2015

Investigating Roles of Information Security Strategy

Roger V. Seeholzer
Nova Southeastern University, seeholze@nova.edu

Investigating Roles of Information Security Strategy

by

Roger V. Seeholzer

A dissertation report submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University

2015

We hereby certify that this dissertation, submitted by Roger Seeholzer, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

_____ _____

Gurvirender P. Tejay, Ph.D. Date
Chairperson of Dissertation Committee

_____ _____

Steven R. Terrell, Ph.D. Date
Dissertation Committee Member

_____ _____

Barry McIntosh, Ph.D. Date
Dissertation Committee Member

Approved:

_____ _____

Eric S. Ackerman, Ph.D. Date
Dean, Graduate School of Computer and Information Sciences

Graduate School of Computer and Information Sciences
Nova Southeastern University

2015

An Abstract of a Dissertation Report Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the degree of Doctor of Philosophy

Investigating Roles of
Information Security Strategy

by
Roger V. Seeholzer
May 2015

A fundamental understanding of the complexities comprising an information security strategy (ISS) in an organization is lacking. Most ISS implementations in government organizations equate anti-virus or installing a firewall to that of an ISS. While use of hardware and software forms a good defense; neither comprises the essence of an ISS. The ISS best integrates with business and information system strategies from the start, forming and shaping the direction of overall strategy synergistically within large government organizations. The researcher used grounded theory and investigated what a large government organization's choices were with the differing roles an information security professional (ISP) chooses to operate with and to develop an information security program. Analysis of the data collected from interviewing 32 chief information security officers (CISOs) revealed how CISOs viewed their programs, aligned their goals in the organization, and selected role(s) to execute strategy. Use of grounded theory coding practices of the interviews showed a deficit in complexities of an ISS and a lack of an ISS in the majority of organizations. The participants came from multiple organizations in the National Capital Region on the east coast of the United States. This study advances the body of knowledge in a qualitative understanding of actions taken by CISOs to select a direction towards ISS implementation, role selection, and development of information security programs. It provides a theory for further testing of strategy development and role maturity.

Acknowledgement

When starting on this voyage to capture the mind of CISOs with a strategy, it seemed to be do-able, but would be and was a long and arduous trip. Over the subsequent four years, I spent many a night perusing the data collected and trying to see behind what had been stated. A grounded theory study is not easy for the uninitiated. It required a great deal of time and commitment to see it through to the end. At many points in time, I wanted to pick up the laptop, place it in the circular file, and move on. Thankfully, I had a very supportive other half who traveled with me on this journey and continually encouraged me to keep going. This work is dedicated to my wife Heike, whom without, I might not have finished. I also am very thankful for Dr. Gurvirender Tejay, who saw more in me than I did myself. He challenged me to dig deeper and find the elusive data at each stage of the dissertation process. I also would like to thank my committee members Dr. Steven Terrell and Dr. Barry McIntosh who both addressed obstacles I encountered along the way with constructive criticism and guidance to re-accomplish difficult transitions. I am thankful for being able to gain access to so many professionals in the field of information security who donated their time for interviews and insights into strategic ways of thinking, by speaking honestly and openly. Last of all and primarily, I give thanks for my faith and Divine guidance. In para phrasing a couple of verses of the Bible, I can say in like manner of Psalms 66:12, by learning many things I passed through the fire and the water to come out on the other side with an abundance. And now, continuing on the path as in Psalms 23, I have leaned on His staff and gone through the valley and will have goodness and mercy following after me.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

1.1 Evidence of the Problem

Traditionally, business forms the overall strategic direction of an organization through its vision disseminated in the business strategy (Cohen & Cyert, 1973; Miller, 1981; Wommack, 1979). With the advent of automation, the information technology department or function creates the information systems strategy to automate and align to the vision of the business strategy (Doherty & Fulford, 2006). The speed and breadth with which information systems penetrated business brought about the need for information systems to consider information security for two reasons. First, to protect the information entrusted to the organization residing in their information systems; second, to keep information technology assets defended from being vulnerable from compromise; and to keep the information owners apprised as to whether a breach occurs with their data and their automated information systems become compromised (Gilbert, 2008; McFadzean, Ezingeard, & Birchall, 2011; Smedinghoff, 2005). Through this, business and information technology are concerned with information security, to ensure an information system's usefulness to their users (Eloff & von Solms, 2000).

One of senior management's objectives is to ensure the prevention of data loss and avoid possible damage to their organizational reputation. Another objective focuses on building defenses to protect automation assets to prevent compromise (Anderson, 2003; Dlamini, Eloff, & Eloff, 2009; Dutta & McCrohan, 2002; Knapp & Boulton, 2006). An organization's reputation and possibly their economic survival depends upon having a secure environment as one of the important factors to operate securely from malicious threats, such as individuals trying to

socially engineer passwords and user names from unsuspecting personnel on the network, who could then infiltrate the network to exfiltrate information by siphoning activities (Bhalla, 2003; Hinde, 2003; Knapp & Boulton, 2006; Oreku & Mtenzi, 2009). The costs associated with remediating data breaches such as notifying victims of lost data and repair of public trust can be excessive (Baskerville, 1993; Doherty & Fulford, 2006; Dutta & McCrohan, 2002; Garg, Curtis, & Halper, 2003; Rowe & Gallaher, 2006). The organization, through senior management interaction seeks to have an effective information security strategy in place (Kayworth & Whitten, 2010; Loveland & Lobel, 2011).

The term information security strategy is often misunderstood. Organizational management views it as a necessary implementation of technical security controls and devices to keep people out of the organization's computers (Chang & Yeh, 2006). Information security is more than just technical security measures implemented, to meet regulatory demands (Damianides, 2005; Doherty & Fulford, 2006; Keen & El Sawy, 2010; Kim, 2004; Luftman & Ben-Zvi, 2010; Luftman & Ben-Zvi, 2011). Information security works with information technology to ensure the automated environment remains secure, preventing outside infiltration and internal misuse of devices and systems. Specifically, information security requires policy and governance (Posthumous & von Solms, 2004; von Solms 2006) and an information security strategy containing structured actions to meet an organization's policy and governance (White & Bruton, 2011); orchestrating an overall plan of action for the organization. The information security function within an organization works to formalize the information security strategy, a plan to implement protection of the information and intellectual property the organization uses to conduct business (Chen, Kataria, & Krishnan, 2011; Hinde, 2003; Knapp & Boulton, 2006; Mahmood, Siponen, Straub, Rao, & Raghu, 2010) from attackers who attempt to copy, delete,

manipulate or destroy information. Information security needs to somehow remain one step ahead of attackers (Bhalla, 2003; Gupta & Hammond, 2005; Howard & Longstaff, 1998).

1.2 Research Problem

In the literature there has been a call for a formal approach to information security that goes beyond implementation of technical controls (Dhillon, 1995; Herath & Rao, 2009; Ma, Johnston, & Pearson, 2008; Parkin & van Moorsel, 2009; Parakktu, 2010). Some researchers have emphasized the need for well developed strategies (Anderson & Choobineh, 2008; Hall, Sarkani, & Mazzuchi, 2011; Kayworth & Whitten, 2010; McFadzean, Ezingeard, & Birchall, 2011; Park & Ruighaver, 2008; Tejay, 2008). There has also been a call for information security to be more proactive rather than being reactive (Tejay, 2008). However, there is a dearth of studies focusing on the subject of information security strategy itself. The purpose of this study is to understand the complexities of information security strategy in a large government organization.

Exploring the problem examines the complexities of information security strategy primarily in what the differing roles an information security professional chooses to operate and how a large government organization proceeds to develop an information security program through the strategy. The latter, how an organization proceeds specifically to develop information security programs is with the vehicle defined as an information security strategy. Delving into the information security strategy composition and answering what an information security strategy means might grant insight into its construction. Looking into the construction can help to ascertain whether certain types of information security strategy are preferable over other forms of information security strategy under certain conditions. If so, it would also be helpful to understand how information security strategies differ within a large governmental

organization under study. Then, assuming there are multiple types of information security strategies, it would be helpful to search for ways in which an information security professional differentiates one information security strategy from another by performing appropriate roles to implement information security.

With the second area, when an information security professional differentiates one information security strategy from another, the person assumes a strategic role in order to perform information security duties. The process of selection leads to exploring the various strategic roles available for the information security professional towards accomplishment of information security. Various aspects of the roles and their selection were explored to assist in furthering an understanding of the process. This effort looks at what the other roles used for information security accomplishment are and what differentiates one role from another, whether each role involves a formal process, and if there is an optimum role for a specific information security strategy.

The argument of this study is that the literature is silent on role selection and explaining how a large governmental organization develops roles. There is a need to investigate what different roles are being used by government organizations. It would be of assistance to understand which types of information security strategy were preferable over other forms of information security strategy and under certain conditions. If so, it would be helpful to understand how a large, multifaceted government organization differs within one another in the accomplishment of information security. Most actions by an information security professional tend to be in response to an action, instead of methodically planning out responses. These reactive responses often lead to sometimes choosing incorrectly for given information security needs. In order to mitigate the reactive approaches, an information security professional should

evaluate the existing security strategies adopted by various organizations. The professional should be able to categorize the observed strategies of other organizations and select the correct direction to move an organization forward to meet the mission specified in the information security program.

Whether consciously or not, organizations do take actions related to information security. There is a need to understand those actions. They are the organization's strategies. Tejay (2008) argued the need to pay attention to the context of an organization in order to be successful. There must be an understanding of the connection between what the information security strategy requires and the role(s) necessary to work out the tenets of the information security strategy. Differing business and information systems requirements drive the contexts with which the information security professional connects the information security strategy to meet objectives of information security. It would be helpful to understand how different information security strategies actually in use in different organizations emphasize meeting their objectives (McFadzean, Ezingeard, & Birchall, 2007; Mintzberg & Waters, 1985). To this end, the goal would be to produce a theoretical model from the collected data. In Chapter 3, a complete discourse covered how the collected data was solicited from professionals and used to construct a possible theoretical model for use in large governmental organizations. This may assist in future studies to understand how organizations differ, utilizing the model to predict role selection. The use of grounded theory research by data collection techniques allowed the emergent data to feed the building of a theory (Eisenhardt, 1989; Corbin & Strauss 2008).

1.3 Definitions

One attribute of establishing understanding is to have a common core of communications between all stakeholders. This can be realized through the establishment of a common lexicon, a

taxonomy of definitions, considering the positions other researchers have adopted and share in common (Alter, 2008). A common lexicon assists people in communicating principles and convey meaning, especially in the area of strategy.

The vast coverage of information systems has had an influence in the field of business strategic management (Chan & Huff, 1992) and has influenced information systems strategy (Chen, et al., 2010). Some discussion has taken place with information security strategy as well (Baskerville & Dhillon, 2008; Ezingread, et al., 2005; McFadzean, et al., 2007; McFadzean, et al., 2011). In this chapter a discussion of strategy from the literature in three areas and moves through definitions of business strategy, information systems strategy and information security strategy.

1.3.1 Strategy.

Gavetti and Rivkin (2005) stated strategy is about choice, choosing what to do and what not to do, which affects the outcomes of an organization. While their article focused on choice, other articles focus on exactly what a strategy is (Alter, 2008; Gavetti & Rivkin, 2005; Mintzberg, 1987a; Mintzberg, Ahlstrand, & Lampel, 1998; Wommack, 1979), what a strategy is composed of (Cohen & Cyert, 1973), and how to develop and shape strategy (Gavetti & Rivkin, 2005; Wommack, 1979). Many researchers have devised models for strategies (Dunkerley, 2011; Ezingeard, et.al., 2005; Kankankalli, Tan, Teo, & Wei, 2003; Ma, Johnston, & Pearson, 2008; McClean & Kark, 2010; Rose, 2011), which attempts to capture the essence of strategy, but none have received discipline wide acceptance (Markides, 1999). Some of these models include Porter's five-forces model (Porter, 1980), and eight more are explained by Mintzberg & Waters (1985) for structuring strategy. The difficulty in an established definition might be explained more easily if consideration of two other aspects of strategy were reviewed, that of the

characteristics of decision making with strategy, and the issues around the differing levels of strategy.

The second subset of strategy is characteristics of decision making. This is the decision between strategic and non-strategic matters over the long term, their expected impacts, and the directional movement of strategy by decisions being made while performing the plan (Chen, et al., 2010). The third aspect is over the level in which a strategy operates. Some identify the corporate level (Porter, 1980), the competitive advantage level (Grant, 2005), and the functional strategy or resource allocation level (Hofer & Schendel, 1978). Others liken the strategy to the strategic, tactical, and operational levels respectively of a complete strategy (Grobler & Louwrens, 2005; da Veiga & Eloff, 2007). Either of these choices drives a strategy into managing the direction of an organization towards achieving a goal.

The strategy as a management plan of action is to achieve an objective, identified by milestones or markers to show progress towards achieving the objective (Chen, et al., 2010; King, 1978). This study observes the strategy in three areas of an organization, the business, information systems, and information security units based upon the business of the organization (McFadzean, et al., 2007).

1.3.2 Strategy in Business

Strategy in business is the integration of an organization's goals, policies, and actions, which appears as a plan or pattern of a cohesive whole (Tejay, 2008). In 'Crafting strategy', Mintzberg (1987b, In Tejay 2008) defined strategy as the five 'P's', which are plan, ploy, pattern, position, and perspective. More specifically, Mintzberg stated:

> "…strategy can be defined as (1) a plan (i.e., some sort of consciously intended course of action); (2) a ploy (which is a specific maneuver intended to outperform a competitor); (3) a pattern (i.e., a stream of realized actions); (4) a position (i.e. a means of matching between an organization and its external environment); and

(5) a perspective (which is shared among organizational members, and the content of which consists of not just a position, but also an ingrained way of perceiving the world) (Mintzberg, 1987, In Chen, et al., 2010)."

1.3.3 Information Systems Strategy

A majority of the literature defines information systems strategy as an outgrowth of business strategy, in how to calculate the output of information systems in order to maximize profits (Chen, et al., 2010). King (1978) states management information systems should contribute by increasing earnings, reducing resources, and increasing reputation. Supporting this, Mata, Fuerst, and Barney (1995) stated information technology is one of the sources for sustaining competitive advantage by reducing costs and or increasing revenue. Johnson and Lederer (2010) built upon the previous by saying the information system's contribution has a fivefold strategic contribution: customer satisfaction, sales revenue, market share, return on investment, and operating efficiency. In all, information systems strategy supports the organization's strategy to increase the output of the organization and streamlining output through information systems (Chen, et al., 2010).

1.3.4 Information Systems Security

Traditionally, ***information systems security*** is perceived to mainly secure the technical and operational aspects of an information system, to protect the data (Anderson, 2003; de Paula, Ding, Dourish, Nies, Pillet, Redmiles, Ren, Rode, & Filho, 2005; Dutta & McCrohan, 2002; Kim, 2004; Ruighaver, 2008; Vijayan, 2005; Zhang & Bao; 2010). There is however, a lack of an acceptable definition across the industry for an information security strategy which hampers the acceptance of a common definition (Alter, 2008; Anderson, 2003). Strategy as presented by White & Bruton (2011), states, "Strategy is a coordinated set of actions that fulfill a firm's objectives, purposes, and goals." Which leads into an observation by Baskerville and Dhillon

(2008), that the term strategy is used very loosely in the literature, even though strategy is quite complex.

The complexity can be seen in how Mintzberg (1987b) examined five views of managing strategy as a plan, ploy, pattern, positioning, and a perspective. To which Baskerville and Dhillon (2008) expand upon the definition, into ten different methods for managing strategy through the schools of *prescriptive* areas of designing and planning, and *descriptive* areas of entrepreneurial, cognitive, learning, power, culture, environmental, and configuration. Individually, they are all aspects of strategy, but together, even though they differ, they give a more holistic view of strategy and its aspects (Baskerville & Dhillon, 2008). The word chosen by Baskerville and Dhillon (2008) is conflated, to describe the meshing, but no specific term or combination of terms that embodies all of 'strategy', rather it is a mixture and the resulting selection that gave meaning to the term strategy.

1.3.5 Information Security Strategy

Information security strategy fits within an organizational structure as the vision of the security of information, providing direction for policy, contributing to governance and governance balancing control through compliance in a synergistic relationship of information security management (Klaić, 2010; Posthumus & von Solms, 2004). The methods chosen for implementation of an information security strategy consisted of choices, the choice of the alignment and the role to execute the information security strategy to contribute to "an overall plan for managing and developing an organization's information security," (Baskerville & Dhillon, 2008). This then is the chosen definition of an information security strategy.

This research included articles which stated information security strategy should be aligned with business strategy, (Caralli, 2004; Dhillon, 1995; Newkirk, Lederer, & Johnson,

2008). The literature defines several broad concepts for aligning business strategy with information systems strategy (Chan & Huff, 1992; Chen, et al., 2010), but not many studies discuss the alignment of information security strategy (Hall, Sarkoni, & Mazzuchi, 2011; McFadzean, et al., 2011).

To reiterate, the industry looks at information security as an afterthought applied to obtain accreditation or answer problems when a compromise takes place. Information security ends up as a reactive response rather than a proactive implementation to mitigate problems before the problem can cause a compromise (Hedström, Kolkowska, Karlsson, & Allen, 2011; Hu, Hart, & Cooke, 2007; Scully, 2011).

Having defined the terms forming the common core of strategy, the following sections delineate coverage of the information security strategy. Chapter 2 covered the treatment of the literature around the alignments and strategic roles of an information security strategy. Chapter 3 introduced the research method chosen to interact with, observe, capture, and analyze the actions of information security professionals in choosing roles. Chapter 3 discussed data collection and the results of the data collection. Chapter 4 analyzes the data to yield a theory of information security strategy in large government organizations. The conclusion, in Chapter 5 delineates the contribution to the field of knowledge in information security, and recommends future areas of research.

Chapter 2

Review of the Literature

2.1 Introduction

The literature covered a broad swath of information security, since the field of information security is relatively young and still forming (Anderson, 2003; Kritzinger & Smith, 2008). This research included articles from a spectrum of information security (governance, policy, management, and compliance) containing sections and items of interest having a direct bearing on strategy (Klaić, 2010; Kritzinger & Smith, 2008; Ohki, Harada, Kawaguchi, Shiozaki, & Kagaua, 2009; Siponen, 2005b).

2.2 Review of the Literature

In many journal articles, the subject of information security strategy was broached, but not directly addressed as such. Authors may not have concerned themselves directly with a discussion of strategy, but did inject references as to vision and contribution to an overall plan of management and development of information security (Bhalla, 2003; Damianides, 2005; Doherty & Fulford, 2005; Doherty & Fulford, 2006). The researcher identified direct and indirect references to information security strategy and categorized them into terms captured in Table 1, Definition Sources.

Forming the information security strategy embodied the outlook of the leader and the organization, which was their vision (Salmela & Spil, 2002). The information security strategy was the outcome of taking the vision's goals, objectives and priorities and matching them to the organizational strategy (Moen & Norman, 2000; Salmela & Spil, 2002). Subsequent steps in the information security strategy development process included consideration of strategic, tactical,

and operational goals of the organization (da Veiga & Eloff, 2007; Grobler & Louwrens, 2005).

Table 1, Definition Sources identifies the multiple terms used and ways in which contributions

Table 1. *Definition Sources*

Term used	Explanation	Source
Cybersecurity -Architecture -Managerial -Security policy	Security was part of the overall strategy	Knapp & Boulton, 2006; McFadzean, Ezingeard, & Birchall, 2007
Cybersecurity Strategy	Advantages and disadvantages revealed in strategies as proactive and reactive	Rowe & Gallaher 2006
	"Protect digital assets" of people and organizations	Ghernouti-Hélie, 2010
Enterprise Strategic Security	Measured at every level, associated with risk acceptance	Anderson & Choobineh, 2008
Information Assurance Strategy	Aligning with corporate strategy to provide best security and availability of information assets	Ezingeard, McFadzean, & Birchall, 2005
Information Security	Security strategy as a part of governance, a driver of the organization	Grobler & Louwrens, 2005
Management Strategy	Used management to implement a strategic approach to security	Doherty & Fulford, 2005
	Information security management strategy and how it aligned with business	Ma, Johnson, & Pearson, 2008
Inductive Strategy	Used to understand individual and organizational levels	Albrechtsen & Hovden, 2009
Information Security Planning	Though not defined, a strategy of risk planning prevailed	Straub & Welke, 1998
Information Security Strategy (with propositions)	Part of security governance along with responsibilities long and short term; A part of the overall program	Da Veiga & Eloff, 2007; Shoraka 2011
	Approaches to answering risks and costs	Daneva, 2006
	Strategically aligned with business; Information Security Strategy aligns with business strategy; Aligns with business strategy to combine business objectives and competitive advantages; Embodied the plan to align with corporate strategy; Was a key enabler of corporate strategy	Amaio, 2009; Chang & Ho, 2006; Dynes, Kolbe, & Schierholz, 2007; Hall, Sarkani, & Mazzuchi, 2011; Kayworth & Whitten, 2010; van Niekerk & von Solms, 2010
	Pro-active to identify and adopt strategy	Arce & Levy, 2009
	Leads to competitive advantage	Vasiu, Mackay, & Warren, (2003)
	Factors for contextual background, common threats, and addresses barriers	Lomprey, 2008
	Information Security Strategy supported strong protection of patient records	Love, 2011
	Directors used risk assessment to draft the information security strategy	McFadzean, et al., 2007
	Information Security Strategy as a technical remediation response	Park & Ruighaver, 2008
	Information security strategy as a part of the governance structure	Posthumus & von Solms, 2004
	Information Security Strategy along with capabilities yields organizational performance	Hall, Sarkani, & Mazzuchi, 2010
Information Systems Security Strategy	Strategy inferred as a part of managing and not a technical solution for implementation	Dhillon & Torkzadeh, 2006
	Well-developed strategies result from balanced strategies in business, information systems and information system security strategies	Chang & Yeh, 2006
	Alignment of business with security strategy and also discusses in great detail about strategic integration to support business strategy	McFadzean, et al., 2011
IT Security Strategy	Evaluation of risk resulted in IT security strategy	Goluch, et. al., 2008
	Technical focus on devices and lock-down of systems	Doughty, 2003
Intrusion Strategy	Compared nature to the methods of strategy	Oreku & Mtenzi, 2009
Defense in Depth Strategy		
IT Information Strategy	Security approached strategically	Von Solms, 2006
IT Security Strategy	IT Security Strategy as a part of risk analysis	Von Solms, 1998a
(Law Enforcement) Strategy	Design strategy from the beginning, then built in afterwards	Anderson & Moore, 2006
Security initiatives	Aligned strategy with business strategy	Booker, 2006
Security Strategy	Formulation of security strategy involved people and processes	Zhang & Bao, 2010
	Compared cost and benefits weighing risks	Geer, 2007
	Methods for instituting strategy through committees for implementation	Smith, 2004
Strategy	Integrated part of the overall strategy	Ahuja, 2009
	Defined as formulating according to the scenarios encountered	Abbas & Hemani, 2010
	Proactive protection needed strategy to be proactive	Bhalla, 2003
Strategic Change	Strategic change enables business goals as new requirements or capabilities emerge	Werlinger, Hawkey, & Beznosov, 2009

were made to an information security strategy. The following captures how these definition sources aligned with information security and the information security strategy. These usually mapped to long range for strategic, mid-range for tactical and short range for operational goals. The information security strategy was divided into three sections allowing personnel to track short, mid, and long range periods of time (King, 1978; Mintzberg & Waters, 1985; Wommack, 1979). Benchmarks or milestones helped to indicate markers for effective performance in security (Allen, 2005; Eloff & von Solms, 2000; McFadzean, et al., 2011; Ohki, et al., 2009). If the information security strategy underperformed, it frequently manifested problems at the tactical and operational levels within an organization (da Veiga & Eloff, 2007). Problems could occur even before an information security strategy was ever implemented in an organization (Scully, 2011). An indication of this might be writing, approving, and then filing away of the information security strategy before anyone ever acted upon it (Rose, 2011). In which case, people or personnel duly responsible for accomplishment of the ideals of the information security strategy may never have known about the strategy. Practical pressures to meet operational or tactical requirements intervened and in such cases, the strategy was put away until time was available to complete the goals of even the operational level (da Veiga & Eloff, 2007; Grobler & Louwrens, 2005). The factors involved with these events are complex and diverse.

Information security has worked to correctly identify, analyze, and correlate organizational factors to improve information security strategy formulation, development, and implementation (Chang & Ho, 2006; Hu, Hart, & Cooke, 2007; Kankanhalli, et al., 2003; Parakkattu, et al., 2010). Through this process, the information security strategy advanced from merely being technical solutions to secure entry and exit points of a network (Ghernouti-Helie, 2010; Hinde, 2003; Seeholzer, 2012; Zhang & Bao, 2010) to become fully developed plans of

action (Aivazian, 1998; Bower & Gilbert, 2007). The information security strategy has even progressed above the stage of composing and implementing many information security management products, such as: policies, checklists, guidebooks, creating multiple governance structures, and identifying many success and effectiveness frameworks (Dunkerley & Tejay, 2009; Eloff & von Solms, 2000; Goluch, Ekelhart, Fenz, Jakoubi, Tjoa, & Mück, 2008, Siponen, 2005b; Zhang, Wuwang, Li, & Zhang, 2010).

What remained in question was why an information security strategy still did not function properly within the structure of policy and governance in the hierarchy of information security management within an organization (Cecere, 2011; Dawson, Berrell, Rahim, & Brewster, 2010; Dhillon, 2007; Kotulic & Clark, 2004; McFadzean, et al., 2007; Wang, 2009, Wood 2000). This study collected data about interactions of information security professionals and the roles chosen to implement information security and analyzed the data to result in a theory.

