A QUALITATIVE STUDY OF THE RELATIONSHIP BETWEEN STRATEGIC INFORMATION SYSTEMS PLAN CONSTRUCTS AND INFORMATION SECURITY

by

Stanley Francois

JELENA VUCETIC, PhD, Faculty Mentor and Chair

VANESSA WOOD, EdD, Committee Member

CHRISTOPHER LUCARELLI, PhD, Committee Member

Todd Wilson, PhD, Dean of Technology

School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

Abstract

The continuing innovation of computer systems and the ambiguity associated with strategic information systems require increased control of information to enable information security success. The purpose of this qualitative multiple case study was to identify the factors that prevented Florida hospitals from obtaining information security (InfoSec) benefits to prevent crypto-malware attacks when implementing strategic information systems plans (SISP). Agency theory served as the theoretical foundation for the study. Four research questions were designed to collect information on the constructs of SISP concerning InfoSec. The four constructs included top management support, the usefulness of information systems plans, the degree of information technology infrastructure flexibility, and the degree of SISP success. The research included face-to-face interviews with managers, senior managers, and directors from for-profit and nonprofit hospitals in Florida. Analysis of the data yielded four themes: the role of top management support in SISP and InfoSec, planning for InfoSec, flexibility, and top management support in SISP success. Practical implications include directors developing SISP plans based on obtaining InfoSec benefits and allowing top management to monitor the execution phases of SISPs. Future researchers should consider pursuing a follow-up study to investigate the relationship between SISP, InfoSec success, and their impact on policy and procedure in Florida hospitals. Future research should also focus on the integration of the four constructs in business strategy, regulatory mandates, and corporate information technology management strategies on hospitals outside of Florida.

Dedication

I am dedicating this dissertation to my mother, Cletha Dossous, without whom I would not have completed this journey. To my Vermont host parents, Eric and Nancy Braman, who were supporting pillars for me in the hardest of days. To my siblings, Max and Maggie, thank you for all of your love, prayers, and patience throughout my doctoral journey. Without all of you, I would not have succeeded. I am dedicating this dissertation my Norwich University friends, Michael Bailey and Mathew Materio, for their support in my doctoral experience.

Acknowledgments

Many thanks to Dr. Jelena Vucetic for her help, patience, and dedication without whom I would not have completed my dissertation in a timely fashion. Dr. Vucetic has helped with my development process both personally and professionally throughout the mentorship process. Many thanks to the two committee members, Doctors Vanessa Wood and Christopher Lucarelli, for their professionalisms and constructive criticisms throughout the many milestones. Without their prudent suggestions and tips made throughout the dissertation milestones, I would have not succeeded. Many thanks to the wonderful people at Statistic Solutions who offered their time and special knowledge to help transform this research into a credible dissertation that adds to the strategic information systems plan body of knowledge. Thank you all indeed.

Table of Contents

List of Tables

List of Figures

CHAPTER 1. INTRODUCTION

Chapter 1 describes seven critical elements of this qualitative multiple case research study. The background of the study comprises the four most critical strategic information systems plans (SISP) constructs, which are top management support, the usefulness of information systems plans, the degree of IT infrastructure flexibility, and the degree of SISP success. The need for the study explores the existing gap for conducting qualitative multiple case research in SISP in Florida hospitals. The purpose of this qualitative multiple case study was to identify the factors that prevented Florida hospitals from obtaining information security (InfoSec) benefits to prevent crypto-malware attacks when implementing SISP. InfoSec benefits protect organizations from crypto-malware attacks, virus attacks, and spyware and worm attacks, which can cause severe disruptions to organizations (Ali, 2017; Georg, 2017; Kenyon & McCafferty, 2016; Richards, 2016). InfoSec benefits also protect data from theft by providing confidentiality, integrity, and availability of information to authorized users (Syväjärvi, Leinonen, Kivivirta, & Kesti, 2017).

InfoSec benefits also involve policies and procedures that protect users from having their passwords compromised (Kitsios & Kamariotou, 2018). InfoSec benefits increase computer performance and reduce computer failures by monitoring automatic updates of operating systems (Pankratz, & Basten, 2018). InfoSec benefits provide remote privacy to users by allowing users to store data and files anywhere without fear of cyberattacks (Ali, 2017; Georg, 2017; Kim, 2018). Obtaining InfoSec benefits is vital for Florida hospitals, so they continue to remain compliant to federal regulations and mandates (Elysee, 2012; Kim, 2018; Lee, Ghapanchi, Talaei-Khoei, & Ray, 2015; Mamonov, & Benbunan-Fich, 2018; Mishra, Caputo, Leone, Kohun, & Draus, 2014; Pankratz, & Basten, 2018).

The significance of the study section consists of two outcomes. The first outcome helps understand the processes that Florida hospitals go through to create their SISP. The next outcome from the study is an understanding of practical SISP approaches to InfoSec within Florida hospital IT settings. The research design section uses the multipl case study methodology to conduct face-to-face interviews on 15 IT professionals, who work at Florida hospitals, to uncover any themes and subthemes based on their responses. The research question section illustrates four main questions that the researcher examined. The assumptions and limitations section verifies theoretical and methodological assumptions limited to IT professionals employed at Florida hospitals. The definitions of terms section list keywords used to gather credible information to complete this qualitative multiple case research. The final section to this chapter summarizes Chapter 1 and describes the organization and general content of the rest of the dissertation.

Background of the Study

Strategic information systems (SIS) are computer systems that implement organizational strategies, which often help organizations maximize profitability (Dubey et al., 2017). Because of its adaptability and portability, SIS delivers new classifications of best practices used in strategies for the management of information systems (MIS) and information technology management (ITM). MIS refers to the management of information, and it provides tools to organizations for better decision-making (Abbasi, Sarker, & Chiang, 2016). ITM provides InfoSec regulatory compliance benefits to an organization, which is the operational core of ITM.

InfoSec reward is possible as it supports relevant empirical future research and the expedient adaptation of new concepts, which, in turn, help provide better decision-making systems for an organization (Ursacescu, 2014). Moreover, federal regulatory mandates require InfoSec benefits during the creation of SISP in organizations (Murphy, 2018). The four most critical SISP constructs include management support, the usefulness of information systems plans, the degree of IT infrastructure flexibility, and the degree of SISP success (Liu, 2015).

Despite the benefits of SISP in enhancing organization-wide operational governance and assisting firms in fulfilling goals and objectives, some industries do not adopt SISP to apply InfoSec best practices and methodologies in complying with federal mandates (Lee et al., 2015). SISP help organizations comply with federal mandates to information security policies (Wilkin, Couchman, Sohal, & Zutshi, 2016). Benefits of SISP occurs when organizations comply with federal regulations (Elysee, 2012; Lee et al., 2015; Mishra et al., 2014). The most notable of these industries is the healthcare industry, which has spurned SISP because of relatively small financial bases, a lack of frameworks that allow for inexpensive and expedient strategic plans, and the associated costs of running the organization while adhering to local, state, and federal regulatory compliance mandates (Trivedi & Rajawat, 2015; Wilkin et al., 2016). As such, these costs result in a growing need for healthcare-based firms, such as hospitals, to produce a sound organization-wide SISP to align their SIS with IT to obtain InfoSec benefits (Wilkin et al., 2016).

