these laws affect their organizations, and manage according to the statutory authority given by the legislators.

Information security policies

It is important to understand information security policies in order to adhere to organizational needs. Information security policies are the guidelines that underline the acceptable and unacceptable employee behaviors in the workplace (Whitman and Mattrod, 2011). Information security policies ensure that polices properly protect all information that is collected, processed, stored, transmitted, and disseminated (Burney, 2003). CISOs' primary technical responsibility is to review, develop, and ensure that all guidelines are understood and applicable to their organizations. According to Whitman and Mattrod there are important criteria that information security policies must have in order to become effectively enforceable. These include:

- *Dissemination: Organizations must be able to demonstrate relevant policy is available for review by any employee.*

- *Review (legible): The organization must be able to demonstrate that policy is circulated in an clear form that includes different versions for reading – impaired employee, non-English reading.*

- *Comprehensive: CISOs must be able to demonstrate that employees understand the requirements and content of policies in place.*

- *Compliance: Compliant employees must be able to comply with polices through the act or affirmation. Common techniques are acknowledgement agreement or signed document clearly indicating that employee has read, understood and agreed to comply.*

- *Uniform enforcement: The organization must be able to demonstrate that policy has been uniformly enforced, regardless of employee status or assignment.*

Each state entity seems to be left with appropriate internal polices according to their needs. Michael Glennon expresses the need for federal intervention in order to help state agencies with policy implementations. Glennon's research focuses on discrepancies between the federal policies that ignore state governments. The study points out that as a result of the lack of federal representation in laws, states have begun implementing comprehensive polices. In his study, Glennon uses California's resident protection plan that demonstrates how laws helped policy formulation. California law requires all entities to notify residents when personal information has been acquired by illegal cybersecurity breaches. This changes the dynamic of state agencies because it uses laws to formulate polices that protect resident information (Glennon, 2012). Nonetheless Goodyear *et al*. suggest that despite challenges, state CISOs are leading cybersecurity dialogues that identify gaps in policies. These CISOs opt for remediation plans that help their organizations' policy formulations.

Procurement and Contracts

Though there is a technical aspect to procurements and contracts knowledge, it takes years of education and training to become an efficient CISO who understands contracts (White, 2007). According to White this person needs to have an understanding of vast and complex processes that govern procurement and contracting. CISOs need technical knowledge in order to precisely describe the products and services they acquire for public agencies. Procurement and Contracts refers to the acquisition of products and services through the knowledge of state policies and prior practices (White, 2007). This practice encompasses the transparency each state agency must have in order to request such products and services.

A state government's goal is to maintain the processes of the procurement systems published in order to communicate trust (Schooner, 2002). It is the responsibility of CISOs to integrate procurement and contract systems in order to avoid corruption in an organization. There are policies and regulations attached to the procurement and contracting processes, but it is more important to show transparency with each transaction (White, 2007).

Ethics

Ethics is the study of morality through human conduct. Ethics uses laws and policies to justify human actions, which are performed concisely, intentionally, and for which individuals are held responsible (Kizza, 2002). Ethics point out constraints in CISOs' array of responsibilities and therefore are very important to mention (Kizza, 2002).

However, scholars agree that information security professionals do not lose their licenses if they are found to act unethically (Whitman and Mattord, 2011). These codes of ethics serve only as a moral reminder of the parameters within the information security profession. These parameters establish CISOs’ accountability for proposed architectural infrastructure of systems’ implementation programs. According to Stephen Northcutt, an ethical way to handle new systems implementation is to communicate to senior management the truth about the new architectural infrastructure (Northcutt, 2004). Architecture schemes are poor, and therefore will not work if it goes live; CISOs should communicate this honestly to senior management (Northcutt, 2004). CISOs should not waste the time and money of the organization by implementing weak architectural infrastructure.

Therefore it is the CISOs’ ethical responsibility to communicate any important assessment to senior management (Northcutt, 2004). Whitman and Mattord also suggest that because information security is not entirely bound by a code of ethics like doctors and lawyers, information security professionals should, “act ethically and according to the policies and procedures of their professional organizations”. CISOs’ responsibilities are defined by ethics, and should be adhered to in order to understand daily operation constraints.

Technical

CISO technical responsibilities are a very important part in an organization’s daily operations. Only highly specialized staff with technical skills can fill a position in any given IT department. The technical responsibilities of this staff keeps the organization updated on the latest processes to protect information technology. The “technical part of this technical responsibility is the understanding of integrated business processes, technologies, and data (Beatty, Arnet and Liu, 2005). This understanding of the definition of “technical” may help a CISO bring about competitive advantage in in the market place.

Therefore, there are state officials who argue that technical solutions are the key to handling government information cybersecurity issues (Goodyear, 2015). In a study to investigate the strategies of different states' government-based approach to information cybersecurity, Goodyear pointed out that some states prefer the technical approach. This approach uses technology and control mechanisms like virtualization. Virtualization is the means of controlling data and access to identify, authenticate, and authorize users and processes (Goodyear, 2015). These states use private sector companies to assess and improve the technical cybersecurity process.

While other responsibilities are important for information security, the implementation of these process are technical in nature. These technical implementations deal with the application of technology (Whitman and Mattord, 2011). This merger between the private and public sectors suggests that there is a need for technical abilities in order to understand both worlds (Fang, *et al.*, 2009). Technical responsibilities' main functions are software development, copyrights, systems acquisitions, and policy.

Software Development

In order to safely secure a network, CISO and IT professionals must understand the principles of software development responsibilities. Software development is the design of a system that prevents security violations (Whitman and Mattord, 2011). This mechanism uses information security considerations with specific design objectives. According to Whitman and Mattord developing a system with a unique software is often accomplished using a methodology such as the systems development life cycle, which creates procedures of creating software to better monitor its security. The goal of this technical responsibility is to prevent security problems before they begin (Whitman and Mattord, 2011).

Douglas Havelka and Jeffery Merhout reveal that amongst the most important technical skills necessary among technology professionals, chief among them is the ability to understand, support and apply software. This study calls for a technical knowledge category with software skills that are acquired through IT disciplines. The authors categorized software development under a technical knowledge. However, in order to keep an organization afloat, CISOs must understand the importance of applying software development into daily operation. Whitten suggests that securing information has become more important for the long-term survival of organizations. CISOs must understand their security initiatives in order to fulfill this position (Whitten, 2008).

Copyright

In addition to software development, CISOs are responsible for establishing policies to prevent the duplication of software. Copyright is the ability to maintain legal software inventory (Burney, 2003). Also, copyright responsibilities include the periodic audit for illegal software. Reddy and Vivenkanda suggest that the current development of information technology has given an easier access to digital information. This easy access has brought problems to organizations because they may lead to illegal copyright.

Organizations keep up with copyright notices in order to prevent illegal copyright distribution. Working together with the information resources department, CISOs perform regular audits in order to track data to target illegal copyright activities. This is used in public information settings where data is the most important asset (Reddy and Vivenkanda, 2014). In a study conducted to find the important technical skills of information security officers, Fang, *et al*. found that recruiters prefer incoming staff with system methodologies to protect information. This means that in order to coordinate safe applications of copyright, CISOs must come up with a method to audit for copyright (Fang *et al*., 2005).

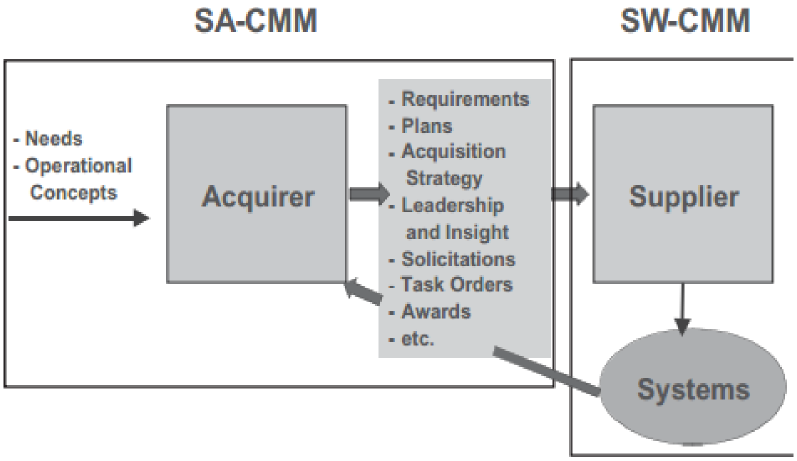
Systems Acquisitions

In order to keep information systems updated, state agencies must acquire systems that help with daily operations. According to Carl Burney, system acquisition safeguards appropriate security requirements, and include acquisition for information systems. System acquisition is the procurement of security features, functions, and controls of newly attained information systems (Burney, 2003).

Systems acquisition procedures ensure that newly acquired systems do not violate existing security policies by working through contracting and procurement processes. Jay White points out the problems that state agencies face while trying to acquire systems. White suggests that trying to go through the system acquisition processes is the most complex facet of modern public administration because of its contract and procurement nature. White simplifies the processes of acquiring technology by describing a Software Acquisition Capability Maturity Model. This model determines an agency's readiness to effectively acquire and develop software applications (White, 2007). The following figure was formulated by Fisher, *et al*. in order to simplify visualize software acquisition capability models

Figure 1: Dr. Matthew J. Fisher, Wolfhart B. Goethert, and Dr. Lawrence G. Jones, 2002
Applying the Software Acquisition Capability Maturity Model

Figure 1: *Areas of Focus for Acquirer and Supplier Models*



Scholars agree that the systems acquisition model helps improve government's ability to acquire systems (White 2007; Fisher, *et al*., 2002). This model was developed to be adaptive to multiple originations and their differing acquisition processes (Fisher, *et al*., 2002). The ability for public organizations that have acquisition capabilities is an alternative approach to software system development. According to White, system acquisition capabilities are extremely comprehensive for state agencies. This optimizes the acquisition of hardware and software in order to implement feasible software implementation (White, 2007). Nevertheless, White argues that systems acquisition comes with a price of extensive understanding of one's organization. Consequently, system acquisition also requires extensive knowledge of policies and regulations (White, 2007).

Career Development

In addition to Technical and Managerial responsibilities, CISOs' positions require an extensive knowledge of computer science. It is widely understood that there is a need for professionals who are able to create cybersecurity systems that are strong against attacks (Namin, *et al*., 2014). This means that it is important to acknowledge the role of computer science in the preparation of CISOs' career development in order to prepare for the position. Career development is knowledge that is attained through experience and prior perpetration. This also means that career development has a level of coaching others in order to grow as a professional (White, 2007).

Therefore, career development strategies include the technical continuity to keep up with changes in the market. Training and Certifications play an important part of career development because they ensure that the CISOs and the rest of the staff are aware of specific information security practices (Burney, 2003). Marilu Goodyear analyzed the career of IT security officers in Higher Education and finds that CISOs are knowledgeable and highly specialized workforce professionals. This study finds that CISOs are also not only responsible for their own knowledge, but of the organization as well (Goodyear, 2009).

Faculty Awareness

Faculty Awareness is the training of all the non-IT staff in an organization in regards to regulations and cybersecurity. The success of any information technology program in any organization depends on the awareness of the entire staff. Information technology programs bring about safe, continuous, and available technology for employees (Goodyear, 2009).

Carl Burney suggests that information security awareness should include all personnel regardless of position in an organization. Scholars agree that professional awareness should be current and periodical in order to ensure effective information security awareness (Burney, 2003).

Whitman and Mattrod add that employee errors are the top threats to information assets, and therefore it is worth spending time training. Information security programs build a sense of accountability from each member of the organization. Through the processes of developing programs, CISOs can establish a plan to correct any misconception. Whitman and Mattrod suggest that CISOs create a specialized program in order to teach specific topics on information security. The sense of a security education, training, and awareness program (SETA) is designed to reduce incidences of security breaches by employees because its design to supplement general information security training an employee usually has (Whitman and Mattrod, 2011). The SETA program's goal is to improve awareness, and develop skills and knowledge.

Figure 1.2 presents the framework of a SETA program suggested by Whitman and Mattrod, 2011 p .36

	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching	Theoretical Instruction	Practical Instruction	Media
Method	- Discussion seminar	-Lecture	-Videos
	- Hands-on Practice	-Case study workshop	-Newsletters
Test measure	Essay(interpret learning)	Problem-solving (apply learning)	-Ture or false -Multiple choice
Impact timeframe	Long term	Intermediate	Short term

Recent programs have focused on data and information management, but Marilu Goodyear adds that it is the responsibility of CISOs to work with an administrator's faculty and staff at all levels in order to meet organizational expectations. In order to help all employees understand different threats to information technologies, it is important to prepare such employees with awareness programs.

Technical Continuity

Technical Continuity is the constant training of an information security employee. This training is necessary, and competes with demands in the workforce. Because IT professionals deal with diverse technological and organizational obstacle CISOs' success depends on the recent preparation. CISOs' technical and non-technical responsibilities encompass all levels of technology, and therefore deserve attention to persistent preparation. In addition to persistent preparation, the success of any information system profession depends on the amount of updated information used in order to attack obstacles.