In some organizations, security was performed at minimum levels, in order to gain initial approval to connect to or operate the network (Anderson & Moore, 2006; Wang, 2009). Afterwards, the organizations relegated security to the level of necessity in order to maintain approval for operational use. Organizations then became complacent about continued use (Dougherty & Fulford, 2005). Evident of this was the fact that organizations conducted many meetings about implementing strategy, but ended up putting off difficult decisions (Wommack, 1979). Organizations implemented a form of security, such as technical security controls to deal with known threats (Damianides, 2005; Gilbert, 2008; Smedinghoff, 2005), but often choose not to employ management of information security to look for the unknown threat, before or as it developed (Anderson, 1993; Butler & Gray, 2006; Dhillon, 1995). Rather, organizations only implemented regulatory requirements, mandated by law. A prevailing presumption was that

security only slowed down the speed of processing on computer systems (Post & Kagan, 2007; Scully, 2011).

Some of the factors used to explain this strategic approach concerned a management approach wherein they were aware of security threats, but refused to believe bad events would happen to them (Knapp & Boulton, 2006; Scully, 2011). In spite of the security threats, management became self-assured, believing they were invincible and data loss would not happen to them (Scully, 2011; Straub, 1990). Possibly, the largest initial hindrance came from program managers, who were charged to keep their programs on time, under budget, and over utilized constrained resources, which invariably ended up as a detriment of security, which eventually removed or limited security from the budget (Hinde, 2000; Kark, 2010; Wang, 2009).

Ideally, the information security strategy developed by organizations evolved from interaction with multiple information security professionals. Their experiences in executing duties were applied to fulfill their portion of the business strategy, information systems strategy, and the information security strategy (Anderson & Choobineh, 2008; Hall, Sarkoni, & Mazzuchi, 2011; Knapp & Boulton, 2006; Parakkattu & Kunnathur, 2010). A method such as compliance, used security controls alone, in order to achieve a minimum level of security. Compliance dominated the Federal sector of organizations (Dhillon, 1995; Herath & Rao, 2009; Ma, Johnston, & Pearson, 2008; Ma, Schmidt, Pearson, 2009; Siponen, 2006). Compliance was undertaken, to meet legal mandates such as the Federal Information Security Management Act (FISMA) and the Health Information Portability and Accountability Act (HIPAA), as the regulating documents of information security (Damianides, 2005). Other organizations used compliance methods such as those for financial organizations using the Graham Leach Bliley Act (GLBA) and or industry regulation under the Payment Card Industry Data Security

Standards (PCI-DSS) for protection of personal financial information (Al-Hamdini, 2009; Damianides, 2005; Gilbert, 2008; Smedinghoff, 2005). Still other methods that information security professionals utilized in information security strategy formulation resulted from the reorganization of the information security structure or the hierarchy of the information security functions within their organization. Reorganization is done to meet new business and or information systems goals set forth from management or to address shortfalls identified and addressed through moving or restructuring of the organization (Avgerou & McGrath, 2007; Cecere, 2008; Hansen, et al., 2011; Kajava & Siponnen, 1996; Kotulic & Clark, 2004).

Compliance and reorganization formed partial responses to the problem investigated, but the study looked at the properties of the concepts of strategy (Smith & Medin, 1981). It focused on the linkages between the alignments of strategic roles under an information security strategy (Chen, et al., 2010; Corbin & Strauss, 2008; Ezingeard, et al., 2005; Leidner, Lo, & Preston, 2011; McFadzean, et al., 2007; Smith & Medin, 1981). The links between the strategies and each of the strategic roles were very complex and intricate (Leidner, et al., 2011). The discussion started with an explanation of the properties of the strategic concepts and their alignments (Chen, et al., 2010; Corbin & Strauss, 2008). As an overview, the alignment of the information security strategy used within the structure of an organization addressed the security of the business strategy and its automation through information systems. The alignment an organization should take was to aim towards a secure, information exchanging environment (Howard & Longstaff, 1998; McFadzean, et al., 2011). The alignment of an information security strategy provided the projected goals, objectives, and priorities the organization needs to attain for a secure, information exchanging environment (Bruton & White, 2011; Doherty & Fulford, 2006; Newkirk, et al., 2008).

There were many studies existing in business strategy and information systems to analyze the alignment of goals to mission and vision in their strategies (Chan & Reich, 2007; Earl, 1993; Johnson & Lederer, 2010; Mata, et al., 1995; Posthumus & von Solms, 2004; Preston & Karahanna, 2009; Salmela & Spil, 2002; Stanton, Guzman, Stam, & Caldera, 2003; Westerman, 2009). However, not many discuss the alignment of information security strategy to either information systems or business level strategies (Leidner, et al., 2011; McFadzean, et al, 2007; Newkirk, et al., 2008; Tejay, 2008). Discussion in the following section covers the areas of alignment unique to the information security strategy for the concepts of strategy.

2.3 Current Alignments for an Information Security Strategy

This section discusses the aligning of the information security strategy to explain the ways in which strategy was performed. There is school of thought that there are many different fashions in which to execute strategy. A total of four, possibly five methods existed for aligning information security strategy. The primary strategy is the business strategy, without which the organization would cease to exist. Also, an organization could not exist with only an information systems or information security strategy alone. Therefore, an information security strategy without a business strategy would result in failure of the organization.

The other four methods of aligning strategy focused in on information security strategy, which were: working with the business strategy in alignment of the information security strategy to the business strategy, alignment of the business strategy to the information systems strategy, alignment of the information security strategy to both the business and information systems strategies, allowing the information security strategy to operate on its own, and when the information security strategy was non-existent, operations does not consciously use any

information security strategy to perform its mission. Refer to Table 2, Alignments with Information Security Strategy for a description of the alignments.

Table 2. *Alignments with Information Security Strategy*

Information Security Strategy	Primary view of strategy, applying Mintzberg (1987b) 5-P's	Assumptions related to the information security strategy development process			Assumptions related to information security strategy's impact and desired impact of information security strategy	Assumptions related to information security strategy/Business strategic alignment
		Starting point when developing information security strategy	Standpoint taken when developing information security strategy	Relationship between IS and Business strategy		
Align to business	Plan, supported the organization directly	Used business Strategy as guide	Business-Centric	Information security strategy developed along with Business	Ensured meeting goals in line with business strategy	Met the strategy
Align to Information Systems	Position, found the niche within Information Systems	Used Information Systems Strategy as guide	Information Systems Centric	Information Security Strategy develops from both	Ensured meeting goals in line with Information Systems Strategy	Assisted the strategy through information systems
Align to Information Systems and Business	Plan & Position, supported & found the niche	Used both Business & Information Systems Strategies	Business & Information Systems Centric	Information Security Strategy developed from both Business & Information Systems Strategy	Ensured meeting goals in line with Business & Information Systems Strategies	Met/Assisted the strategy through information systems
Operated on its own	Perspective, focused on strict role of law	Used law & regulation as guide	Business & Organization Centric	Information Security Strategy developed in isolation, met Information Security Requirements	Identified asset requirement and ensured awareness	Informed the strategy of requirements
Was non-existent	Ploy, as it changed according to the flow	Used information Security Professional attitude towards strategy	Organization Centric	Information Security Strategy was not really developed, it may result as an after action or gap analysis	Provided an understanding of security and follows ISP guidance	Met the Information Security Professionals requirements for strategy

Each type of strategy set a vision, defined the mission and asserted the activities necessary for the implementation of strategy (Anderson & Choobinah, 2008; Cohen & Cyert, 1973; Kankankalli, et al., 2003; Kotulic & Clark, 2004; Mintzberg & Waters, 1987). A majority of literature identified the need for alignment, but most of the focus was on information systems alignment to business strategy. Very little literature existed to cover information security strategy aligning to either business or information systems (Newkirk, et al., 2008; Rudd, Greenley, Beatson, & Lings, 2008; Thompson & James, 2001).

The information security strategy supported information systems and the business strategy to secure the information of the business (Alter, 2008; Chen, et al., 2010; Stanton, et al., 2003). Protecting information and information systems at all levels becomes complex and diverse (Leidner, et al., 2011). Part of the process of meshing information and information systems together was identified within the difficulties of aligning strategies (Doherty & Fulford, 2006; Segars & Grover, 1998). An area, researchers have studied was the integration of information security strategy to business strategy (Newkirk, et al., 2008; Tejay 2008) and the information security strategy to information systems (Dutta & McCrohan, 2002; Straub & Welke, 1998).

One of the alignments of the information systems strategy was that of information systems strategy aligning completely with the business strategy through automation of data process, input, storage, and output (Chen, et al., 2010; Stanton, et al., 2003). Another information security strategy was discussed as that of aligning to the business strategy by transparently passing through the information systems strategy. This information system alignment was concerned only with automating the business strategy (Chen, et al., 2010). A further case was one in which the information security strategy supported only one of the

strategies, such as the business or information systems strategies, this aligned only with that specific strategy, ignoring the other strategy (Caralli, 2004; Hall, et al., 2010; McFadzean, et al., 2011). The last type of strategy, called a non-existent strategy, had the information security program operating entirely on its own with no form or distinct process. However in reality, the aspect of no strategy would quickly evolve into adopting the business strategy, since information security operates within an organization and its existing structure.

Table 2, Alignments with Information Security Strategy, summarized the five alignment concepts of strategy and how they relate to definition, the assumption of information security strategy development, the impact of the desired information security strategy assumption, and the outcomes when assessed with the overall business strategy. The following sections briefly detail the concepts of alignment through strategy types.

2.3.1 Align to Business Strategy

Aligns to business strategy has the information security strategy aligned to the business strategy (Caralli, 2004). This identified the first concept of how alignment of the strategy was performed within an organization (Siponen, 2005b; Westerman, 2009). The information security strategy was written to follow or augment the requirements of the business strategy (Cerpa & Verner, 1999; Hall, et al., 2010; McFadzean, et al., 2007; McFadzean, et al., 2011; Parkin & van Moorsel, 2009). Communicating information security in business terms, while maintaining the security of the organization helped align the two strategies (von Solms & von Solms , 2004; von Solms & von Solms, 2005). The challenge was in explaining the information security strategy in understandable language for the business executive to comprehend information security (Lindström & Hägerfors, 2009). The information security strategy followed and worked with the overall goals of the organization; drawing from the requirements set forth from the

organization's leadership (Hall, et al., 2010; Kayworth & Whitten, 2010). Alignment to the business strategy also resulted in ensuring the accomplishments of the same, by meeting the goals of the strategy (Amaio, 2009; Lomprey, 2008).

2.3.2 Align to Information Systems Strategy

The information security strategy used the information systems strategy as a guide. As an overall objective, the information security strategy was developed in tandem with and aligned to the information systems strategy. While the information systems strategy was often information systems centric, the information security strategy attempted to ensure the secure attainment of goals of the information systems strategy. The goals of information systems helped to ensure information tools were readily available, but sometimes may not align with business needs, thus not providing the organization with optimum value (Alter, 2008: Chen, et al., 2010; Stanton, et al., 2003).

2.3.3 Aligns to Information Systems and Business Strategies

Information security strategy as the shared view of the information security program goals in an organization aligned with both the information systems and business strategies. Operating in the most proficient manner, to identify business opportunities and align them, along with the most opportune automation techniques providing increased productivity and savings in equipment costs by optimizing efficiencies between the information systems strategy and the business strategy (Baptista, Newell, & Currie, 2010; Leidner, et al., 2011; Straub & Welke, 1998).

2.3.4 Information Security Strategy Operates on its Own

Alignment four covered the domain in which the information security strategy developed almost in a vacuum and did not consider the business or information system strategies for

development (Badr, Biennier, & Tata, 2010). For its focus, development occurred within its own realm and might depend upon consideration of only federal law and regulation to specify what the goals and objectives would be, regardless of the constraints of business and information system requirements. Rather the information security strategy tended to be authoritative in dictating what the requirements for compliance would be from the information system and business strategy viewpoint (Eloff & von Solms, 2000; von Solms & von Solms, 2004).

2.3.5 Information Security Strategy is Non-Existent

Alignment five considered the lack of any organized strategy from the external sources of business or information systems (Pfeffer, 1992). The information security strategy existed in the form of interactions through an information security executive working on a day to day basis (Mintzberg, 1987b; Mintzberg & Waters, 1985; Porter, 1996; Reich & Benbasat, 2000) without any structured method in place. The executive provided direction, but without formalizing the information security strategy in writing or other channels of communication to subordinates or peers. Strategy resulted from periodic changes in direction of the senior executive on a continual basis. Allen (2005) and Leidner, Lo, and Preston (2011) assert that security cannot be missing, it must be represented.

2.3.6 Summary of the Alignments

Table 2, Alignments with Information Security Strategy, summarized and listed the characteristics of all the alignments, listed as concepts, showing where they intersected as distinct types of strategies. The author adapted the style of the table from the work by Chen, Mocker, Preston, & Teubner (2010) into an information security strategy related structure. The discussion of the alignments presented covered the most probable ways in which an information security strategy could be developed; considering strategies which used business, information

systems or both types of strategy to accomplish a mutual set of goals. In addition, another alignment consisted of preparing a strategy running on its own to serve internal needs, but failed to encompass overall organizational goals. If in the case of a new organization, not having a strategy might comprise the only situation where it was advisable to have no strategy; but, having none usually resulted in a very short sighted execution of duties and resulted in much re-work and duplication of effort (Baskerville & Dhillon, 2007). The next section consists of discussing the external influences upon the information security strategy, through the roles an information security professional could exert over the information security strategy.

2.4 Proposing Role Recognition for an Information Security Strategy

Previous studies in information systems (Chen, et al., 2010) recognized three roles of strategy performance (Information Systems Innovator, Information Systems Conservative, and Information Systems Undefined), but opted not to explore other variables of roles in which to perform the strategies. Leidner, Lo, and Preston (2011), built upon the original article by including an additional role. They have suggested the addition of Information Systems Ambidextrous (Leidner, et al., 2011), which attempted to capture additional variance of the three roles. The necessary next step was to build upon the previous two studies by adding a workable theory to test. To that end, a grounded theory approach might grant the emergence of a theory to test (Pandit, 1996). In both works, the authors opted to keep the study in the theoretical realm without conducting actual research into the validity of their propositions (Chen, et al., 2010; Leidner, et al., 2011). Rather, they presented propositions that could lead to an intellectual basis for discussion of information systems strategy to contribute to the field of information systems. Since the actual study did not gather rigorous evidence, this study gained extensive data from information security professionals and used a rigorous analysis reaching saturation under

theoretical sampling (Corbin & Strauss, 2008; Creswell, 2011; Devadas, Silong, & Ismail, 2011). This study used the existing study (Chen, et al., 2010) to spur the validity of information security strategy in qualified strategic role selection by information security professionals.

Studies identified the formal and informal interactions between business executives and information systems executives and that those interactions had an impact on how information systems implementation occurred (Pyburn, 1983; Johnson, 2009). Often the interactions were rare, occurring sporadically during appraisals or when meeting to discuss strategy formation (Johnson, 2009). Since the interactions were infrequent and that information systems were viewed as coming into alignment with business goals, the qualified strategic roles proposed by business might not always be coordinated with information systems. It was assumed information systems follow business blindly (Pyburn, 1983). However, interactions do need to be coordinated and communicated to yield an effective strategy.

With the definition of an information security strategy established as the implementation of an information security strategy, it consisted of choices contributing to "an overall plan for managing and developing an organization's information security," (Baskerville & Dhillon, 2007). Baskerville & Dhillon (2008) recognized a good information security strategy drove information security policies that information security management used to implement information security processes and practices. They asserted that an integrated strategy for information security management was necessary to achieve organizational objectives. Participants in securing information must clearly define their roles and responsibilities to achieve objectives.

The implementation roles utilized by information security professionals varied by just as many backgrounds as the individuals who implemented the information security strategy

(Ashenden, 2012; von Solms, 2001). The intricate interplay of an information security professional with business and information security executives is puzzling (Johnson, 2009). Part of the puzzle was having information security management weigh their appropriate human interactions (Ashenden, 2012), the preferences of the leader and selection of the category to envelop their performance of the information security strategy under the information security program. As a part of this equation, the qualified strategic roles information security professionals chose from consisted of a set of broad categories identified in Table 3, Qualified Strategic Roles of Information Security. These broad categories of qualified strategic roles for implementing the information security strategy are identified as top down, public image, competitor, continual change, best practices, re-organization, power relationships, and compliance. In Table 3, a summation of the major roles information security professionals' exhibit for implementing information security strategies are listed and briefly covered. The following paragraphs give a more detailed review of the eight identified qualified strategic roles.

2.4.1 Top down

The positioning school of thought looks at strategy performance as a reasoned top down approach, where executives moved and shifted strategy performance to take advantage of positions as the leader sees the direction change (Slaughter, Levine, Ramesh, & Pries-Heje, 2006). The top down role managed from top to bottom, the executives became involved with decisions and captured their vision in the strategy and policy, governing the actions of all personnel within an organization (Baskerville & Dhillon, 2008; Clark & Sitko, 2008; Dawson, et al., 2010; Kajava & Siponen, 1996; Lederer & Mendelow, 1988; Salmela & Spil, 2002). The authority for decisions resided with the upper echelon and they directed the actions of all. In this manner a select few made decisions for the greater good and it tied directly back to operations of

Table 3. *Qualified Strategic Roles of Information Security*

Qualified Strategic Role	Definition	Information Systems Source	Information Security Source
Top Down	The strategy as a shell and have the insides declared by outlining the goals, adding objectives and priorities over time, allowing the strategy to develop inside of defined boundaries.		Clark & Sitko, 2008; Jones, 2001; Kajava & Siponen, 1996
Public Image	Public image, the image was to contend for the public's opinion as a means by which security was not necessarily observed, but perceived as implemented. Security became an external façade, willing to pay fines than ensure security.		Anderson & Moore, 2006; Knapp & Boulton, 2006
Competitor	The competitor or benchmark worked to achieve the best condition. Competition could be like an arms race to devise strategies to outwit opponents. Innovation or countermeasures produced to outperform each other resulting in competition amongst the players.	Howard & Kilmartin, 2006; Lacity & Hirscheim, 1995	Damianides, 2005; Ohki, et.al., 2006
Continual Change	Strategy adapted to continuous and unpredictable change. Information Security adjusted as threat actor intentions and malware deployments changed. Strategy moved from a once a year or longer cyclical repetition into an almost daily operational change environment.	Bechtold, 1997; Fairholm, & Card, 2009; Huebler, Foster, & Phelps, 2007; Lacey, 2009; Levy, 1994; Valle, 2000; Yarger, 2006	Collins, 2001
Best Practice	The best business practices (BBP) attempted to institutionalize and accept best practices across the organization. Use of methods such as an information security capability maturity model, to find best practices.	Keen & El Sawy, 2010; Luftman & Kempaiah, 2008; von Solms, 2006	Kark, Penn, & Dill, 2009; Kark, 2010; Kayworth & Whitten, 2010; Luftman & Ben-Zvi, 2010; Luftman & Ben-Zvi, 2011; McClean & Kark, 2010
Re-organization	Used the excuse for organizational change as an argument, that since security had deficiencies in the past, management required a change in the structure of the organization; hoping to stave off negative reactions, the organization re-organized. This used the ISS to encourage organizational change.		Aivazian, 1998; Norman & Yasin, 2010; Zhang, et. al., 2010
Power Relationship	Power exerted through the strategy, establishing organizational direction. Individuals used strategy to exercise will and or drive conformance by employees. Power was wielded in two ways, effectively to advance organizational goals and to coerce individuals and organizations to achieve a short term objective, but usually resulted in security being ineffective over time.	Dhillon, 2004; Dhillon, Caldeira, & Wenger, 2011; Herath & Rao, 2009; Minztberg, 1985;	Lapke, 2008
Compliance	Compliance used federal laws to center the information security strategy around. Compliance was very procedurally oriented. People were not heavily involved with the process, except to perform procedures, within the process.		Damianides, 2005; De Paula, et al., 2005; Gilbert, 2008; Hedström, Kolkowska, Karlsson, & Allen, 2011; Hu, Hart, & Cooke, 2007; McFadzean, et al., 2011; Siponen, 2005b; Siponen, 2006; Smedinghoff, 2005; von Solms, 1998a; von Solms, 1998b;

the organization and conformed to regulatory guidance. Personnel often perceived this as an umbrella form of strategy (Mintzberg & Waters, 1987). The overall direction was established by management, the details were worked out as goals and objectives, added over time and as

management revealed direction to fan out amongst the ribs of the umbrella (Jones, 2001; Mintzberg & Waters, 1987).

2.4.2 Public Image

There was a perception that information security was required to protect users and assets from various threats in the Internet directed towards the users (Huang, Rau & Salvendy, 2010). The public image sought to display an image to the public of the organization as a secure environment for information security. This was another role of an information security professional to implement an information security strategy. The image contended for the public's opinion as a means by which security was not necessarily observed, but perceived to be implemented, to the extent necessary to make an observer believe the organization was secure and trusted (Knapp & Boulton, 2006). Mintzberg and McHugh (1985) asserted that organizational strategy focused on form, but not substance. Part of the public image role was projecting the stability of security, ensuring the customer and the organization as a whole has confidence in the security of information entrusted to them (Johnson, 2009). Security became an external façade, superficial in nature, which projected the image of security protecting the public from actual security breaches (Baskerville, 1993). The organization asserted the existence of security, yet when they suffered loss, the organization opted to just pay the fines assessed, rather than invest sufficient funds to implement proper security measures. The cost of the fine was lower than the cost of proper implementation of security controls (Anderson & Moore, 2006).

2.4.3 Competitor

The competitor role consisted of benchmarking or competition resulted in striving for top position amongst organizations trying to achieve best condition. Each unit competed, trying to outperform the other in providing security (Vannoy & Salam, 2010). Remaining secure was

compared to an arms race to devise strategies that outwit opponents (Chang & Ho, 2006; Robson, 2005). Each competitor created innovation or countermeasures to the innovation produced by other competitors. Illustrative of this was the 'Red Queen' effect explained by Robson (2005) and was the result of competitors competing against one another. Strategy strove to maximize profits (Mintzberg, Ahlstrand, & Lampel, 1998; Vannoy & Salam, 2010). Information security strategy looked to devise goals to keep out malware (Chan & Reich, 2007: Chang & Ho, 2006; Mintzberg, Ahlstrand, Lampel, 1998; Tejay, 2008; Vannoy & Salam, 2010). By adapting the 'Red Queen' effect, security became the objective and industry benefits when all the parties attempt to eliminate all information security threats. Information security served to spur more profits with proper implementation as competition drives down costs and ends up preventing loss due to data breaches (Baskerville, 1993; Ohki, et al., 2009; Robson, 2005).

2.4.4 Continual Change.

One thought leader in the information systems technical and strategic areas predicted the rise of chaos or continual change as the new normal within information technology (Costello, 2011). Costello (2011), stated information technology leaders and by extension information security must prepare for rapid device, application, and services deployment. This continual change portended that the current un-predictableness of an organization's environment required continuous changes in strategy to adapt to ever changing needs (Siponen & Iivari, 2006). For business, information systems and information security strategy, they all needed to react to the changing requirements of customers, information system assets and information handling. Continual change became hard, especially when commensurate information security change is required (Slater, 2002) and as threat actor intentions and malware deployment changed rapidly (Choo, 2011). Strategy would need to move from a long cyclical period of time into a much

shorter operational change environment. The continual change theory of strategy involved nonlinear changes and accepting feedback that may cause program redirection, by either sudden changes (bifurcation points) or more gradual evolution (Bechtold, 1997).

Continual change worked along a continuum, ranging between deliberate and emergent strategy, but not at either of the extremes (Mintzberg & McHugh, 1985). One form of continual change was that of adhocracy, where an organization worked in an environment that was both complex and dynamic (Leidner, et al., 2011). The environment was always unique and changing (Leidner, et al., 2011; Mintzberg & McHugh, 1985). Uniqueness was delineated in five areas, first it was dynamic and complex with each output being unique. Second, different outputs caused a need for experts to be resident. Third, experts were housed in teams, to address issues as they arose. Fourth, mutual adjustment of strategy was coordinated through working groups and committees. Lastly, organizations were decentralized, and power was distributed to task accomplishment by experts within teams (Mintzberg & McHugh, 1985). Overall, the role of continual change was one of dynamic and complex changes occurring continually.

2.4.5 Best Practice

The best business practices (BBP) attempted to ensure BBP institutionalization and acceptance across the organization as a strategic role. The organization executed established policy to obtain the best results when addressing security issues (Dawson, et al., 2010). One of the methods information security personnel advanced was best practices in the form of a model or method to mitigate risk in a repeatable fashion (Shariati, Bahmani, & Shams, 2010). Rezakhani, Hajebi, and Mohammadi (2011) advanced standardization as a method of best practices. They sought standardization across the industry and cited instances of standard acceptance through programs such as Information Technology Infrastructure Library (ITIL),

Information Security Management System (ISMS), Information Security Maturity Management Model (ISM3), International Organization for Standardization (ISO) and International Engineering Consortium (IEC) (Rezakhani, Hajebi, & Mohammadi, 2011). Use of methods such as checklists, capability maturity models and other practices abound in best practices environments (Baskerville, 1993; Shariati, Bahmani, & Shams, 2010; von Solms & von Solms, 2005; Zuccato, 2007). The highest level of a capability maturity model demonstrated the pinnacle of the best practices model, corresponding to the fifth level of a capabilities maturity model (Ahuja, 2009; Kayworth & Whitten, 2010; Luftman & Ben-Zvi, 2010; Xiao-yan, Yu-qing, & Li-lei, 2011).

End user expectations of best practices could be summarized as protecting a customer's data confidentiality, ensuring accuracy of the data (Johnson, 2009). Implemented best practices could be used to increase trust between partners and meet requirements levied by partners (Johnson, 2009), in the case of the government, public trust. Costs must also be considered as there was a tradeoff between being really secure and insecurely achieving BBP, yet avoiding extravagant spending on security. Lastly, best practices met the overall strategic plan for business objectives by providing short and long range returns on investment (Johnson, 2009).