The researcher chose this problem or phenomenon for investigation because Elysee (2012) suggested adding to the body of SISP knowledge by conducting qualitative research in SISP, as little empirical research has been conducted to assist healthcare-based organizations, such as hospitals, to obtain the expected InfoSec benefits when implementing SISP (Kardan, &

Akbarnejad, 2014; Ursacescu, 2014; Weech-Maldonado et al., 2018). Furthermore, the researcher is interested in this phenomenon because various researchers have conducted studies related to different aspects of SISP. However, only a limited number of qualitative studies have been conducted using the case study approach to assess the alignment of SISP with IT to create an InfoSec benefit in Florida hospitals (Coronado, & Wong, 2014; Jaana, Teitelbaum, & Roffey, 2014; Mishra et al., 2014).

The general theory used to understand the phenomenon is Shapiro's (2005) agency theory. Agency theory is commonly encountered in the study of ITM because it provides guidelines to parties to behave in their own best interests. Mahaney and Lederer (2011) found that agency theory was the developed relationship between principals and agents, but agents were employed to represent the interests of the principals. Agency theory contributes to ITM and MIS project success by calculating for costs associated with contracting agreements between principals and agents, and by analyzing for transactional costs, or costs incurred while making economic exchanges (Sirisomboonsuk, Gu, Cao, & Burns, 2017).

Need for the Study

SISP helps establish and refine corporate strategies associated with existing technological limitations and provides robust structure-based methods organizations use to audit policies and procedures concerning InfoSec and IT outsourcing (Kardan & Akbarnejad, 2014). As such, organizations that use different IS strategies can vary their planning practices. However, the healthcare industry has not used SISP because of various concerns related to finances and federal compliance mandates (Kardan & Akbarnejad, 2014; Sirisomboonsuk et al., 2017). While various researchers have conducted studies related to different aspects of SISP, there is a dearth of qualitative, specifically multiple case study, research on assessing the alignment of SISP with IT to create InfoSec benefit in healthcare, especially for hospitals (Jaana et al., 2014; Mishra et al., 2014). Kardan and Akbarnejad (2014) have suggested that the main reason that hospitals do not experience InfoSec benefits is because of the misalignment of SISP and IT. Because of the dearth of preexisting research on the alignment of SISP with IT, little empirical research has been conducted to assist Florida hospitals to obtain the expected InfoSec benefits when implementing SISP (Kardan & Akbarnejad, 2014; Ursacescu, 2014). A gap in the literature regarding InfoSec benefits during the SISP process exists in Florida hospitals, and there has been no new research added to the SISP body of knowledge while conducting this multiple case research (Kisekka, & Giboney. 2018; Mishra et al., 2014; Shoufan & Damiani, 2017). However, there are ongoing interests in InfoSec benefits (Nicho, 2018). Therefore, the problem to be addressed within the study is why SISP does not return the expected InfoSec benefits in for-profit and nonprofit hospitals in the United States, specifically in Florida (Lee et al., 2015).

Purpose of the Study

The purpose of this qualitative multiple case study was to identify the factors that prevented Florida hospitals from obtaining InfoSec benefits to prevent crypto-malware attacks when implementing SISP. By investigating the four SISP constructs, this study contributed to the body of knowledge in research of information technology in industry and social-science research. This contribution may assist Florida hospitals in acquiring InfoSec benefits (Elysee, 2012; Lee et al., 2015; Mishra et al., 2014).

Significance of the Study

The significance of the study relates to InfoSec benefits within Florida hospitals. One outcome is an understanding of the processes that Florida hospitals go through to create their SISP. As such, there is an investigation regarding the top management support construct for any influences that occur to facilitate those processes. Another potential outcome from the study is an understanding of practical SISP approaches to InfoSec within Florida hospital IT settings. The penultimate benefits of the study are that a closer examination of the extent to which SISP benefits have been achieved in InfoSec using goal-centered judgments. The final significant advantage of this qualitative multiple case study investigative research is its review of practices that Florida hospitals use to adopt SISP successfully. By investigating the four SISP constructs as they pertain to Florida hospitals, lessons learned can be applied to help construct better procedures in future SISP implementations for hospitals outside of Florida.

Research Questions

The research questions that underpin the study are as follows:

RQ 1: How do IT managers describe the process their organization went through to secure top management support before initiating strategic information systems planning as an InfoSec advantage?

RQ 2: How do IT managers describe the usefulness of SISP to obtain InfoSec benefits?

RQ 3: How do IT managers describe the InfoSec benefits to the degree of information technology infrastructure flexibility?

RQ 4: How do IT managers describe the degree of SISP success to their InfoSec environments?

Definition of Terms

Agency relationship is a contract where principals engage agents to perform service on their behalf, in which agents have some decision-making authority (Hoenen & Kostova, 2015).

Crypto-malware are viruses that infect computers, lock and encrypt computer functionalities, and demand that a ransom be paid in Bitcoin to a designated routing address (Ali, 2017; Georg, 2017; Kenyon & McCafferty, 2016; Richards, 2016).

Enterprise resource planning consists of software packages that allow users to understand the real-time environment based on data models regarding the user's enterprise (Esteves, 2014).

For-profit hospitals are hospitals owned by investors (Davis, 2014; Trivedi, & Rajawat, 2015; Weech-Maldonado et al., 2018).

Hidden actions arise after the principal has entered a relationship with agents (Gorla & Somers, 2014).

Hidden characteristics are an agency theory predicament, which occurs before the principal enters a relationship with the agent (Gorla & Somers, 2014).

Information systems plans assist organizations with achieving their information technology objectives (Grabara, Kolcun, & Kot, 2014).

InfoSec benefits provide protection from data theft, protect organizations from hackers, and allow users to store data and files anywhere without fear of cyber-related attack (Georg, 2017; Kim, 2018; Kitsios & Kamariotou, 2018; Mamonov, & Benbunan-Fich, 2018; Pankratz, & Basten, 2018; Syväjärvi et al., 2017).

Multiple hospital organizations are entities designed to coordinate the decision-making of hospitals with market needs (Jemal, Kechaou, Ayed, & Alimi, 2015).

Multiple hospital systems are hospitals within a series of hospitals that are at multiple sites and locations, including their respective IT departments (Davis, 2014; Trivedi, & Rajawat, 2015; Weech-Maldonado et al., 2018).