Michael Whiteman and Herbert Mattrod suggest that anyone who is in the IT profession should continuously train. They state that IT education is never complete, for it is a fact that information technology is ever evolving. In order to be equally competitive with information security changes, IT professionals should have the latest technical training, and education available (Whitman and Mattrod, 2011). Scholars believe that continuous training in an organization is beneficial for any IT professional because it incorporates a wide range of topics: "Given the active environment in relation to federal and state legislation and regulations, it is understandable that CISOs see a need for training in the knowledge of regulation and standards" (Goodyear, 2009). Goodyear adds that most CISOs have the need to be updated in different topics of information security.

Namin, *et al*. (2014) also see the benefits of continuous training of information security professionals, and add that is it especially important for CISOs to be cybersecurity proficient. Namin, *et al*. state that the preparation of future cyber security professionals depends on education, training, and defense preparation (Namin, *et al*., 2014, p. 91). Technical continuity ensures that CISOs continue to safely protect information systems by constantly training each professional in different areas.

Certifications

The concept of certification is the objective measure of professional expertise within the information security profession (Tipton and Krause, 2003). CISOs can take advantage of professional certifications and benefit their organizations. Certifications are the best choice of any information security professional because it provides organizational recognition. CISOs may also need professional certifications as effective enhancement skills in order to complete daily operations (Tipton and Krause, 2003).

Whitman and Mattord add that many organizations seek specific certifications in their candidates in order to measure their technical levels. There is debate over which certification best fits all types of organizations. However, there is overall agreement on the fact that professional certifications are needed in order to enhance certain skills like cybersecurity. Inan, *et al*. state, "The preparation of future cybersecurity professionals and workforce primarily depends on certification programs offered by higher education."

Furthermore, evidence supports the idea that certifications are designed to recognize experts in respective fields (Whitman and Mattrod, 2012). Also, Whitman and Mattrod agree on the fact that certifications help staff prepare with daily operations. Overall certifications are an important part of CISOs' daily operations because they add to many technical skills. It is important to recognize professional certifications as part of CISOs' responsibilities because they add to technical skills and provide overall organizational recognition.

Information Security

Information Security is the protection of information systems against unauthorized access (White 2006). Today, public and private organizations are working together to build a safer information system (Kaijankoski, 2015). Cyberattacks are a common problem faced by organizations, but security ensures that different sections within information security are protected (Kaijankoski, 2015). Security goals include the protection of the data an organization uses and collects while safeguarding the network in which the organization operates (Whitman and Mattord, 2011). Also, information security ensures that technological assets are safely accounted for and protected (Whitman and Mattord, 2011). Marilu Goodyear (2009) states that, “Concerns about confidentiality, integrity and availability of data and the need for security in order to avoid institutional embarrassment are reasons for organizations choose to invest in information security programs” (p. 5). Because information security manages different tasks within the organization, it is essential to point out such important responsibility. CISOs responsible for the security of an organization carry a huge weight, for they are liable of any threat that jeopardizes the organization.

Jay White suggests that information security must possess qualities like: confidentiality, integrity, availability, and assurance. These qualities serve a theoretical way to address information security. Confidentiality helps information by providing accessibility only to those authorized to specific personnel. Information security should use its integrity in order to protect data destruction and modification. In order for specialized personnel to have access to data when needed, availability of information systems that is operational and functional is needed. Lastly, according to White, assurance is, “information systems is broader management concept that looks to see if confidentiality, integrity m and availability qualities are met.”

However, Kim *et al*. also propose a solution for future professionals in need of a secure information systems. Kim, *et al*. suggest that future information security professionals should be evaluated through the quality of security protection they proposed in their past experience (Kim, Park and Hyunko, 2015). This ensures that the information security measures proposed could be investigated and proofed to be secure. These suggestions only cover the surface of information security. Kaijankoski suggests that since government agencies have become more dependent on technology, there is a need for interconnection between the private and public sector in order to address vulnerabilities within security systems. The security programs implemented by CISOs are important because they deal with data, network security, and assets. Overall, information security tries to protect its organization by taking into account many components. These components are data, network, and security systems by using different measures of protection.

Data Security

Data security is the protection of information stored electronically. Data security uses database management systems to secure information (White, 2006). Private and Public entities use information from their customers in order to examine their consumers. Information like date of birth and social security numbers are only a few pieces of information used in a large database file. For this reason, E-governments that use information stored in order to take into account daily transactions are in danger of confidential information being misused, published, or destroyed.

According to MacManus, *et al*., (2012) E-governments that possess digital information are in danger of violating privacy information (p. 454). MacManus, *et al*. suggest that E-governments' efforts of a more transparent government are unrealistic because they manage data that is sensitive in nature (MacManus, *et al*., 2012). Data and transparency have boundaries that according to MacManus, *et al*. are violated if all the data is misused or stolen. Data security ensures a balance between governments and citizens because it manages the data accordingly. Data security also encourages increasing the possibilities of government data accountability. Whitman and Mattrod also stress the importance of data security in that it attracts attackers to any organization with sensitive data. However, Havelka and Merhout stress the importance of IT professional's knowledge when they deal with sensitive information (Havelka and Merhout, 2009). According to

Havelka and Merhout (2009) one of the important categories of an IT professional's competence is the ability to safely store and use data (p. 111).

Network Security

Network security is the protection of multiple information systems that are connected to each other, and that form a local area of networks (LANs) (Whitman and Mattrod, 2011). Network functions are important because they restrict accesses to important components of information systems like its hardware and software. Networks security systems are also connected to the Internet in order to monitor its daily systems in which the organization is operating. CISOs need extensive knowledge of network security in order to safely guard the Internet connections and cross-organizational communications.

The academic literature related to CISOs' sets of skills needed in a competitive market include an extensive knowledge of the network vulnerabilities (Whitten, 2008). According to Whitten, amongst the most important IT security skills are network security systems. These skills ensure that CISOs' importance in organizations are due to the level of expertise in this matter (Whitten 2008). Studies suggest that a majority of CISOs have a responsibility to support network security in their organizations (Goodyear, 2009). According to Marilu Goodyear, CISO respondents state that some primary responsibilities within information security is supporting network security. Because network security is such an important part of any organization, CISOs must have the necessary skills to safely secure their organizations.

Access Controls

Access control is the method in which users' access is determined into areas of an organization (Whiteman and Mattrod, 2012). This authentication can be physical or electronic; for example, only recognized staff admitted into a computer room that holds sensitive information. It is important to recognize this responsibility because CISOs are in charge of securing areas within the organization.

Whitman and Mattord suggest that general strategies to manage access control should rely on identification, authentication, authorization, and accountability. These strategies help CISOs secure important information security programs in that they provide support for identifying rightful users. Furthermore, Jay White points to some measures taken by the federal government in order to protect access. According to White, “CIO council established that federal employee are restricted to internet base technology for personal needs,” this points out the limited accesses employees have to avoid hackers from targeting employees (White, 2006). In conclusion, organizations trying to protect sensitive information use access control measures. These measures can vary, but the goal of all of them is to safely protect the organization.

The literature has suggested that CISOs’ roles have numerous responsibilities that are no longer just technical. Common elements from the literature emerged from studies conducted in other States. What has been lacking in the literature are studies regarding responsibilities of Texas CISOs specifically. This leads to underestimating CISOs and their importance at any Texas organization. Though the role of a CISO is fairly new, there is a need for a skilled worker who understands technology and has the capacity to manage other daily operations (Goodyear, 2015).

As technology changes, so do the threats to cybersecurity. In response, CISOs use their skills and manage important aspects of information technology. These aspects are described as important responsibilities. Soft skills come from these non-technical responsibilities that allow a CISO to understand other duties. Throughout the literature, authors stressed the importance of a

CISO who handles non-technical responsibilities in a professional manner. Clearly, CISOs are at the top of the organizational tier, and it is imperative to describe these responsibilities.

Conceptual Framework

The descriptive categories regarding the responsibilities of CISOs in Texas will include managerial, legal, technical, career development, and information security. Each category will be discussed further, and the content analysis will be conducted on a random sample of job announcements to examine Texas CISOs responsibilities required.

Table 2.1 Conceptual Framework

<table>
<tr><td colspan="2"><b>Title</b>: A Descriptive Study of Chief Information Security Officers’ Responsibilities in Texas State Government Agencies
<b>Purpose</b>: The purpose of this research is to describe the responsibilities of Texas CISOs. This ARP uses descriptive categories drawn from Carl Burney, Marilu Goodyear, Douglas Havelka Dwayne Whitten and, Michael Whitman.</td></tr>
<tr><td><b>Category</b></td><td><b>Supporting Literature</b></td></tr>
<tr><td><b>1.Managerial</b></td><td>Burney (2003); Goodyear, et al.(2009); Goodyear,et al.,(2015); Kouns and Kouns (2011)</td></tr>
<tr><td>1.1 Risk Management</td><td>Burney (2003); Goodyear, et al..,(2009); Goodyear,et al.,(2015); Whitman and Mattord (2011)</td></tr>
<tr><td>1.2 Incident Response</td><td>MacManus et al., (2013); Goodyear, et al..,(2009); Goodyear,et al..,(2015);Caruson et al (2012); Whitman and Mattrod (2011) ; Whitten (2008); Coronado and Wong (2014)</td></tr>
<tr><td>1.3 Budgeting</td><td>Caruson et al (2012);Goodyear et at..,(2015) Havelka and Merhout (2009)</td></tr>
<tr><td>1.4 Telecommunication</td><td>Whitman and Mattrod (2012); White (2006)</td></tr>
<tr><td><b>2.Legal</b></td><td>Fitzgerald and Krause (2007);Whitman and Mattord (2011);Powner (2014)</td></tr>
<tr><td>2.1 Information Security Policy</td><td>Goodyear et al..,(2015);Glennon (2012); Whitman and Mattrod (2011);Burney (2009) Heiman (2002)</td></tr>
<tr><td>2.2 Procurement and Contracts</td><td>White (2007);Schooner (2002)</td></tr>
<tr><td>2.3 Ethical</td><td>Whitman and Mattord (2011);Kizza (2002); Northcutt (2004)</td></tr>
</table>

3.Technical	Havelka and Merhout (2009); Whitman and Mattord (2011); Beatty et al.(2005);Goodyear et al.,(2015)
3.1 Software Development	Whitten (2008); Havelka and Merhout (2009);Whitman and Mattrod (2011)
3.2 Copyright	Fang, et al., (2005); Burney (2003) ;(Reddy and Vivenkanda 2014).
3.3 System Acquisition	Burney (2003); White (2007); Fisher et al.,(2007)
4. Career Development	Burney (2003); Goodyear, et al..,(2009); Namin et al.,(2009);Whitman and Mattrod (2011)
4.1 Faculty Awareness	Burney (2003); Goodyear, et al..,(2009); Goodyear,et al..,(2015); Namin et al., (2014)
4.2 Technical Continuity	Whitten (2008); Havelka and Merhout (2009) ;Goodyear et al.,(2009);Namin et al..,(2009)
4.3 Certifications	Tipton and Krause (2003); Namin et al.,(2014); Whitman and Mattrod (2011)
5. Information Security	Kaijankoski (2015); Whitman and Mattrod (2011); Kim et al (2015)
5.1 Data Security	Havelka and Merhout (2009),MacManus (2013); Whitman and Mattrod (2011);White (2006)
5.2 Network security	Coronado and Wong (2014);Whitman and Mattrod (2012);Goodyear et al.,(2009)
5.3 Accesses Controls	White (2006); Whitman and Mattrod (2011)

Chapter 3: Methods

Chapter Purpose

The main purpose of this chapter is to describe the research design and methods used in this Applied Research Project. Using the literature, the former chapter developed a categorical conceptual framework of CISO responsibilities. These categories are used to create a survey which is used to describe the responsibilities of CISOs. This chapter then operationalizes the conceptual framework and demonstrates how the survey method was developed. Moreover, this chapter addresses characteristics of the sample and constraints of the study. Additionally, this chapter includes information on the research setting, study participants (sample), and data collection procedures. The operationalization table provided at the end of this chapter shows how survey questions were aligned with the different CISO roles laid out in the conceptual framework.

Research Setting and Study Participants

This research was conducted in Texas. The main objective was to capture the nature of responsibilities and roles undertaken by CISOs in Texas. The sample for this study consisted of CISOs in Texas. To obtain a comprehensive list of CISOs at the state level, the Texas State Library and Archives Commission website was researched thoroughly. The next step was to gather an accurate list of potential participants. A public information request was sent out to each state agency listed on the Texas State Library and Archives Commission website. This request asked for the name, email, and phone number of the CISO in that state agency.

While most state agencies had an individual with this title, some who responded to the researcher’s request stated that they had no individuals with that set of responsibilities. Unfortunately, not all state agencies had this position available, and many used a private company to manage their information security needs. For example, in an email sent to the city of Denton, the response was as follows, "*Denton County does not have any positions with those titles*." After carefully sifting through the responses received for the open records request, a total of 100 names of CISOs or titles similar to that were obtained. The questionnaire was sent out to all respondents (100) using *Qualtrics* (www.qualtrics.com).

Human Subjects Protection

In an effort to keep the identity of respondents confidential, neither respondents' names nor cities will be identified in this research. Respondents' emails were also kept anonymous in order to protect the location and names. Once the details of study participants were finalized, a request for exemption was submitted to Texas State University's Institutional Review Board (IRB). Since this research was meant solely for the purposes of advancing knowledge on the roles of CISOs without the express intent of harming the respondents physically or psychologically, this request for exemption from full review of the IRB was deemed appropriate. This research was exempted from IRB review; full details can be found in Appendix B. A copy of the email relating to this exemption is likewise provided in Appendix B.