2.4.6 Re-Organization

With the use of the excuse for organizational change as an argument, the re-organizer operated under the premise that since security had been found deficient in the past, management required a change in the reporting structure of the organization; hoping to stave off negative reactions or placate audit findings, the organization re-organized (Cecere, 2011). Several areas are stated as complicit with failure, amongst them was the strategy (Rose, 2011). A major problem with using the information security strategy as a tool to drive organizational and

structural change (Aivazian, 1998) was that management might try to use the information security strategy as a vehicle to encourage organizational change (Aivazian, 1998; Kotulic & Clark, 2004). Some offices in an organization may justify that they did not have enough workers to meet inspection findings. A recommendation to re-assign people around the organization helped to re-distribute and theoretically improve the information security strategy performance. The organizational chart was the primary artifact used with the information security strategy to communicate the structure and mission of the information security strategy (Norman & Yasin, 2010).

A positive use of re-organization, could be seen in things such as resource availability and could be redistributed to ensure competent information security personnel, software and hardware, and adequate information security budget was disbursed to appropriate parts of the organization (Johnson, 2009). Another positive use might be that non-effective initial review by management required a change to re-direct assets towards the goal of secure information technology (Emery, 1991).

2.4.7 Power Relationships

Power could be exerted through the strategy, directing the way in which an organization moved forward (Backhouse, Hsu, & Silva, 2006). Individuals used the information security strategy to exercise will and or drive conformance by employees, as a way in which the information security strategy could be wielded as an instrument of power within the organization (Mintzberg, 1985; Salancik & Pfeffer, 1977). Wielding power to achieve information security goals was perceived to increase the stature of security overall. Using power to coerce individuals and organizations might achieve a short term objective, but usually resulted in security being ineffective over time (Backhouse, et al., 2006; Dhillon, 1995; Dhillon, 2004; Dhillon, Caldeira,

& Wenger, 2011). Power and accountability could impact the development and implementation of information security. The lack of an effective information security strategy, led to ineffective security policy, which resulted in ineffective information security (Lapke, 2008; Loveland & Lobel, 2012). Side effects from the use of power indicated that the use of power to negatively influence personnel did not have the desired effect of causing someone to behave correctly. Rather when positive reasoning was employed, users responded more positively (Herath & Rao, 2009).

2.4.8 Compliance

Compliance looked at using federal laws and regulations to center the entire information security strategy around. Compliance was very procedurally oriented (da Veiga & Eloff, 2007). People were not heavily involved with the process, except to perform procedures, and record results within the process (Hedström, et al., 2011). One article stated that as a result of data breaches, multiple acts and laws to ensure compliance were passed and enacted (Smedinghoff, 2005). Reactive implementation of controls is a precursor to complacency in that after the initial flurry of activity to comply, the organization went back to business as usual, with security not at the forefront (Damianides, 2005; Scully, 2011). Another article stated that technological controls were fine, as long as people were not involved with the process (Hedström, et al., 2011). If people, policies, and culture were involved the risk to security exists (Hu, Hart, & Cooke, 2007).

One of the positive aspects of compliance was that compliance helped to ensure risk management, through minimizing risk that could occur from a data breach. Ensuring accurate company data leads to informed management decisions (Hong, Chi, Chao, & Tang, 2003).

Compliance led to protection from external intruders, employee accidental or intentional damage, and to deter potential attacks (Johnson, 2009).

2.4.9 Summary of Roles

The literature consisted of information that led to the identification of eight possible categories of roles an information security professional could assume. This chapter captured and discussed the possible roles that could be taken from extant literature. Exploration of the role selection process and possible alignment inside an organization was part of a possible information security strategy development process (von Solms, 2001). The next chapter explored in detail the research method selected to rigorously collect data and analyze it to theorize over role selection in accomplishing the mission of the information security program.

Chapter 3

Research Method

3.1 Introduction

Of the different research methods available, quantitative, mixed methods, and qualitative, this study will use a qualitative method. The reasoning behind non selection of the quantitative method is the dearth of literature on information security strategy and measuring against known models. The reason to not choose mixed methods is the need to have measurable entities, but there are no established empirical norms for information security strategy. Selection of the qualitative method centers on the fact that information was scarce on the subject of information security strategy (Lapke, 2008; Loveland & Loebel, 2012). As such, the methods of research for utilizing models and theories are minimal. Grounded theory data collection allows for the analysis of data; using the interpretive techniques of interviews and artifact collection of data (Allan, 2003; Corbin & Strauss, 2008). Much data was collected and conceptually analyzed to understand organizational use of the role of information security strategy through a grounded theory approach by using theoretical sampling techniques (Glaser & Strauss, 1967; Javinen, 2000; Lee & Hubona, 2009; Pauleen, Corbitt, & Yoong, 2007; Ransbotham & Mitra, 2009; Yoong, 1996). Extensive collection, analysis, and comparison of the data ensured rigor (Lee & Hubona, 2009).

Grounded theory works inductively, by collection of artifacts and interviews, then working through stages of coding to develop an emergent theory (Pandit, 1996). The steps begin with interviews and transcription; coding of the interviews using open, axial, and selective coding techniques; and then developing the theory (Allan, 2003; Jones & Alony, 2011; Glaser, 2012b; LaRossa, 2005; McFadzean, et al., 2007). At each step capturing thought, procedure, and

process through memoing helped develop understanding and insights as the compilation of collected data occurred and analysis was conducted (Charmaz, 2006; Corbin & Strauss, 1990; Corbin & Strauss, 2008; Glaser & Strauss, 1967; Pauleen, Corbitt, & Yoong, 2007; Rich, 2012). Grounded theory is very useful in instances when the area under study, such as this, does not have considerable research being performed and the nature of the study involved human experience and interaction to obtain data (Corbin & Strauss, 2008; Yoong, 1996). The objective of the study investigated the connections between the information security strategy and the role(s) necessary to execute the information security program in order to meet organizational requirements for information security. It could also prove helpful to information security professionals if the outputs from this grounded theory methodology resulted in constructing a formal approach to information security strategy selection that goes beyond the implementation of technical controls. Additionally, it could be beneficial to forming a proactive approach to information security strategy, if a model could be predictive of role selection. The following sections: open coding, axial coding, and selective coding present more detail over the rigor practiced throughout the steps of the data collection process.

3.2 Research Method

The grounded theory methodology followed in this study allowed and encouraged probing for information in how an information security professional was influenced to select roles and make choices to perform their information security programs. The interview questioning and exploration for data granted insight into how construction of an information security strategy took place (Duffy, Ferguson, & Watson, 2004; Wimpenny & Gass, 2000). Further, the analysis of the data led to an understanding whether certain types of strategy were preferable over others and how strategies differed from one another as perceived by executive

level members in an organization from business, information system, and information security sections (Fitzgerald, 2010; Johnson, 2009). It also helped to ascertain how information security personnel differentiated between types of information security strategies. Chapter 2 presented a possible way in the process of selection of a role to perform information security strategy could be made. Chapter 4 covers the process of selection to reveal if there is an optimum role for a specific information security strategy. The aim of this study was to derive theory from analyzed, collected data (Corbin & Strauss, 2008; Siponen, 2005a; Vannoy & Salam, 2010), and present an emergent theory (Eisenhardt & Graebner, 2007; Glaser, 2012a; Goldkuhl & Cronholm, 2010; Pandit, 1996; Scott & Howell, 2008). The data was collected from the artifacts, interviews, observations, and documents, and then coded and analyzed into a theory which was used to verify the problem statement and research questions (Huehls, 2005; Lee & Hubona, 2009; Wimpenny & Gass, 2000). The emergent concepts from the coding steps were grouped into concepts and categories, and categories integrated to form a theory (Corbin & Strauss 2008; Huehls, 2005). A theory then depicted adaptable ways of theorizing how an information security professional selects a role (Fitzgerald, 2010; Siponen, 2005a).

As an initial foray into information security strategy using grounded theory, it was useful to discover a process for qualified strategic role selection by an organization, which would have a positive impact on organizational performance. The primary contribution was a theory allowing an organization to evaluate its needs, select, and then possibly implement an information security strategy. The first step in the process was gathering the data and the following section illustrates how data was collected.

3.3 Proposed Data Collection

The data collection process consisted of multiple steps or stages in grounded theory

methodology. Figure 1, Developing a Grounded Theory, highlights the steps required to arrive at a theory from the collected data. To start, the researcher conducted interviews with participants in the study. After the interviews were conducted, they were transcribed and reviewed by the researcher, to ensure complete information was captured and transferred to print medium (Duffy, et al., 2004; Wimpenny & Gass, 2000). During the process of transcription, the researcher recorded memos, capturing the researcher's impressions expressed by the participant, for use in the coding process (Charmaz, 2006; Corbin & Strauss, 2008; Stocker & Close, 2013). Cycling between the interview and transcription forms the data collection portion of interviews. Other sources for collection are the observations of the researcher in the environment wherein the participant operated (Backman & Kyngaes, 1999; LaRossa, 2005). The researcher collected document artifacts which ranged from strategy documents, standard operating procedures, and internal letters covering mission goals and objectives (Lee & Hubona, 2009), which complemented the data collected during the interviews with executives. The follow-on for the interview was taking the information and coding it into usable data for building a theory (Charmaz, 2006; Corbin & Strauss, 2008).

With grounded theory, there are very few guidelines to establish an optimum number of subjects for interviews (Eisenhardt, 1989; McFadzean, et al., 2007; McFadzean, et al., 2011). One source recommends a minimal sampling of fifteen to twenty subjects for grounded theory, where prior data is almost nonexistent (Corbin & Strauss, 2008; Creswell, 2011). Another source recommends to almost double the amount for the recommended minimums, of 20 to 30 subjects (Creswell, 2002). Charmaz (2006), advanced that the researcher should query their participants and add interviews until reaching saturation, which may be a small amount of

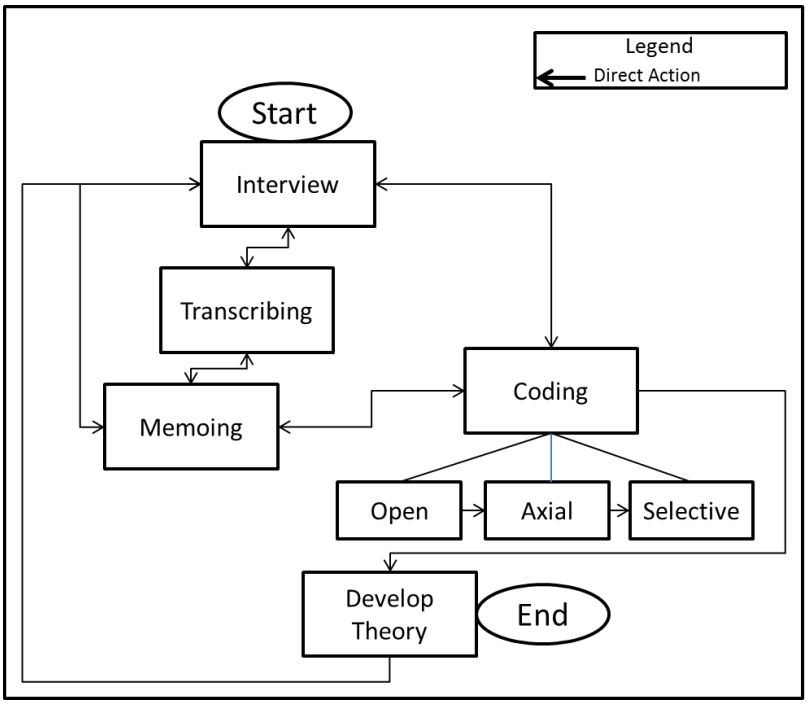

***Figure 1*. Developing a Grounded Theory**

individuals on up to approximately 30 different participants. Saturation occurs when, as a researcher, one collects and comparatively analyzes data and a point is reached when no new categories or areas are discovered from discussions with CISOs or gleaning data from documents. The estimation being that once saturation is reached, the need for more interviews no longer exists (Charmaz, 2006). The researcher for this study queried twenty five participants from one large government organization, and expanded this to several within the Federal government, interviewing seven other chief information security officers (CISOs) in order to reach saturation of the categories.

The researcher reached out to the organizations and queried executive level participants to take part in interviews, asked for copies of documents pertaining to their strategy and their mission goal accomplishments, and obtained permission to observe day to day operations for a time within their organization (Backman & Kyngaes, 1999; LaRossa, 2005). This study did not conflict with the researcher's professional duties and complete anonymity of position and

location was practiced with the organizations. Initial interviews with 13 CISOs and their deputies, for a total of 25 from the 13 sub units of the large organization comprised the main participants in the study. An additional seven CISOs and or deputies were approached from other large organizations in order to reach saturation (Charmaz, 2006; Corbin & Strauss, 2008). This involved four additional organizations to reach an adequate level of saturation (Charmaz, 2006).

The chief information security officers (CISOs) from the information security sub units were the primary interviewees for the grounded theory study. Johnson (2009) asserted that the best mix of data comes from executives of equal rank and from peer levels in the organization. This allowed for viewpoints from similar background levels on information security from CISOs in the overall organization, but also from differing sub units (Johnson, 2009). And, it granted the review of the roles they deemed necessary to meet organizational sub unit information security requirements. What one level of the organization deemed necessary does not always equate to what the other organizations deemed necessary (Chen, et al., 2010). Each organization had differing mission requirements. The interviews gained key enabler data from top level management insights "(b)y exploring what managers were thinking, why they acted as they did, and what they wanted to accomplish within the organizational context," (Vannoy & Salam, 2010) for the subject of strategy and strategic roles.

In order to gauge the length of time required at each site in the use of grounded theory, the researcher reviewed the number, location, and parts of the large governmental organization (Corbin & Strauss, 2008; Glaser, 2002). The main organization covered here was dubbed the 'Branch of the Fatherland' which consisted of 13 smaller subunits performing differing portions of the mission of the overall large organization. Of these 13 smaller sub units, a number of

CISOs and their deputies were selected and interviewed, observed, and documented. A brief, sanitized unit organizational mission statement, collected from each of the unit sources yielded information about its number, location(s) and composition (Pitt, Parent, Junglas, Chan, & Spyropoulou, 2011), except for one sub unit who did not want information captured. Refer to Table 4, Participant Sub Unit Characteristics, for a brief explanation of each sub unit.

The most complex portion of the data collection was the actual interview of participants. There are several types of interview styles to choose from such as semi-structured, structured, and open ended interviews (Allan, 2003; Duffy, et al., 2004; Wimpenny & Gass, 2000). The narrowness of the information required and the small area of the overall information security program recommended the semi-structured form of interviewing as the most effective (Charmaz, 2006, Corbin & Strauss, 2008; Duffy, et. al., 2004). The reason being that open ended interviews may end up gathering volumes of extraneous data, not pertinent to the study and structured interviews may tend to be overly biased (Duffy, et al., 2004; Wimpenny & Gass, 2000). Therefore, the use of semi-structured interviews was selected.

The researcher asked executive level personnel, in the information security field, from the sub units of a large government organization to take part. The participants agreed to answering questions and were assured of confidentiality and anonymity in their responses. In order to have consistent interviews with all the participants, the researcher agreed to and observed the ground rules for the interview utilizing an approved Institutional Review Board (IRB) consent form to give the participant a frame of reference and keep the interactions of the interview within a bounded area (Allan, 2003; Corbin & Strauss, 2008).

For each interview, the researcher wrote down notes from all the answers to the questions, jotting down details as they occurred. Outlines of the discussion provided the skeleton

Table 4. *Participant Sub Unit Characteristics*

Name*	Size (Information Security Personnel)	Mission Statement
AXXX	22	Watches over Fatherland's banking and payment systems to ensure integrity. Also protects national leaders, dignitaries, special locations, and Fatherland events.
UHJY	210	Helps the public by responding, recovering, and remediating from all hazards. Helps the Fatherland to be prepared for any emergencies.
FRT	0**	Watches over the Fatherland's transportation systems to make sure citizens and commerce can move freely.
UKO	135	Enforces Fatherland's civil and national laws for the border, customs, trade, and immigration.
ERF	171	Primarily keeps invaders and supplies for invader groups out from the Fatherland. Ensures trade conducted fairly and all bureaucratic rules are obeyed.
CFTY	240	Patrols the Fatherland's coastal edges against unlawful entry and assists people who may be in danger along the coast.
GHY	5	Independently validates subunits for optimum performance, by identifying areas of improvement and ways to attain compliance.
GHJK	14	Facilitates training for law enforcement to assist them with skills development for public safety.
ERFT	177	Ensures immigration procedures followed and teaches principles and benefits of Fatherland are communicated to all citizens.
WFRT	102	Helps to ensure risk resilience throughout Fatherland in government and industry, by an integrated method for both cyber and physical threats.
WER	39	Performs research and development for all levels of government used to find emerging technology to support and protect the Fatherland.
NKOP	181	Responsible for Fatherland's information technology systems and equipment, and the identification and tracking of performance measurements.
WDC	21	Responsible for protecting information and intelligence from being exploited.

*NOTE: Specific names and some aspects of their function changed to avoid disclosure.
**NOTE: At the time of collection, FRT deemed it essential not to reveal full complement of information security personnel figures.

of the interview notes and assisted the researcher in analyses made. Most executives enjoyed having their thoughts taken down and preserved in reports, documents, and in this instance for the interviews (Johnson, 2009). Ample time was set aside during the interview to allow the

participants to form their thought, considering their perceived factors with the information security strategy provided to them by management in the organization and to express their driving compassion for information security (Charmaz, 2006). Notes were transcribed as soon as possible after the interview was conducted (Duffy, et al., 2004; Wimpenny & Gass, 2000) via memoing. The researcher also wrote down an initial interpretation immediately afterwards (Stocker & Close, 2013). While every effort was made to collect exhaustive data during the initial session, the option was kept open to conduct multiple sessions with all the participants at a future point in time, if necessary (Charmaz, 2006; Corbin & Strauss, 2008).

Several direct and indirect questions were asked of the interviewees to lead discussion during the interview. In this way through open ended questions in a semi structured interview, it elicited information from the executives operating in the actual information security environment, as they supported the business, information systems, and information security missions (Allan, 2003; Charmaz, 2006; Corbin & Strauss, 2008; Duffy, et al., 2004). The researcher planned out the questions as probing, but not aimed at any pre-selection of roles, alignments, or construction of a strategy. The source for interview questions came from knowledge gained and based on the literature available and reviewed in Chapter 2. The questions focused on discovering how the interviewee developed their role within the organization where they were assigned. Also, the discussion sought to have the interviewee explore their reasoning for picking particular roles. Table 5, Interview Question Rationale, listed the questions used, the source for the question, and the rationale for their formation of a response during the interview. The nature of theoretical sampling allowed and encouraged participants to be free in their response and to follow no set path in revealing data about their understanding of the complexities of the formation of information security strategy in government organizations

and what the differing roles individuals used to perform information security applied to their unit in the organization (Corbin & Strauss, 2008). The researcher did ask clarifying questions to elicit further open ended responses from the participants. During the process of data collection, the researcher avoided reaching conclusions with participants (Corbin & Strauss, 1990; Corbin & Strauss, 2008). The epoche or the conscious decision centered on objectivity was to remove any preconceived notions during an interview (Allan, 2003; Kwok, McCallin, & Dickson, 2012). Keeping distance from the data sources helped to prevent developing a theory closely tied to the data that might otherwise look more like a quantitative observation with empirical data (Corbin & Strauss, 2008; Eisenhardt, 1989) than an impartial collection of the data evaluated using the grounded theory approach. No preconceived agendas guided collection in response to the research questions or the research problem (Allan, 2003). Accomplishing interviews in this fashion brought rigor to the collection process and ensured bias avoidance from introduction by the researcher (Allan, 2003; Corbin & Strauss, 2008; Kwok, et al., 2012).

Theoretical sampling allowed the researcher to obtain practitioner data directly from the professionals closest to the process, obtaining firsthand information more applicable to addressing the research problem. Utilizing constructivist grounded theory techniques (Allen, 2010; Charmaz, 2006; Devadas, Silong, & Ismail, 2011; Glaser, 2012a; Rich, 2012), the researcher crafted questions to elicit a story and a history of the participant without feeling under pressure to perform (Charmaz, 2006; Corbin & Strauss, 2008; Wimpenny,& Gass, 2000). The participant felt more comfortable in answering honestly. Once participants yielded data in the interview, concepts were then derived (Charmaz, 2006; Corbin & Strauss, 2008; Huehls, 2005). Theoretical sampling also enabled the researcher to discover practitioner concepts relevant to the problem and the population, because of the unexplored organizational areas of the information

Table 5. *Interview Question Rationale*

Question	Sources	Rationale
In your opinion, what is information security strategy?	Baskerville & Dhillon, 2008; White & Bruton, 2011	Find out and elicit from the participant the level of understanding they have of the subject of strategy and especially information security strategy.
What does security strategy mean to you? And to this organization?	Hall, Sarkoni, & Mazzuchi, 2010	More opinion based, to ascertain the information the participant operates with in the performance of their job and how they see themselves supporting the business mission through strategy.
What is the role you take to accomplish information security strategy?	Johnson, 2009; Johnson & Lederer, 2010	Trying to get the participant to evaluate their perceived role of operation within the organization. The most direct question to ascertain their perception of roles.
Can you elaborate on how you arrive with your strategic priorities for information security?	Mintzberg & Waters, 1985	Attempting to gain insight into their selection process and how they operate with their leadership's direction for strategic development. The participant evaluates their activities and matches them to the priorities they need to achieve for success.
Can you describe the model (framework or system) of your information security strategy?	Mintzberg & Waters, 1985	An attempt to gain from the participant the viewpoint they have of the information security strategy and where it fits in the information system and organizational strategy. The participant plays a role in meeting outside objectives.
Can you describe how the implementation of information security strategy is tracked?	McFadzean, et al., 2007; Johnson, 2009	A question to try and find out if they have metrics established and how they measure success in completion of goals and objectives in an organized plan. Assuming a role, the participant tracks success and keeps track of it.
Thinking of security strategy, how do you manage the priorities of the large organization?	Gavetti & Rivkin, 2005	Does the participant track and use the strategy as a tool or does the plan not work correctly as written. This also illustrates the role the participant takes to be able to accomplish the priorities.
Can you explain what capabilities are necessary for a successful information security strategy?	McFadzean, et al., 2007; McFadzean, et al., 2011	To try and ascertain what the participant views as being successful with an information security strategy. How they approach the strategy and what role they may assume to make it successful.

Note: Some sources are from business and information systems strategy research, as the guiding principles apply also to information security strategy.

security program that became important to this study (Charmaz, 2006; Corbin & Strauss, 2008; Creswell, 2002; Jirasek, 2012; Mcfadzean, et al., 2007).

Data collection led to analysis. Analysis led to concepts. Concepts generated questions. Questions led to more data collection. As analysis ensued, it kept revealing concepts and if questions persisted, the researcher made arrangements to gain further clarification from the participants (Corbin & Strauss, 2008; Huehls, 2005). The cycle of more collection continued until all possible data collection and coding for new concepts yielded no new concepts from the analysis. Continuous data collection happened with participants until reaching saturation. Saturation occurs until the point, "when no new categories or relevant themes are emerging," (Corbin & Strauss, 2008). At that point, data collection was completed. In the following data analysis section, the process for performing open, axial, and selective coding is covered to construct categories on multiple levels and develop the theory from the data (Allan, 2003; Charmaz, 2006; Corbin & Strauss 2008; Jones & Alony, 2011; LaRossa, 2005; McFadzean, et al., 2007).

3.4 Proposed Data Analysis

Data analysis was where coding took place. Grounded theory uses the comparative method of data analysis, analyzing elements of the data within and from one source to another (Allan, 2003; Jones & Alony, 2011, Rich, 2012). The process starts with collecting data from individual interviews and artifacts and then constantly comparing and contrasting data between collected interviews and artifacts. The outcomes of these comparisons should identify categories and the core category through this coding process identified in Figure 1, Developing a Grounded Theory (Allan, 2003; Backman & Kyngaes, 1999; Hallberg, 2006; LaRossa, 2005; Vannoy & Salam, 2010). The coding process consisted of three separate, yet interrelated steps in data analysis. Figure 1, depicts the first step as open coding which builds multiple categories and as a result of analysis in the open coding step a central or core category began to emerge

(Hallberg, 2006). The second step, axial coding, establishes connections between categories that are identified and built into the structure of the analysis. The third step, selective coding, developed the outputs of axial coding and weaves them together to build the narrative of the analysis (Allan, 2003; Corbin & Strauss, 2008; Jones & Alony, 2011; Siponen, 2005a).

Overall, comparative analysis was inductive and led to building a theory from the data (Allan, 2003; Devades, Silong, & Ismail, 2011; Rowlands, 2005). To assuage the notion of skepticism over the use of grounded theory, strict methods were followed that granted repeatability, should someone desire to take the information collected and attempt to re-create the same categories or arrive with the same theory. Opening the sources and identifying this method adds rigor to ensure obtaining similar results. The researcher also used two tools adapted from other grounded theory exemplars, called the conditional relationship guide and reflective coding matrix (Scott & Howell, 2008). The conditional relationship guide introduced a step by step procedure to obtain and verify the dissection of collected data into high level categories. The reflective coding matrix adds rigor by the way in which it aids the researcher to collect and comparatively analyze similarities together during axial and selective coding, assisting with identifying the properties of what will become the emergent theory (Scott & Howell, 2008).