Nonprofit hospitals are hospitals that remain in operation through research contributions and through educational and religious charitable funds (Davis, 2014; Trivedi, & Rajawat, 2015; Weech-Maldonado et al., 2018).

SISP success is the successful creation of a SISP within the timeframe and budget set by senior managers (Ribes & Polk, 2014).

SISP theory is an elaborate set of actions that represent an organization's step-by-step planning method philosophies (Arvidsson, Holmström, & Lyytinen, 2014).

Strategic information system plans are elaborate sets of actions that represent an organization's step-by-step planning method philosophies (Arvidsson et al., 2014).

Strategic information systems are computer systems that implement organization strategies (Arvidsson et al., 2014).

Top management support is the complete cooperation obtained from a firm's most senior-level managers or executive officers in allocating budget, setting goals and objectives, and maintaining the initiatives of a project (Peppard, Galliers, & Thorogood, 2014).

Health-information technology (HIT) refers to systems that are designed to improve patient care, which include electronic medical record, pharmacy information system, and computer-based physician orders entry system (Gabriel, Jones, Samy, & King, 2014).

The healthcare sector comprises of companies, such as hospitals, which specialize in products and services related to health and medical care (Elysee, 2012; Georg, 2017; Richards, 2016).

Health Insurance Portability and Accountability Act is a Federal law established in 1996 that restricts access to individuals' medical information (Murphy, 2018).

Research Design

The study used a multiple case study methodology to conduct face-to-face interviews on 15 IT professionals, who work at Florida hospitals, to uncover any themes and subthemes based on their responses. All participants chosen for this research were senior managers, directors, senior directors, and Chief Information Security Officers (CISO) who oversee day-to-day operations of IT departments at Florida hospitals (Yin, 2013). Each participant was asked a series of questions based on the four SISP constructs. To investigate the first construct, IT professionals participating in this research were asked to describe the process their organization went through to secure top management support before initiating SISP as an InfoSec advantage. To investigate the second construct, participants were also asked to describe the usefulness of information systems plans in obtaining InfoSec benefits. To investigate the third construct, participants were asked to describe the InfoSec benefits on the degree of IT-infrastructure flexibility in their environments. Finally, to investigate the last construct, participants were asked to describe the degree to which SISP was successful at improving their InfoSec environment. Participants were also asked to describe the outcomes or effects that occurred because of those actions.

Setting

In recent years there has been a new type of denial of service attack aimed explicitly at the healthcare sector, which primarily targets hospitals in the United States. The healthcare sector comprises of companies, such as hospitals, which specialize in products and services related to health and medical care (Elysee, 2012; Georg, 2017; Richards, 2016). Attacks such as these have new names, crypto-malware, and they are powerful, devastating, and challenging to mitigate (Georg, 2017; Kenyon & McCafferty, 2016; Richards, 2016). Hospitals in Pennsylvania and California have been the biggest victims of these latest attacks (Georg, 2017). The crypto-malware infects the SIS of a hospital, locks its functionality, and demands a ransom payment in Bitcoin to a designated routing address (Kenyon & McCafferty, 2016). In some cases, the victim hospitals have only a few hours to pay the suggested ransom; if they do not pay, then attackers delete the data residing in the SIS system (Georg, 2017; Kenyon & McCafferty, 2016; Richards, 2016).

Given these recent attacks, there is a need for qualitative multiple case research aimed at the hospitals to gather empirical evidence of the four constructs mentioned in the work by Hartono, Lederer, Sethi, and Zhuang (2003) to find out why healthcare-based organizations do not obtain full InfoSec benefits when implementing SISPs (Jaana et al., 2014). The researcher chose the state of Florida as the research study site because it is a primary destination for retirees. Retirees require more healthcare assistance, and SIS systems must remain online always (Jaana et al., 2014). Hospital administrators in Florida are also beginning to ask for assistance in spearheading programs against crypto-malware attacks, their implications for SIS systems, and strategies to revise their SISP for InfoSec success (Ali, 2017; Georg, 2017; Mishra et al., 2014; Richards, 2016).

Assumptions and Limitations

Assumptions

A theoretical assumption for this qualitative multiple case study research was that using the four SISP constructs for InfoSec benefits should enable Florida hospital IT professionals to become more informed when creating policies and procedures to secure their environment. Literature has shown that SISP and its constructs allow organizations, in general, the ability to create robust IT environments. Investigators of the SISP and its constructs have also explored improvements in InfoSec in Florida hospitals (Hoque, Hossin, & Khan, 2016).

Another theoretical assumption for this qualitative multiple case study research was that top management support should be the determinant factor enabling Florida hospitals to obtain Infosec benefits when implementing SISP. InfoSec in IT environments are not inherently insecure, but most organizations deploy InfoSec poorly (Young & Poon, 2013). This problem is because of inadequate top management support in the merger of SISP with their IT environment to yield InfoSec benefits (Young & Poon, 2013). A methodological assumption was that participants chosen for this research would understand their agency, IT environment, and corporate culture. Another assumption was that face-to-face interviews would reflect the honesty and objectivity of participants' answers in this study (Saldaña, 2015).

Limitations

Limitations of this qualitative multiple case research study included the following:

First, this study was limited to Florida hospitals' IT departments. Second, the initial introductory outreach and recruitment letters were limited to top management who work at Florida hospitals listed in the 2015 Directory of Hospitals. Third, the sample size was limited to Florida hospital IT professionals, whose top managers have identified and endorsed for this research. Fourth, the recruitment emails were limited to Florida hospital IT professionals who have been selected by their top managers to be contacted for this research. Finally, the sample frame was limited to Florida hospital IT professionals with five or more years of experience in SISP and InfoSec.

The data for this study came from Florida hospital IT professionals who have experience in SISP and InfoSec. The strength of this qualitative multiple case study was in its design, as it uses standardized face-to-face, open-ended interviews of Florida hospital IT professionals who had experience with both SISP and InfoSec. The introductory outreach and recruitment letters sent to Florida hospitals' top management enabled them to identify only IT professionals who had direct experiences with SISP and InfoSec to be contacted by the researcher. This method gave the researcher assurance that the population chosen for the study represented only those with expertise on the topic. Using standardized face-to-face, open-ended interviews of Florida hospital IT professionals allowed these professionals to evaluate and map specific factors and traits deemed active and critical to the success of SISP and InfoSec in their IT environments.

The present qualitative multiple case study was designed to identify the factors that prevented Florida hospitals from obtaining InfoSec benefits to prevent crypto-malware attacks when SISP. The questions that drove this multiple case research were as follows: How do IT managers describe the process their organization went through to secure top management support before initiating SISP planning as an InfoSec advantage. How do IT managers describe the usefulness of SISP to obtain InfoSec benefits? How do IT managers describe the InfoSec benefits to the degree of information technology infrastructure flexibility? How do IT managers describe the degree of SISP success to their InfoSec environments? These questions helped understand the process that participating Florida hospitals went through to create a SISP. The study was designed to investigate the four most critical constructs that influence SISP: top management support, the usefulness of information systems plans, the degree of IT infrastructure flexibility, and the degree of SISP success (Liu, 2015).