Operationalization of Conceptual framework

The operationalization of the conceptual framework is based on the methods of Dr. Shields and Dr. Rangarajan (2013). The conceptual framework developed helped organize this research and provide a complete base for the developed survey. The operationalization of the framework is the conversion of categories and elements into variables (Shields and Rangarajan 2013, p. 77). The survey is created from the conceptual framework table, ensuring that items of the survey are directly related to the research purpose (Shields and Rangarajan 2013, p. 77).

The survey instruments used to gather the responsibilities of CISOs was developed by constructing questionnaire items based on the categories of the conceptual framework. Each survey question addressed a specific element of the five categories of the conceptual framework. For example, the category “Managerial” has four subcategories, one of which is “Risk Management.” Moreover, two questions are developed for each subcategory, one is the perceived importance of risk management, and how often the respondents use risk management. For example, questions include: “Rate the importance of risk management as a managerial responsibility,” and “how often do you manage risk?”

Other questionnaire items were included to provide respondents’ information. Items like *official title* and *education* provide information on the sample. The operational relationship between categories and survey questionnaire items are illustrated in table 3.1. Finally, the operationalization of the conceptual framework involved two steps. Operationalization 1) Convert each element into questionnaire items that are answered on a Likert-Type scale, 2) included a selection of open-ended questions.

Survey Research Strengths

Survey research was chosen for this study because it allows many detailed questions on a specific topic (Babbie 2004, p. 275). Data for this study was collected using a web-survey that was created using *Qualtrics*. As outlined in Table 3.1, respondents were presented with 32 questions regarding responsibilities. Detailed questions were necessary to cover information regarding the respondents. As Babbie observes (2001: pp. 238-253), “questions in a survey should be clear, short, relevant, unambiguous, unbiased and mutually exclusive. An uncluttered, well-ordered format allowing the respondent to finish in a short period of time increases the instrument’s viability.” Since the aim was to obtain perspectives of a large number of CISOs in Texas, survey research was deemed most appropriate; describing perceptions of CISOs (in the Texas state agencies) was a key component of completing this study. Using survey research, large amounts of data collected through the survey would be manageable.

The survey was designed such that it would elicit responses from CISOs on each of the roles identified in the conceptual framework. In particular, the survey was designed to measure the importance given to each role by the CISOs and the frequency with which they engaged in each role. Thus, data for each role and associated sub-roles were collected using two survey items as shown in Table 3.1. The first item targeted the importance of each role and was measured on a 5-point Likert type scale which ranged from “not at all important” to “extremely important.” The frequency with which each role was performed was measured on a 4-point Likert type scale which ranged from “rarely” to “frequently.” A copy of the survey instrument in its entirety is presented in Appendix A: *Questionnaire “Chief Information Security Officer Survey.”*

Survey Research Weaknesses

Although survey research was the best method of data collection for this study, there were some limitations associated with choice of this method. A common problem with survey research is poor response rate, which may result in data that is not representative of the entire population (Babbie, 2004). This research did not offer an incentive for respondents to combat poor response rates. A reminder email was sent to all respondents who failed to take the survey after it was sent to them the first time. A second request increased the number of respondents who took the survey.

Four bounced emails and reluctant respondents were another concern. In this study, a public information request was sent out to state agencies that had a current CISO, but some may have flagged the survey as scam or were reluctant to respond to the survey. A method to combat low response rates would have been to travel to those agencies and request a meeting. Due to the time constraints of this project a multi-method system was not a viable option.

Data Collection Procedure

Once the web-survey was pilot-tested a few times to fix any issues and to track potential completion times, it was sent to all 100 potential respondents via email. The email that contained the link to the survey told study participants about the overall objective of the study, the importance of their participation, and their rights to participation in the study. Participants were promised confidentiality. The survey was available for completion for two weeks in March 2016. After the initial mailing of the survey link to participants, two reminders were sent to those who had not responded.

Statistics

Descriptive statistics were used to analyze the collected data. Frequency distribution tables are provided to display how many participants answered each question. The use of descriptive statistics was selected because it is the best technique for descriptive analysis. These data may prove to be valuable in the future. (Please see results chapter).

Table 3.1: Operationalization of the Conceptual Framework

Title: A Descriptive Study of Chief Information Security Officers' Responsibilities in Texas State Government Agencies **Purpose:** The purpose of this research is to describe the responsibilities of Texas CISOs. This ARP uses descriptive categories drawn from Carl Burney (2003), Marilu Goodyear (2009), Havelka and Merhout (2009), Dwayne Whitten and, Michael Whitman (2011).	
Category	**Questionnaire Items**
1.Managerial	
1.1 Risk Management	Rate the importance of risk management as a managerial responsibility.* How often do you use risk management in your daily operations?**
1.2 Incident Response	Rate the importance of Incident response as a managerial responsibility * How often do you use Incident response in your daily operations?**
1.3 Budgeting	Rate the importance of budgeting as a managerial responsibility * How often do you use budgeting in your daily operations?**
1.4 Telecommunications	Rate the importance of telecommunications as a managerial responsibility * How often do you use telecommunications in your daily operations?**
2.Legal	
2.1 Information Security Policy	Rate the importance of information Security Policy as a legal responsibility * How often do you use information Security Policy in your daily operations?**
2.2 Procurement and Contracts	Rate the importance of procurement and contracts as a legal responsibility * How often do you use procurement and contracts in your daily operations?**
2.3 Ethical	Rate the importance of ethics as a legal responsibility* How often do you use ethics in your daily operations?**
3.Tecncial	
3.1 Software Development	Rate the importance of software development as a technical responsibility* How often do you use software development in your daily operations?**
3.2 Copyright	Rate the importance of Copyright as a technical responsibility* How often do you use Copyright in your daily operations?**

3.3 System Acquisition	Rate the importance of System Acquisition as a technical responsibility * How often do you use System Acquisition risk management in your daily operations?**
4. Career Development	
4.1 Faculty Awareness	Rate the importance of Faculty Awareness as a career development responsibility* How often do you use Faculty Awareness in your daily operations?**
4.2 Technical Continuity	Rate the importance of Technical Continuity as a career development responsibility * How often do you use Technical Continuity in your daily operations?**
4.3 Certifications	Rate the importance of Certifications as a career development responsibility * How often do you use Certifications in your daily operations?**
5. Information Security	
5.1 Data Security	Rate the importance of Data Security as an information security responsibility* How often do you use Data Security in your daily operations?**
5.2 Network Security	Rate the importance of System Acquisition as an information security responsibility* How often do you use System Acquisition risk management in your daily operations?**
5.3 Access Controls	Rate the importance of Access Controls as an information security responsibility* How often do you use Access Controls in your daily operations?**
6. Additional Questions	
6.1 Recommendations	Do you have any comments or insights into the role of the CISO/IT Security officer in public institutions? (Open-ended)
7.Demographic Variables	
7.1 Gender	What is your gender? (Multiple Choice)
7.2 Age	What is your age? (Number)
7.3 Title	What is your official title? (Open-ended)
7.4 Education	What is your highest earned degree? (Multiple Choice)

*Response scale: (1) Not at all important, (2) Slightly important, (3) Moderately Important , (4) Very Important, (5) Extremely Important
** Response scale (1) Daily, (2)Weekly, (3) Monthly , (4) Quarterly, (5) Other, Please specify

Chapter Summary

In conclusion, Chief Information Security Officer (CISOs) of Texas were surveyed in order to measure how frequent and important each responsibility was. The conceptual framework guided the creation of the survey. The following chapter will present results from survey data collected and discuss findings from the study.

Chapter 4: Results

Chapter Purpose

The purpose of this chapter is to present and discuss results of a survey administered to Chief Information Security Officers (CISOs) in Texas. A thorough review of the literature helped determine five major roles for the CISOs. Additionally, a web-based survey administered to the CISOs in Texas gathered data on CISOs' perception of the importance of these roles and the frequency with which they engaged in these roles. This chapter presents results obtained from the survey.

Survey Response Rate

A public information request was submitted to receive contact information for CISOs in Texas. The public information request asked for the name, email, position title, and phone number for each of the CISOs. Consequently, a web-based survey was administered to 100 of these CISOs by sending them an email link to the survey. Once the survey was administered, six emails bounced back. As a result, the survey was administered to a total of 94 potential respondents.

A total of 27 individuals responded to the survey, resulting in a response rate of 28%. Out of the 27 respondents, only eleven of them explicitly identified themselves as Chief Information Security Officers. Nine respondents indicated their position as Information Security Director. As mentioned in the literature review, "'director of information security' is a title commonly applied to this position and frequently modified as chief information security officer to highlight the individual's responsibility across the origination" (Goodyear 2009).The following sections of this chapter provide details of results obtained from the survey.

Risk Management was seen as an important role for CISOs based on review of the literature. In my survey, the importance that CISOs attributed to risk management and frequency with which they managed risk was measured by two specific questions. Question 1.1a and 1.1b in the survey asked respondents to rate the importance of risk management as a CISO role, and to indicate the frequency with which risk was used by CISOs. As indicated in table 1.1a below, only a negligible percentage (3.6%) of all respondents felt that is was *not an important role* for CISOs. Almost 78% of the respondents felt that risk management was *very important* (33.3%) or *extremely important* (44.4%).

Table 1.1a- Importance of Risk Management as Managerial Responsibility

1.1a Rate the importance of risk management as a managerial responsibility		
	Number of Respondents	**Percentage of Respondents**
Not at all important	0	0%
Slightly important	0	0%
Moderately important	1	3.7%
Very Important	9	33.3%
Extremely important	12	44.4%
Total of Respondents that not answer	5	18.6%
Total Number of respondents	27	100%

Respondents were also asked how often they engage in risk management. As indicated in table 1.1b, below, 33.3% of the respondents engaged in risk management on a *daily* basis, and 11.1% on *weekly* basis and in risk management, while 14.8% of the respondents engaged in risk management on a *monthly* basis. Only two of the respondents noted that they were less likely to manage risk on a daily to *monthl*y basis.

Table 1.1b Frequency of Engagement in Risk Management

1.1b How often do you manage risk?		
	Number of Respondents	Percent of Respondents
Daily	9	33.3%
Weekly	3	11.1%
Monthly	4	14.8%
Quarterly	1	3.7%
Annually	1	3.7%
Other, Please specify	2	7.4%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100

Incident responses provided CISOs with the tools to manage possible threats to information assets and infrastructure. Such management is an important responsibility mentioned in the literature review because it uses specific skills that assess threats. The importance of incident response was measured, and is displayed in table 1.2a. More than ten respondents indicated that incident response was *extremely* important, with an additional 37% rating it is *slightly* important (see table 1.2a). These results are also reflected in the responses from one of the participants that noted incident response as *moderately* important. Amongst *other* responses, participants indicated that they manage risk as problems come about (7.4%). Seven participants (25.9%) did not respond to this question.

Table 1.2a- Importance of Incident Response as a Managerial Responsibility

1.2a Rate the importance of Incident response as a managerial responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%
Slightly important	0	0%

Moderately important	1	3.7%
Very Important	10	37%
Extremely important	11	40.7%
Total of Respondents that did not answer	5	18.6%
Total Number of respondents	27	100%

In regards to the frequency with which CISOs managed information security incidents, about 29.6% of the respondents showed that they respond to incidents on a *daily* to *weekly* basis (see table 1.2b). Only 7.4% of the respondents indicated that they respond to information security incidents on at least a *quarterly* basis. However, 22.2% of the *other* respondents specified an “as needed” response to threats as they occur.

Table 1.2b Frequency of Engagement in Information Security Incidents

1.2b How often do you respond to Information Security Incidents?		
	Number of Respondents	Percent of Respondents
Daily	3	11.1%
Weekly	5	18.5%
Monthly	4	14.8%
Quarterly	1	3.7%
Annually	1	3.7%
Other, Please specify	6	22.2%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

Budgeting is likewise an important managerial responsibility for CISOs. CISOs take on the task of budgeting for equipment, software, training, and other information management related activities. Results presented in table 1.3a below show how CISOs rate the importance of budgeting as a managerial activity. Table 1.3a shows that more than 14 respondents indicated that managing a budget was *very* or *extremely* important. Roughly 51% of the respondents reported budgeting as a *very* or *extremely* important responsibility. Eight 29.6% of the respondents also reported that budgeting was *moderately* important. Other (22.2%) respondents noted they respond to information security incidents as problems arise, and five respondents did not answer this question (25.9%).

Table 1.3a- Importance of Budgeting as a Managerial Responsibility

1**.3a Rate the importance of budgeting as a managerial responsibility**		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%
Slightly important	0	0%
Moderately important	8	29.6%
Very important	7	25.9%
Extremely important	7	25.9%
Total of Respondents that did not answer	5	18.9%
Total Number of Respondents	27	100

In table 1.3b respondents are shown responding to the frequency with which they engage in budgeting tasks. Two respondents indicated that they engage in budgeting tasks on at least a *daily* or *weekly* basis. 18.5% budgeted for information related tasks on a *quarterly* basis and nearly 22.2% of the respondents engaged in budgeting tasks on an *annual* basis. Three *other* (11.1%) respondents indicated that they engage in budgeting tasks as the office needs the funds. Only four of the respondents considered engaging in budget tasks on a *monthly (14.8%)* basis.