The first step of the open coding process worked to identify the concepts, categories and properties, captured in interviews, memos and code notes. During open coding, analysis can be as granular as analyzing word for word, a line at a time, two to three sentences or whole paragraphs to surmise meaning into categories (Corbin & Strauss, 2008; LaRossa, 2005; Vannoy & Salam, 2010). Open coding gathered the data, built the background, and focused on the words chosen and used. Open coding also looked at how comparisons were made with the discovered categories and how similar categories were placed into groupings (Allan, 2003; LaRossa, 2005;

McFadzean, et al., 2007). The conditional relationship guide is a simple matrix that assists with establishing and capturing initial categories for use in open coding. The matrix assisted by expanding researcher experience and interpretive creativity through asking several questions of the data to allow the development of categories (Scott & Howell, 2008). The consistent use of the questions to establish categories added to the rigor in the treatment of data and ensured identification of all possible categories. Scott and Howell (2008) suggested the use of the matrix to add rigor as it established an audit trail in how categories were developed, using the interview questions. After grouping together terms into categories, the next step built the linkages or connections between the categories.

Axial coding sought to find the relationships or links between categories. Axial coding analysis considered interconnections of categories and if terms or phrases should be moved around or placed in different categories. During the second step, the areas of interest were built through the connecting of narratives together. Axial coding looked for causal conditions and if any intervening connections occurred between the categories, for building of stories amongst the categories (LaRossa, 2005; McFadzean, et al., 2007; Vannoy & Salam, 2010). The primary purpose of the reflective coding matrix was to develop the core category and contextualize it with all the other minor categories identified from the collected data (Hallberg, 2006; Strauss & Corbin, 1998). Scott and Howell (2008) observed that the reflective coding matrix helped to build the categories into an evolving storyline, refining the order and sequence of categories. The researcher used the reflective coding matrix to flow from left to right, moving categories around and kept the story flowing from start to finish, which all centered around the core category or central phenomenon (Brown, Stevens, Troiano, & Schneider, 2002; Hallberg, 2006). The end result of using both the conditional relationship guide and the reflective coding matrix

led to the theory development and emergence from the data (Brown, et al., 2002). The reflective coding matrix feeds selective coding.

Selective coding was the combining together of all the plots into a more coherent outcome from all the analysis of information. The story behind all the data collected during interviews and from artifacts retrieved and analyzed from files (Jones & Alony, 2011; LaRossa, 2005; McFadzean, et al., 2007; Vannoy & Salam, 2010). This third step, selective coding, was where the data analysis of threading the categories into the core category together to define how things resolved into an emergent theory (Hallberg, 2006). The last part of the selective coding step revealed the relationships amongst the data to show the theory from the collected data (Backman & Kyngaes, 1999; Devadas, Silong, & Ismail, 2011; Siponen, 2005b). With the successful coding of data, the results of open, axial, and selective coding are reviewed in detail in Chapter 4.

Chapter 4

Data Collection, Analysis, and Findings

4.1 Introduction

Outcomes for this study developed as the collection, analysis, and results stages progressed. The researcher interviewed participants, dissected the inputs of the interviews and correlated the results into a theory on the roles individuals used for an information security strategy. The following sections elucidate the steps taken and tied them together to produce a theory to advance the information security program through the analysis of information security strategy.

4.2 Data Collection

Using the procedure for conducting interviews as prescribed in Chapter 3, the researcher conducted interviews with 32 chief information security officers (CISOs) and their deputies (DCISOs). Primarily, 25 interviews were conducted from units within one large government organization. An additional seven interviews were conducted with CISOs and DCISOs from like or sister units within other large government organizations. Table 6, Sister Unit Characteristics, identifies the sister or similar organizations and how they would equate to CISOs and DCISOs from the large 'Fatherland' organization (Table 4, Participant Sub Unit Characteristics). Table 6 contains a short sanitized mission statement of the sister units and then a cross reference to Table 4 to illustrate where the units are similar. The seven interviews served two purposes. Primarily, to reach saturation in the collection of data, but also to test and observe whether like or sister organizations responded with the same kinds of responses. The seven respondents did answer the questions in a very similar manner. Table 7, Interviewee Index, captured a breakdown of all of the study participants. It shows the respondent identifier to the unit type and whether the

organization was small or large; also, whether the participant was from sister organizations or not. Small organizations are sub parts of a large organization.

Each interview was carried out per the arrangements identified within the Institutional Review Board (IRB) approved agreement. The researcher met with each individual at a local coffee shop, meeting room, or an agreed upon CISO designated meeting location. The interviewer reviewed the entire IRB agreement paragraph by paragraph with each interviewee

Table 6. *Sister Unit Characteristics*

Sister Unit Name	Name from Table 4, Participant Sub Unit Characteristics	Mission Statement
LLA	UHJY	Helps the public by responding, recovering, and remediating from all chemical and bio hazards. Helps the country to be prepared for those emergencies.
MSD	FRT	Watches over the country's high energy systems to make sure citizens of the country are safe.
BAUD*	ERF	Primarily keeps terrorists and supplies for terrorist groups out from the country. Ensures order and civility in the country and all bureaucratic rules are obeyed.
VTEB	WER	Performs research and development for all levels of government used to find emerging drugs to support and protect the country.
POKE	NKOP	Responsible for country's information technology systems and equipment, and the identification and tracking of performance measurements.
ABC	WDC	Responsible for protecting information and intelligence from being exploited in the country.

*NOTE: The agency BAUD had two participants from the same organization

and obtained a commitment to be available for follow-on questioning, if necessary. The interviewer asked the same set of questions, in the same way, from each individual to ensure appropriate rigor (Allan, 2003; Corbin & Strauss, 2008; Lee & Hubona, 2009). The interviewer wrote the text of the responses verbatim and took observational notes during each session. Immediately afterwards, the interviewer transcribed the notes into a capture of the interview. The interviewer also kept a journal of interviewees after conducting the interview of each

participant. Each respondent was assigned an arbitrary, random alpha numeric designator, as noted in Table 7, Interviewee Index, and the resultant transcript of the interviews were used in the coding analysis.

Table 7. *Interviewee Index*

Respondent Identifier	A0	B3	C7	D2	E3	F5	G7	H8	I5	J7	K2	K5	L9	M2	M7	N5	P4	P5	Q3	R2	S1	T8	X4	Y4	Z7	Totals
CISO Large Agency														1												1
DCISO Large Agency					1																					1
CISO Small Agency	1					1		1	1		1	1	1		1	1			1	1		1		1	1	14
DCISO Small Agency		1	1	1			1			1							1	1			1		1			9
Total																										25

Respondent Identifier	B8	O9	T5	U2	V8	W3	X9	
CISO Sister Large Agency	1			1	1	1	1	5
DCISO Sister Large Agency			1					1
CISO Sister Small Agency		1						1
Total								7

The researcher conducted the interviews over a six month period of time. The bulk of the interviews took place within the first three months (December 2013 to February 2014), as the availability of CISOs was optimal. For the second three months (March to May 2014), schedules and availability of CISOs prevented a few interviews from taking place as planned. Inclement weather did play a role with two interview attempts and obtaining those interviews stretched over two months before resolving schedule conflicts and the actual interview taking place. The researcher persisted in obtaining interviews and reached saturation before the thirty second interview. It would not be possible to say exactly when saturation was reached, because of the comparative analysis process occurred alongside conducting interviews. As stated in Chapter 3, the point of saturation was reached when no new data for categories surfaced during the interviews of CISOs.

It should be noted, that during the entire interview process two invited CISOs were not able to participate. One CISO had intervening reasons for not conducting an interview, by continually stating information security issues and other meetings took priority over an

interview. A second CISO, who initially agreed to be interviewed, had been extremely difficult to contact and has been traveling constantly around the United States since their arrival. After May 2014, the point of saturation was reached. Two additional new CISOs have been hired into units within the large organization, but lack expertise in the field and in the large 'Fatherland' organization precluded the need to interview the CISOs. In the end, saturation was reached through the 32 contacted and participated CISOs and no further interviews have been deemed necessary. However should the opportunity arise, the researcher does remain open and invitations have been extended to CISOs who would still like to participate.

4.3 Data Analysis

The researcher began the analysis of data by taking the whole interviews of the participants and summarized them individually into a high level analysis overview. The initial results captured in Table 8, Overall Initial Analysis, illustrated where each CISO stood in the general areas under the study. The initial analysis considered four specific areas of interest. Proactive versus reactive approach; whether they have a written strategy or not, who they aligned with, and what their perceived role might be. All this information was captured in the individual highlighted sections of Table 8, Overall Initial Analysis. The first area was whether the CISO viewed their information security program as operating with a reactive, proactive, or a combination of both a reactive or proactive approach towards their information security program. One specific instance can be related, according to Respondent M7 (personal communication, April 14, 2014) who stated, "it (information security strategy) needs to clearly articulate the risk of a decision by management that would put data at risk and it must be proactive and not reactive in decisions." The second area asked was whether the CISO had an information security strategy of some sort, did not have one, or stated that one was not necessary. One indicative example of

Table 8. *Overall Initial Analysis*

Strategy	Proactive	Reactive	Have one	Don't have one	Not Needed	Business	Bus/IT	IT	On its own	Ad-hoc	Top Down	Public Image	Competitor	Continual Change	Best Practice	Re-Organization	Power Relationship	Compliance
Respondent																		
A0	X			X			X				X				X			
B3		X		X				X										X
B8	X	X		X					X	X	X			X	X			
C7		X		X			X					X						X
D2		X							X					X				X
E3		X	X				X		X					X				
F5	X	X			X		X			X	X			X				X
G7		X	X	X				X		X	X							X
H8		X		X				X							X			X
I5	X	X					X		X					X	X			
J7		X		X							X			X		X		X
K2		X		X			X				X				X			X
K5	X			X		X						X		X	X			
L9	X								X					X	X			
M2	X		X				X				X			X	X			
M7		X	X				X			X	X							X
N5	X	X		X			X			X	X			X				X
O9		X		X					X		X		X					X
P4	X			X					X						X			X
P5		X			X		X								X			X
Q3		X		X			X				X				X			
R2		X		X			X								X			X
S1		X		X			X		X		X				X			X
T5	X			X		X			X						X			X
T8		X		X						X	X						X	
U2	X		X				X		X					X	X			X
V8	X		X				X		X			X		X	X			
W3	X			X			X							X	X			
X4	X	X		X			X						X	X				X
X9	X			X		X			X	X				X	X		X	
Y4		X		X			X								X			X
Z7		X		X					X	X				X			X	

an isolated case came from Respondent F5 (personal communication, December 30, 2013) who said, "What we do, is we have developed, rather we have the CIO strategic plan." As a qualitative measurement, most of the CISOs either had a written strategy, one was in the process of approval, or they used a higher level organizational strategy, such as the information systems strategy or the business strategy. The CISOs who stated it as not being necessary relied upon having the information systems strategy from the Chief Information Officer (CIO) as their prescriptive strategy. The third area looked at the way in which the CISO aligned their activities in the information security program towards one that used the goals of the business, business and information systems, information systems, information security operating on its own or using ad-hoc (no goals in their leadership) working issues as they were confronted. One example of a business driven strategy came from Respondent M2 (personal communication, January 8, 2014) who said, "My role is to act as a conduit to political appointees. I deal with political appointees and the overarching drivers of the organization." In the fourth section of the spreadsheet, an initial assessment was made in how the CISOs viewed and or operated in a role for the performance of their duties. Some stated they operated in one particular role and some CISOs displayed performance of multiple roles to meet their assessed information security program goals (Carter, Grover, & Bennett Thatcher, 2011; Weill & Woerner, 2013). The roles identified from the participants consisted of top down, public image, competitor, continual change, best practice, and compliance very similar to the categories identified in Chapter 2.

A closer look at the overall analysis revealed that for the most part CISOs viewed themselves as reactive in response to leadership. Most CISOs do not have an established information security strategy. The overwhelming majority worked with business and information systems sections of the organization. They decried the lack of security, but

conformed to either the CIO or business leadership. Lastly, most CISOs performed primarily in a compliance mode of operations. The main reason surfacing in most interviews was the fact that by Federal law the CISOs must comply with the Clinger Cohen Act of 2002, under the section known as the Federal Information Security Management Act (FISMA) 2002 (Burwell, 2013; Corbet, 2014). The initial overall analysis highlighted individual overviews of what individual CISOs viewed for their information security programs. The actual analysis in this study used coding to bring all the inputs from all of the respondents and weave them all into an overall review. Using the agreed upon approach in Chapter 3, the researcher began coding data from the transcribed interviews. The researcher proceeded into the coding process to perform the open, axial, and selective coding of the collected data.

4.3.1 Open Coding

The interviewer transcribed the sentence by sentence breakdown of the interviews conducted with CISO executives. There was no paraphrasing or summarization of thought in the transcriptions of the interviews. The researcher utilized an open coding process to review all the sentences collected from interviews with 32 CISO executives. As an example of the rigor performed, on the interview can be illustrated in taking one particular portion, at random and following through open coding. The portion selected were parts of Respondent Y4 in the first steps of the comparative analysis inside of the open coding process leading to categorization of the interview. In particular, Respondent Y4, Question 6 is used for this analysis. The interview question (Table 5, Interview Question Rationale) was, "Can you describe how the implementation of information security strategy is tracked?" and the response from Respondent Y4 was:

> Implementation is tracked through a number of ways in our program. First it is measured through compliance activities taking a given standard and incorporating

> these policies and standards into a checklist of activities of which all team members affiliated with these actions and tasks are responsible for. Another way is through management activities in understanding the day to day mission and the approvals that must accompany certain activities and an effective communication process which allows managers to remain insightful about the activities of their stuff. Another way of tracking it is through mandatory reporting or inspections by the organization office of the inspector general. I believe that all of these methods allows for us to successfully gauge the effectiveness of the program and provides key indicators as to the effectiveness of the implementation strategy. Lastly, customer feedback cannot be overlooked in assessing the implementation of the program.

The researcher used a manual form to take the captured sentences of Question 6 from Respondent Y4, dividing them up into a sentence for each cell in Table 9, Question 6, Respondent Y4. The left hand column states the respondent's sentence and then next to it in the adjacent right hand column, the initial first pass of comparative analysis towards categorization

Table 9. *Question 6, Respondent Y4*

Response Broken into Sentences	Analysis of the sentence
Implementation is tracked through a number of ways in our program.	Number of ways of tracking
First it is measured through compliance activities taking a given standard and incorporating these policies and standards into a checklist of activities of which all team members affiliated with these actions and tasks are responsible for.	Compliance through checklists is one
Another way is through management activities in understanding the day to day mission and the approvals that must accompany certain activities and an effective communication process which allows managers to remain insightful about the activities of their staff.	Business understands mission approves staff working in locations
Another way of tracking it is through mandatory reporting or inspections by the organization office of the inspector general.	Auditing of systems to IG
I believe that all of these methods allows for us to successfully gauge the effectiveness of the program and provides key indicators as to the effectiveness of the implementation strategy.	Strategy is realized through use of compliance auditing and approvals
Lastly, customer feedback cannot be overlooked in assessing the implementation of the program.	Customers are key in working

by open coding techniques. The side by side analysis in the open coding form captured the transcript of CISOs on the left hand side and open coding review for categorization on the right

hand side. The reviews were produced as short evaluation statements, used for identifying categories. This step became the background to the comparative analysis, conducted within the open coding step in an ongoing basis (Corbin & Strauss 2008; Charmaz, 2006).

The 'in vivo' summation in the right hand column attempted to keep the respondent's own words as much as possible for the category comparative analysis. The researcher performed the side by side analysis of 1,783 sentences from the 32 interviews conducted. After the first few interviews conducted, the interviewer surmised that the interview questions being asked accomplished exactly what was desired. The responses gained from the interviewees produced thoughtful exchanges between the interviewer and the CISO executives based upon the intended areas as identified in Chapter 3, Table 5, Interview Question Rationale.

The researcher took the information resulting from the analysis of the sentence in the initial open coding comparative analysis and grouped like sentences together. To illustrate how a collected respondent's responses fit into the overall collected candidate's grouping, the researcher depicted it as in Table 10, Comparative Analysis Groupings. The table consisted of a column, on the left, identifying the individual Respondent Y4, Question 6, analysis of the sentence, from Table 9, Question 6, Respondent Y4. These entries were added to the other sentences from subsequent interviews into the middle column, which showed the current total of collected candidates for a proposed category from all interviews conducted to that point in the process of data collection. The sentences represented the 'in vivo' responses from the aggregate respondents and collected these like responses together to yield the number of times a response occurred. The third column was the in process count of the number of times a like response was received up to the point in time. The number merely represented whether a candidate for a

category was substantial by the number of occurrences or if it only had a few occurrences throughout the collection of data from interviews. This constant comparing cycle continued as

Table 10. *Comparative Analysis Groupings*

Individual Respondent Y4, Question 6	Collected candidates grouped together from all interviews	Number of times occurring from initial open coding pass
Number of ways of tracking	ISS becomes a tracking mechanism (which assists in making it live); ISS should identify the tracking methods; ISS overall increased in applicability; Multiple methods of tracking; Multitasker; Tracking should take place experimentally; CISO tracks team leaders to accomplish ISS; CISO wants to have a way to track security; CISO tracks through system inspections; The ISS helps us keep track of all the activities that the mission captures	11
Compliance through checklists	Compliance through checklists is one; Compliance checklist; Use standard checklists to configure and modify; Use checklists to configure equipment-compliance; Tracking performed by checklists, standards; ISS is a checklist; ISS is a checks & balance document; If not told, find the best checklist; We are shifting to automated checklists; Nothing special, checklists; Following accepted procedure is key	15
Business understands mission approves staff working in locations	Business understand mission approve staff working in locations	1
Auditing of systems to IG	Auditing of systems to IG	1
Strategy is realized through use of compliance auditing and approvals	Compliance is centralized; CISO does compliance only; Strategy is realized through use of compliance auditing and approvals	3
Customers are key in working	Rank order top priorities; Customers are key in working; Prioritize the major priorities, use the tear line for top priorities; Align requirements to rank priorities; Strategy team ranks them and then cuts them off according to budget; Identify the major priorities; Funding drives some priorities	10

interviews were conducted and from the previously analyzed interviews of CISOs. The entire category candidates started out from the combined total of 1,783 analysis of sentences created during the interview process and reduced the number until the open coding cycle was completed.

In this discussion, the researcher continued to use one comparatively analyzed sentence from Respondent Y4, Question 6, analysis of a sentence ('number of ways of tracking'), response and folded this into the grouping called ensures compliance as represented in Table 11, Raw Sentence to Short Category.

Table 11. *Raw Sentence to Short Category*

Raw Sentences	Short Category
CISO ensures compliance met with; CISO considers current situation and compliance and then moves forward; CISO ensures compliance through baseline; CISO inspects systems for compliance; CISO leads compliance effort; Compliance by default; Compliance adherence illustrates delivery of security; Continued to achieve compliance; CISO must be compliance oriented; Individual compliance over systems formed out of ISSOs; ISSOs perform direct compliance; ISSOs responsible for systems; ISS also depends upon inspecting systems; A lot of ISS' get stuck in compliance mode; Compliance is centralized; CISO does compliance only; Strategy is realized through use of compliance auditing and approvals; Oversight is centralized; Compliance is lacking in some places; Compliance to check security; Compliance used to track implementation; Business views security as compliance based; Baseline is compliant and operational to bridge risk; Compliance identifies requirements; Compliance helps to identify shortfalls; Compliance still used for security in plan; ISS used compliance for ISS; desires compliance as a strategy; Compliance drives strategy; Compliance used to measure ISS accomplishment; ISS should be compliance; ISS tracked by compliance; Used balanced scorecard to measure compliance; Compliance used through logging; Created metrics from logs; Inventory for compliance; Auditing of systems to IG; Compliance is needed for end to end; Compliance is key; Compliance is required; Compliance needs to be there; Worked to improve compliance; Compliance/it is good enough for Government work; ISS is compliance driven; ISS is compliance□□	Ensures Compliance (Compliance provides a score of security, good or bad, that the CISO tracks according to law)

Once the number of groupings reached a manageable number of possible categories, 35 groupings, that resulted from the process. Table 12, Proposed Category Grouping, showed the

results of comparative analysis, taking the sentences from all 32 CISOs and grouping like responses into groups that represented the data collected. The single group in the table showed

Table 12. *Proposed Category Grouping*

Category	Grouping
Aligns Business	CISO aligns ISS to business goals. Often business sets goals for CISO
Aligns Business and IS	CISO aligns with both business and IT goals
Aligns IS	CIO often dictates for CISO to align
On its own	Some CISOs have own budget and set goals themselves
Ad Hoc	CISOs have no guidance and mostly work on putting fires out, Use project plans as strategy
Top Down	Management driven
Public Image	Business did not support security, public image worth more, No support from Business
Competitor	Seeking to outdo everyone in the large organization, Competitiveness
Continual Change	Change is imminent and needing to be protected, Flexible, Adaptable, Agile
Best Practice	CISO looked to other examples in order to build their ISS for the best possible results; a lot of CISOs build once and use many times, mindset across government
Re-Organization	(While advanced, not much information obtained)
Auditing	Some performed audits to verify compliance
Measurement and metrics	Many measured results
Ensures Compliance	Majority tended to compliance as it is the law
InfoSec Prg	Recognition of an overall program as needed
Priorities	Prioritizing what matters in their program and according to whom it is a priority for
Visionary	Recognized the need to see a goal and have a vision for each goal
Framework model method	Looked to have a model to use for reaching a goal
Structure of an ISS	The actual process of developing a strategy (3 or 4 goals, max)
Putting the Strategy to work	Once devised, the strategy must work
Shelfware	Must be used or reverts to D2D or tactical
Trust	Customers must be able to trust CISO
'Know' Security	Recognized security as primary first step in process
Protect	Protection of data and information systems
Communications & Collaboration	Talking and getting message across is crucial to success
Buy-in	Recognition that buy-in from leadership (business/IT) is fundamental to the program
Automation	Speed of change requires automation or succumb to threats
Operations & Risk	Some recognized InfoSec and ISS is more than compliance and should fit to operations
Paradigm	Showed the shift from operations to threat
threat driven, proactive, change	While pursuing a standard CISO pursued next generation or preventing threat as opposed to chasing after and patching
Qualified Staff	Can't do the job if you don't have the resources-People, re-organization as it applies to having enough people
Tools	Can't do the job if you don't have the resources-Tools
Training	Can't do the job if you don't have the resources-Training
Budget	Can't do the job if you don't have the resources-Budget

one category proposal. The number of major groupings or category candidates from the entire study whittled down to 35 total candidates. Then a tool could be used to test the candidates for validity. Scott and Howell (2008) advanced two tools for use by grounded theory researchers to use in testing candidates for categories. The first tool, the conditional relationship guide (CRG) would be utilized to test groupings by answering a series of questions to establish category viability.

The final step of the open coding review utilized the conditional relationship guide (Scott & Howell, 2004). For each candidate category, the information was extracted from the grouping and entered into the CRG, which was designed to answer questions about the what, when, where, why, how, and to what consequence the resulting category would have on the emergent theory yet to be realized (Scott & Howell, 2008). Table 13, Conditional Relationship Guide, illustrates one category, ensures compliance, through the answering of the questions. For the discussion, the researcher utilized this grounded theory tool, during open coding analysis that would assist in testing candidates for validity as categories.

4.3.2 Open Coding Results

As each proposed category was systematically tested with the CRG, the reviewer used the questioning techniques to populate a conditional relationship guide (Scott & Howell, 2008) for each proposed category. Each cycle produced a varying amount of responses. After several passes of evaluation by comparative analysis, an additional six groupings were combined into other groupings and it reduced the overall unique category list to 29 distinct categories. The two columns of Table 12, Proposed Category Grouping, listed the tested categories of the CRG tool. Taking the categories to the next step, axial coding, the researcher sought to deduce the core category or central phenomenon of the study (Brown, et al., 2002; Hallberg, 2006).

Table 13. *Conditional Relationship Guide*

Conditional Relationship Guide						
Category	What	When	Where	Why	How	Consequence
Ensures Compliance (Category sentence- Compliance provides a score of security, good or bad, that the CISO tracks according to law)	ISS needs to cover compliance. Compliance consists of checklists. Compliance measured through checklist completion.	When systems are installed, compliance is a requirement for operation. Baseline used by scanners to check compliance on all assets. Checklists formed major portion of compliance to ensure standardization of checking.	Compliance checked on every device, system, and asset connected to the network Checklists established the standard for each device to be verified with. Scanning of assets also verified the completeness of configuring to the standard.	Without standardization, organizational elements may be able to install assets with differing configurations. Standardization would also prevent different versions from being installed, especially those with deficiencies or vulnerabilities.	Implement checklists to ensure compliance. Review and update checklists to ensure completeness, especially after an update or vulnerability patching.	Without checklists, standardization or compliance would be harder to ensure. Without scanning for vulnerabilities it would be hard to identify weaknesses.

4.3.3 Axial Coding

In the second step of the grounded theory coding process, axial coding, the researcher proceeded to further refine the initial grouping of categories and surmise the central or core phenomenon. The researcher used constant comparison in coding and each time the researcher made a pass on the collected data it reduced or combined categories and brought similarities together into combined larger groupings. For example, the researcher looked at the possibility of roles an information security professional could perform and found from the data that they could be grouped into several distinct role groupings. There were several distinct types stated by respondents as captured in Table 14, Role Groupings to Categories.

Bringing all the different types of roles into one large grouping resulted in a combination grouping or mapping to one large category called roles. The combinations can then be called a

higher level or super category, one the researcher labeled as roles. The process of further combining through comparative analysis of the categories ended with the result of four super group categories emerging from the data. The labels of those super groupings could be characterized as roles, alignments, complexities, and resources that emerged from the data. This began the start of analysis of each of the groups to be considered for the core category or central phenomenon (Brown, et al., 2002; Hallberg, 2006). The researcher objectively evaluated each of the super categories for consideration as the core category.