Organization of the Remainder of the Study

There are four additional chapters associated with this research. In Chapter 2, the researcher includes a theoretical framework and literature review sections, a synthesis of the research findings based on the four constructs, critiques of previous studies based on SISP, and a chapter summary. Chapter 3 contains the purpose of the research, research questions, research design, target population and sample, procedures, instruments, ethical considerations, and a summary of the chapter. Chapter 4 consists of the research methodology, description of the sample, presentation of data, and results of the analysis. Chapter 5 consists of a summary of the results, discussion of the results, conclusions based on the results, comparison of findings with the theoretical framework, interpretations of the findings, limitations, implications for practice, recommendations for further research, and concluding remarks.

CHAPTER 2. LITERATURE REVIEW

Because of the dearth of preexisting research on the alignment of SISP with IT, little empirical research had been conducted to assist Florida hospitals to obtain the expected InfoSec benefits when implementing SISP (Kardan & Akbarnejad, 2014; Ursacescu, 2014). Therefore, the problem addressed within the study was why SISP does not return the expected InfoSec benefits in for-profit and nonprofit hospitals in the United States, specifically in Florida. As such, the purpose of this qualitative multiple case study was to identify the factors that prevented Florida hospitals from obtaining InfoSec benefits to prevent crypto-malware attacks when implementing SISP. By investigating the four SISP constructs, this study contributed to the body of knowledge in research of information technology in industry and social-science research.

Chapter 2, the literature review, contains an overview of the search-related methods used to obtain literature for the chapter. Chapter 2 consists of the theoretical orientation of the study section, which focuses on the application of the review to the body of knowledge of SISP. Chapter 2 illustrates relevant methodological constraints to the problem and the purpose of this research. Following the theoretical orientation is a review of the literature related to the fundamental concepts of the study, with a focus on SIS, top management support, information system plans, infrastructure flexibility, and SISP success. Chapter 2 concludes with a critique of the previous research and a summary before transitioning to Chapter 3, the methodology.

The researcher obtained peer-reviewed articles compiled for this chapter through comprehensive online library search methods from Capella University Library. The comprehensive online library search methods included the exploration of databases that produced the most significant results such as the following: Academic Search Premier, ACM

Digital Library, Dissertations and Theses Global, EBSCOhost, Elsevier, Google Scholar, JSTOR, ProQuest, Researchgate, and Sage Research Methods, and included articles within the last five years. Among the keywords used to search for peer-reviewed articles include the following: *agency theory, healthcare, for-profit hospitals, nonprofit hospitals, Florida hospitals, crypto-malware, strategic information system plans, top management support, information technology flexibility, information systems plans, SISP success, InfoSec benefits, strategic information systems,* ***e****nterprise resource planning, for-profit, hidden actions, hidden characteristics, multiple hospital organizations, and multiple hospital systems*.

The researcher accessed other databases in the search process to ensure that all the literature generated would fit this designation. The researcher reviewed literature published within the last five years that contain empirical research in the applicable areas, which appeared in a wide range of publications, such as the following: *International Journal of Project Management, International Journal of Business and Management, International Journal of Information Management, Information & Management, Journal of International Business Studies, Journal of Information Security and Applications, International Journal of Technology Assessment in Health Care*, and *Health Care Management Review*. The researcher read all peer-reviewed articles, identified principal authors and reviewed the corpus of their work for other relevant themed issues, for other relevant work.

Theoretical Orientation for the Study

Agency Theory Seminal Work

The theoretical underpinning of the study is Shapiro's (2005) agency theory. Agency theory comprises of two main parties, owners (principals) and directors (agents), and revolves around employees work for the owners (Shapiro, 2005). However, owners or principals need to entrust agents to act in their best interests, as principals must understand costs of audits, must be fluent in auditing tools, chair and understand general meeting requirements, and conduct meeting briefings that are often associated with running an agency (Shapiro, 2005). Principals achieve successful outcomes by using business practices, which involve generating appropriate creative messages to deliver and execute milestones that will guarantee success (Shapiro, 2005).

Agency theory consists of two key assumptions. The first assumption is that agents behave or make decisions that benefit their self-interests, while principals similarly work to their advantage (Shapiro, 2005). The second assumption is that agents in a position of power have access to sensitive information but make decisions that work to their advantage (Shapiro, 2005). However, agency theory does not capitalize on the joint effect of principals and agents but exploits the usefulness of principals and agents (Shapiro, 2005). The usefulness of principals translates to maximizing profit. The usefulness of agents is limited and considered as being a constraint, depending on the firm (Shapiro, 2005). For agents, usefulness is converted to direct compensation, which can be in forms of salary increase, long-term or short-term incentive plans, or paid expenses (Shapiro, 2005).

Agency Theory in Current Practice

Agency theory addresses two issues facing principals: hidden characteristics and hidden actions (Hoenen & Kostova, 2015). Hidden characteristics occur before principals engage in a relationship with agents, and principals will often scrutinize agents' corporate culture, capabilities, and capacities during this stage (Foss & Stea, 2014). To mitigate hidden characteristics, an organization can perform preliminary interviews using vetting techniques before electing and confirming agents to their positions (Steinle, Schiele, & Ernst, 2014). Hidden actions occur when principals enter a relationship with agents, which includes providing agents with incentives as a form of motivation to be optimal for the principal (Steinle et al., 2014). There are several issues with hidden actions, such as the principals and agents having different goals, the attitudes toward risk being different, each party having information that the other party does not possess, and environmental uncertainties presenting external forces beyond the control of agents, which could influence results (Bøe, Gulbrandsen, & Sørebø, 2015). However, the objective of hidden actions is to construct distinctions to align the objective of principals and agents to help motivate both parties while optimizing the principals' profits as well as compensating agents adequately (Bøe et al., 2015).

Agency theory is commonly encountered in the study of ITM because it provides guidelines for parties to behave in their own best interests. Toivonen and Toivonen (2014) found that agency theory was the developed relationship between principals and agents, where agents were hired to represent the interests of the principals. Within ITM, however, organizations that employed contractors, or agents, to represent their interests were very successful at creating lasting relationships that benefited both agents and principals (Toivonen & Toivonen, 2014). Agency theory helps researchers understand ITM and MIS project success in several ways. First, the theory helps calculate for costs associated with contracting agreements between principals and agents (Sirisomboonsuk et al., 2017). Agency theory further helps researchers analyze transactional costs, or costs incurred while making economic exchanges. However, transaction costs are limited to calculating for supervision and administration costs incurred when making sure that all parties agree to the terms and conditions of the contract. Litigation actions may be taken against such person in the event one or more parties involved do not act by the terms and conditions of the agreed-upon contract (Sirisomboonsuk et al., 2017).