Table 1.3b Frequency of Engagement in Budgeting Tasks

1.3b How often do you engage in budgeting tasks?		
	Number of Respondents	Percent of Respondents
Daily	1	3.7%
Weekly	1	3.7%
Monthly	4	14.8%
Quarterly	5	18.5%
Annually	6	22.2%
Other, Please specify	3	11.1%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

Since telecommunications assure the safety of all the devices used in an organization, it is an important part of managing information technology. CISOs reported, as shown in table 1.4a below, 44.4% of the respondents indicated that managing telecommunications was *very important* or extremely important. While 11.1% of respondents indicated that managing telecommunication was *slightly* important, only 3.7% of respondents reported that it is *not at all important*.

Table 1.4a- Importance of Telecommunications as a Managerial Responsibility

1.4a Rate the importance of telecommunications as a managerial responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	1	3.7%
Slightly important	3	11.1%
Moderately important	6	22.2%
Very important	9	33.3%
Extremely important	3	11.1%
Total Respondents that did not answer	5	18.9%
Total Number of Respondents	27	100%

The frequency with which CISOs manage telecommunications varied. As shown in table 1.4b, nearly a quarter of the respondents (22.2%) managed telecommunication on a *weekly* basis. Six respondents (22.2%) indicated that telecommunications were handled randomly and as needed by the office.

Table 1.4b Frequency of Engagement in Telecommunication

1.4b How often do you manage telecommunications devices?		
	Number of Respondents	Percent of Respondents

Daily	2	7.4%
Weekly	6	22.2%
Monthly	3	11.1%
Quarterly	1	3.7%
Annually	2	7.4%
Other, Please specify	6	22.2%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

Substantial evidence within the literature review noted that CISOs' responsibilities encompassed the legal dissemination and development of information security policies. 44.4% of the respondents rated information security policies as an *extremely* important responsibility in addition to the 29.9% of participants who rated it a *very* important responsibility. 7.4% responded to information security as a *moderate* importance. None of the respondents thought that information security was neither *not at all important* nor *slightly important*.

Table 2.1a Importance of Information Security Policies as a Legal Responsibility

2.1a Rate the importance of information Security Policy as a legal responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%
Slightly important	0	0%
Moderately important	2	7.4%
Very important	8	29.9%
Extremely important	12	44.4%
Total Respondents that did not answer	5	18.3%
Total Number of Respondents	27	100%

29.6% of participants reported *annual* implementation of security policies. 11.1% of respondents considered a quarterly review of implementing these policies. One 3.7% of the respondents indicated that they implement information security policies on a *daily* or *weekly basis.* 18.5% of respondents who chose “other”. However, there was no clear indication of the exact frequency with which they implemented information security policies.(See table 2.1b).

2.1b Frequency of Implementing Information Security Polices

2.1b How often do you implement Information Security Policies?		
	Number of Respondents	Percent of Respondents
Daily	1	3.7%
Weekly	1	3.7%
Monthly	2	7.4%
Quarterly	3	11.1%
Annually	8	29.6%
Other, Please specify	5	18.5%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

As shown in table 2.2a participants rated the importance of procurements and contacts as a legal responsibility. In the literature review this section accounted for prior legal polices in place in order for CISOs to integrate information systems through a binding contract. In my survey, an average of 40.7% participants noted that procurement and contracts were *very* important and 29.6% of the participants thought this responsibility was *extremely* important. Only 11.1% percent of the participants rated this as *moderate*ly important.

Table 2.2a Importance of Procurement and Contracts as a Legal Security Responsibility

2.2a Rate the importance of procurement and contracts as a legal responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%

Slightly important	0	0%
Moderately important	3	11.1%
Very important	11	40.7%
Extremely important	8	29.6%
Total of Not answered Respondents	5	18.6%
Total Number of Respondents	27	100%

The frequency with which CISOs managed procurements varied across respondents. Table 2.2b presents results related to this role. Equal percentages of participants indicated managing procurements were done on a *monthly* (18.5%) and *annual* (18.5%) basis. A total of 14.8% indicated that they managed procurement on a *weekly* (7.4%), or *quarterly* (7.4) basis. 14.8% manage procurements on a daily basis.

Table 2.2b Frequency of Managing Procurements

2.2b How often do you manage procurements?		
	Number of Respondents	Percent of Respondents
Daily	4	14.8%
Weekly	2	7.4%
Monthly	5	18.5%
Quarterly	2	7.4%
Annually	5	18.5%
Other, Please specify	2	7.4%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

Findings related to importance of contract management are displayed in table 2.2c. The same number of participants indicated that they managed contracts on a *daily (7.4%)*, *weekly (7.4%)*, or *other* "as needed" (7.4%) basis. Table 2.2c also shows that nearly 25.9% of the respondents managed contracts on an *annua*l basis. Small numbers of participants showed that they managed contracts on a *monthly* (11.1%) or *quarterly* basis (14.8%).

Table 2.2c Frequency of Managing Contracts

2.2c How often do you manage contracts?		
	Number of Respondents	Percent of Respondents
Daily	2	7.4%
Weekly	2	7.4%
Monthly	3	11.1%
Quarterly	4	14.8%
Annually	7	25.9%
Other, Please specify	2	7.4%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

In addition to legal responsibilities, ethics represent CISOs moral obligation to comply with the law. The literature review pointed out that this is worth mentioning because ethics represents CISOs' responsibility to act professionally. This view was also reflected in that more than 81.4% of the participants rated ethics as a *very* (40.7%), and *extremely* (40.7%) important responsibility as shown in table 2.3a.

Table 2.3a Importance of Ethics as a Legal Responsibility

2.3a Rate the importance of ethics as a legal responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%
Slightly important	0	0%
Moderately important	0	0%

Very important	11	40.7%
Extremely important	11	40.7%
Total Respondents that did not answer	5	18.6%
Total number of Respondents	27	100%

Some participants reported that they enforce ethics on a *daily* (25.9%) and *weekly* (7.4%) basis. A small number of participants enforced them on a *monthly* (3.7%) basis. Other participants also noted that they enforce ethics on a *quarterly (*3.7%) basis. In contrast, a large number of participants (29.6%) specified that they enforce ethics as problems arise. Table 2.3b also represents a percent of participants (18.9%) who manage ethics at an *annual* basis. Unfortunately, 8 out 27 participants did not answer how often they manage ethics.

Table 2.3b Frequency of Enforcing Ethics

2.3b How often do you enforce ethics?		
	Number of Respondents	Percent of Respondents
Daily	7	25.9%
Weekly	2	7.4%
Monthly	1	3.7%
Quarterly	1	3.7%
Annually	3	11.1%
Other, Please specify	5	18.5%
Total Number of Respondents that did not answer	8	29.6%
Total Number of Respondents	27	100%

CISOs technical responsibilities also distinguish them from many other professionals in the information systems field. Software development represents an important part of technical responsibilities because it represents a way to ensure systems are uniquely and safely created. Consistent with participants who answered software development as an *extremely important* (18.5%) responsibility, participants also distinguished software development as a *very importan*t (18.5%) responsibility. Large numbers of participants also reported software development as a *slightly* (11.1%) and *moderately important* responsibility (22.2%). A small number of participants indicated software development as *not at all important* (3.7%). There were 26% of participants who did not answer the importance of software development as a technical responsibility. (See table 3.1a)

Table 3.1a Importance of Software Development as a Technical Responsibility

3.1a Rate the importance of software development as a technical responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	1	3.7%
Slightly important	3	11.1%
Moderately important	6	22.2%
Very important	5	18.5%
Extremely important	5	18.5%
Total Respondents that did not answer	7	26%
Total number of Respondents	27	100%

As illustrated in table 3.1b, it was interesting to see that 66% of the respondents reported that they did not develop software. A small number of participants noted that they developed software on a *daily* (7.4%), *quarterly* (11.1%), and *annual* (3.7%) basis.

Table 3.1b Frequency of Software Development

3.1b How often do you Develop Software?		
	Number of Respondents	Percent of Respondents
Daily	2	7.4%
Weekly	0	0%

Monthly	1	3.7%
Quarterly	3	11.1%
Annually	1	3.7%
Other, Please specify	13	66%
Total Number of Respondents that did not answer	7	29.6%
Total Number of Respondents	27	100%

Table 3.2c presents feedback from the participants who had the opportunity to respond to an important technical responsibility of CISOs. Since copyright helps the organization maintain inventory of software and hardware products by ensuring they are up to date, participants were asked to rate the importance of copyright as a technical responsibility. Nearly half of the respondents thought that copyrights were *moderately* (25.9%) or *very* (22.2%) important. Less than half of the respondents recorded that copyright was *not at all* (3.7%) or *slightly* (14.8%) important. However only two respondents recorded copyright as an *extremely important* (7.4%) technical responsibility, and seven respondents did not answer to this question.

Table 3.2a Importance of Copyright as a Technical Responsibility

3.2a Rate the importance of Copyright as a technical responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	1	3.7%
Slightly important	4	14.8%
Moderately important	7	25.9%
Very important	6	22.2%
Extremely important	2	7.4%
Total Respondents that did not answer	7	26%
Total Number of Respondents	27%	100%

In addition to the importance of copyrights, participants were also asked to state the frequency with which they ensure copyrights are up to date (table 3.2b). While some participants recorded that they ensure copyrights on an *annual* (37%) basis, another five CISOs noted that this was not part of their job function (18.5%). None of the participants indicated they ensure copyrights on a *daily* basis. Furthermore an even smaller amount of participants indicated that they ensure copyrights on a *weekly* basis. CISOs also recorded they ensure copyrights on a *monthly* (7.4%) basis, with an additional (7.4%) on a *quarterly* basis. Seven participants did not answer how often they ensure copyrights are up to date.

Table 3.2b Frequency of Ensuring Copyrights

3.2b How often do you ensure that copyrights are up to date?		
	Number of Respondents	Percent of Respondents
Daily	0	0%
Weekly	1	3.7%
Monthly	2	7.4%
Quarterly	2	7.4%
Annually	10	37%
Other, Please specify	5	18.5%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

Though copyrights were an important part of technical responsibilities, the literature suggests that acquiring software systems is a key responsibility because it ensures that technical infrastructure is up to date. About 44.4% participants responded to systems as being a *very* (33.3%) and *extremely* (11.1%) important technical responsibility. It is important to note that none of the respondents recorded systems acquisitions as *not at all important*. 29.6% of the respondents rated systems acquisition as slightly *or moderately important*. (See table 3.3a).

Table 3.3a Importance of System Acquisition as a Technical Responsibility

3.3a Rate the importance of System Acquisition as a technical responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%
Slightly important	1	3.7%
Moderately important	7	25.9%
Very important	9	33.3%
Extremely important	3	11.1%
Total Number of Respondents that did not answer	7	26%
Total Number of Respondents	27	100%

When CISOs were asked to state how often they acquired license and software systems, more than one fourth of the participants noted that they do this *annually* (37%). In addition, five respondents (18.5%) indicated *other* times they acquire license and software as needed by the organization. One respondent answered that he/she acquires licenses and software systems on a daily basis (3.7%), and two respondents (7.4%) indicated this as a *monthly* responsibility. Two respondents also indicated they acquire software license on a *quarterly* basis (7.4%). None of the respondents indicated acquiring licensees and software systems as a *weekly* responsibility. (See table 3.3b). Seven participants did not answer how often they acquire licenses and software systems.

Table 3.3b Frequency of Acquiring Licenses and Software Systems

3.3b How often do you acquire licenses and software systems?		
	Number of Respondents	Percent of Respondents
Daily	1	3.7%
Weekly	0	0%
Monthly	2	7.4%
Quarterly	2	7.4%
Annually	10	37%

Other, Please specify	5	18.5%
Total Number of Respondents that did not answer	7	26%
Total Number of Respondents	27	100%

In addition to technical and managerial responsibilities, CISOs' positions require an extensive knowledge of computer science. The literature presents the importance of career development responsibilities that enable CISOs to grow further in their fields. Table 4.1a presents mixed responses about these issues. A little over half of participants responded to the importance of faculty awareness to be a *very important* (25.9%) or *extremely important* (37%) responsibility. None of the participants responded to faculty awareness being not at all important (0%). There were 3 participants who stated that faculty awareness was *slightly* (3.7%) or *moderately* (7.4%) important.

Table 4.1a Importance of Faculty Awareness as a Career Development Responsibility

4.1a Rate the importance of Faculty Awareness as a career development responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%
Slightly important	1	3.7%
Moderately important	2	7.4%
Very important	10	37%
Extremely important	7	25.9%
Total of Respondent that did not answer	7	26%
Total Number of Respondents	27	100%

Table 4.1b shows that 14.8% trained staff on a *weekly*, *monthly* and *annual* basis. 11.1% said that they trained staff on a quarterly basis and another 11.1% indicated that they engaged in

this role at different times of the year. Only two respondents recorded that they trained staff on a *daily* basis.