Table 14. *Role Groupings to Categories*

Role Proposal	Category Nomination
Management driven	Top Down
Business did not support security, public image worth more, No support from Business	Public Image
Seeking to outdo everyone in the large organization, Competitiveness	Competitor
Change is imminent and needing to be protected, Flexible, Adaptable, Agile	Continual Change
CISO looked to other examples in order to build their ISS for the best possible results; a lot of CISOs build once and use many times, mindset across government	Best Practice
(While advanced, it was not utilized)	Re-Organization

Expanding the titles of the candidates for the four super categories were the roles CISOs chose, alignments of information security strategies, the complex structure of information security strategies, and the resources for performing information security strategy. Since the researcher can not totally ignore the fact that a literature review was conducted, the researcher had to acknowledge the fact that many similarities existed in the roles and alignments. Recognizing this, the researcher consciously let only the collected data drive the construction of categories. The first two proposed super categories seemingly echoed the results of the literature review in Chapter 2, in that there were several roles information security professionals adopted

to implement their information security programs in the large government organization through the information security strategy (Carter, Grover, & Bennett Thatcher, 2011; Weill & Woerner, 2013). Second, the alignment of the information security strategy in the large government organization closely followed the discussion conducted in Chapter 2, Review of the Literature, which illustrated possible types of strategy alignments within an organization, in general (Wagner & Weitzel, 2012). It should be noted that the literature review considered literature that was oriented and focused primarily from non-public sector organizations. The data collected here represented public sector information security, in that it came completely from large government organizations. The results then should reflect purely what public sector organizations experience. For the third category, the analysis of the collected data looked at the complex structure of an information security strategy. Resources, the fourth category might fall outside the scope as a core category. Resources primarily aided in sustainment of the information security strategy efforts and could be a factor in keeping it moving, affecting long term changes, but not in the development of the strategy. The four categories are expanded in the next four paragraphs to highlight an overview of how each of the four super group categories were derived.

4.3.3.1 Proposed Roles Category

The first of the super categories was that of the roles category, which had CISOs primarily expressing the need to keep compliance at the forefront, because of mandated, regulatory law to report on system compliance utilizing recommended security controls as a major part of their job (Corbet; 2014). In addition, most CISOs utilized other roles to varying degrees that needed to be performed, such as having top down leadership, ensuring the public

image, competing with other organizations, always changing their approach, adopting or adapting to best practices, and or in rare occasions re-organizing to accept resource constraints.

4.3.3.2 Proposed Alignments Category

Alignments considered the way in which CISOs lined up goals to meet business and or information systems goals and objectives. Additional alignments looked at how CISOs performed security on their own and addressed daily breaches and incidents. Some CISOs also expressed concern that they had no direction from leadership. Respondent T8 (personal communication, February 19, 2014) stated, "But we do not have a written down strategy. We make decisions as we go along. We do not have it written down, we just do it. It is not written, it is in people's heads," which summarizes the lack of direction in some units. The CISOs made the best of their unique situations addressing information security on their own. The categories under the alignment super category were captured as business, business and information systems, information systems, information security on their own, and ad-hoc or no security.

4.3.3.3 Proposed Complexities Category

Complexities of the information security strategy surfaced in every interview, be it from the whole strategy being too complex to start or being as simple as the strategy being a three step process used each and every day. The complexities involved with the information security strategy surfaced throughout the whole process of strategy creation to finish and what the strategy should be composed of: vision, mission needs, communications and collaboration, knowing security, trust, buy-in, and developing a strategy.

4.3.3.4 Proposed Resources Category

CISOs expressed that resources as an area essential to keeping an information security program operating, but was not essential for its formation. Resources are important to CISOs as

attention was given to ensure qualified personnel are working for them, along with needing recurring training and having appropriate security tools being made available for day to day use in performing duties. Respondent F5 (personal communication, December 30, 2013), emphasized tools when stating, "What tools are we using now and then six months down the road and how that fits into the architecture." Another category within the resources super category was that of having enough budget to sustain operations, to purchase tools, hire personnel, and keep the [security] skills current (Office of the Inspector General (OIG); (2013). The results of the combining of categories into larger groupings of a similar nature also shared the focus of the study shifting from the strategy as a focal point to that of the CISO being the fulcrum or leveraging point.

4.3.4 Axial Coding Results

Through the continued use of the CRG, the researcher combed the collected data and the 35 proposed categories that advanced from open coding. Each proposed category was entered into the CRG form and evaluated. Some ended up being very similar to others and the researcher subsequently combined them together. As the process continued, the researcher began to group unique, but similar categories together. As this continued, the first cut of grouping categories under the roles grouping (Table 14, Role Groupings to Categories) showed one batch of similar categories. Three other grouping also emerged from the CRG review process, for a total of 24 categories within the resultant four groupings. Table 15, Alignment Groupings to Categories; Table 16, Complexities Groupings to Categories; and Table 17, Resources Groupings to Categories emerged to capture the other possibilities that categories could be combined from Table 12, Proposed Category Grouping. These four main groupings: roles, alignment, complexities, and resources were then advanced to the selective coding process.

Table 15. *Alignment Groupings to Categories*

Role Proposal	Category Nomination
CISO aligns ISS to business goals. Often business sets goals for CISO	Business
CISO aligns with both business and IT goals	Business and Information Systems
CIO often dictates for CISO to align	Information Systems
Some CISOs have own budget and sets goals themselves	Information Security
CISOs have no guidance and mostly work on putting fires out. Use project plans as startegy	None

Table 16. *Complexities Groupings to Categories*

Role Proposal	Category Nomination
Recognized the need to see a goal and have a vision for each goal	Visionary
Prioritizing what matters in their program and according to whom it is a priority for	Mission Needs
Talking & getting message across is crucial to success	Communications
Recognized security as primary first step in process	Know Security
Customers must be able to trust CISO	Trust
Recognition that buy-in from leadership is fundamental to the program	Buy-in
The actual process of making a strategy (3 or 4 goals, max)	Develop

Table 17. *Resources Groupings to Categories*

Role Proposal	Category Nomination
Need to have adequate funds to operate the program	Budget
Must have appropriate tools to perform inspection	Tools
Need to have qualified people to use tools and find security anomalies	Personnel
Personnel need to obtain training to maintain skills	Training

4.3.5 Selective Coding

The researcher continued the analysis of the collected data into the final step of selective coding to consider what makes an information security strategy complex; how it is formed; what sustains it; how it lines up with other strategies; and what role(s) the CISO selected to meet the tenets of the information security program.

The initial research problem stated the researcher should review the data collected and it might produce an understanding of the complexities of an information security strategy. The study should reveal what the differing roles are for an information security professional and the ways in which an information security professional differentiates one information security strategy from another. Additionally, the study might help identify how information security strategies differ within a large government organization and the way in which the organization might drive the information security strategy. The four large areas revealed from the study were ones to look at roles, alignments, complexities, and resources. Each of which is key to developing the core category of CISO actions to achieve a strategy.

4.3.5.1 Roles

The majority of CISOs expressed the main role category in use was compliance, it was central to functioning in the organization. Conversely, a majority of CISOs also revealed that couple of minor roles were not used frequently within the category. The main roles not used frequently by information security professionals were public image, competitor, re-organization and power relationships, of which, power relationships was not in use at all. The four major roles in use by the information security professionals were compliance, continual change, best practices, and top down (Seeholzer, 2012). Figure 2, Roles, illustrates the centrality of roles that the CISO used. Compliance was the one all the CISOs used (depicted as central) and to varying

degrees parts of the other roles were utilized in the public sector. The root or purpose of the information security program was to protect and ensure confidentiality, integrity, and availability (CIA) of data and information systems entrusted to information security (Krutz & Vines, 2001). The compliance role an information security professional uses was to classify each information system according to guidelines published by the National Institute of Standards and Technology (NIST) (Computer Security Division (CSD); 2004). The information security professional must also comply with FISMA scorecard requirements (Burwell, 2013; Corbet, 2014).

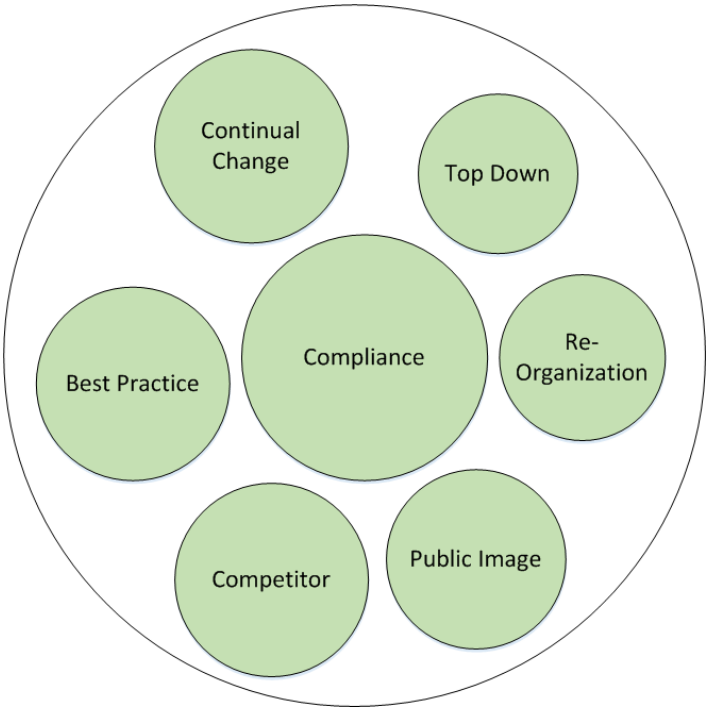

Figure 2. Roles

Information security professionals also expressed the need for continual change, adapting to events as they evolved over time between updates of their information security strategy. The CISOs saw this in two ways. Illustrative of this was what Respondent E3 (personal communication, December 26, 2013), who stated, "Within the CISO organization it is an adaptive process of realizing that our priorities can change…operations tempo, threat movement,

emerging technology and other factors in order to realize your overall vision." First, continual change meant that the business section of the organization continually changed the way in which security was to operate and periodically levied new requirements on the information security section, sometimes without prior coordination. Respondent E3 (personal communications, December 26, 2013), said, "Basically, the ground rules must be prioritized then the stakeholders can understand when they have skin in the game and when they need to prioritize; when and where they need to re-prioritize against competing priorities." Multiple CISOs confirmed that their management did in fact change course several times over the entirety of a fiscal year. The second method CISOs explained was a more agile approach, one in which they looked at the way the information security professional should continually evaluate their progress towards meeting the goals of their strategy and making adjustments as necessary. Many did not, but a few of the CISOs did use their plan and adjusted it periodically over the course of the fiscal year. Respondent P5 (personal communications, April 23, 2014), captured this when stating, "Some of the priorities are out of your control. The organization will set them for you. The chief information officer is going to set them and you are going to have higher organizational goals. The priorities are set from up channel." Those that did adapt, regularly met the objectives of their strategy. Those that did not might have, but often just reacted to situations as they arose.

Information security professionals explored industry best practices as well. Best business practices covered the entire range of activities from using step by step instructions of a keep it simple basic instructional book (Olsen, 2007) to trying to achieve level five of a capability maturity model integration (CMMI) framework (Bunker, 2012; CMMI Team, 2010). Respondent J7 (personal communication, December 31, 2013), summed it up in saying, "Information security strategy means to me that it is very, very simple, it is how we are going to

accurately and effectively accomplish our mission. It is the stepping stones from point A to point B and without honesty and a logical process, you will never have an accurate strategy…" Information security professionals also reviewed and selected practices from business process reengineering, and efficiency models like the plan-do-check-act (PDCA) and strengths, weaknesses, opportunities, and threats (SWOT) methodology (Moen & Norman, 2009; Team Free Management Ebooks (FME), 2014). Top down driven structures existed and the CISO reacted as a result of being driven or driving information security with the work force. Many CISOs had priorities placed upon them by upper management dictating or guiding how they should perform the information security program. One respondent pointed out that the CIO can change their direction when stating, "Priorities may also change by chief information officer (CIO) mandated priorities. When the CIO says so, then it is so" (Respondent C7, personal communication, December 17, 2013)." In driving their work force, CISOs also had some autonomy to mirror image the top down driven nature by guiding or directing how their work force performed. These were the roles observed from the interviews conducted with the CISOs from the organizations. Another super category that helped them realize potential was through resources and the ways in which CISOs utilized personnel.

4.3.5.2 Alignments

Some CISOs stated that information security has been seen as just an additional expenditure by business, the information security program has far too often been given bare minimums to meet regulatory law and then allowed to function in any way possible to meet the additional regulatory requirements. Respondent S1 (personal communication, February 12, 2014) captured this when stating, "It is hard to get funding with so many competing priorities. It is hard because information security is not seen, but when something goes wrong, everyone

comes screaming." CISOs that operate in an ad-hoc manner are left to address one issue after another and do not have a formal strategic plan to work towards measuring whether they are successful or not in accomplishing their information security program. Respondent P5 (personal communication, April 23, 2014) identified the problem when stating they always tracked the fires before working the strategy. "But, when fires do flare up, no matter where they happen, I drop everything and then track those. We do work the CIO's priorities after the fires are extinguished, but we will address fires when they come up first." The CISO organizations that operate on their own tend to operate correctly, if the CISO operates correctly, but tend to fail if the CISO is forced to accomplish tasks that increase risk across the organization. Figure 3, Alignments, illustrates the possible alignments for information security strategies.

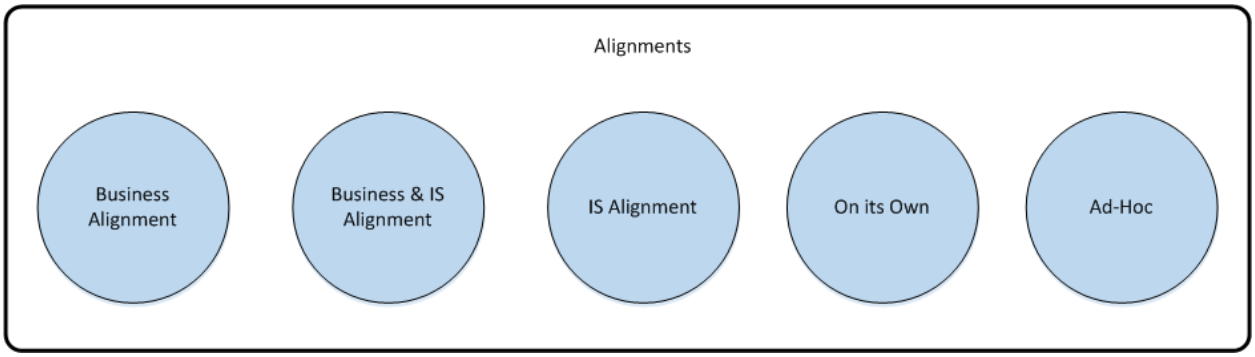

Figure 3. Alignments

Each organization operated differently, to meet their particular mission needs. The researcher found that CISOs in each sub-section of the large organization had parts that were similar and some that differed in their mission from the overall large organization. Each sub-section or small unit aligned their information security strategy to meet mission need. All five of the proposed alignments covered in Chapter 2 were in operation in the large organization and among the different participant sub organizations. The two most numerous types of alignments were the information security strategy aligned with both business and information systems strategies and the second was that quite a few organizations operated in an ad-hoc fashion,

having no strategy and no internal system other than tactically moving to address one crisis after another.

4.3.5.3 Complexities

As a part of the comparative analysis and combining of statements during the coding process, several categories combined and made up the parts of what was termed the super category of complexities of an information security strategy. This super category, complexities, was divided up into the sub categories called: vision, mission needs, communications and collaboration, knowing security, trust, buy-in, and developing strategy. Each of the sub categories meshed into the others, but is also a component part of the entire super category of complexities. Figure 4, Complexities, illustrates the connectedness of sub parts combining and resulting in a coherent strategy based upon the goals of the information security professional, business, and information security strategy goals.

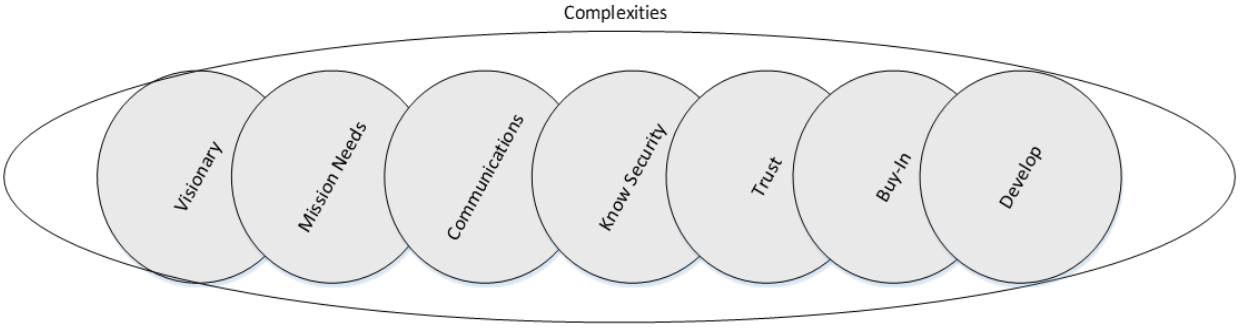

Figure 4. Complexities

Vision really focused on the CISO having an outlook for the next three to seven years as to where they wanted to take the organization in a secure manner, identifying risk, and informing leadership of actions necessary to address risk. "We look towards the next five to seven years in our projections via the roadmap," (Respondent A0, personal communication, December 11, 2013). The CISO considered mission needs to set priorities for the information security strategy. He or she conferred with stakeholders to ensure security gets involved at the start of a project

instead of finding out about projects affecting security that have already been deployed. CISOs must communicate and collaborate with everyone involved in information systems and business. Respondent P5 (personal communication, April 23, 2014) stated it best as, "Information security takes a collective, collaborative approach that is rare for an organization that can actually achieve it. So your information security strategy is really one of collaborative team building and focusing on value to the business unit." Communications must take place whenever there is the chance to discuss threats and take advantage of opportunities to talk about mitigations to threats (Scully, 2014).

Knowing security is key when working to get security built into the beginning of the systems development lifecycle. CISOs must investigate emerging technology, keeping one step ahead of what is currently in use on the network. The ability of CISOs to build trust, to keep stakeholders informed, and gain their assurance that they are kept apprised of all issues involving security is another key element. Respondent L9 (December 19, 2013) posed the question about trust as, "How strong is your relationship, the level of support and trust by your leadership?" Leadership must receive correct information from CISOs in order to gain and to maintain the trust of leadership. The CISO must also be able to market security to executives throughout the organization and obtain buy-in or support from top level executives. Buy-in is fundamental to the success of strategy (Hu, Dinev, Hart, & Cooke, 2012). The art of developing the strategy takes place by building it from the start using all the pieces of the complexities super category, keeping it small, but encompassing all of the information security program. CISOs stated the strategy should be limited to three or four overarching goals. One respondent touched upon it when stating, "The information security strategy needs to be simple. Complexity is the enemy of strategy," (Respondent L9, personal communication, December 19, 2013). And, Respondent V8

(personal communication, January 31, 2014) narrowed it when stating that, "…seven or eight elements gets down to three or four goals. Then we can look at an information security strategy in a three year plan." The goals should be achievable within the allotted timeframe of the strategy. And, most important of all, the goals should be written in such a way as to allow them to be used and checked periodically for completion.

A comparative analysis of CISO statements showed that the complexity of an information security strategy is a chain of events, yet it is interconnected and meshed. Figure 5, Complexities, illustrates the chain of events flowing from one end to the other for accomplishment. The information security strategy is a dynamic operation centered on the vision of the CISO and aligning to the goals of a higher order strategy. Developing a strategy is an active process requiring constant attention. It also requires shaping through alignment in the organization and leadership from the CISO actively working through various roles.

4.3.5.4 Resources

CISOs highlighted the need for resources again and again when asked the question of "…what a successful information security strategy needed..," (Table 5, Interview Question Rationale) to sustain it. Resources consisted of four categories, those of training, qualified personnel, tools, and budget. CISOs wanted to have recurring training for personnel, especially information security skills, but also a greater emphasis on business training--in order to learn how to communicate with stakeholders. Respondent J7 (personal communication, December 11, 2013) pointed this out when saying, "…qualified staff to support the priorities of the organization is paramount." Figure 5, Resources, depicts how the categories of resources related, how they are interactive with one another, and that each category helps to sustain the super category. One of the other primary goals of the CISO was

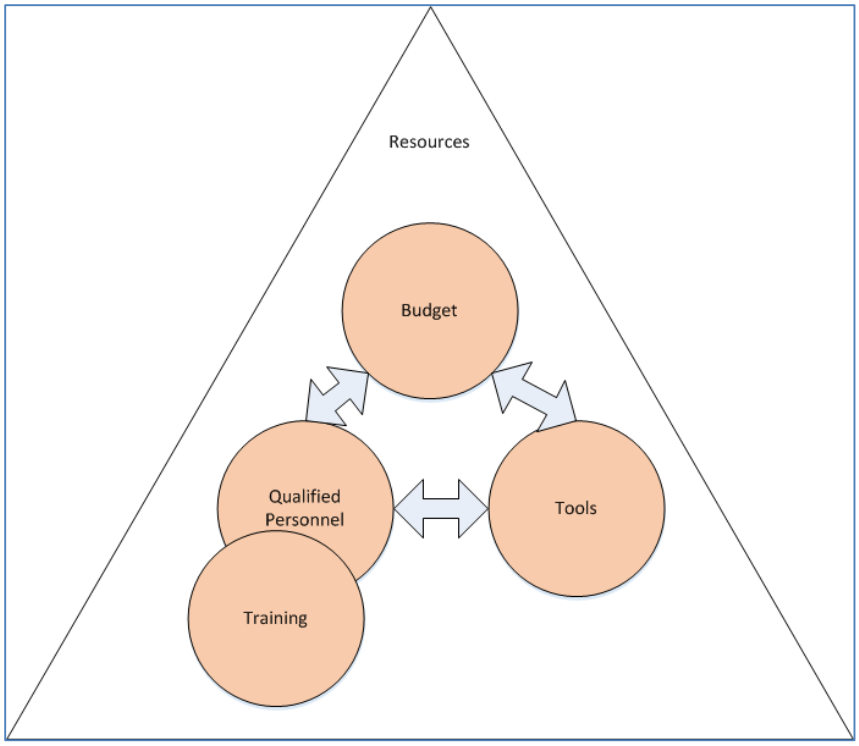

Figure 5. Resources

that they must also hire qualified personnel. CISOs recognized they were competing with commercial sector organizations that can pay much more for equivalently trained security personnel. This made it much harder for the CISOs to keep experienced personnel. CISOs noted that training was complicated and could cause problems in that while training up personnel is good, once they were trained many could move on to higher paying jobs. Figure 5, Resources, illustrates that training is an integral part of being qualified personnel. The challenge for the CISO was to identify what skills workers needed and attempt to gain the opportunity of obtaining the necessary skills to build all the workers to the same level. The CISOs wanted to allow for people to stay and develop. Some CISOs wanted to have career paths to help personnel remain and develop through the ranks of being a novice, learner, peer, trainer, and eventually a supervisor. The CISO must always be proactive in developing the individual, allowing them to mature or run the risk of people moving to other jobs. Mentoring is a prime requirement. Not

only should the CISO be training his or her replacement, but also explaining what goes on in their decision making process. Teaching the recruits was the means for critical thinking and how the CISO arrived at their decisions would help to recruit and to also cement relationships with management.

Tools are also necessary to keep current with ever evolving malware. CISOs were always searching for ways to improve software tools through added capabilities and or automation, to get the full usage of the features of the software tools. Lastly, it is imperative to have a budget to allow security to function efficiently. The CISO must become business development experts. The CISO must find and build the examples that can show return on investment, not so much in security, but as a result of security, in how much the organization can save in prevention (i.e., keeping the organization from exploits and the action that saves the organization a certain amount of money per asset, because a compromise usually results in lost time, productivity, assets, and or the possibility of even needing to replace an asset). Figure 5, Resources, depicts how all of these categories meld together to form the super category of resources which are the way the information security strategy is sustained.

Having identified the four super categories, the researcher sought to allow each to fit together in different ways and see how the super categories would identify the core category or central phenomenon (Brown, et al., 2002; Hallberg, 2006). Figure 6, Super Categories, shows the four super categories and how each affects the outcomes of the others. The arrows indicate dependence of one category upon the others. There are multiple ways to weave the categories together into a story. The process of meshing or weaving the categories together using selective coding should reveal the core category in the results.