Agency Theory in Hospital IT Practice

Agency theory relates to hospitals by helping researchers analyze the alignment of the interests of principals and agents, which is believed to be a challenge facing hospitals (Singh, Mindel, & Mathiassen, 2017). Without the practical application of agency theory, there may be misalignment between principals and agents, which can force a hospital system to consolidate with other hospitals to form a multi hospital system. Hospitals facing financial hardship because of net revenue erosion and poor financial positioning may choose to merge with other hospitals within the same region of operation (Singh et al., 2017). However, problems occur wherever hospitals have ignored the economics of the market where they serve. Once a hospital merger is complete, the agency theory framework helps to articulate and implement strategic alliances between principals and agents who are members of the newly created multiple hospital system (Singh et al., 2017).

The agency theory framework provides insights into principals' approaches for coordinating hospital decision making with agents (Vähäsantanen, Paloniemi, Hökkä, & Eteläpelto, 2017). The most successful multiple hospital systems are efficient at using agency theory, enabling principals to formulate strategies that offer the best partnership balance with agents, and facilitating technological innovations for constructing SISP (Pepper & Gore, 2015). Strategies that offer principals and agents partnership also create effective programs that meet the needs of the community and control costs of jointly pursuing economic achievements among member hospitals (Bendickson, Muldoon, Liguori, & Davis, 2016).

The current research uses agency theory in investigating the four SISP constructs in Florida hospitals, including for-profit and nonprofit hospitals. Data collected for this research includes face-to-face interviews from single as well as multiple hospital systems. Collin, Paloniemi, and Vähäsantanen. (2015) mentioned that researchers interested in using the agency theory in single nonprofit hospitals, in face-to-face interview settings, should consider focusing on the new behavior of participants and highlight those participants who exhibit traits of advantage-seeking behaviors. This advice is based on the idea that single nonprofit hospitals seek principals of managerial and organizational expertise and require agents to provide knowledge and human capital (Collin et al., 2015). Conversely, in multiple nonprofit hospitals, principals are continually seeking ways to leverage innovation as a means to adapt to their community of operations. This strategic approach requires different recruitment of agents, as they are considered strategic entrepreneurs (Collin et al., 2015).

Agency theory plays a significant role in identifying agents who directly support administrative, clinical, and strategic health-information technology (HIT) systems in hospitals. HIT refers to systems that are designed to improve patient care, which include electronic medical record, pharmacy information system, and computer-based physician orders entry system (Gabriel et al., 2014; Pepper & Gore, 2015). Applications that administer HIT operations are intended to improve and modernize internal data processing activities of hospitals, such as payroll processing, billing, and patient registration systems (Gabriel et al., 2014; Pepper & Gore, 2015). Strategic HIT includes applications meant for improving critical decision-making activities in hospitals, including nursing staffing, managed care, and executive information software systems (Gabriel et al., 2014; Mullaly, 2014).

Agency theory helps explain how hospitals gain control and use HIT resources by looking at the roles of principals and agents, mainly to analyze opportunity-seeking and advantage-seeking behaviors to address IT and InfoSec-related concerns facing hospitals (Glinkowska & Kaczmarek, 2015). The differences in mechanisms used to align hospitals' business strategies with clinical support, administrative support and HIT support suggest the value of exploring how to use agency theory as a baseline in three different governance systems (Bendickson et al., 2016; Collin et al., 2015; Gabriel et al., 2014; Mullaly, 2014).

Participants at Florida hospitals, for this multiple case qualitative face-to-face research, include those who work for nonprofit single and multiple hospital systems, as well as those who are working for for-profit single and multiple hospital systems. Credible insights of participants are abstracted as transformative, which includes segmenting from actions of principals and agents or separating actions taking to initiate and transform IT/IS in nonprofit single and multiple hospital systems, as well as for-profit single and multiple hospital systems (Bendickson et al., 2016). Transformative actions are the variety of new positions in a hospital IT/IS setting and through internal change (Pepper & Gore, 2015). In a hospital, the conceptualization of IT/IS agency theory is as a relational agency involving the capacity to align the actions of principals with agents to interpret concerns in response to interpretations and engagements of the top management disposition of the four SISP constructs. Bendickson et al. (2016) and Glinkowska and Kaczmarek (2015) expunged relational agency from principals who interpreted practices and activities from the viewpoint of agents instead should be the act of principals pursuing opinions from agents to produce opportunities for learning and understanding the point of views of agents.

The research expands on the SISP scientific body of knowledge by presenting the established a two-tiered theoretical framework based on the quantitative seminal research survey of Ragu-Nathan, Apigian, Ragu-Nathan, and Tu (2004). The two-tiered theoretical orientation depicted in Figure 1 examines existing direct or indirect relationships fostered by the top management support and resulting in SISP success (Ragu-Nathan et al., 2004). Top management's support was one of four constructs established by Lederer and Hannu (1996). In their seminal work, Lederer and Hannu (1996) further identified the degree of information system plan, the degree of information technology flexibility, and SISP success as three more constructs for successfully adapting to an organization wide SISP. These four constructs were later reinforced by Yang and Tanner (2011) in a comprehensive case study review of SISP in a sizeable Korean firm.