Table 4.1b Frequency of Staff Training

4.1b How often do you train staff?		
	Number of Respondents	Percent of Respondents
Daily	2	7.4%
Weekly	4	14.8%
Monthly	4	14.8%
Quarterly	3	11.1%
Annually	4	14.8%
Other, Please specify	3	11.1%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

The literature review also pointed out the importance of keep up with the workforce environment. CISOs are often faced with changing technology, and need to constantly take classes in order to train for new technical skills. CISOs in my survey were asked to rate the importance of technical continuity and indicate how often they update their technical skills. Tables 4.2a and 4.2b indicate the responses on this dimension. It was interesting to see that respondents rated technical continuity as a *very important* (37%) responsibility. In addition to respondents who rated it an *extremely important* (22.2%) responsibility, technical continuity shows that it is a highly important skill. Some respondents did say that technical continuity was *moderately important*. Further, there were zero respondents who rated technical continuity as *not at all important* or *slightly important.*

Table 4.2a Importance of Technical Continuity as a Career Development Responsibility

4.2a Rate the importance of Technical Continuity as a career development responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%
Slightly important	0	0%
Moderately important	4	14.8%
Very important	10	37%
Extremely important	6	22.2%
Total of Respondent that did not answer	7	26%
Total Number of Respondents	27	100%

Table 4.2b shows the frequency in which CISOs update their technical skills. It was interesting to see that some CISOs update their skills on a *daily* (7.4%) basis. Some (14.8%) update their technical skills on a *weekly* basis. The rest of the participants' responses are similar to each other. A similar number of participants recorded updating their technical skills on a *monthly* (14.8%), *quarterly* (14.8%), and annual (14.8%) basis. There were only two participants who noted that they update their technical skills on the grounds as often as needed. Seven out of twenty-seven (25.9%) of the respondents did not answer how often they update their technical skills.

Table 4.2b Frequency of Updating Technical Skills

4.2b How often do you update your technical skills?		
	Number of Respondents	Percent of Respondents
Daily	2	7.4%
Weekly	4	14.8%
Monthly	4	14.8%
Quarterly	4	14.8%
Annually	4	14.8%
Other, Please specify	2	7.4%

Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

In addition to updating technical skills, certifications also measure the preparation a CISO goes through in order to compete in the contemporary workforce. The literature often presented technical skills and verifications as one inclusive definition, but certification alone was often required by the organization. A little over half of the respondents recorded certification as a *moderately* (40.7%) or *very important* (18.5%) responsibility. Some respondents indicated that certifications as a career development tool was *slightly important* (14.8%). Six of the twenty-seven respondents did not answer this question, and zero percent thought that certification was *not at all important* as a career development.

Table 4.3a Importance of Certification as a Career Development Responsibility

4.3a Rate the importance of Certifications as a career development responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%
Slightly important	4	14.8%
Moderately important	11	40.7%
Very important	5	18.5%
Extremely important	1	3.7%
Total number of respondents that did answer	6	22.3%
Total number of respondents	27	100%

Information security responsibilities represented an important responsibility because they assure the organization of safety of their infrastructure. Data security presented in the literature was especially important because ensures protection of private information. A large percentage (63%) of respondents identified data security as an *extremely* important information security responsibility. In addition to respondents that thought data security was *very important* (7.4%), respondents felt this was an important responsibility. While a lower percentage (3.7%) of respondents see data security as *moderately* important, none of the respondents thought that data security was *not at all important*. Also, none of the respondents thought that data security was *slightly* important, and 25.9% of the total represents the respondents that did not answer this question. (See table 5.1a)

Table 5.1a Importance of Data Security as an Information Security Responsibility

5.1a Rate the importance of Data Security as an information security responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%
Slightly important	0	0%
Moderately important	1	3.7%
Very Important	2	7.4%
Extremely important	17	63%
Total number of respondents that did not answer	7	25.9%
Total number of respondents	27	100%

Table 5.2b shows the frequency with which they deal with data security issues. It was surprising to see such mixed results amongst participants. Almost one third of the respondents dealt with data security on a *daily* (14.8%) or *weekly* (18.5%) basis. However, a small number of participants said that they dealt with data security on a *monthly* (14.8%) or *quarterly* (7.4%) basis. Only one participant dealt with data security on an *annual* (3.7%) basis. Other (14.8%) participants identified data security issues as a problem to be dealt with when needed.

Table 5.1b Frequency of Dealing with Data Security Issues

5.1b How often do you deal with data security issues?		
	Number of Respondents	Percent of Respondents
Daily	4	14.8%
Weekly	5	18.5%
Monthly	4	14.8%
Quarterly	2	7.4%
Annually	1	3.7%
Other, Please specify	4	14.8%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

Because organizations are connected through a network, many organizations invest in professionals who are prepared to protect it. Network security is only handled by professionals, and represents an important factor of information security within the organization. In table 5.2a participants were asked to rate the importance of network security. A little over half of the participants rated network security as *extremely important* (59.3%) or *very important* (11.1%). There was only one participant who rated network security as *moderately important*. Furthermore, none of the participants rated network security as *not at all important* or *slightly important*.

Table 5.2a Importance of Network Security as an Information Security Responsibility

5.2a Rate the importance of Network Security as an information security responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%

Slightly important	0	0%
Moderately important	1	3.7%
Very important	3	11.1%
Extremely important	16	59.3%
Total Number of respondents that did not answer	7	25.9%
Total number of respondents	27	100%

Table 5.2b measures the frequency with which they engage in network security responsibilities. Several of the respondents dealt with network security on a *daily* (22.2%) or *weekly* basis (14.8%). Six participants (22.2%) recorded that they work on securing a network on a *monthly* basis. Several participants recoded working on network security on *other* (11.1 %) occasions, as needed. Only one participant noted working on network security on an *annual* basis.

Table 5.2b Frequency of Securing a Network

5.2b How often do you work on securing the network?		
	Number of Respondents	Percent of Respondents
Daily	6	22.2%
Weekly	4	14.8%
Monthly	6	22.2%
Quarterly	0	0%
Annually	1	3.7%
Other, Please specify	3	11.1%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

CISOs carry the burden of granting access to *people* within an organization. CISOs were asked to rate the importance of access controls as an information security responsibility. Table

5.3a shows the pattern of responses relating to this important dimension. Table 5.3b measures the frequency with which CISOs engage in granting access to users. In table 6.1a, more than half of the respondents indicated granting access as a *very* (40.7%) or *extremely important* (25.9%) responsibility. It was also interesting to see that none of the participants recorded access controls as a *slightly* (0%) or *not at all important* responsibility (0%).

Table 5.3a Importance of Access Controls as an Information Security Responsibility

5.3a Rate the importance of Access Controls as an information security responsibility		
	Number of Respondents	Percentage of Respondents
Not at all important	0	0%
Slightly important	0	0%
Moderately important	2	7.4%
Very important	7	25.9%
Extremely important	11	40.7%
Total number of respondents that did not answer	7	26%
Total Number of Respondents	27	100%

A vast number of participants indicated that they grant access on a *daily* (44.4%) and *weekly* basis (11.1%). A very small number of respondents indicated that they granted access controls on a *quarterly* (0%), or *annual* (3.7%), basis. Only two respondents noted that they granted access controls as needed by the organization. Seven of the respondents did not respond to how often they grant access. (See table 5.3b).

Table 5.3b Frequency of Granting Access Controls

5.3b How often do you grant access controls?		
	Number of Respondents	Percent of Respondents
Daily	12	44.4%

Weekly	3	11.1%
Monthly	2	7.4%
Quarterly	0	0%
Annually	1	3.7%
Other, Please specify	2	7.4%
Total Number of Respondents that did not answer	7	25.9%
Total Number of Respondents	27	100%

In order to get a demographic perspective of the respondents, the following tables will show the respondents' genders, ages, titles, and educational attainment. 48.1% of the participants identified themselves as males. Only seven respondents (25.9%) identified as females. About a quarter of the respondents (25.9%) who did not respond to this question. (See table 6.1a)

Table 6.1a Gender Distribution of Respondents

6.1a What is your gender?		
	Number of Respondents	Percent of Respondents
Male	13	48.1%
Female	7	25.9%
Missing	7	25.9%
Total	27	100%

Table 6.1b shows that about a third (29.6%), of all participants were between the ages of 45 to 54. About 22% of all participants were in the 55-64 age range. Only one participant indicated to be between the ages of 25 to 34 (3.7%). Further 18.5% participants reported being in the 35 to 44 year range, but none of the respondents recorded being over the age of 64. Similarly none of the respondents indicated being under the age of 21. Also, none of the participants indicated being between the ages of 21 to 24 years old. Seven of the participants did not record their age.

Table 6.1b Age Frequency

6.1b What is your age?		
	Number of Respondents	Percent of Respondents
Under 21	0	0%
21 to 24	0	0%
25 to 34	1	3.7%
35 to 44	5	18.5%
45 to 54	8	29.6%
55 to 64	6	22%
64 older	0	0%
Missing respondents	7	25.9%
total	27	7.4%

About 37% of the participants had a *master's* (33.3%) or *PHD* (3.7%) degree. Only six participants recorded having just a four-year college degree. Several participants indicated having *some college to no degree,* and none of the participants said they had a *two year college degree*. Several respondents did not answer the college education experience question. (See table 6.1c)

Table 6.1c Frequency of Highest Degree Earned

6.1c What is your highest earned degree?		
	Number of Respondents	Percent of Respondents
Some college to, No degree	4	14.8%
Two –year College degree	0	0%
Four-year College degree	6	22.2%
Master/Graduate degree	9	33.3%
PHD	1	3.7%
Missing respondents	7	25.9%
total	27	100%

67% percent of surveyed CISOs indicated that they manage 1 to 20 employees. Only one participant indicated managing 41 or more employees. None of the respondents identified managing 21 to 30, and 31 to 40 employees. There were eight of the respondents who did not answer how many employees they managed (see table 6.1d).

Table 6.1d Frequency of Employees Managed

6.1d How many employees do you manage?		
	Number of Respondents	Percent of Respondents
1 to 20	18	66.7%
21 to 30	0	0%
31 to 40	0	0%
41 more	1	3.7%
Missing respondents	8	25.9%
total	27	100%

Finally, as shown in table 6.1e, participants were asked to state the experience they had in their current position. A small percentage of participants indicated they were less than 1 year (3.7%) and 1 to 2 years (7.4%) in their current position. Seven participants recorded having between 2 to 5 years (18.5%), in addition to respondents with 6 to 10 years (11.1%) in their current position. Nine of the respondents stated they held their current position for 10 plus years, and 25.9% of the respondents did not answer this question.

Table 6.1e Years of Experience Frequency

6.1e How many years of experience do you have in your current position?		
	Number of Respondents	Percent of Respondents
Less than 1 year	1	3.7%
1 to 2 years	2	7.4%
2 to 5 years	5	18.5%
6 to 10 years	3	11.1%
10+	9	33.3
Missing respondents	7	25.9%
total	27	100%

Chapter 5: Conclusion

Chapter Purpose

The purpose of this chapter is to review and summarize the research presented in this study. Results from the previous chapter will be discussed. Finally, this chapter will explain the purpose behind this study, and recommendations for potential research are presented.

Research Summary

This Applied Research Project described the emerging responsibilities of Chief Information Security Officers. Existing literature was used to develop a conceptual framework that organized various responsibilities of Chief Information Security Officers in Texas state agencies. The conceptual framework was used to create a survey and help describe to emerging responsibilities of CISOs identified by the literature.

The literature review introduced responsibilities that were divided into five independent categories. These categories were used to develop the conceptual framework presented in chapter 2. The first responsibility was managerial and entailed risk management, incident response, budgeting and telecommunications as subcategories. The second category consisted of three sub categories with respect to legal responsibilities, information security polices, procurement and contracts and ethics. Thirdly technical responsibilities had three subcategories which were software development, copyright and system acquisition. The fourth set of career development subcategories include faculty awareness, technical continuity, and certifications. Finally information security responsibility had data security, network security and access controls as subcategories.

Each descriptive category was developed to explain the extent to which CISOs valued each responsibility and the frequency in which they engage in such responsibilities. The survey was sent out to CISOs in state agencies in Texas. A web based survey was administered to 100 CISOs and once the email was sent, only six emails bounced back. As a result the survey was administered to a total of 94 potential respondents. A total of 27 individuals responded to the survey, and out of 27 respondents only eleven explicitly identified as Chief Information security Officers.

Summary of Findings

This study suggest that CISOs represented in this study regard various responsibilities as extremely important. Though the frequency in which some of these responsibility changes according to the needs of the state agency, CISOs are attempting to address the importance of information security protection. While information security directors also responded to the questionnaire, more than half of the respondents in this study did directly represent the CISO title. It is important to point out that because technology is changing quickly, so are the daily responsibilities of CISOs. The results showed that CISOs not only take on technical responsibilities, but are having deep concern about information security policies.

However, each survey item was individually analyzed and was used to understand the importance each responsibility. In order to describe the important responsibilities of CISOs in Texas state agencies, survey questions where developed that addressed each five categories. A summary of the survey results is presented in table **5.1** listed below.