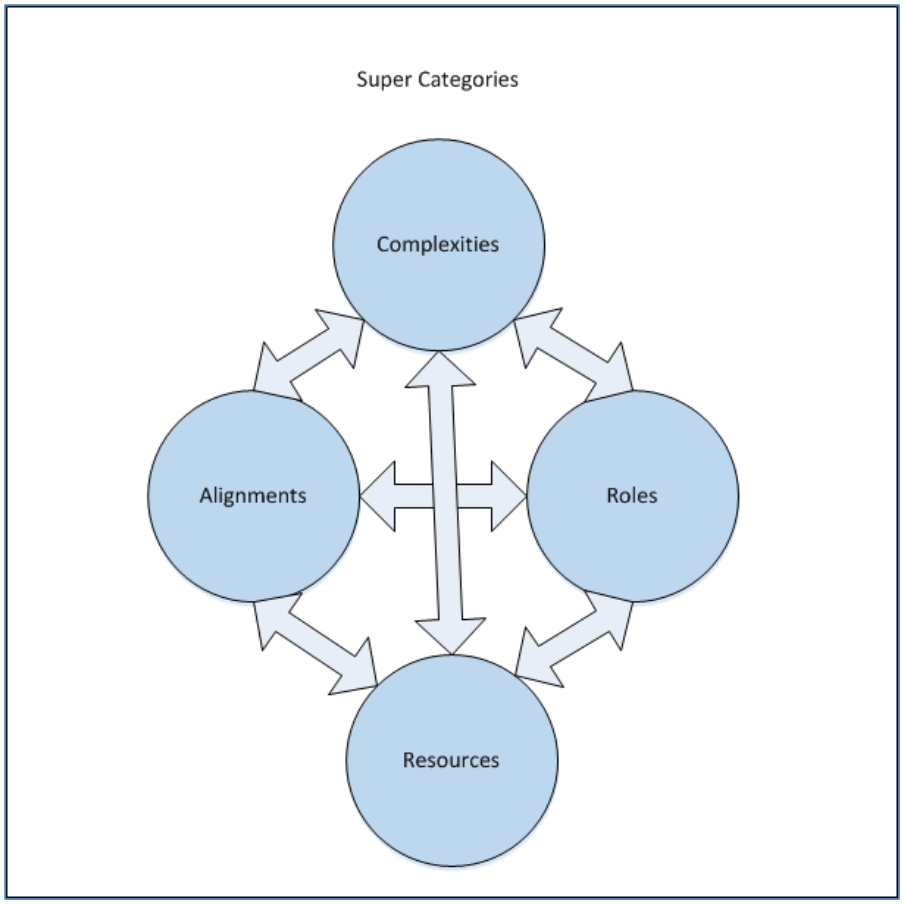

Figure 6. Super Categories

4.3.6 Selective Coding Results

The researcher used the second tool of grounded theory, called the reflective coding matrix (RCM) as the tool for the grounded theory coding process. According to Scott and Howell (2008), obtaining the theory or model from the data is the most difficult part of the coding process. The selective coding step results from the building of a story extracted from the data. By presenting the data from the collected categories in the form of collected categories one can deduce a logical flow as the relationships are built from the coding process. The story is of how all these super categories feed together and focus upon telling the story from the CISO's viewpoint in how they hierarchically work together and culminate into a core category (Hallberg, 2006).

To capture the results of the axial coding step, the researcher borrowed and used the second tool that Scott and Howell (2008) introduced that was called the reflective coding matrix (RCM), which allowed comparative analysis to proceed in whittling the selections down into a core category from the four super category groups. The process of the RCM assisted the researcher in developing a form to capture the processes, properties, dimensions, contexts, and

Table 18. *Reflective Coding Matrix*

Reflective Coding Matrix				
Core Category	*CISO Actions to Achieve a Strategy*			
Processes	Selecting the proper role	Adjusting to the proper alignment	Figuring out complexities of strategy	Obtaining enough resources
Properties	Observe and adapt to the climate	Align to proper direction	Decide on what is right	Lobbying for stuff
Dimensions	Selecting to either be management driven, assume public image worth more, seek to outdo everyone, adopt best possible result from others, reinvent the structure, always change, and or comply with law	To be business, information system, or information security driven, or have no direction	Market for Buy-in Gain trust Know security Have a vision Limit the scope Establish priorities Adopt proactive approach	Have qualified people Get enough tools to perform information security tasks Acquire the correct training Gain enough funding to complete the strategy
Contexts	Support the mission	Coordinating and deciding linkages	Establishing mutual goals	Scoping reality
Modes for understanding the consequences	Bounds the proper approach	Reaching compromise that meets objectives	Collaborate on results	Having sufficient funds to obtain needs

modes for understanding the consequences put forth through the CRG. The RCM depicted several interactions between the aspects of the core category (processes, properties, dimensions, contexts, and modes) in the left hand column for each of the four super categories or categories (roles, alignments, complexities, and resources) in the successive columns moving from left to

right. Each assesses an aspect of the category and how it reflects into the core category of 'CISO actions to achieve a strategy.'

Through the steps of filling in and assessing the areas of the RCM, the results were clear that the actions taken to achieve the strategy itself were the most critical part of the core category and one the CISOs also started time after time during the interviews. They, the CISOs, were the core to taking the action in achieving a strategy. Table 18, Reflective Coding Matrix illustrated the intricate relations of the four super categories into the core category of 'CISO actions to achieve a strategy.' The researcher used the selective coding process to build the story of the core category selection and the emergent theory that came forth using the RCM elements (Hallberg, 2006; Pandit, 1996; Scott & Howell, 2008).

From the data collected and analyzed, the researcher presented a way to depict a breakdown of the super categories discovered from the data. Figure 7, Mapping the Categories, captured in an image from breaking down each of the super categories into the categories found to comprise each individual super category. This figure shows each category (underlined) as a

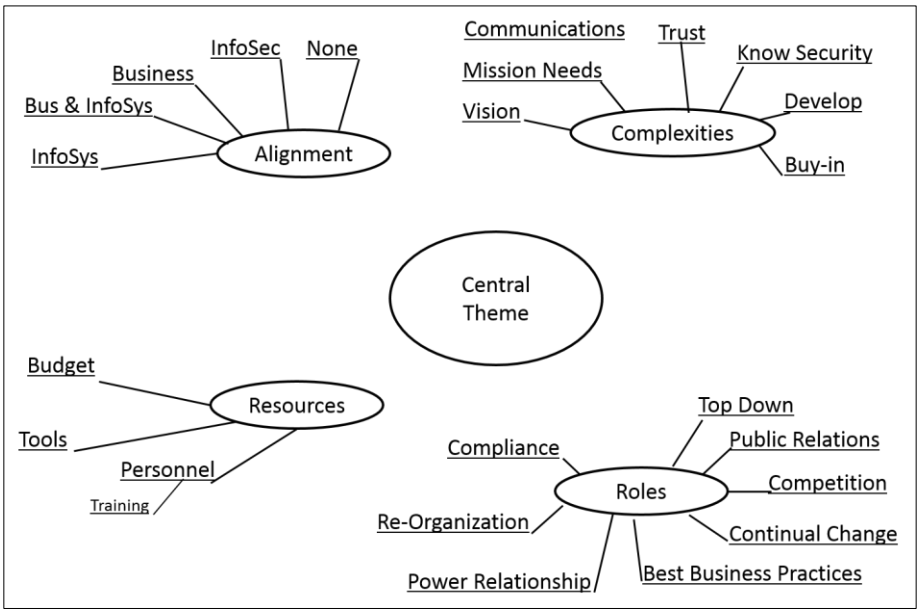

Figure 7. Mapping the Categories

part of each super category (circled) and that the relation to the central theme was yet to be structured. Figure 6, Super Categories, depicts how the dependencies exist between the super categories. The way in which a model emerges is if the CISO is inserted at the start of the decision making process; meaning that the CISO defines how to utilize roles, takes part in alignment, participates in complexities, and lobbied for resources then the ISS is formed.

In order to arrive at the core category, the researcher compared and contrasted the four super categories on their own merits to possibly identify the central or core category. The categories listed in Table 19, Table of Outcomes to Select, as 12 possible sequences of accomplishment of a theory covered all the possible combinations of the four super categories.

Assuming the CISO is the only participant in investigating the roles of information security strategy and having a direct effect on the information security program, then there would be three areas that are out of their direct control: complexities, alignment, and resources. Resources would be beyond the scope of this study, since the evaluation here is upon investigating the roles of an information security strategy. Resources would be useful for evaluating sustainment and supporting day-to-day activities. Hence, resources would be apt to be in the last position of the four super categories. This action would eliminate outcomes 2, 3, 4, 6, 8, 9, 10, 11, and 12. Outcomes 1, 5, and 7 would be the only viable ones. Since the CISO starts with a role, outcome 1 and 7 could also be eliminated leaving outcome 5 as the only selectable outcome to evaluate.

To consider outcomes 1 and 7, the study focuses on actions taken to move the direction of an information security program towards achieving confidentiality, integrity, and availability of data and systems. Alignments may receive input from the CISO, but is mostly arrived at by a combination of business and or information systems decisions to support mission along with the

Table 19. *Table of Outcomes to Select*

Outcome				
1	Complexities	Alignments	Roles	Resources
2	Complexities	Roles	Resources	Alignments
3	Complexities	Resources	Alignments	Roles
4	Roles	Complexities	Resources	Alignments
5	Roles	Alignments	Complexities	Resources
6	Roles	Resources	Alignments	Complexities
7	Alignments	Roles	Complexities	Resources
8	Alignments	Complexities	Resources	Roles
9	Alignments	Resources	Roles	Complexities
10	Resources	Complexities	Alignments	Roles
11	Resources	Alignments	Roles	Complexities
12	Resources	Roles	Complexities	Alignments

CISO. In lieu of having any alignment, the CISO may institute a self-sufficient approach on its own or opt to practice no alignment, just operate from one situation to the next. Hence, alignments should be considered of importance, but placed in the second position of the equation above complexities in the outcome, further justifying outcome 5.

Complexities may exist in varying stages from the three stakeholders within a range of strategy being derived from information systems, business, or information security. The actual strategy results from the interaction or lack of interaction between stakeholders of the organization. The CISO creates the strategy based upon inputs from the stakeholders. The CISO must then consider all the factors or complexities of building the strategy that would then align with the alignments agreed upon with management and resources that are available. Hence, the complexities fit in the third position after alignments, but before resources thus limiting outcome to number 5.

As an alternative view of the previous analysis and one that uses storylines for the analysis, the researcher began to view as a CISO would from the data collected. The CISO must select the story most likely to succeed in meeting management's selection of a goal and align

next with the role to the mission of their organization using supplied resources. CISOs look at the summarized possible outcomes from Table 19, Table of Outcomes to Select, and read the story of using super categories in possible outcomes to create the most viable one. Thus, each plot would read as follows:

- Develop complexities of an information security strategy, consider strategic alignment, execute necessary roles, and be supplied by resources
- Develop complexities of an information security strategy, execute necessary roles, be supplied by resources, and consider strategic alignment
- Develop complexities of an information security strategy, be supplied by resources, consider strategic alignment, execute necessary roles
- Execute necessary roles, develop the complexities of an information security strategy, be supplied by resources, and consider strategic alignment
- Execute necessary roles, consider strategic alignment, develop the complexities of an information security strategy, and be supplied by resources
- Execute necessary roles, be supplied by resources, consider strategic alignment, and develop complexities of an information security strategy
- Consider strategic alignment, execute necessary roles, develop complexities of an information security strategy, and be supplied by resources
- Consider strategic alignment, develop complexities of an information security strategy, be supplied by resources, and execute necessary roles
- Consider strategic alignment, be supplied by resources, execute necessary roles, and develop complexities of an information security strategy
- Be supplied by resources, develop complexities of an information security strategy, consider strategic alignment, and execute necessary roles
- Be supplied by resources, consider strategic alignment, execute necessary roles, and develop complexities of an information security strategy
- Be supplied by resources, execute necessary roles, develop complexities of an information security strategy, and consider strategic alignment

From the statements in the bulleted list, analysis could help eliminate the majority of assertions. The first set of three bullets can be dismissed, since the 'develop complexities of an information security strategy' is the outcome of alignments working together to reach consensus. The strategy captures the agreements. The second set of three bullets, 'executing necessary roles' captures the essence of what a CISO does as a result of aligning to a strategy, which is a primary outcome. The third set of three bullets, 'consider strategic alignment' is the action a CISO performs to gauge leadership of the organization, aligning it to the way in which the

strategy is crafted and is an outcome of the alignment of leadership working together to reach consensus. Alignments work in tandem with the strategy as it is the way work is done to codify the strategy. The fourth set of three bullets, 'be supplied by resources' considers the sustainment of the information security program after consensus is reached among leadership for a role and an alignment and a strategy or a plan is codified to propose the way to achieve the information security strategy, but it is the actions taken by the CISO which implements the strategy. The CISO must choose the role they play in moving towards completion. Thus the outcome would come from the second set of three.

Looking again at the second set of three, beginning with the words 'execute necessary roles,' The CISO investigates management's alignment, as one where security operates on its own, with information systems, with business, or with the cooperation of business and information systems, recognizing who is in charge and working through the process to reach an outcome. This is the alignment that the CISO moves towards to achieve the goals of their information security program. The complexities are the vision of the CISO to gain alignment and consensus to achieve the desired outcomes of confidentiality, integrity, and availability of data and the information systems they are responsible for and to work with available resources provided to accomplish the information security program.

The story from the matrix presented in Table 19, Table of Outcomes to Select, shows the best outcome of a CISO as the ability to select a role, determine an acceptable alignment and match complexities to a desired outcome. The CISO accomplishes all these actions while working within the scope of available resources. The CISO should "execute necessary roles, consider strategic alignment, develop the complexities of an information security strategy, and be

supplied by resources." The following discussion looks at an analysis of the data after selecting this narrative or story of the super categories.

The researcher needed to select and support the statement best capturing the results of open and axial coding. Using the reflective coding matrix, the researcher combined the super categories and found that the CISO recognizes and selects a role or combination of roles they deem necessary to perform the mission of information security. The CISO seeks to align their vision of the strategy to the direction of the organization. In their organization they may need to be with business, information system, on their own, or some combination of the three. The CISO then begins to construct the strategy to achieve the vision and align to stakeholder's requirements using the supplied resources. Evaluating the processes or casual conditions in the reflective coding matrix, the information revealed that CISOs focused on the roles chosen to implement a strategy. Role selection was seen as the primary area the CISO could control, because they had the freedom to decide in which way to operate. Role selection turned into a complicated process that they had to consider the outside factors of alignment and the strategy developed to meet their mission which also had to support organizational goals. While designing the way in which their part of the organization formed, the CISOs, by consensus stated their program must be forward looking. Respondent Q3 (personal communication, January 23, 2014) stated, "The information security strategy boils down to and in its simplest definition is the forward looking strategy a leader has in their head to address information security problems of today, but also for tomorrow as well." They needed to have a strategy of a manageable size consisting of three to four goals, and these goals needed to be achievable or attainable within a set period of time. Mostly this was defined as a fiscal year, from October first through September thirtieth of the following year. The strategy must define what is important and what is to be protected. It must also foster a

culture of security presenting ways in which to develop and foster a participative community amongst users of the organization. Information security professionals must be communicative and collaborative around the organization. Cultivating and germinating security to the general populace of the organization. The next section considers the CISO as the linchpin of the organization and the deciding factor in which way the information security program leans using their role, alignment, and complexity (strategy) in the organization.

4.4 The Result

The previous sections considered the categories used by the CISOs and discovered ways to work and implement their information security programs. In this final section, the analyzed data is studied to produce the steps a CISO follows to investigate their role with the information security strategy. Using the data collected, following the discovery process the CISO investigates where or how they should align with leadership and choose the best role to start with. If receptive, the CISO aligns with business and or information systems, and participates with the development of a strategy, forming the framework of a strategy. If leadership is not receptive, the alignment either leans towards information systems or remains within the information security environment leaning on regulatory requirements as their force for compliance by law. If there is an unlikely situation where leadership does not participate, yet dictates that no security shall be practiced or only to a level such as that which only obtains system certification and accreditation to operate. The organization devolves into an ad hoc situation wherein the CISO is always reactive and does not achieve desired goals. Respondent J7 (personal communication, December 31, 2013), stated it best by saying, "Unfortunately, our priorities are based on a reactive methodology. I have priorities clearly communicated to leadership, to my staff, and to others, but unfortunately being we are so short staffed, we cannot

execute those priorities effectively and when something happens all those priorities are pushed to the side to fix a top priority at hand." The data in the study revealed that none of the programs reached the extreme end of having no security, but in certain situations some CISOs were required to implement systems without proper controls, especially where new technology was involved.

The way to explain this is that the CISO works to align their strategy by speaking directly with leadership. From the start, the CISO seeks where in the alignment process they are situated. Whether they are operating on their own, or with information systems, business, or both. The formation of a strategy is devised by a consensus process of the three stakeholder groups (business, information systems, and information security) working together or by being directed and agreeing to some form of direction. A discussion ensues back and forth from the CISO during the forming stage of the strategy and there are some possible extra steps back through leadership as the CISO confers with leadership on a direction (in the alignment step), until consensus is reached. Once the strategy is formed, the CISO identifies the goals listed and makes the decisions to select a role for implementation of the strategy to achieve the goals. Figure 8, CISO Actions to Achieve a Strategy, depicts this aforementioned process.

Once decided, the role selected was applied, the strategy is implemented and resources are utilized to accomplish the implementation. The CISO then makes the final decision as to which role to select that is then used to work the strategy goals and implement them for the completion of the information security program, realizing the agreed upon goals. Resources help to implement the strategy and achieve goals. Figure 8, CISO Actions to Achieve a Strategy, depicts this emergent method of action, the story of how CISOs in a large organization systematically operated.

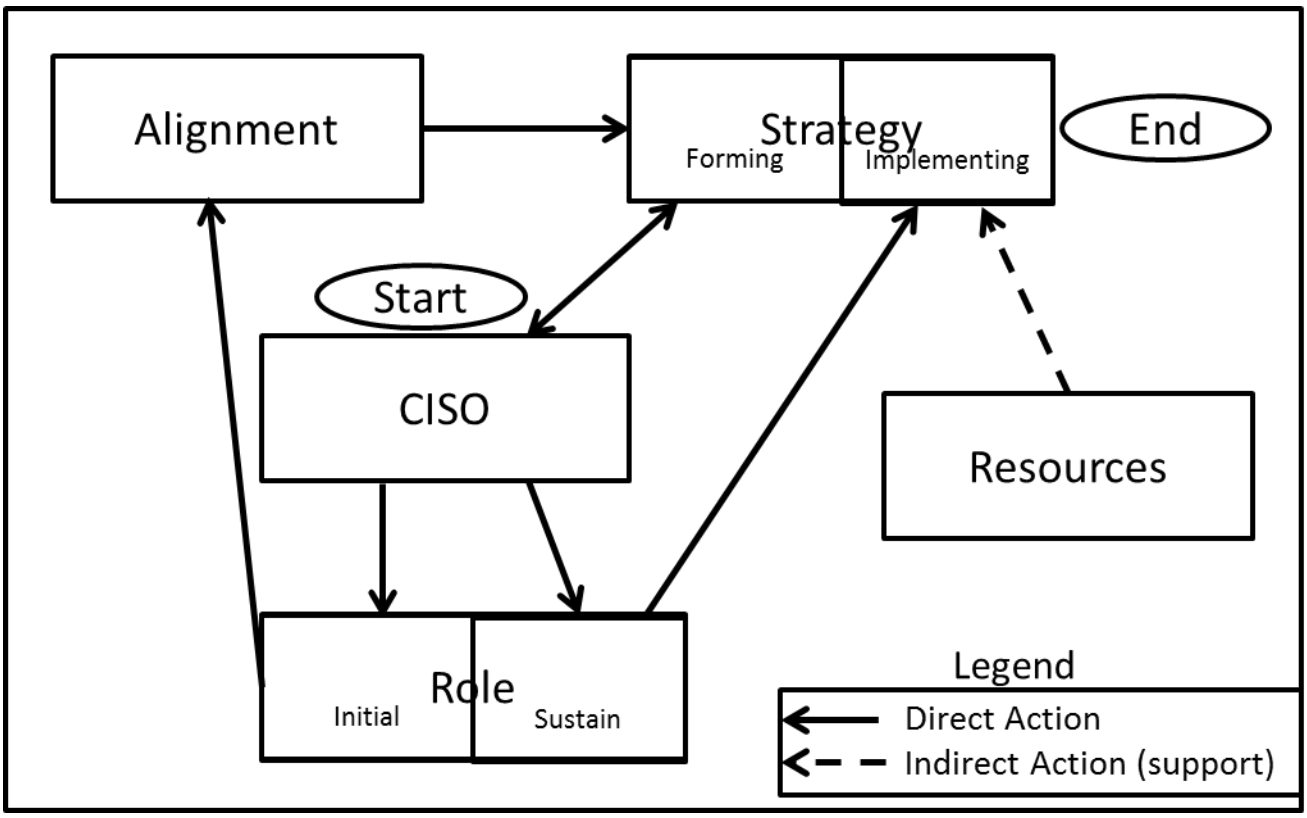

Figure 8. CISO Actions to Achieve a Strategy

As a step by step explanation of the process, the CISO initially chooses a role (most often one of compliance, based in law). The CISO coordinates with stakeholders to decide upon on alignment. The alignment step is a cyclic action between CISO, role, alignment, Strategy (formation), until stakeholders form a strategy. Once the strategy is formed, the CISO in the second part selects role(s) to sustain operations for implementing the strategy and is indirectly assisted with resources to achieve the strategy at the end.

Conspicuously, the four super categories have dependencies that show relationships between roles, alignments, complexities, and resources (refer to Figure 6, Super Categories). A breakdown of the four super categories is covered under the axial coding results section and is illustrated in Figure 7, Mapping the Categories. Taking figure 6, Super Categories and Figure 7, mapping the categories, the researcher deduced the interplay into Figure 8, CISO actions to

achieve a strategy. In most organizations, CISOs have assumed a role, have an alignment, and they have limited resources, but most do not have a strategy. They are left to fend for themselves in many situations where incidents occur. As Respondent Q3 (personal communication, January 23, 2014) reported, "If I sum it up, we react to fires every day and would not be able to keep up with it. So when you have an information security strategy, it would allow you to be proactive and address the problems."

CISOs have assumed a role. By the analysis, many CISOs were left to find out their own roles for any given situation. Either management did not give any direction as to what was required and the CISO ended up creating their own strategy or the CISO just reacted to each incident as it transpired. The role most often assumed was that of compliance, as depicted in the super category roles (refer to Figure 2, Roles) and depicted in the lower right hand corner of Figure 7, Mapping the Categories. The compliance role had a central position, as all CISOs identified compliance as a must do activity. This section details the CISO action to select an initial role.

Most CISOs had an alignment. The information gleaned from an analysis of the data collected showed there were two main alignments for CISOs. Firstly, there was a large number of CISOs who were aligned with the CIO (information systems) and business. These CISOs had a relationship built with their leadership and kept them informed of risk and abided by the decisions leadership specified. Secondly, there was a large number of CISOs who had no alignment and were left out of the leadership's activities and essentially these CISOs were always performing information security duties in a purely reactive mode. "Unfortunately, our priorities are based on a reactive methodology (Respondent J7, personal communication, December 31, 2013). They were always working on cleaning up incidents as opposed to having

a strategy that could look to prevent events from transpiring. The CISOs without an alignment did desire to know what leadership was involved with and ultimately could help leadership make informed decisions, but were excluded from taking part in system development prior to implementation. There were a few CISOs who operated solely under the direction of the CIO and a single CISO who worked directly with the business function. For the most part, the CISOs that associated and worked with business and the CIO were from larger units in the organization. The CISOs from smaller units in the large organization were left to either create their own rules or were always remediating situations management found themselves in by ignoring information security. This covered the interactions between CISOs, roles, and alignments as depicted in Figure 8, CISO actions to achieve a strategy.

Most CISOs did not have a strategy. When pressed closer, the CISOs stated that they did not have a formal strategy. The CISO that had only an informal strategy stated they did not have time to write a formal strategy and they simply performed duties as they were required, operating very tactically patching one incident after another without gaining any headway in the process. One CISO stated they had a formal strategy, but it was not approved yet. Respondent Z7 (personal communication, February 19, 2014), stated, "There is nothing in place, we try to build a management directive, internal for an information security strategy, but it is not formalized, so I will not elaborate on it until it is finalized." A few other CISOs said they utilized the CIO's strategy as their own. It was most preferable to have their own, but the CISO stated they would accept the larger organization's strategy or even working under the CIO as a back up plan. Many stated they referred to the strategy written by the CISO from the headquarters or lead unit in the organization. All stated that the strategy involved a lot of hard work. The work involved teams, coordination, and mechanics for developing the vision against mission needs and arriving at

goals for information security. Much of the development process goes beyond the scope of the study here. The main thrust being to coordinate the inputs to capture goals, and codify them with other stakeholders in their organization. This embodies the hard work of forming the strategy through interactions of stakeholders, CISOs, and teams who work for the CISO.

Having the strategy, the cycle would be almost complete, but the influence of resources does play a part in investigating roles of the information security strategy. Most CISOs have limited resources. Some CISOs had an abundance of funds and were able to guide personnel into career paths beneficial to the large organization. Most had budgets that would only allow some assets to be expended towards personnel development. Resources were a vital enabler of the CISO's ability to perform the information security program. Funds were dispersed and the CISO always balanced the addressing of risk by its highest priority. Often the CISO did not have enough, but did make do with the amounts of funding allotted to them.

Therefore, as presented in Figure 8, CISO Actions to Achieve a Strategy, this represents all the actions associated with the CISO achieving strategy. The interview question rationale was sound and resulted in the grounded theory coding process of all the collected data to reveal a theory. The story emerging from the data and hence the theory coming forth from the data fits this statement: The CISO selects a role to align with the mission and develops a strategy (complexities) that uses available resources. The statement can be shortened form is the CISO actions to achieve a strategy and in a longer form could be the following story. The CISO starting with compliance as a role works with business and information systems in alignment to develop a strategy that addresses mission risk adequately with a budget to support qualified personnel adequately trained and equipped with pertinent tools. The CISO adjusts the role to suit the needs of addressing mission risk to the business and information system executives.

Chapter 5

Conclusion, Implications, Limitations, and Recommendations

5.1 Introduction

Through this study, the research has been around investigating information security strategy and the roles a CISO can choose to implement it (Chen, et al., 2010; Leidner, et al., 2011), how the information security strategy and role selection can be advanced and to be more proactive (Seeholzer, 2012). And, that this advancement can contribute towards yielding a proactive implementation of a strategy through the proper role selection, alignment direction, and usage of resources towards accomplishing objectives. Future research may validate the theory that emerged from the collected data in Chapter 4 and resultant model of the CISO actions to achieve a strategy.