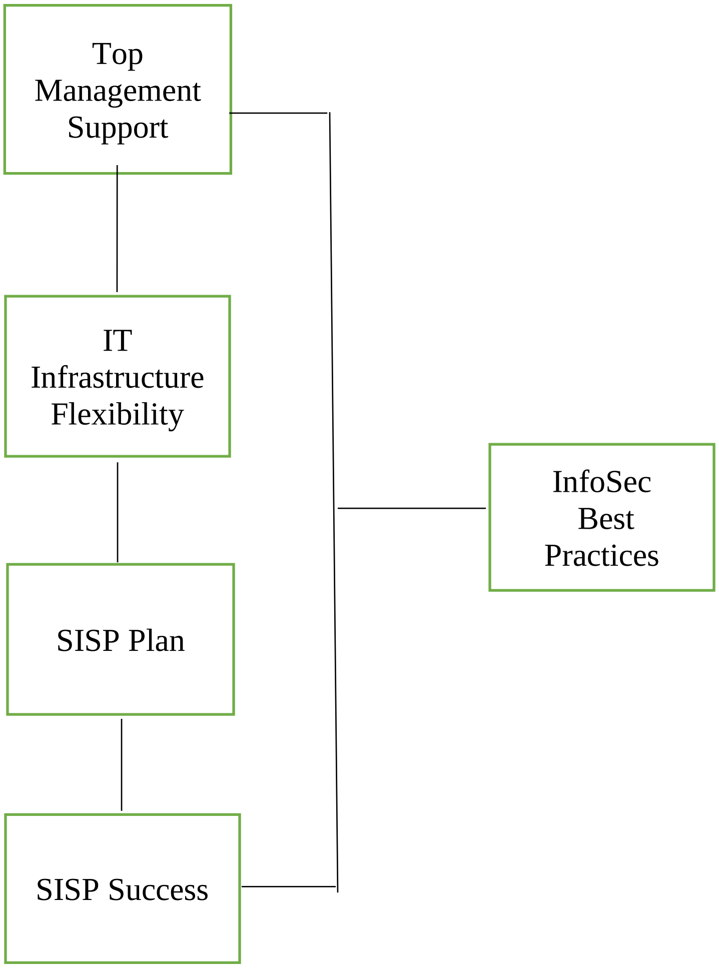

Figure 1. Researcher-designed conceptual framework of the four SISP constructs. Adapted from text by "Toward a theory of strategic information systems planning," by A. L. Lederer and S. Hannu, 1996, *Journal of Strategic Information Systems, 5*(3), pp. 237–253, doi:10.1016/S0963-8687(96)80005-9, and "Top management support: Mantra or necessary?" by R. Young and S. Jordan, 2008, *International Journal of Project Management, 26*(7), 713–725, doi:10.1016/j.ijproman.2008.06.001.

Review of the Literature

The researcher organizes the following review of the literature by constructs, and it contains an exhaustive overview of previous research related to the fundamental concepts of the study. The literature review includes sections on SISP theory as it relates to business environments, SISP successes, interrelationships among InfoSec success, and factors of SISP projects in organizations that align with top management objectives. There is a section on top management support that makes a case for obtaining approval from a firm's most senior-level managers or executive officers to allocate budget, set goals and objectives, and maintain the initiatives of a project. Additionally, there is an overview of the importance of infrastructure flexibility that illustrates how the construct allows for a better understanding of what is needed to implement to achieve InfoSec success. The section about information systems plans makes the case on how such plans assist organizations with achieving their information technology objectives. The section regarding SISP success gives the main points for the creation of a SISP within the timeframe and budget set by top management.

Strategic Information Systems Plan Theory

Strategic information systems plan (SISP) theory is rooted in the establishment of SISPs, which are elaborate sets of actions that represent an organization's step-by-step planning method philosophies (Arvidsson et al., 2014). The following section on SISP theory consists of a definition, previous knowledge related to SISP theory, and its applications in current use. As such, the following section includes an understanding of SISP theory as it pertains to dynamic business environments, SISP successes, interrelationships among InfoSec success, and factors of SISP projects in organizations that align with top management objectives.

Segars and Grover (1998) introduced SISP theory as being activities requiring substantial resources from top management in term of time and budget. The process of SISP theory must deliver benefits outside the resources necessary to sustain and contribute positively to InfoSec success (Segars & Grover, 1998). SISP theory renders many benefits that are both tangible and intangible for measuring how well SIS incorporates SISP constructs to MIS and ITM system processes (Segars & Grover, 1998). One of SISP theory's benefits includes the creation of SISP frameworks such as that developed by Lederer and Hannu (1996), which is an essential beginning for measuring InfoSec success. A SISP framework theoretically develops and statistically tests measurement model of an organization's MIS and ITM systems' InfoSec success. Furthermore, a SISP framework develops measures and contemporary statistical techniques of organizations effectiveness, aimed at the use and operational structures or construct space for factors indicative of InfoSec success (Segars & Grover, 1998).

Borrowing from Lederer and Hannu (1996), Brown (2004) conducted an extensive review to test the SISP theory, identifying where further research is required. According to Brown (2004), the theory of SISP was introduced by Lederer and Hannu (1996) to showcase their findings as a baseline for firms who wanted to measure success between SISP and a function such as InfoSec. In addition to InfoSec, Lederer and Hannu (1996) emphasized that in dynamic business environments such as MIS or ITM, SISP theory could be useful at measuring functions such as the following: acquisitions and mergers, strategic alliances, new technologies, and regulatory changes.

Peppard et al. (2014) explained that the dynamic business environment affected top management support in MIS and ITM business strategies and processes yielding to InfoSec success. Kitsios and Kamariotou (2018) considered the necessary top management alignment to business needs with MIS and ITM capabilities while considering the benefits to InfoSec. The SISP theory was found to be an essential process in the configuration of MIS and ITM systems to business requirements. The significance of an appropriate SISP theory in MIS and ITM systems could enable investigation in organization wide SISP to enable InfoSec success whenever the finding of different factors influencing SISP success occurs in the SISP plan (Peppard et al., 2014).

Hung, Huang, Yen, Chang, and Lu (2016) defined the importance of SISP theory as characteristics observed to facilitate effective planning on an aggregate scale of a limited number of SISP successes. An effective SISP plan includes several constructs that focus on directing SISP processes to organizational characteristics, which can impact top management business justifications to provide the company effectiveness measures of scales (Peppard et al., 2014). Within the context of the SISP theory, similar structures of interrelated constructs can likely be used with different theoretical definition to constitute the measurement space of SISP and InfoSec success (Hung et al., 2016). Interrelated constructs, as defined by Lederer and Hannu (1996), assessed the extent and specific organizational MIS and ITM systems benefits rendered by SISP activities.

Interrelated constructs also measure the effectiveness of theoretical and operational multi-dimensional concepts of SISP success that have interrelationships among InfoSec success (Hung et al., 2016). The SISP theory provides a more accurate diagnostic of SISP activities within organizations to developed concepts of varying criteria of SISP planning that yield InfoSec success (Yang & Pita, 2014). A useful SISP theory that is used to create SISP and InfoSec success could inhibit external factors such as hacking, which could attempt to compromise MIS and ITM systems (Yang & Pita, 2014). Therefore, not identifying practical approaches to SISP in addition to InfoSec success, Yang and Pita (2014) asserted that MIS and ITM managers could be without a sound framework, which resources devoted to InfoSec activities could not be easily and accurately justified to top management.

Through extensive literature review, Hartono et al. (2003) extended the seminal SISP theory to include four additional constructs, which are top management support, the usefulness of information systems plans, the degree of information technology infrastructure flexibility, and the degree of SISP success. Other recent researchers have also worked on Hartono et al.'s (2003) extended theory and have included further constructs such as complexity risk (Liu, 2015), hybrid approaches for allocating resources (Hoque et al., 2016), and strategy execution (Srivastava & Sushil, 2015). However, this research used the original theory put forth by Hartono et al. (2003). Brown (2004) conducted a meta-analysis on the SISP theory and found the inclusion of the four constructs, which were identified by Hartono et al. (2003), were vital to SISP success. Hartono et al. (2003) used meta-analysis, which is a statistical procedure for combining data from multiple studies. Because of a meta-analysis on the SISP theory, Hartono et al. (2003) found the inclusion of the four constructs. SISP theory constructs can be investigated and presented in a comprehensive, coherent, and rigorous method (Kardan & Akbarnejad, 2014). However, literature about SISP reveals that there has been little empirical qualitative research conducted that showcase the SISP theory to provide a complete illustration of the constructs that can influence SISP success (Kardan & Akbarnejad, 2014; Ursacescu, 2014). Based on extensive literature reviews, this research added to the SISP body of knowledge by qualitatively investigate the relationship of four constructs in Florida hospitals, and the selected constructs are (a) top management support, (b)the usefulness of information systems plan, (c) the degree of information technology infrastructure flexibility, and (d) the degree of SISP success.