Table 5.1 Summary of Results

	Survey Question	Results
Managerial		
Risk Management	Rate the importance of risk management as a managerial responsibility. How often do you manage risk?	77% Extremely or Very Important 44% Daily or Weekly
Incident Response	Rate the importance of Incident response as a managerial responsibility. How often do you respond to Information Security Incidents?	77% Extremely or Very Important 30% Daily or Weekly
Budget	Rate the importance of budgeting as a managerial responsibility. How often do you engage in budgeting tasks?	51% Extremely or Very Important 40% Quarterly or Annually
Telecommunication	Rate the importance of telecommunications as a managerial responsibility How often do you manage telecommunications devices?	44% Extremely or Very Important 30% Daily or Weekly
Legal		
Information Security Policies	Rate the importance of information Security Policy as a legal responsibility. How often do you implement Information Security Policies?	74% Very or Extremely Important 48% Annually or Other "when needed"
Procurement and Contracts	Rate the importance of procurement and contracts as a legal responsibility Frequency of Managing Procurements? Frequency of Managing Contracts	70% Very or Extremely Important 26% Monthly or Quarterly

		33% Annually or Other “when Needed”
Ethics	Importance of Ethics as a Legal Responsibility Frequency of Enforcing Ethics	81% Very or Extremely Important 33% Daily or Weekly
Technical		
Software Development	Rate the importance of software development as a technical responsibility How often do you Develop Software?	33% Very or Extremely Important 66% Other “did not develop software”
Copyright	Rate the importance of Copyright as a technical responsibility How often do you ensure that copyrights are up to date?	30% Slightly or Moderately Important 37% Annually or 18.5% Other “not part of responsibility ”
System Acquisitions	Rate the importance of System Acquisition as a technical responsibility. How often do you acquire licenses and software systems?	44% Very or Extremely Important 55% Annually or Other “when needed”
Career Development		
Faculty Awareness	Rate the importance of Faculty Awareness as a career development responsibility. How often do you train staff?	63% Very or Extremely Important 26% Monthly or Quarterly
Technical Continuity	Rate the importance of Technical Continuity as a career development responsibility How often do you update your technical skills?	59% Very or Extremely Important 30% Quarterly or Annually
Certification	Rate the importance of Certifications as a career development responsibility	56% Slightly or Moderately Important
Information Security		

Data Security	Rate the importance of Data Security as an information security responsibility How often do you deal with data security issues?	89% Very or Extremely Important 33% Daily or Weekly
Network Security	Rate the importance of Network Security as an information security responsibility How often do you work on securing the network?	70% Very or Extremely Important 37% Daily or Weekly
Access Controls	Rate the importance of Access Controls as an information security responsibility How often do you grant access controls?	67% Very Extremely Important 56% Daily or Weekly
Demographics		
Gender	What is your gender?	48% Male 25.9% Female
Age	What is your age?	29.6% 45 to 54 22% 55 to 64
Highest earned degree	What is your highest earned degree?	22% Four-Year College Degree 33.3 Masters/Graduate Degree
Employees Managed	How many employees do you manage?	67% 1 to 20
Years of Experience	How many years of experience do you have in your current position?	18.5% 2 to 5 Years 33% 10+

An overwhelming number of respondents supported risk management, incident response, budget and telecommunication as an important managerial responsibility. This indicates that there is a notion among respondents that recognizes managerial responsibilities as very or extremely important. Significant numbers of respondents thought Legal responsibilities were very or extremely important. Respondents indicated that information security policies (74%), procurement and contracts (70%), and Ethics (81%) are very or extremely important. Ten respondents identified software development as very or extremely important responsibility (33%).

However, survey results contrast with the recent literature which includes software development as part of a CISO responsibilities. For example, 66% of respondents indicated that they do not develop software in their current position. In contrast with technical responsibilities, forty-four percent respondents favored system acquisition as a very or extremely important responsibility. Similarly, thirty percent of respondents indicated copyrights as slightly or moderately important.

Several other interesting finding were revealed through survey results. Respondents thought that faculty awareness and technical continuity were very or extremely important career development responsibilities. In contrast to certifications, fifty six respondents thought such responsibility was slightly or moderately important.

One of the most controversial responsibility was information security related because they deal with classified information. Eighty-nine percent of the respondents thought that data security was very or extremely important. Seventy percent of respondents indicated that network security was very or extremely important. Likewise, 67% of respondents also indicated that access controls were very or extremely important.

Recommendations

This study can be extended in many different ways in the future. A more nuanced understanding of each responsibility could be undertaken. Also future research can focus on how management controls information security tasks. Moreover, future research may find that my conceptual framework does not include all possible responsibilities. These categories, however, provide a baseline to which additions can be made.

Concerns over “legal” responsibilities from respondents of this survey indicated that more research should be included to investigate the relationship between federal legal regulations and constraints they pose on state agencies. A comprehensive definition of Chief Information Security Officers truly needs to be developed. As respondents to this survey suggested, director of information security also fall under this job description. Also respondents suggested that development of software technical responsibilities were part of other divisions of the state agency. Technical responsibilities in public information systems should be further investigated though the MPA programs. Additionally, it would be important to improve on emerging responsibilities. What were the exact responsibilities of CISOs before? When did the shift towards managerial positions begin?

Though the literature touches on the budgetary allocations, future research can also look at the amount of money spent on programs used to improve information security systems. CISOs should reflect on whether or not information security projects actually enhance security systems. If requesting a budget does not push the agency to spend on cybercrime protection, CISOs should question the importance they place on information systems.

REFERENCES

Babbie, E. (2001). *The Practice of Social Research.* Belmont: Wadsworth/Thomson Learning.

Babbie, E. (2004). *The practice of social research 10th* ed. Belmont, California: Wadsworth Publishing Co

Burney, C. (2003). ROLES AND RESPONSIBILITIES OF THE INFORMATION SYSTEMS SECURITY OFFICER. *Data Security Management*, 26(2),1.

Caruson, K., MacManus, S. A., & McPhee, B. D. (2012). Cybersecurity Policy-Making at the Local Government Level:An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. *Journal Of Urban Affairs*,(2012):1-22.

Coronado , A. J., & Wong, T. L. (2014). Healthcare Cybersecurity Risk Managment:Keys To an Effective Plan . *Biomedical Instrumentation & Technology / Association For The Advancement Of Medical Instrumentation*, 26-30.

Cunningham , J. M. (2015, January/February). A Public-Private Approach to Cybersecurity. *NACD Directorship*, pp. 41(1), 26-27.

Diane, R. (2014, July). Why Customized Cybersecuirty Training is Essential . *Security: Solutions For Enterprise Security Leaders*, pp. 51(7),50.

Don, H. (2002, October). Public-Sector Information Security : A Call to Action for Public-Sector CIOs. National Association of State Chief Information.

Epstein, A. J. (2015, September). Thinking Strategically About Cyber Risk . *NACD Directorship*, pp. 40(5), 32.

Fang, X., Lee, S., & Koh, S. (2005). Transition of Knowledge/Skills Requirment For Entry-Level IS Professionals: An Exploratory Study Based on Recruters' Perception. *The Journal of Computer Infotmaiton Systems*, 46(1), 58.

Fitzgerald, T., & Krause, M. (2007). *CISO Leadership: Essential Principles for Success.* CRC Press.

Goodyear , M., Nelson, M. R., Peterson, R., & Portillo, S. (2009). The Career of the IT Security Officer in Higher Education . *EDUCASE Center for Applied Research*, 1-49.

Goodyear, M., Portillo, S., Goerdel, H. T., & Williams, L. (2015). Cybersecurity Management in the States: The Emerging Role of Chief Informaiton Security Officers. *SSRN Electronic Journal SSRN Journal*, 1-42.

Havelka, D., & Merhout, J. W. (2009). Toward a Theory Of Infomtaiton Technology Professional Competence . *The Journal of Computer Information Systems*, 50(2), 106.

Kaijankoski, E. A. (2015). Cybersecurity information sharing between public–private sector agencies. *Networked Digital Library of Theses & Dissertations*. EBSCOhost. Retrieved September 13, 2015

Kim, S.-Y., Park, S. T., & Ko, M. H. (2015). Analysis of the Compentencies of Infomation Security Consultants: Camparison between Required Level and Retention Level. *Indian Journal of Science and Technology*, 8(21).

Kouns, B. L., & Kouns, J. (2011). *The chief information security officer [electronic resource] : insights, tools and survival skills / Barry L. Kouns & Jake Kouns.* IT Governance Pub.

MacManus , S. A., Caruson, K., & McPhee, B. (2013). Cybersecurity at local governments level:balancing demands for transparency and privacy rights. *Journal of Urban Affairs*, 35(4), 451-470.

Migga Kizza, J. (2002). Computer Network Security and Cyber Ethics. Jefferson, N.C.:

Namin, A., Hewett, R., & Inan, F. (2014). Builing Cyber Security Instructional Plan Through Faculty Development Program. *Annual International Conference On Infocomm Technologies In Competitive Strategies*, 91-100.

Northcutt, S., & Northcutt, S. (2004). *IT ethics handbook. [electronic resource] : right and wrong for IT professionals*. Rockland, MA. : Syngress Pub., 2004

Perez, E., & Prokupecz, S. (2015, June). *First on CNN: U.S. data hack may be 4 times larger than the government originally said.* Retrieved from CNN Politics: http://www.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html

Powner , D. A. (2014). Agencies Need to Establish and Implement Incremental Development Policies. *GAO Reports* (pp. 1-61). EBSCOhost.

Ritchey, D. (2014). The Information Chief. Security. *Security: Solutions For Enterprise Security Leaders*,, pp. 51(1),14-42.

Schooner, S. L. (2002). Desiderata: Objectives for a system of government contract law. *Public Procurement Law Review*, *11*, 103.

Shields, P. M., & Rangarajan, N. (2013). *A playbook for research methods: Integrating conceptual framewoks and project managment.* New Forums Press.

Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government Information Quarterly*, pp. 316–322.

Tipton, H. F., & Krause, M. (2003). *Information Security Managment Handbook.* CRC Press.

Weintraub Schifferle, L. (2015, June 4). *OPM data breach-what should you do ?* Retrieved from Federal Trade Commission: https://www.consumer.ftc.gov/blog/opm-data-breach-what-should-you-do

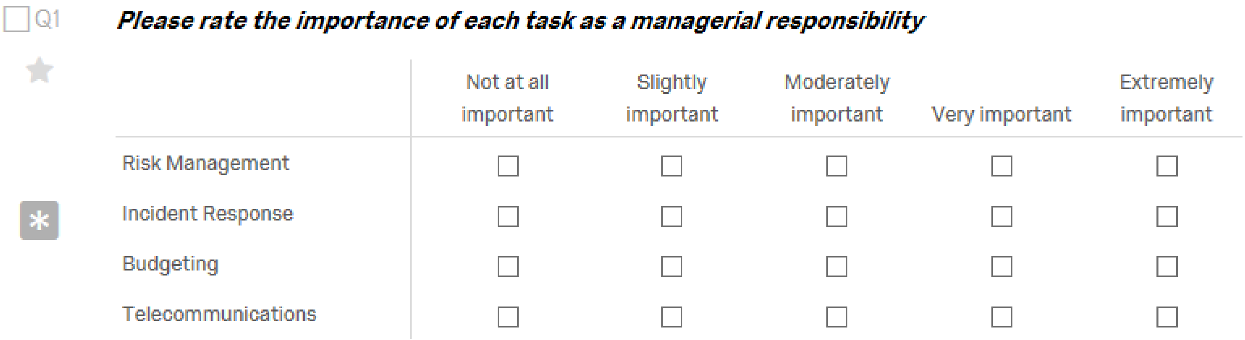
White, J. D. (2007). *Managing Information in the Public Sector.* Armonk, N.Y.: M.E.Sharpe,c2007.

Whitman , M., & Mattrod, H. (2011). *Principles of infomration security.* Cengage Learning.

Whitten, D. (2008). The Chief Information Seucirty Officer: An Analysis of The Skills Required For Success. *Journal of Computer Information systems*, 48(3)15.