5.2 Conclusion

The results of this study led to an understanding of the complexities with information security strategy in a large government organization. It revealed a theory that can help CISOs to ascertain whether certain types of information security strategy are preferable to other forms of information security strategy and how to tailor it. The study might also prove helpful to evaluate how information security strategies differ within large governmental organizations, by using the model to investigate specific scenarios, depending upon the variables supplied for all the inputs. This study's findings might feed into an advanced theory of role selection to assist information security professionals in selecting role(s) appropriate to implementation of an information security program.

The researcher asserted that from the review and analysis of the available literature and data collected, that several results came from the analysis. One of the expected results found that

many of the role categories advanced in the literature review, held as written. Some participants expressed the roles with differing names, but the categories tracked along the same explanations advanced for the categories in the review of the literature. It did come to pass that four of the role categories proved to be somewhat inconsequential in a large government organization. Those roles were public image, competitor, re-organization and power relationships. The categories identified in roles, even though found inconsequential in the large government organization, may however hold up under educational, commercial, or other public sector environments. The review of the literature did advance several cases in the commercial sector for the categories listed as inconsequential.

The section of the literature review on alignment of strategies did find the same categories, but with differing results. The majority of CISOs in the public sector had fewer written strategies as opposed to the ideals presented in the literature review. This was verified from the interviews, as CISOs expressed their support of the business and information systems strategies, but identified the lack of their own information security strategies. Further, the interviews revealed a severe lack of models for dealing with strategy inside of information security offices within organizations.

The results of the collected data revealed more than just definitions of information security and basic information about the information security program. Most of the CISOs went into detailed discussions of obstacles and challenges they faced on a near daily basis as they struggled to prevent data loss breaches and incident responses to the new threats and exploits the network is exposed to from every entry point (Hutchins, Cloppert, & Amin, 2011; OIG, 2012; Suddaby, 2006). Table 20, Challenges and Obstacles, gleaned the major challenges CISOs faced within their organizations.

Some CISOs led complicated discussions of how information security supported and often supplemented the business strategy, adding value in unexpected areas. For example, in cases where security is involved from the start, it gets built in and prevents unnecessary expenditures later on. The researcher conducted the interviews using a repeatable process, with the results that all the interviews reflected unbiased views from the differing sub organizations of the large organization, that all ended up supporting an overall organizational security program (Duffy, et al., 2006; Hirose, Itao, & Umeda, 2012; Wimpenny & Gass, 2000).

Table 20. *Challenges and Obstacles*

Respondent	Challenge Faced
G7	-Helping the organization see the big picture of information security was often a challenge. Often I had to devise creative ways, many times behind the scenes to get some semblance of information security incorporated into the system.
H8	-The challenge for us is that we have a lot of things to do, but our budget is so severely slashed. So it has been really hard to do. -It was a challenge to try and align all the various strategies, plans and guide books for the overall organization. Also, the White House came out with things to make it harder still to align all the pieces.
M7	- We are always fighting over budget, having the budget authority to obtain the necessary equipment. The CIO has a different prioritization which tends to be a challenge.
V8	- I have the challenge of sub organizations. I have to build on information security strategy that is compelling enough that others will want to align with ours. I do not do it in a vacuum. I don't want to put it in a paper and make it something they must, but rather something they went to support and adopt. What do I need to push to have them get behind it. Get them involved rather with you, then you can get buy-in. -Often times the challenge of the job here is that we have all the responsibilities and accountability, but we do not have the authority. Even though the Clinger Cohen Act gives it, we do not have the authority. You have to have the ability to have political influence to get them to move priority to catch up and get done.
X9	- There is a problem in quantifying the risk. With this, it is challenging to build a repeatable process. I built the proposed model for characterizing threat, but I do not know if it reached the point of repeatability. It is very hard to build the repeatable process and without a repeatable process it is even harder to get measurements or metrics of the process.

5.3 Implications

Since the fundamental understanding of information security roles used to implement an information security strategy in an organization is lacking, most implementations in government organizations equated the information security strategy to a technically related solution, implementing tools and monitoring controls (Seeholzer, 2012). This was supported by the interviews conducted with the majority of CISOs as they highlighted their ad-hoc security environments. The challenge is to distribute the information presented in this study, so that the CISOs can assist executives in aligning strategic goals and objectives and help them in developing roles that fit into an agreeable alignment. The use of constructivist grounded theory complicated and required interpretive skills to correctly delve into the collected data and extract the categories from the myriad levels of responses given by the executives taking part. Considerable time was necessary to arrive at a coherent story through coding of the data and use of comparative analysis.

5.4 Limitations

The main limitation was obtaining unbiased responses from the participants. For each of the interviews, the researcher kept the interviews unrehearsed, not allowing the CISOs to preview the questions prior to the interview, it was a spontaneous discussion of the questions. The researcher also limited the boundary of the questions, remaining explicitly in the arena of information security strategy and the roles an individual could assume to meet the objectives and goals. A delimitation for this study kept the study focused solely on the questions without deviating from the subject; maintaining the same core questions with each participant. The researcher also kept distant with the participant in order to obtain unbiased responses.

Another limitation was the population selected the number of CISOs in the geographic area was limited. The generalizability to the greater population was a consideration, in that the research utilized individuals residing within the National Capital Region of the United States, generally around the greater Washington, DC area. Even though this study queried respondents from each of the sub units of the large government organization, it might not represent all organizations. Further, since it is difficult to assimilate the key factors from all studies within the information security domain, it cannot be assumed that all roles influencing information security strategy were represented within this study. It could be surmised that other roles not part of this study may impact an information security strategy of an organization.

Finally, while participants were assured of non-disclosure and that data was collected in a way to minimize respondent reservation, it would be difficult to ensure respondents were completely free of mistrust. There could be some underlying fear of providing information security information to an outside source. This assumption has been seen as problematic when conducting research into information security areas (Kotulic & Clark, 2004).

5.5 Recommendations

The phenomena or properties of the roles a CISO must consider needs to encompass how to address threats, vulnerabilities, and weaknesses common to the information security strategy (Ransbotham, Mitra, & Ramsey, 2012). The information security field stands on the precipice of going from a purely reactive world, addressing threat as it is discovered to be one of a more predictive nature of the threats being encountered prior to an actual exploit. CISOs currently and expressly focus on a reactive approach documenting and implementing static controls to protect data and assets under their purview. This must change in that as the protections increase the threat moves to other more unprotected areas. For example, the main CISO of an organization

lobbied and obtained permission to block webmail, the single greatest entry point of malware, through directed emails, attachment downloading, and execution. Now, threat actors have moved and evolved their attacks towards other attack vectors as Heartbleed (Durumeric, et al., 2014) and Bash/Shellshock did (Security Research and Emergency Response Center of Anity Labs (Anity CERT), 2014; Trend Micro Threat Research Lab (TMTRL, 2014) in an attempt to gain logon credentials. CISOs need to adapt and change from reactive towards a more proactive approach. The beginnings of this shift were gleaned from the interview responses to the interview questions, such as "…what capabilities are necessary for a successful information security strategy?" (Chapter 3, Table 5, Interview Question Rationale). This question found a shift in response from CISOs of the desire to move from reactive towards a proactive outcome. Respondent M7 (personal communication, April 14, 2014) said the CISO must, "Clearly articulate the risk of a decision by management that would put data at risk and it must be proactive and not reactive in decisions." The researcher gained a vision for a trend of moving from reactive, through an interim stage of a hybrid approach with both reactive and proactive approaches, and then towards a more proactive, threat driven approach. Figure 9, Trends, illustrates the move from a reactive to a proactive information security program.

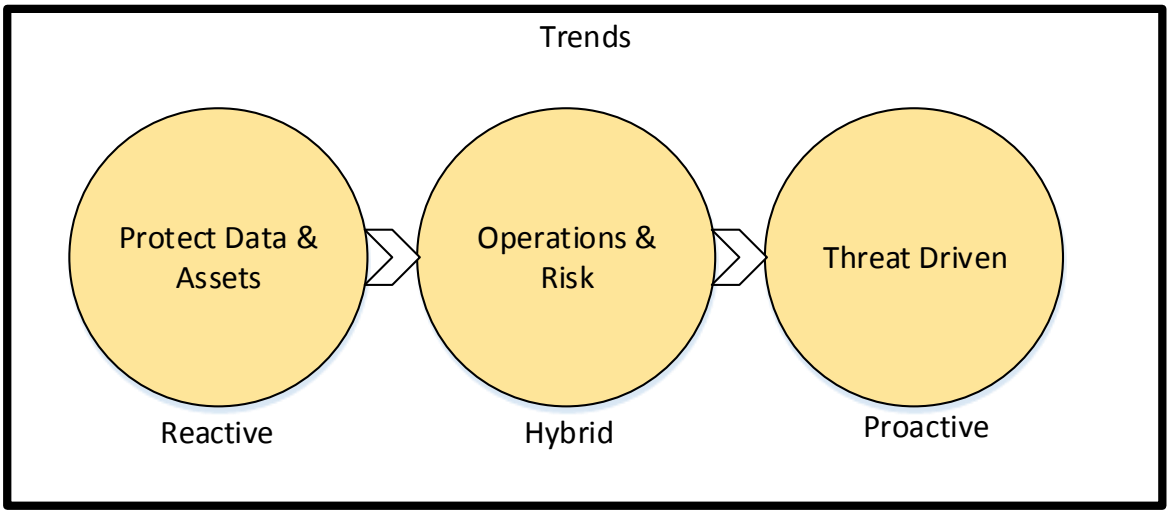

Figure 9. Trends

Future work can expand into how this could take place and how roles, alignments, and strategy (complexities) adapt to the new fluid environment. Lastly, CISOs indicated that for years, the model of a hardened perimeter has held and was easily defended against. Now however, with the introduction of cloud, mobile, big data, virtualization, and other emerging technologies, those boundaries no longer hold. How does the CISO change to react to the new paradigm of network layers vice a perimeter defense model? These would be areas to explore in the future.

The relevance and significance of the study adds to the knowledge base around understanding the complexities of information security strategies and roles associated in adopting methods to accomplish the goals and objectives of the information security strategy. The problem developed in that the complexity of an information security strategy has not been explored for developing strategy and the selection of roles to support it. The population segment of the information security community affected by this phenomenon are executives in information security, the CISOs and other executives charged with oversight of information security for an organization. The problem ranges over all of the organizations with information security programs and to a lesser extent in smaller organizations. The focus of the study centered on large government organizations, but might be helpful if the emerging model scales down to smaller organizations or could be scaled to fit any size organization in the public sector. Adapting the findings by applying the theory may result in tailoring an information security strategy and role development for organizations.

Other studies might attempt to address the problems of complexity, but possibly might not arrive with a theory for selecting a role development model for information security strategy. Without the theory developed here, the perpetuation of role selection schizophrenia will

continue, with a reactive selection of roles to address immediate problems as they occur instead of evaluating an overall direction and proactively investigating root causes to eliminate the core of the problem. Too often the easier route is to gain temporary results, than to address the root problem. Avoiding it will only see the problem resurface six months to a year later in the same vein; albeit with slight modifications, such as the newest variant of a virus to fool the heuristic analysis of an anti-virus program. The introduction of Stuxnet (Lee, 2012), followed by Flame (Bencsáth, Pék, Buttyán, and Félegyházi, 2014), and then by Regin (Symantec Security Response (SSR), 2014) illustrates the adaptive nature of the threat that CISOs and businesses must adapt to in order to secure data and assets.

This research study addressed the issue of information security strategy complexity by offering a theory that allows the practitioner to assess, analyze, and adapt roles for meeting the objectives and goals of the information security program through said strategy. Implementation of the theory will assist in proactively addressing the need to get past the cyclic reactive nature of information security and get to a proactive culture of security moving forward in an organization. Acceptance of the theory and testing of various organizational sizes and types will prove its generalizability and usefulness across a spectrum of organizations. Future studies may consider other qualitative methods. Also, further implementation may lead to organizations adopting the theory, creating a model and quantifiably test the theory for empirical data.

5.6 Summary

This study presented research that has implications for practitioners of information security. On one level, organizations having reactive information security strategies will find guidance to assist in their efforts to identify which role to select to accomplish their information security program goals and objectives. Organizations with large and unfocused information

security can utilize the findings to focus their role selection to proactively accomplish the goals and objectives identified in their information security strategy. Having a more focused selection process will save an organization money and time. Finally, the theory developed from emergent data will allow a CISO to adapt to changing situations according to the data supplied by outside factors. Once establishing the theory and testing empirically, then further usage of the theory may take place to develop metrics and measures to lend to the quantitative testing of the model and provide further empirical evidence of the model's effectiveness.

Appendix A

Interview Questions

1. In your opinion, what is information security strategy?

2. What does security strategy mean to you? And to this organization?

3. What is the role you take to accomplish information security strategy?

4. Can you elaborate on how you arrive with your strategic priorities for information security?

5. Can you describe the model (framework or system) of your information security strategy?

6. Can you describe how the implementation of information security strategy is tracked?

7. Thinking of security strategy, how do you manage the priorities of the large organization?

8. Can you explain what capabilities are necessary for a successful information security strategy?

Appendix B:

Initial Overall Analysis

Table B. *Overall Interview Analysis*

Strategy	Proactive	Reactive	Have one	Don't have one	Not Needed	Business	Bus/IT	IT	On its own	Ad-hoc	Top Down	Public Image	Competitor	Continual Change	Best Practice	Re-Organization	Power Relationship	Compliance
Respondent																		
A0	X			X			X				X				X			
B3		X		X				X										X
B8	X	X		X					X	X	X			X	X			
C7		X		X			X					X						X
D2		X							X					X				X
E3		X	X				X		X					X				
F5	X	X			X		X			X	X			X				X
G7		X	X	X				X		X	X							X
H8		X		X				X							X			X
I5	X	X					X		X					X	X			
J7		X		X							X			X		X		X
K2		X		X			X				X				X			X
K5	X			X		X						X		X	X			
L9	X								X					X	X			
M2	X		X				X				X			X	X			
M7		X	X				X			X	X							X
N5	X	X		X			X			X	X			X				X
O9		X		X					X		X		X					X
P4	X			X					X						X			X
P5		X			X		X								X			X
Q3		X		X			X				X				X			
R2		X		X			X								X			X
S1		X		X			X		X		X				X			X
T5	X			X		X			X						X			X
T8		X		X						X	X						X	
U2	X		X				X		X					X	X			X
V8	X		X				X		X			X		X	X			
W3	X			X			X							X	X			
X4	X	X		X			X						X	X				X
X9	X			X		X			X	X				X	X		X	
Y4		X		X			X								X			X
Z7		X		X					X	X				X			X	

Table B1, Overall Interview Analysis, consists of an overall evaluation of each of the interviews and classifying them under four separate areas. First, each respondent's interview was evaluated for being proactive, reactive, or having elements of each within the interview responses given to the interviewer. The second area considers the respondent's status as having a strategy of some sort, not having one, or stating they do not need a strategy. By some sort, the person either had a written strategy, one in the process of approval, or used a higher level organizational information security strategy. The two instances of stating they did not need a strategy stems from the fact that the respondent stated they used the chief information officers (CIOs) strategy instead of an information security strategy. The third area under review evaluated the strategy alignment that the respondent steered their organization towards, either business, business and information systems, information systems, information security, or ad hoc alignments. There were instances where a respondent exhibited more than one type of alignment. The fourth area evaluated the respondent's role as described in response to the interview questions as either one of the following or a combination of multiple roles: top down, public image, competitor, continual change, best practice, re-organizer, power relationship, and or compliance.

References:

Abbas, H., & Hemani, A. (2010). Addressing dynamic issues in information security management. *Information Security Management, 19*(1), 5-24.

Ahuja, S. (2009). *Integration of COBIT, balanced scorecard and SSE-CMM as a strategic information security management (ISM) framework.* (CERIAS TR 2009-21), West Lafeyette, IN: Perdue University. Retrieved from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2009-21.pdf.

Aivazian, C. (1998). Information security during organizational transitions. *Information Strategy: The Executives Journal, 14*(3), 21-26.

Al-Hamdani, W. A. (2009). Three models to measure information security compliance. *International Journal of Information Security and Privacy, 3*(4), 43-67.

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

Allan, G. (2003). A critique of using grounded theory as a research method. *Electronic Journal of Business Research Methods, 2*(1). 1-10.

Allen, J. (2005). *Governing for Enterprise Security.* (Technical Note CMU/SEI-2005-TN-023), Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute. Retrieved from http://www.cert.org/governance/, 1-81.

Allen, L. M. (2010). A critique of four grounded theory texts. *The Qualitative Report, 15*(6), 1606-1620.

Alter, S. (2008). Defining information systems as work systems: Implications for the IS field. *European Journal of Information Systems, (17)*5, 448-469.

Amaio, T. E. (2009). *Exploring and examining the business value of information security: Corporate executives' perceptions.* Available from ProQuest Dissertations and Theses database (UMI No, 3351834).

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

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313.

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

Arce, I., & Levy, E. (2009). An analysis of the slapper worm. *IEEE Security & Privacy, 1*(1), 82-87.

Avgerou, C., & McGrath, K. (2007). Power, rationality, and the art of living through socio-technical change. *MIS Quarterly, 31*(2), 295-315.

Backhouse, J., Hsu, C.W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly, 30*(Aug2006 Supplement), 413-438.

Backman, K., & Kyngaes, H. A. (1999). Challenges of the grounded theory approach to a novice researcher. *Nursing and Health Sciences, 1*(1), 147-153.

Badr, Y., Biennier, F., & Tata, S. (2010). The integration of corporate security strategies in collaborative business processes. *IEEE Transactions on Services Computing, 99*(1), 1-14.

Baptista, J., Newell, S., & Currie, W. (2010). Paradoxical effects of institutionalization on the strategic awareness of technology in organisations. *Journal of Strategic Information Systems, 19*(3), 171-183.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys, 25*(4), 375-414.

Baskerville, R. L., & Dhillon, G. (2008). Information systems security strategy, a process view. In D. W. Straub, S. Goodman, & R. L. Baskerville (Eds.), *Information Security, Policies: Processes and Practices, Advances in Management Information Systems,* Volume 11, (15-45). Armonk, NY: M. E. Sharpe, Inc.

Bechtold, B. (1997). Chaos theory as a model for strategy development, *Empowerment in Organizations, 5*(4), 193-201.

Bencsáth, B., Pék, G., Buttyán, L., and Félegyházi, M. (2014). The cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet 2012*(4), 971-1003.

Bhalla, N. (2003). Is the mouse click mighty enough to bring society to its knees? *Computers & Security, 22*(4), 322-336.

Booker, R. (2006). Re-engineering enterprise security. *Computers & Security, 25*(1), 13-17.

Bower, J. L., & Gilbert, C. G. (2007). How managers' everyday decisions create-or destroy-your company's strategy. *Harvard Business Review, February*(2007), 2-9.

Brown, M., & Cregan, C. (2008). Organizational change cynicism: The role of employee involvement. *Human Resource Management, 47*(4), 667-686.

Brown, S. C., Stevens Jr., R. A., Troiano, P. F., & Schneider, M. K. (2002). Exploring complex phenomena: Grounded theory in student affairs research. *Journal of College Student Development, 43*(2), 1-10.

Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. *Information Security Technical Report, 17*(2012), 19-25.

Burwell, S. M. (2013). Fiscal year 2013 reporting instructions for the Federal information security management act and agency privacy management. *Executive office of the president, Office of Management and Budget,* Retrieved from http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf

Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems. *MIS Quarterly, 30*(2), 211-224.

Capability Maturity Model Integration (CMMI) Team. (2010). CMMI(r) for development, version 1.3. *Carnegie Mellon University, Software Engineering Institute, Technical Report, CMU/SEI-2010-TR-033,* Retrieved from http://www.sei.cmu.edu/reports/10tr033.pdf

Caralli, R. A. (2004). Managing for Enterprise Security. *Software Engineering Institute, Carnegie Mellon University.* Retrieved from http://www.sei.cmu.edu/reports/04tn046.pdf.

Carter, M., Grover V., & Bennett Thatcher, J. (2011). The emerging CIO role of business technology strategist, *MIS Quarterly Executive, 10*(1), 19-29.

Cerpa, N., & Verner, J. M. (1999). Case study: The effect of IS maturity on information systems strategic planning. *Information & Management, 34*(4), 199-208.

Chan, Y. E., & Huff, S. L. (1992). Strategy: An information systems research perspective. *Journal of Strategic Information Systems, 1*(4), 191-204.

Chan, Y. E., & Reich, B. H. (2007). IT alignment: What have we learned? *Journal of Information Technology, 22*(4), 297-315.

Chang, A. J.-T., & Yeh, Q.-J. (2006). On security preparations against possible IS threats across industries. *Information Management & Computer Security, 14*(4), 343-360.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361.

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis.* Thousand Oaks, CA: Sage Publications Ltd.

Chen, D. Q., Mocker, M., Preston, D. S., & Teubner, A. (2010). Information systems strategy: Reutalization, measurement, and implications. *MIS Quarterly, 34*(2), 233-259, A1-A8.

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly, 35*(2), 397-422.

Choo, K.-K., R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731.

Clark, T. L., & Sitko, T. D, (2008). Information security governance: Standardizing the practice of information security. *EDUCAUSE Center for Applied Research, Research Bulletin, 2008*(17), Retrieved from http://net.educause.edu/ir/library/pdf/ERB0817.pdf.

Cohen, K. J., & Cyert, R. M. (1973). Strategy: Formulation, implementation, and monitoring. *The Journal of Business, 46*(3), 349-367.

Collins, J. S. (2001). Pockets of chaos: Management theory for the process of computer security. *SANS Institute InfoSec Reading Room,* Retrieved from http://www.sans.org/reading_room/whitepapers/infosec/pockets-chaos-management-theory-process-computer-security_602.

Computer Security Division (CSD). (2004). Federal Information Processing Standards Publication (FIPS PUB) 199. Standards for security categorization of Federal information and information systems. *Information Technology Laboratory, National Institute of Standards and Technology,* Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

Corbet, B. (2014). Annual report to Congress: Federal Information Security Management Act. Office of Management and Budget, Retrieved from http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_report_05.01.2014.pdf.

Corbin, J., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criterias. *Qualitative Sociology, 13*(1), 3-20.

Corbin, J., & Strauss, A. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory.* (3rd ed.). Los Angeles, CA: Sage Publications, Inc.

Costello, T. (2011). 2011 IT tech and strategy trends. *IT Professional,13*(1), 61-64.

Creswell, J. W. (2002). *Research design: Qualitative, quantitative, and mixed methods approaches.* (2nd ed.). Thousand Oaks, CA: Sage Publications Ltd.

Creswell, J. W. (2011). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. (4th ed.). Upper Saddle River, NJ: Pearson Education.

da Veiga, A., & Eloff, J.H.P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372.

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. *EDP Audit, Control, and Security, 31*(10), 1-14.

Daneva, M. (2006). Applying real options thinking to information security in networked organizations. *Technical Report TR-CTIT-06-11, Centre for Telematics and Information Technology University of Twente, Enschede.* Retrieved from http://eprints.eemcs.utwente.nl/5703/01/0000018c.pdf.

Dawson, M., Berrell, D. M., Rahim, E., & Brewster, S. (2010). Examining the role of the chief information security officer (CISO) & security plan. *Journal of Information Systems Technology & Planning, 3*(6), 1-5.

de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D. F., Ren, J., Rode, J. A., & Filho, R. S. (2005). In the eye of the beholder: A visualization-based approach to information system security. *International Journal Human-Computer Studies, 63*(1-2), 5-24.

Devadas, U. M., Silong, A. D., & Ismail, I. A. (2011). The relevance of Glaserian and Straussian grounded theory approaches in researching human resource development. *Proceedings of the 2011 International Conference on Financial Management and Economics, 11*(2011), 348-352.

Dhillon, G. S. (1995). Interpreting the management of information systems security. *Department of Information Systems, London School of Economics and Political Science, Houghton Street, London WC2A 2AE, England*. Retrieved from http://csrc.lse.ac.uk/research/theses/dhillon.pdf.

Dhillon, G. (2004). Dimensions of power and IS implementation. *Information & Management, 41*(5), 635-644.

Dhillon, G. (2007). *Principles of information systems security, text and cases.* Hoboken, NJ: John Wiley & Sons, Inc.

Dhillon, G., Caldeira, M., & Wenger, M. R. (2011). Intentionality and power interplay in IS implementation: The case of an asset management firm. *Journal of Strategic Information Systems, 20*(4), 438-448.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293-314.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers and Security, 28*(3), 189-198.

Doughty, K. (2003). Implementing enterprise security: A case study. *Information Systems Control Journal, 2*(2003), 99-114.

Doherty, N. F., & Fulford, H. (2005). Do information policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal, 18*(4), 21-39.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security, 25*(1), 55-63.

Duffy, K., Ferguson, C., & Watson, H. (2004). Data collecting in grounded theory – some practical issues, *Nurse Researcher, 11*(4), 67-78.

Dunkerley, K. D. (2011). *Developing an information systems security success model for organizational context*. Available from ProQuest Dissertations and Theses database. (UMI No. 3456547).

Dunkerley, K. D., & Tejay, G. (2009). Developing an information systems security success model for egovernment context. *Americas Conference on Information Systems*, San Francisco, CA, 1-8.

Durumeric, Z., Li, F., Kasten, J., Amann, J., Beekman, J., Payer, M., Weaver, N., Adrian, D., Paxson, V., Bailey, M., Halderman, J. A. (2014). The matter of Heartbleed. Proceedings of the Internet Measurement Conference (IMC), Vancouver, BC, Canada, 1-14.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

Dynes, S., Kolbe, L. M., & Schierholz, R. (2007). Information security in the extended enterprise. *Proceedings in Americas Conference on Information Systems*, Denver, CO, 1-11.