Silvius and Stoop (2013) used SISP theory to reference factors of SISP projects in organizations and to demonstrate approaches to create a SISP plan tailored to organizations' top management objectives. Showcasing processes that influence SISP was motivated by the authors' experiences as consultants in MIS, and ITM systems (Silvius & Stoop, 2013) tailored their findings to a single organizational setting of a specific SISP project. Silvius and Stoop (2013) analyzed their findings to include situational factors, configuration variables, and procedures for SISP success. The authors' analyses led to a detailed conceptual model of their study to reveal the research method of the study, which qualified as being explorative (Silvius & Stoop, 2013).

Silvius and Stoop (2013) performed an empirical exploration based on 16 SISP case studies in the Netherlands, seeking to investigate the reason for a top management context of the configuration of a SISP process and its influence on SISP success. Silvius and Stoop (2013) found that there was a relationship between SISP success and SISP process configuration based on their analyses of 16 SISP cases. However, there was no relationship between top management context with situational factors in the researched firms (Silvius & Stoop, 2013). Additionally, there was an established relationship between SISP process configuration and SISP success variables, explained as being clear goals, strategic comprehensions, and decisions of top management with regards to SISP success (Silvius & Stoop, 2013). There was also the appearance of a relationship between the specificity and comprehensiveness of decisions, goals, and strategies in participating organizations. Silvius and Stoop (2013) comprehensive examination found some positive effect on SISP success in certain firms they studied. One of such positive effect was in observing substantial connection that appeared in the role of participating firms within their MIS or ITM departments that adapted formal a SISP methodology. Silvius and Stoop (2013) demonstrated that a more dominant role of participating firms using SISP processes as part of their MIS or ITM positively influenced the quality of the SISP deliverable. However, SISP processes in MIS or ITM has had adverse effects on building IT and business partnership with participating organizations (Silvius & Stoop, 2013). Furthermore, Silvius and Stoop (2013) asserted that there was no effect on SISP success in cases where participating firms that did not adopt a formal SISP methodology.

Silvius and Stoop (2013) found that there was a lack of alignment between IT and business imperatives, which continues to plague top management decisions despite decades of research. Maharaj and Brown (2015) used SISP theory in their research to create methods that can coordinate the relationship between IT and the business imperatives to align top management decisions with IT. Maharaj and Brown (2015) used the shared domain knowledge (SDK) concept, which referred to as being essential factors that hypothesized ways to improve IT with business alignment using the SISP theory as a baseline. Additionally, SDK can enhance the efficiency and effectiveness of strategic ITM processes that included SISP. Maharaj and Brown (2015) examined the impact of SDK on SISP and alignment by gathering data from top management in a large, global IT-based organization using a structured questionnaire. The implementation of SDK can directly impact business and IT alignment in research through investigations regarding various relationships between SDK, top management MIS, and ITM alignment.

Maharaj and Brown (2015) viewed SISP as the principal activity in organizations' ITM and MIS systems, primarily as a means to improve the level of business alignment between top management and IT. Top management has consistently ranked both ITM and MIS system alignment as the primary issue facing organizations globally, which highlights the importance of researchers to add to the SISP body of knowledge regarding these phenomena (Maharaj & Brown, 2015; Yoshikuni, & Albertin, 2018). Business imperatives that align top management decisions with IT are an essential result of SISP success (Maharaj & Brown, 2015; Yoshikuni, & Albertin, 2018). Furthermore, top management IT and business alignment, when used because of SISP success, is defined as the state where IT and top management business planning strategies are coherently interrelated. The interrelationship of IT was equivalent to top management vision on business and IT strategies (Maharaj & Brown, 2015; Yoshikuni, & Albertin, 2018).

Using the SISP theory as a baseline, Maharaj and Brown (2015) demonstrated that there was a definite SDK influence on SISP characteristics. Additionally, Maharaj and Brown (2015) found that top management participation in business planning influenced the social dimension of aligning high levels of prudence in SISP positively influenced the logical dimension of alignment; SDK was found to have a bearing on all SISP characteristics measured. Furthermore, SDK was found to impact both the intellectual and social dimensions of alignment positively, and Maharaj and Brown (2015) concluded that the implications of their findings promoted a knowledge-sharing environment for top management to improve alignment that steers SISP success.

Maharaj and Brown's (2015) study contributed to SISP body of knowledge by demonstrating the validity and reliability of measures for investigating SISP characteristics, aligning the reliability of top management with SDK taken from different sources. The study revealed a two-factor structure for SDK business knowledge of MIS and ITM, the intellectual dimension of top management alignment in SISP plan and business plan alignment, and the long-term and short-term social dimension of alignment in keeping with the conceptualization of the four SISP constructs (Maharaj & Brown, 2015; Yoshikuni, & Albertin, 2018). The authors' findings could benefit top managers when implementing improved rationality of SISP processes. The findings also benefit the intellectual dimension of alignment that incorporates IT managers' strategic inputs in business plans, establishing a knowledge sharing culture to construct mechanisms to share knowledge in the organization, and implementing top management initiatives to improve on future SISP plans to obtain InfoSec success (Maharaj & Brown, 2015; Yoshikuni, & Albertin, 2018).

Top Management Support

Top management support is the complete cooperation obtained from a firm's most senior-level managers or executive officers in allocating budget, setting goals and objectives, and maintaining the initiatives of a project (Peppard et al., 2014). Within this section, there is a discussion regarding the lack of top management support of SISP, the effects this lack has on SISP, and the expansion of SISP research. Also, in this section, there is a discussion regarding the necessity of top management support.

In most cases, SISP lacks the support of top management; this is problematic for firms' project success support (Peppard et al., 2014). Karahanna and Preston (2013) affirmed that top management support was the full cooperation obtained from a firm's chief executive officer in allocating a budget, setting goals and objectives, and maintaining the initiatives of a SISP project. Peppard et al. (2014) asserted that top management support is one of the leading critical human resources phenomena that assist with SISP success.