Appendix A: Questionnaire

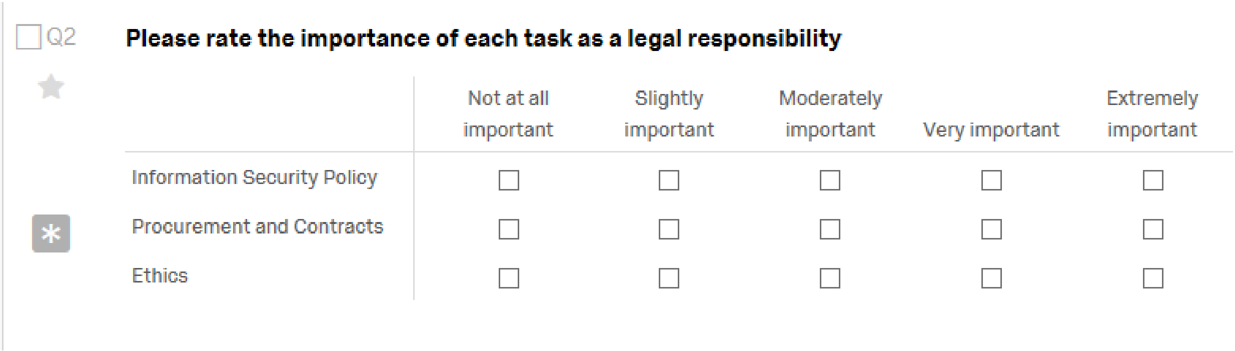
Chief Information Security Officer Survey



□ Q1

Please rate the importance of each task as a managerial responsibility

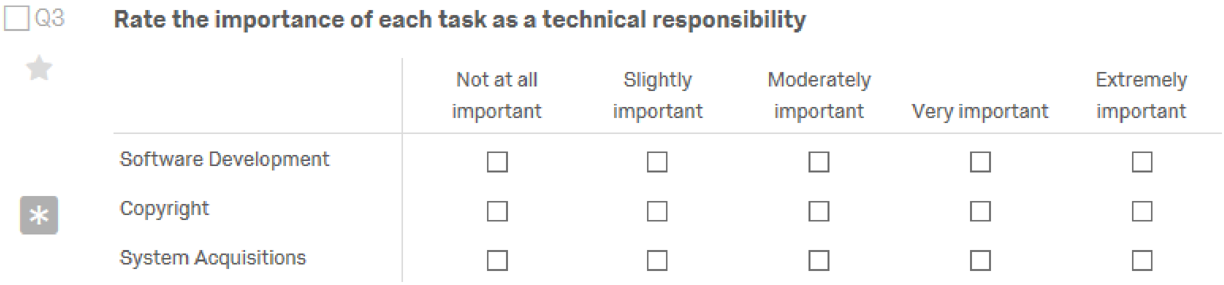
	Not at all important	Slightly important	Moderately important	Very important	Extremely important
Risk Management	□	□	□	□	□
Incident Response	□	□	□	□	□
Budgeting	□	□	□	□	□
Telecommunications	□	□	□	□	□



□ Q2

Please rate the importance of each task as a legal responsibility

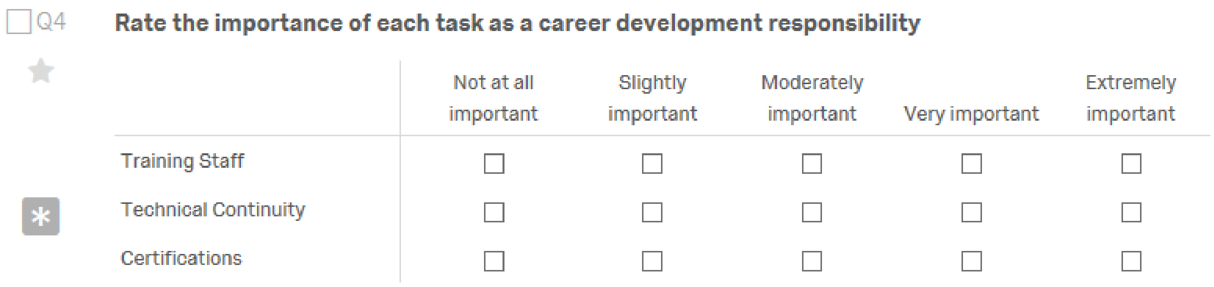
	Not at all important	Slightly important	Moderately important	Very important	Extremely important
Information Security Policy	□	□	□	□	□
Procurement and Contracts	□	□	□	□	□
Ethics	□	□	□	□	□



□ Q3

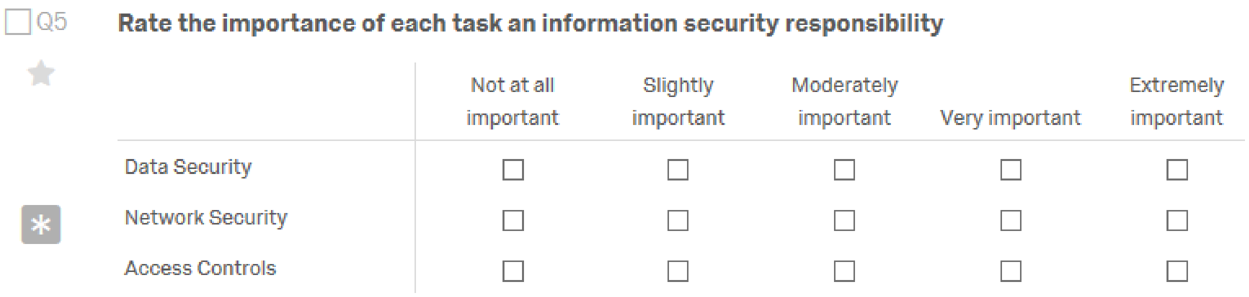
Rate the importance of each task as a technical responsibility

	Not at all important	Slightly important	Moderately important	Very important	Extremely important
Software Development	□	□	□	□	□
Copyright	□	□	□	□	□
System Acquisitions	□	□	□	□	□



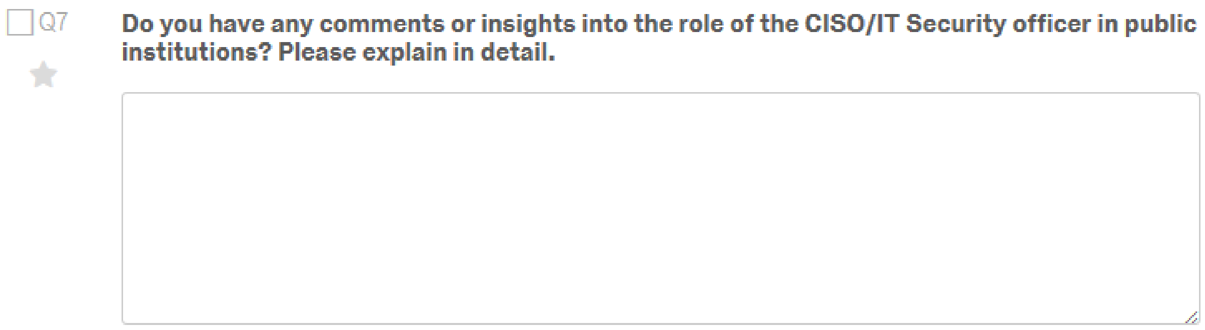
□ Q4 **Rate the importance of each task as a career development responsibility**

	Not at all important	Slightly important	Moderately important	Very important	Extremely important
Training Staff	□	□	□	□	□
Technical Continuity	□	□	□	□	□
Certifications	□	□	□	□	□

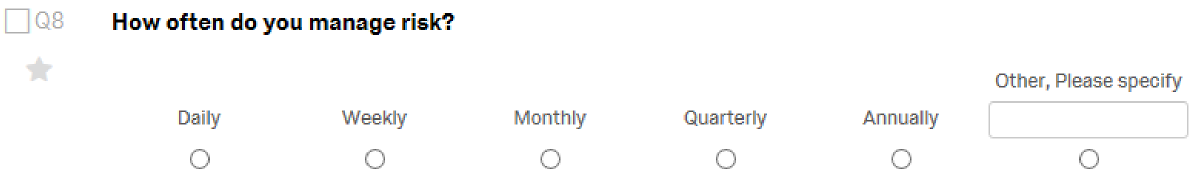


□ Q5 **Rate the importance of each task an information security responsibility**

	Not at all important	Slightly important	Moderately important	Very important	Extremely important
Data Security	□	□	□	□	□
Network Security	□	□	□	□	□
Access Controls	□	□	□	□	□

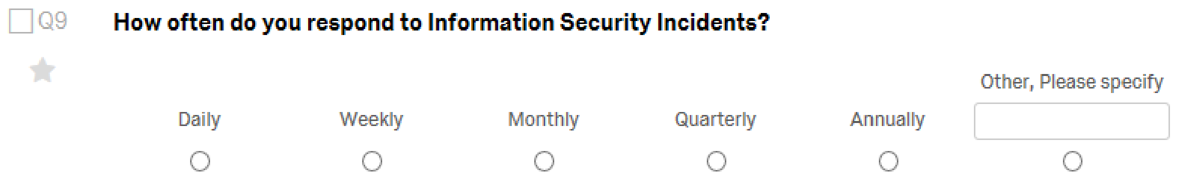


□ Q7 **Do you have any comments or insights into the role of the CISO/IT Security officer in public institutions? Please explain in detail.**



□ Q8 **How often do you manage risk?**

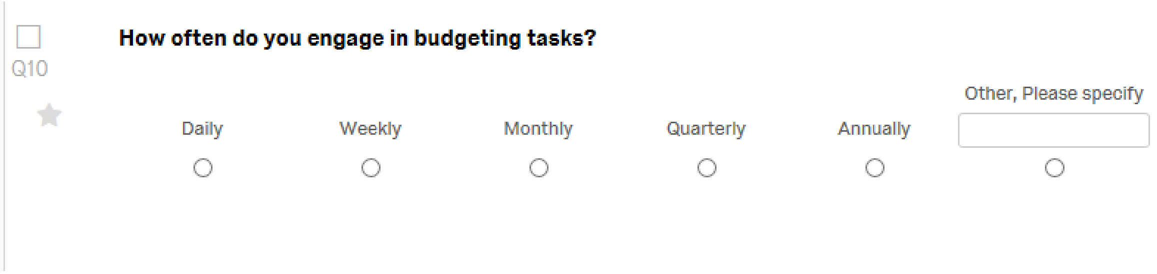
Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○



□ Q9

How often do you respond to Information Security Incidents?

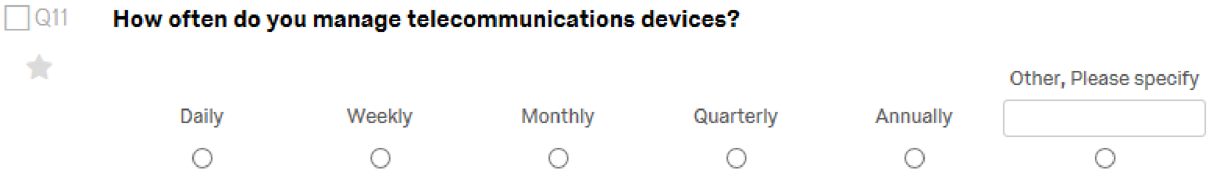
Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○



□ Q10

How often do you engage in budgeting tasks?

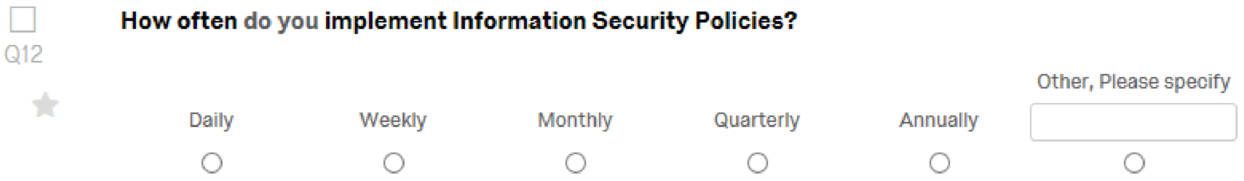
Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○



□ Q11

How often do you manage telecommunications devices?

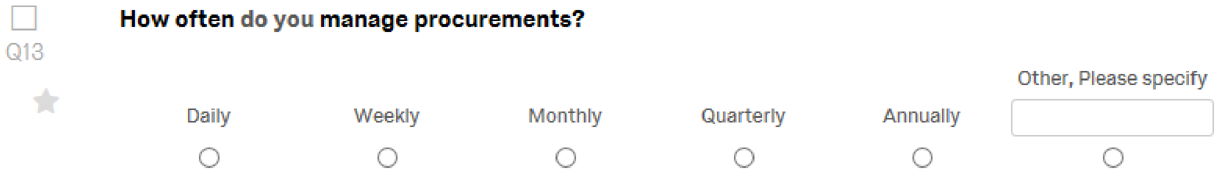
Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○



□ Q12

How often do you implement Information Security Policies?

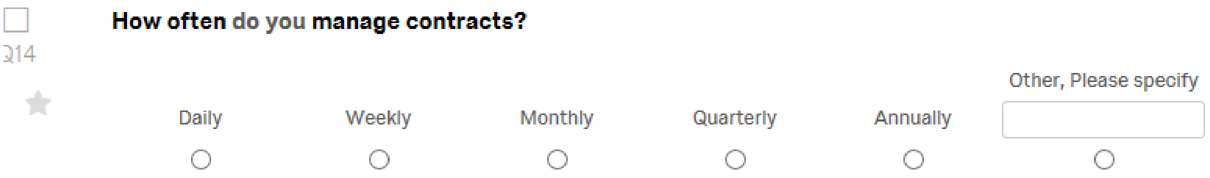
Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○



□ Q13

How often do you manage procurements?

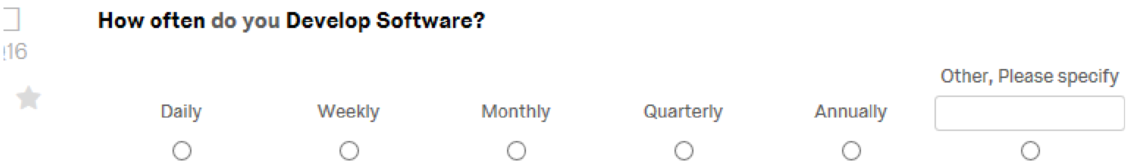
Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○



□ Q14 ★

How often do you manage contracts?