Earl, M. J. (1993). Experiences in strategic information systems planning. *MIS Quarterly 17*(1), 1-24.

Eisenhardt, K. M. (1989). Building theories from case study research, *The Academy of Management Review, 14*(4), 532-550.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal, 50*(1), 25-32.

Eloff, M. M., & von Solms, S. H. (2000). Information security management: A hierarchical framework for various approaches. *Computers & Security, 19*(3), 243-256.

Ezingeard, J.-N., McFadzean, E., & Birchall, D. (2005). A model of information assurance benefits. *Information Systems Management Journal, 22*(2), 20-29.

Fairholm, M. R., & Card, M. (2009). Perspectives of strategic thinking: From controlling chaos to embracing it. *Journal of Management & Organization, 15*(1), 17-30.

Fitzgerald, T. (2010). Clarifying the roles of information security: 13 questions the CEO, CIO, and CISO must ask each other. *Information Systems Security, 16*(2007), 257-263.

Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT security breaches: What do investors think? *Information Systems Security, 12*(1), 22-33.

Gavetti, G., & Rivkin, J. W. (2005). How strategist really think, tapping the power of analogy. *Harvard Business Review, 83*(4), 54-63.

Geer, D. (2007). *Measuring security.* Paper presented at the Metricon 2.0 Conference. Retrieved from all.net/Metricon/measuringsecurity.tutorial.pdf.

Ghernouti-Hélie, S. (2010). A national strategy for an effective cybersecurity approach and culture. *Proceedings of the International Conference on Availability, Reliability and Security,* Krakow, PN, 370-373.

Gilbert, F. (2008). Is your due diligence checklist obsolete? Understanding how information privacy and security affects corporate and commercial transactions. *The Computer & Internet Lawyer, 25*(10), 13-18.

Glaser, B. G. (2002). Conceptualization: On theory and theorizing using grounded theory. *International Journal of Qualitative Methods, 1*(2), 1-31.

Glaser, B. G. (2012a). Constructivist grounded theory? *The Grounded Theory Review. 11*(1), 28-38.

Glaser, B. G. (2012b). Stop. Write! Writing grounded theory. *The Grounded Theory Review 11*(1), 2-11.

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative Research.* Hawthorne, NY: Aldine Publishing Co.

Goldkuhl, G., & Cronholm, S. (2010). Adding theoretical grounding to grounded theory: Toward multi-grounded theory. *International Journal of Qualitative Methods, 9*(2), 187-205.

Goluch, G., Ekelhart, A., Fenz, S., Jakoubi, S., Tjoa, S., & Mück, T. (2008). Integration of an ontological information security in risk aware business process management. *Proceedings of the 41st Hawaii International Conference on Systems Sciences,* Maui, HI, 1-9.

Grant, R. M. (2005). Contemporary strategy analysis: s, techniques, applications. In D. Q. Chen, M. Mocker, D. S. Preston, & A. Teubner. (2010). Information systems strategy: Reutilization, measurement, and implications. *MIS Quarterly, 34*(2), 233-259.

Grobler, T., & Louwrens, B. (2005). New information security architecture. Retrieved from http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/046_Article.pdf, 1-12.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security, 13*(4), 297-310.

Hall, J. M., Sarkani, S., & Mazzuchi, T. A. (2010). Moderating roles of organizational capabilities in information security. *Proceedings of the 5th International Conference on i-Warfare & Security*, Dayton, OH, 427-436.

Hall, J. M., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, *19*(3), 155-176.

Hallberg, L. R.-M. (2006). The "core category" of grounded theory: Making constant comparisons. *International Journal of Qualitative Studies on Health and Well-being, 2006*(1), 141-148.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems, 20*(4), 373-384.

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

Hinde, S. (2000). New millennium, old failures. *Computers & Security, 19*(2), 119-127.

Hinde, S. (2003). Cyber-terrorism in context. *Computers & Security, 22*(3), 188-192.

Hirose, Y., Itao, K., & Umeda, T. (2012). Generating a new interview method. *Proceedings of the 11th European Conference on Research Methods*, Reading, United Kingdom, 161-170.

Hofer, C. W., & Schendel, D. (1978). Strategy formulation: Analytical s. In D. Q. Chen, M. Mocker, D. S. Preston, and A. Teubner. (2010). Information systems strategy: Reualization, measurement, and implications. *MIS Quarterly, 34*(2), 233-259.

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243-248.

Howard, J. D., & Longstaff, T. A. (1998). A common language for computer security incidents. *Sandia Labs,* SAND98-8667. Retrieved from www.cert.org/research/taxonomy_988667.pdf.

Howard, M., & Kilmartin, W. (2006). Assessment of benchmarking within government organizations. *Accenture,* Retrieved from http://www.accenture.com/us-en/pages/insight-assessment-benchmarking-public-service-organizations-summary.aspx.

Hu, Q., Dinev. T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-659.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security - a neo-institutional perspective. *Journal of Strategic Information Systems, 16*(2), 153-172.

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

Hübler, A., Foster, G., & Phelps, K. (2007) Managing chaos: Thinking out of the box, *Complexity, (12)*3, 10-13.

Huehls, F. (2005). An evening of grounded theory: Teaching process through demonstration and simulation. *The Qualitative Report, 10*(2). 328-338.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Lockheed Martin Corporation,* Retrieved from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

Jirasek, V. (2012). Practical application of information security models. *Information Security Technical Report, 17*(2012), 1-8.

Johnson, A. M. (2009). Business and security executives views of information security investment drivers: Results from a Delphi study. *Journal of Information Privacy and Security, 5*(1), 3-27.

Johnson, A. M., & Lederer, A. L. (2010). CEO/CIO mutual understanding, strategic alignment, and the contribution of IS to the organization. *Information & Management, 47*(3), 138-149.

Jones, P. (2001). Organizational information security from scratch - a guarantee for doing it right. *SANS Institute InfoSec Reading Room*, Retrieved from http://www.sans.org/reading_room/whitepapers/standards/organizational-information-security-scratch-guarantee_541.

Jones, M., & Alony, I. (2011). Guiding the use of grounded theory in doctoral studies - an example from the Australian film industry, *International Journal of Doctoral Studies,* 6(2011), 95-114.

Kajava, J., & Siponen, M. (1996) Security management and organizations - bottom up or top down approach? *Proceedings of Nordic Workshop on Secure Computer Systems*, Gothenburg, Sweden, 1-12.

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

Kark, K. (2010). Twelve recommendations for your 2011 security strategy. *Forrester database,* Retrieved from http://www.forrester.com.

Kark, K., Penn, J., & Dill, A. (2009). Twelve recommendations for your 2009 information security strategy. *Forrester database*, Retrieved from http://www.forrester.com.

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

Keen, P. G. W., & El Sawy, O. A. (2010). Engaging in CIO-CxO "Conversations that matter": An interview with Peter Keen. *MIS Quarterly Executive, 9*(1), 61-64.

Kim, G. (2004). Does security set the right goals? *Security Management, 48*(6), 182.

King, W. R. (1978). Strategic planning for management information systems. *MIS Quarterly, 2*(1), 27-37.

Klaić, A. (2010). Overview of the state and trends in the contemporary information security policy and information security management methodologies. *Proceedings of the 33rd International Convention on Information and Communications Technology, Electronics and Microelectronics,* Opatija, HR, 1203-1208.

Knapp, K. J., & Boulton, W. R. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. *Information Systems Management Journal, Spring*(2006), 76-87.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security, 27*(5), 224-231.

Krutz, R. L., & Vines, R. D. (2001). *The CISSP prep guide: Mastering the ten domains of computer security.* New York, NY: John Wiley & Sons, Inc.

Kwok, K., McCallin, A., & Dickson, G. (2012). Working through preconception: Moving from forcing to emergence. *The Grounded Theory Review, 11*(2), 1-12.

Lacey, D. (2009). Understanding and transforming organizational security culture. *Information Management & Computer Security, 18*(1), 4-13.

Lacity, M. C., & Hirscheim, R. (1995). Benchmarking as a strategy for managing conflicting stakeholder perceptions of information systems. *Journal of Strategic Information Systems, 4*(2), 165-185.

Lapke, M. (2008). *Power relationships in information systems security policy formulation and implementation.* Retrieved from Virginia Commonwealth University Digital Archives http://etd.vcu.edu/theses/available/etd-05052008-164921/.

LaRossa, R. (2005). Grounded theory methods and qualitative family research. *Journal of Marriage and Family, 67*(November 2005), 837-857.

Lee, A. S., & Hubona, G. S. (2009). A scientific basis for rigor in information systems research. *MIS Quarterly, 33*(2), 237-262.

Lee, R. M. (2012). The history of Stuxnet – Key takeaways for cyber decision makers. *Armed Forces Communications and Electronics Association (AFCEA),* Retrieved from http://www.afcea.org/committees/cyber/documents/TheHistoryofStuxnet.pdf.

Leidner, D. E., Lo, J., & Preston, D. (2011). An empirical investigation of the relationship of IS strategy with firm performance. *Journal of Strategic Information Systems, 20*(4), 419-437.

Levy, D. (1994). Chaos theory and strategy: Theory, application, and managerial implications. *Strategic Management Journal, Summer 94*(15), 167-178.

Lindström, J., & Hågerfors, A. (2009). A model for explaining strategic IT-and information security to senior management. *International Journal of Public Information Systems, 2009*(1), 17-29.

Lomprey, G. R. (2008). Critical elements of an information security management strategy. *University of Oregon, Applied Information Management,* Retrieved from http://scholarsbank.uoregon.edu/jspui/bitstream/1794/7613/1/2008-lomprey.pdf.

Love, V. D. (2011). IT security strategy: Is your health care organization doing everything it can to protect patient information? *Journal of Health Care Compliance, 13*(6), 21-28, 64.

Loveland, G., & Lobel, M. (2011). Eye of the storm: Key findings from the 2012 global state of information security survey®. *Pricewaterhouse Coopers LLP*, Retrieved from http://www.pwc.com/giss2012.

Loveland, G., & Lobel, M. (2012). Changing the game: Key findings from the global state of information security® survey 2013. *Pricewaterhouse Coopers LLP*, Retrieved from http://www.pwc.com/giss2013.

Luftman, J., & Ben-Zvi, T. (2010). Key issues for IT executives 2009: Difficult economy's impact on IT. *MIS Quarterly Executive, 7*(2), 99-112.

Luftman, J., & Ben-Zvi, T. (2011). Key issues for IT executives 2010: Judicious IT investments continue post-recession. *MIS Quarterly Executive, 9*(4), 263-273.

Luftman, J., & Kempaiah, R. (2008). Key issues for IT executives 2007. *MIS Quarterly Executive, 9*(1). 49-59.

Ma, Q., Johnston, A.C., & Pearson, J.M. (2008). Information security management objectives and practices: A parsimonious framework. *Information Management & Computer Security, 16*(3), 251-270.

Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An integrated framework for information security management. *Review of Business, 30*(1), 58-69.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly, 34*(3), 431-433.

Markides, C. C. (1999). In search of strategy. *Sloan Management Review, 40*(3), 6-7.

Mata, F. J., Fuerst, W. L., & Barney, J. B. (1995). Information technology and sustained competitive advantage: A resource-based analysis. *MIS Quarterly, 19*(4), 487-505.

McClean, C., & Kark, K. (2010). Introducing the Forrester information security maturity model: A framework for describing and evaluating a comprehensive security program. *Forrester database*. Retrieved from http://www.forrester.com.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review, 31*(5), 622-660.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2011). Information assurance and corporate strategy: A delphi study of choices, challenges, and developments for the future. *Information Systems Management, 28*(2), 102-129.

Miller, D. (1981). Toward a new contingency approach: The search for organizational gestalts. *Journal of Management Studies, 18*(1), 1-26.

Mintzberg, H. (1985). The organization as political arena. *Journal of Management Studies, 22*(2), 133-154.

Mintzberg, H. (1987). Crafting strategy. *Harvard Business Review, 65*(4), 66-75.

Mintzberg, H. (1987b). The strategy concept I: Five Ps for strategy. In D. Q. Chen, M. Mocker, D. S. Preston, and A. Teubner. (2010). Information systems strategy: Reutilization, measurement, and implications. *MIS Quarterly, 34*(2), 233-259.

Mintzberg, H., Ahlstrand, B., & Lampel, J. (1998). Strategy safari: A guided tour through the wilds of strategic management. In R. L. Baskerville, & G. Dhillon, (2008). Information systems security strategy, a process view. In D. W. Straub, S. Goodman, & R. L. Baskerville (Eds.), *Information Security, Policies: Processes and Practices, Advances in Management Information Systems*, Volume 11, (15-45). Armonk, NY: M. E. Sharpe, Inc.

Mintzberg, H., & McHugh, A. (1985). Strategy formation in an adhocracy. *Administrative Science Quarterly, 30*(2), 160–197.

Mintzberg, H., & Waters, J. A. (1985). Of strategies, deliberate and emergent. *Strategic Management Journal, 6*(3), 257-272.

Moen, R. D., & Norman, L. C. (2000). Evolution of the PDCA Cycle. *Profound Knowledge Products Inc.*, Retrieved from http://pkpinc.com/files/NA01_Moen_Norman_fullpaper.pdf.

Moen, R. D., & Norman, L. C. (2009). The history of the PDCA cycle. *Proceedings of the Seventh Asian Network for Quality Congress,* Tokyo, JP, 1-12.

Newkirk, H. E., Lederer, A. L., & Johnson, A. M. (2008). Rapid business and IT change: Drivers for strategic information systems planning? *European Journal of Information Systems, 17*(3), 198-218.

Norman, A. A., & Yasin, N. M. (2010). An analysis of information systems security management (ISSM): The hierarchical organization vs. emergent organization. *International Journal of Digital Society, 1*(3), 230-237.

Office of the Inspector General (OIG). (2013). Evaluation of DHS' information security program for fiscal year 2012. *Department of Homeland Security,* Retrieved from http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-04_Oct12.pdf.

Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., & Kagaua, T. (2009). Information security governance framework. *Proceedings of the first Workshop on Information Security Governance,* Chicago, IL, 1-6.

Olsen, E. (2007). *Strategic planning for dummies.* Hoboken, NJ: Wiley Publishing, Inc.

Oreku, G. S., & Mtenzi, F. J. (2009). Using nature to best clarify computer security and threats. *Proceedings of the eighth annual International Conference on Dependable, Autonomic and Secure Computing,* Chengdu, CN, 702-707.

Pandit, N. R. (1996). The creation of theory: A recent application of the grounded theory method. *The Qualitative Report, 2*(4), 1-13.

Park, S., & Ruighaver, T. (2008). Strategic approach to information security in organizations. *Proceedings of the International Conference on Information Science and Security,* Seoul, KR, 26-31.

Parkin, S. E., & van Moorsel, A. (2009). *An information security ontology incorporating human-behavioral implications*. Newcastle University, Computing Science, Technical Report Series, CS-TR-1139, Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?, 1-15.

Pauleen, D. J., Corbitt, B., & Yoong, P. (2007). Discovering and articulating what is not yet known: Using action learning and grounded theory as a knowledge management strategy, *The Learning Organization, 14*(3), 222-240.

Pfeffer, J. (1992). Understanding power in organizations. *California Management Review, 34*(2), 29-50.

Pitt, L. F., Parent, M., Junglas, I., Chan, A., & Spyropoulou, S. (2011). Integrating the smartphone into a sound environmental information systems strategy: Principles, practices and a research agenda *Journal of Strategic Information Systems 20*(1), 27-37.

Porter, M. E. (1980). Competitive strategy: Techniques for analyzing industries and competitors. In D. Q. Chen, M. Mocker, D. S. Preston, & A. Teubner. (2010). Information systems strategy: Reutalization, measurement, and implications. *MIS Quarterly, 34*(2), 233-259.

Porter, M. E. (1996). What is strategy? *Harvard Business Review, 74*(6), 61-78.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security, 26*(3), 229-237.

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*(8), 638-646.

Preston, D. S., & Karahanna, E. (2009). Antecedants of IS strategic alignment: A nomological network. *Information Systems Research, 20*(2), 159-179.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121-139.

Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Are markets for vulnerabilities effective? *MIS Quarterly, 36*(1), 43-64.

Reich, B. H., & Benbasat, I. (2000). Factors that influence the social dimension of alignment between business and information technology objectives. *MIS Quarterly, 24*(1),81-113.

Rezakhani, A., Hajebi, A., & Mohammedi, N. (2011). Standardization of all information security management systems. *International Journal of Computer Applications, 18*(8), 4-8.

Rich, P. (2012). Inside the black box: Revealing the process in applying a grounded theory analysis. *The Qualitative Report, 17*(49), 1-23.

Robson, A. J. (2005). Complex evolutionary systems and the red queen. *The Economic Journal, 115*(504), F211-F224.

Rose, A. (2011). Information security frameworks fail without a supporting management system: Why security is not about controls. *Forrester database*, Retrieved from http://www.forrester.com.

Rowe, B. R., & Gallaher, M. P. (2006). Private sector cyber security investment strategies: An empirical analysis. *Proceedings of fifth Workshop on the Economics of Information Security,* Cambridge, UK, 1-23.

Rowlands, B. H. (2005). Grounded in practice: Using interpretive research to build theory. *Electronic Journal of Business Research Methodology, 3*(1), 81-92.

Rudd, J. M., Greenley, G. E., Beatson, A. T., & Lings, I. N. (2008). Strategic planning and performance: Extending the debate. *Journal of Business Research, 61*(2), 99-108.

Ruighaver, R. A. (2008). Organisational security requirements: An agile approach to ubiquitous information security. *Proceedings of the sixth Australian Information Security Management Conference,* Perth, AU, 1-7.

Salancik, G. R., & Pfeffer, J. (1977). Who gets power – and how they hold on to it: A strategic-contingency model of power. *Organizational Dynamics,* 5(3), 2-21.

Salmela, H., & Spil, T. A. M. (2002). Dynamic and emergent information systems strategy formulation and implementation. *International Journal of Information Management, 22*(2002), 441-460.

Scott, K. W., & Howell, D. (2008). Clarifying analysis and interpretation in grounded theory: Using a conditional relationship guide and reflective coding matrix. *International Journal of Qualitative Methods, 7*(2), 1-15.

Scully, T. (2011). The cyber threat, trophy information and the fortress mentality. *Journal of Business Continuity & Emergency Planning, 5*(3). 195-207.

Scully, T. (2013). The cyber security threat stops in the boardroom. *Journal of Business Continuity & Emergency Planning, 7*(2), 138-148.

Security Research and Emergency Response Center of Antiy Labs (Anity CERT). (2014). A comprehensive analysis on Bash Shellshock. *Anity Labs,* Retrieved from http://www.antiy.net/p/a-comprehensive-analysis-on-bash-shellshock-cve-2014-6271/.

Segars, A. H., & Grover, V. (1998). Strategic information systems planning success: An investigation of the construct and its measurement. *MIS Quarterly, 22*(2), 139-163.

Seeholzer, R. V. (2012). Information security strategy: In search of a role. *Proceedings of the Eighteenth Americas Conference on Information Systems (AMCIS),* Seattle, WA, 1-18.

Shariati, M., Bahmani, F., & Shams, F. (2010). Enterprise information security, a review of architectures and frameworks from interoperability perspective. *Procedia Computer Science, 3*(2011), 537-543.

Shoraka, B. (2011). *An empirical investigation of the economic value of information security management system standards.* Available from ProQuest Dissertations and Theses database (UMI No. 3456209).

Siponen, M. T. (2005a). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and Organization, 15*(2005), 339-375.

Siponen, M. T. (2005b). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems, 14*(3), 303-315.

Siponen, M. (2006). Information security standards focus on the next existence of process, not its content. *Communications of the ACM, 49*(8), 97-100.

Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems, 7*(7), 445-472.

Slater, D. (2002). Mistakes: Strategic planning don’ts (and dos). *CIO,* Retrieved from http://www.cio.com/article/print/31106, 1-4.

Slaughter, S. A., Levine, L., Ramesh, B., Pries-Heje, J., & Baskerville, R. (2006). Aligning software processes with strategy. *MIS Quarterly, 30*(4), 891-918.

Smedinghoff, T. J. (2005). The new law of information security: What companies need to do now. *The Computer & Internet Lawyer, 22*(11), 9-25.

Smith, E. E., & Medin, D. L. (1981). *Categories and concepts,* Cambridge, MA: Harvard University Press.

Smith, P. (2004). Developing & implementing an information security policy and standard framework. *SANS InfoSec Reading Room.* Retrieved from http://www.sans.org/reading_room/whitepapers/hipaa/developing-implementing-information-security-policy-standard-framework_1401.

Stanton, J. M., Guzman, I., Stam, K., & Caldera, C. (2003). Examining the linkage between organizational commitment and information security. *Proceedings of the IEEE Systems, Man, and Cybernetics Conference,* Washington, DC, 1-6.

Stocker, R., & Close, H. (2013). A novel method of enhancing grounded theory memos with voice recording. *The Qualitative Report, 18*(1), 1-4.

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

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(2), 441-469.

Suddaby, R. (2006). From the editors: What grounded theory is not. *Academy of management Journal, 49*(4), 633-642.

Symantec Security Response (SSR). (2014). Regin: Top-tier espionage tool enables stealthy surveillance. *Symantec Corporation,* Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf.

Team FME (Free Management Ebooks). (2014). SWOT analysis: Strategy skills. *Free Management Ebooks,* Retrieved from http://www.free-management-ebooks.com/dldebk-pdf/fme-swot-analysis.pdf.

Tejay, G. (2008). *Shaping strategic information systems security initiatives in organization*s Available from ProQuest Dissertations and Theses database (UMI No. 3346492).

Thompson, S. H., & James S. K. (2001). An examination of major IS planning problems. *International Journal of Information Management, 21*(6), 457-470.

Trend Micro Threat Research Lab (TMTRL). (2014). Shellshock: A technical report. *Trend Micro Incorporated*, Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-shellshock.pdf.

Valle Jr., V. (2000). Chaos, complexity and deterrence. *National War College*, Retrieved from http://www.au.af.mil/au/awc/awcgate/ndu/valle.pdf.1-13.

van Niekerk, J. F., & von Solms, R. (2010). Information Security culture: A management perspective. *Computers & Security, 29*(4), 476-486.

Vannoy, S. A., & Salam, A. F. (2010). Managerial interpretations of the role of information systems in competitive actions and firm performance: A grounded theory investigation. *Information Systems Research, 21*(3), 496-515.

Vasiu, L., Mackay, D., & Warren, M. (2003). The tri-dimensional role of information security in e-business: A managerial perspective. *Proceedings of the Hawaii International Conference on Business,* Honolulu, HI, 1-9.

Vijayan, J. (2005). Strategic security. *Computerworld.* Retrieved from http://www.computerworld.com/s/article/100916/Strategic_Security?taxonomyId=017.

von Solms, B. (2001). Information security - a multidimensional discipline. *Computers & Security, 20*(6), 504-508.

von Solms, B. (2006). Information security: The fourth wave. *Computers & Security, 25*(3), 165-168.

von Solms, R. (1998a). Information security management (2): Guidelines to the management of information technology security (GMITS). *Information Management & Computer Security, 6/5*(1998), 221-223.

von Solms, R. (1998b). Information security management (3): The code of practice for information security management (BS 7799). *Information Management & Computer Security, 6/5*(1998), 224-225.

Wagner, H.-T., & Weitzel, T. (2012). How to achieve operational business-IT alignment: Insights from a global aerospace firm. *MIS Quarterly, 11*(1), 25-36.

Wang, C. (2009). The underground economy of security breaches. In A. Oram, and J. Viega (Eds.), *Beautiful security: Leading security experts explain how they think,* (63-72). Sebastopol, CA: O'Reilly Media, Inc.

Weill, P., & Woerner, S. L. (2013). The future of CIO in a digital economy. *MIS Quarterly Executive, 12*(2), 65-75.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 4-19.

Westerman, G. (2009). IT risk as a language for alignment. *MIS Quarterly Executive, 8*(3), 109-121.

White, M. A., & Bruton, G. D. (2011). *The management of technology and innovation: A strategic approach.* (2nd ed.). Mason, OH:Thomson South-Western, Cengage Learning.

Wimpenny, P., & Gass, J. (2000). Interviewing in phenomenology and grounded theory: Is there a difference? *Journal of Advanced Nursing, 31*(6), 1485-1492.

Wommack, W. W. (1979). The board's most important function. *Harvard Business Review, 57*(5), 49-54.

Wood, C. C. (2000). An unappreciated reason why information security policies fail. *Computer Fraud & Security, 2000*(10), 13-14.

Yarger, H. R. (2006). Strategic theory for the 21st century: The little book on big strategy. *Director, Strategic Studies Institute, U.S. Army War College, 122 Forbes Ave, Carlisle, PA 17013-5244*. Retrieved from http://www.StrategicStudiesInstitute.army.mil/.

Yoong, P. (1996), "A grounded theory of reflective facilitation: making the transition from traditional to GSS facilitation", Thesis, Victoria University of Wellington, NZ.

Xiao-yan, Yuan, Y., & Lu, L. (2011). An information security maturity evaluation mode. *Procedia Engineering, 24*(2011), 335-339.

Zhang, N., & Bao, H. (2010). Design and formulation of security strategy in network. *International Conference on Future Networks,* Sanya, Hainan, CN, 216-220.

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information risk management framework for the cloud computing environments. *International Conference on Computer and Information Technology,* Bradford, Yorkshire, UK, 1328-1334.

Zients, J., Kundra, V., & Schmidt, H. A. (2010). FY 2010 Reporting instructions for the Federal Information Security Management Act and agency privacy management, OMB Memo M-10-15, *Executive Office of the President, Office of Management and Budget,* Retrieved

from http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf.

Zuccato, A. (2007). Holistic security management framework applied to electronic commerce. *Computers & Security, 26*(3), 256-265.