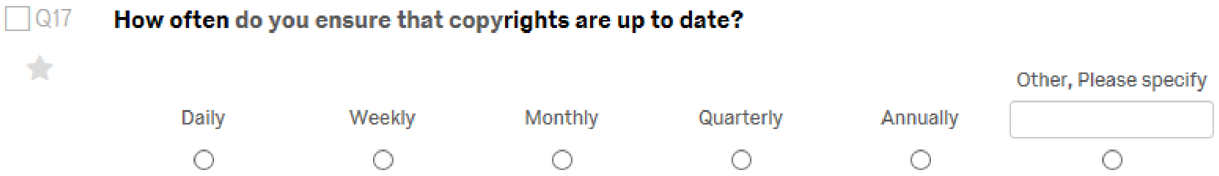
Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○



□ Q16 ★

How often do you Develop Software?

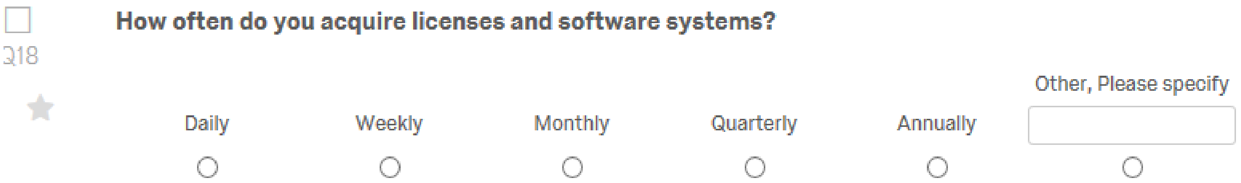
Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○



□ Q17 ★

How often do you ensure that copyrights are up to date?

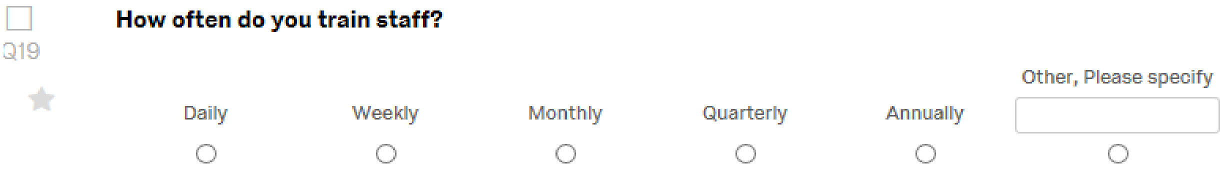
Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○



□ Q18 ★

How often do you acquire licenses and software systems?

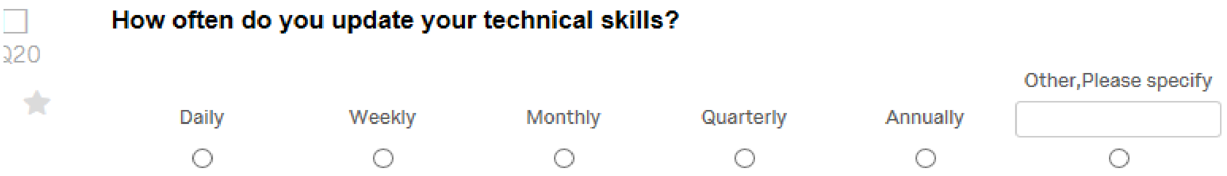
Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○



□ Q19 ★

How often do you train staff?

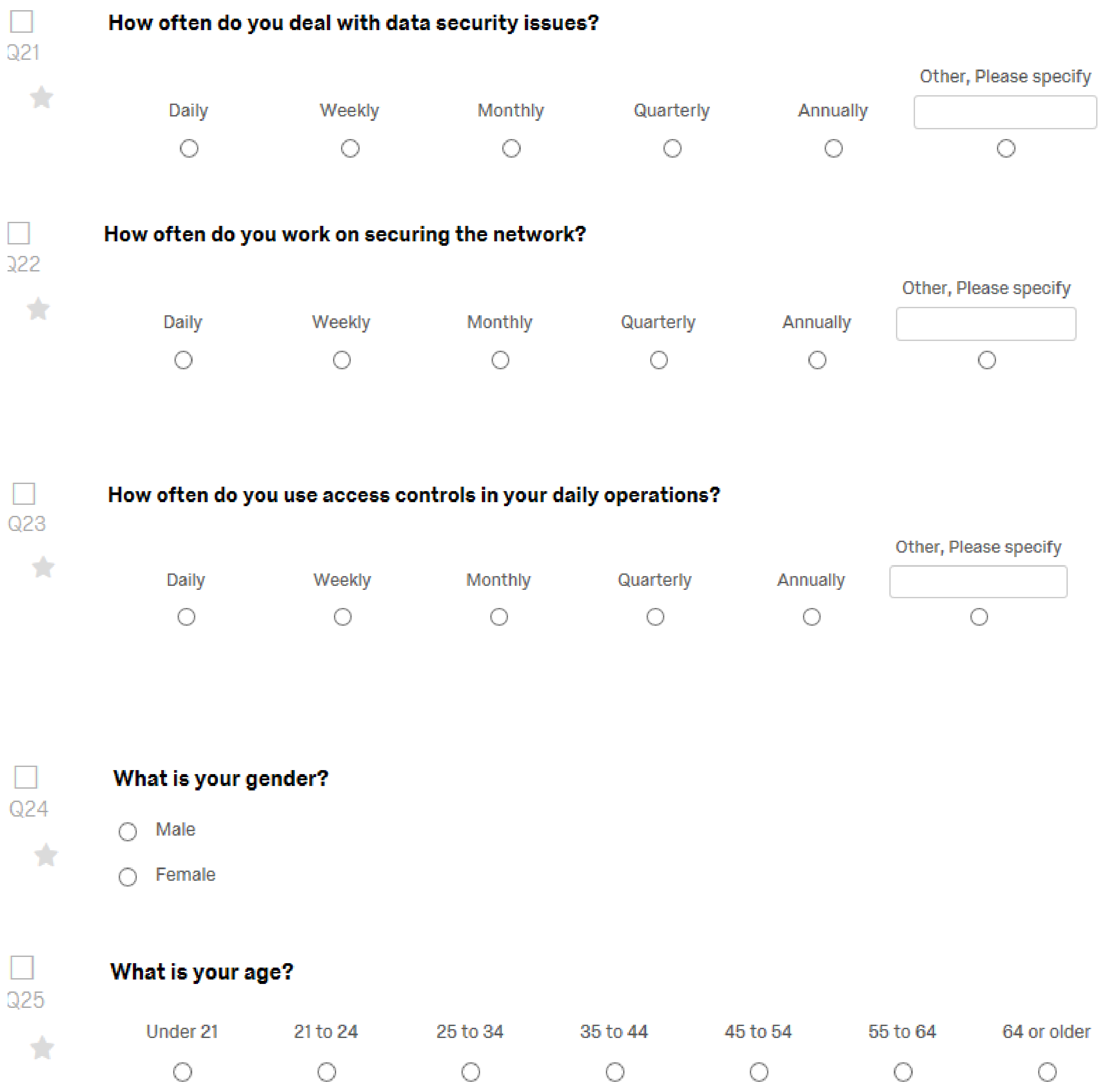
Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○



□ Q20 ★

How often do you update your technical skills?

Daily	Weekly	Monthly	Quarterly	Annually	Other,Please specify
○	○	○	○	○	○



□ Q21 ★

How often do you deal with data security issues?

Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○

□ Q22 ★

How often do you work on securing the network?

Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○

□ Q23 ★

How often do you use access controls in your daily operations?

Daily	Weekly	Monthly	Quarterly	Annually	Other, Please specify
○	○	○	○	○	○

□ Q24 ★

What is your gender?

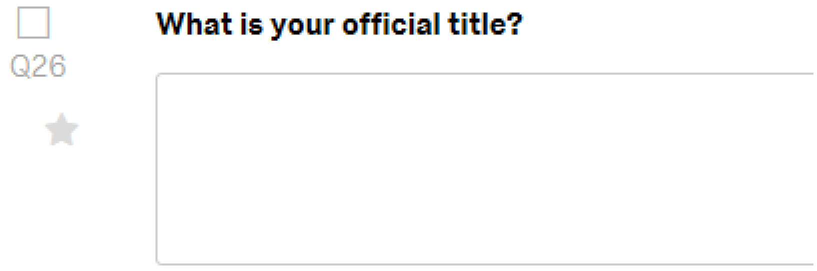
○ Male

○ Female

□ Q25 ★

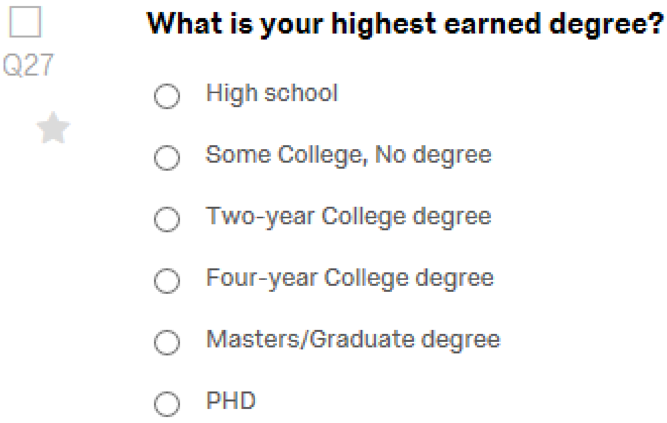
What is your age?

Under 21	21 to 24	25 to 34	35 to 44	45 to 54	55 to 64	64 or older
○	○	○	○	○	○	○



□ Q26 ★

What is your official title?



□
Q27
★

What is your highest earned degree?

○ High school

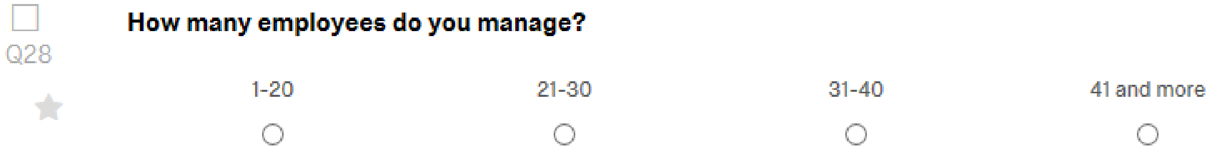
○ Some College, No degree

○ Two-year College degree

○ Four-year College degree

○ Masters/Graduate degree

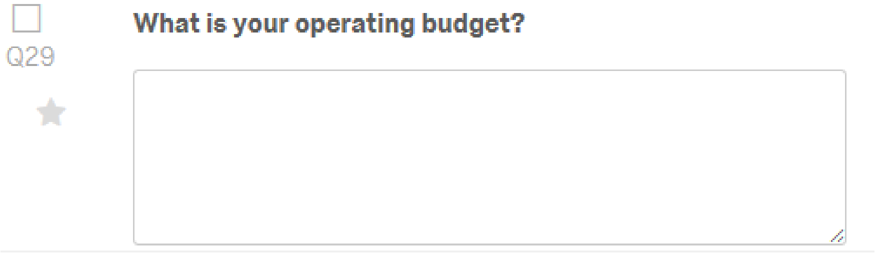
○ PHD



□
Q28
★

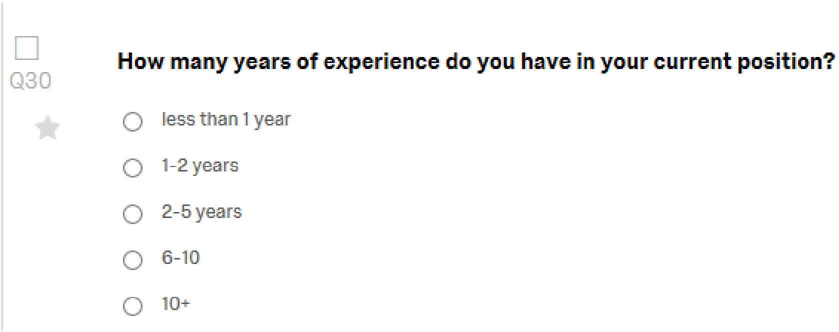
How many employees do you manage?

1-20	21-30	31-40	41 and more
○	○	○	○



□
Q29
★

What is your operating budget?



□
Q30
★

How many years of experience do you have in your current position?

○ less than 1 year

○ 1-2 years

○ 2-5 years

○ 6-10

○ 10+

**Name, operating budget, official title will be used for statistical analysis and record keeping. Respondents will not be identified individually.

Appendix B : Texas State Institutional Review Board

Exemption Request EXP2016A550233Z - Approval
AVPR IRB [ospirb@txstate.edu]

You forwarded this message on 1/12/2016 9:43 AM.

Sent: Tuesday, January 12, 2016 9:37 AM
To: Velazquez, San Juanita G

IRB APPROVAL EMAIL

DO NOT REPLY TO THIS MESSAGE. This email message is generated by the IRB online application program.

Based on the information in IRB Exemption Request EXP2016A550233Z which you submitted on 01/02/16 11:15:11, your project is exempt from full or expedited review by the Texas State Institutional Review Board.

If you have questions, please submit an IRB Inquiry form:

http://www.txstate.edu/research/irb/irb_inquiry.html

Comments:
No comments.

==

Institutional Review Board

Office of Research Compliance

Texas State University-San Marcos

(ph) 512/245-2314 / (fax) 512/245-3847 / ospirb@txstate.edu / JCK 489

601 University Drive, San Marcos, TX 78666

Texas State University is a member of the Texas State University System