Premkumar and King (1994) presented the construct in a survey of 246 information systems IS/IT top managers, abstracting human resources regarding tangible and intangible assets, also referred to as “counter-implementation of top management’s participation” (p. 59). The information in this survey showed that the involvement and activities of the top management community significantly enhanced the planning and skills of IS/IT employees to create SISP success. However, top management support should be present in the initiating phase of project management plans of a SISP project, to increase the likelihood of SISP project success during the duration of the project (Alobaidly, Wainwright, & Waring, 2014).

In a subsequent study of 69 firms, Bajwa, Rai, and Brennan (1998) found that during the initiating phase of SISP projects, high levels of top management support created a supportive context for the observed IS/IT organizations. As a result, top management support at the initiating phase of a SISP project resulted in an unflagging commitment of organizations to make sure that the likelihood of project success- remains high (Alobaidly et al., 2014).

Kearns (2006) proposed further expansion of top management support research and for project planners to support SISP project planners to be in congruence with the goals of the organization. Kearns (2006) explained that a lack of support from project planners might not be useful, and top managers may not support the implementation of SISP; thus, SISP may be unsuccessful. Teo and Ang (2001) provided evidence of the importance of project planners being in congruence with top management. Teo and Ang (2001) performed a study in which they articulated IS project planning to consist of three phases: launch, development, and implementation. Teo and Ang (2001) found that seeking top management support at the launching, developing, and implementing phases was fundamental to SISP success. The most critical factor affecting SISP is the lack of top management support at all levels in a project plan (Gerow, Grover, Thatcher, & Roth, 2014; Rahimi, Møller, & Hvam, 2016).

Information Systems Plan

Information systems plans (ISPs) are plans that assist organizations in achieving their information technology objectives (Grabara et al., 2014). In the following section, a detailed review of ISPs is discussed, including the basic tenets of ISPs and the importance of ISPs. Alobaidly et al. (2014) found that ISPs contain detailed proposals for achieving a business' goals. Information systems plans assist organizations in achieving IS objectives. The document of information systems plan focused on the goals and objectives of the corporation and expressed needed IS projects to assist the organization to obtain its objectives (Alobaidly et al., 2014). The most critical aspect of an information systems plan was the clear communications of top management of business goals, and consistent revision of the intentions of top management on executing and implementing the plan (Alobaidly et al., 2014; Peppard et al., 2014).

Subsequent research by Gottschalk (1999a) described the information systems plan as a model consisting of several IT-related projects aimed at achieving organizational goals. The incorporation of defined business goals into information systems plan documentation is necessary so that top management support and needed human resources can be allocated to make sure that implementation of the plan is executed successfully (Gottschalk 1999a). Consistent with this characterization, Kitsios and Kamariotou (2018) maintained that the information systems plan document must focus on the business. Otherwise, the plan may not reflect the goals of the corporation adequately. However, Gottschalk (1999a) cautioned that top management should not support ISPs if they did not reflect the goals of the corporation.

In this qualitative multiple case study research, the usefulness of the information systems plan document is an important construct to evaluate. This construct helped explain the extent to which information systems plan and its documentation reflects the business goals on provided InfoSec success on Florida hospital IT environments (Ahmad, Maynard, & Park, 2014). Further, this study looked at the two conditions that direct relationship between top management support and InfoSec success can change. One of the conditions is the communications of top management on business goals. The other condition is the frequency of revisions of the intentions of top management on executing and implementing ISPs (Alobaidly et al., 2014).

Infrastructure Flexibility

Infrastructure flexibility is essential because it allows for a better understanding of what is needed to obtain SISP success. In a seminal study on IT infrastructure flexibility, Duncan (1995) identified essential components of IT infrastructure flexibility, proposed characteristics of flexibility, and discussed of the concept of IT infrastructure flexibility. Duncan (1995) described IT infrastructure flexibility as those essential technological components that include both tangible and intangible resources. Tangible and intangible resources include hardware technologies, systems technologies, network communication technologies, key data technologies, operating systems technologies, and data processing applications (Chen et al., 2014).

The study proposed two levels, where researchers interested in IT infrastructure flexibility can create sets of questions to evaluate an organization. At the organizational level, Duncan (1995) proposed an evaluator to ask if IT infrastructure flexibility regarding tangible and intangible resources was formal or informal. At the operational level, a researcher should consider investigating healthcare-based IT professionals’ perceptions to formal, or tangible and intangible IT infrastructure flexibility resources (Chen et al., 2014; Duncan, 1995).

Byrd and Turner (2000) confirmed that IT infrastructure flexibility consisted of tangible and intangible resources such as hardware, systems, network communications, critical data, operating systems, and data processing technologies. Also, Byrd and Turner (2000) suggested that IT infrastructure flexibility facilitates increasing customer demands without increasing costs. Top managers could accomplish IT infrastructure flexibility if they focus on implementation speed by including efficiency as a critical factor (Byrd & Turner, 2000; Li, Shepherd, Liu, & Klein, 2017). The study found the inclusion of efficiency to IT infrastructure flexibility adequately respond to new market conditions to assist organizations with future integration (Byrd & Turner, 2000; Li et al., 2017).

Chanopas, Krairit, and Khang (2006) found that IT infrastructure was a long-term asset that created long-term values for shareholders in an organization. Furthermore, Chanopas et al. (2006) explained that the IT infrastructure flexibility represented long-term options for an organization, and the construct involved substantial investments that affected an entire firm. In their findings, Chanopas et al. (2006) established credible support for top management in any organization to realize that the construct must sustain organizational changes, and top managers must not delay those changes past the allocated implementation budget. Similarly, Tawaha (2015) found that the construct directly contributed to business performances in customer orientation, service quality, organizational trust, and business performance. Subsequent research on IT infrastructure flexibility, Ward (2012) confirmed that organizations need to include IT infrastructure flexibility to allow for a flexible IT infrastructure that can adapt to change. Ward (2012) found that top management that focused on efficiency, responsiveness, and flexibility in their IT environment increase their infrastructure flexibility when implementing tangible and intangible resources including InfoSec.

Ribes and Polk (2014) developed three IT infrastructure flexibility sensitizing concepts, which became the groundwork of being able to perform investigative research in IT infrastructure. Sociotechnical changes were alterations found in organizations, which included data sharing techniques, ITM coordination, and collaboration techniques (Ribes & Polk, 2014). Ribes and Polk (2014) asserted that sociotechnical changes in IT infrastructure enabled organizations to monitor practical and technological arrangements capable of assessing pitfalls in long-term IT flexibilities. Organizations that understood sociotechnical changes were able to modify their environments to meet current user demands efficiently, and expediently deploy counter-measures to mitigate risks in enterprise resource planning systems deployment (Ribes & Polk, 2014). In large organizations, because of changes in technology demands and regulatory requirements, sociotechnical changes forged techno-scientific changes throughout IT infrastructure (Ribes & Polk, 2014). One such change in technology demands and regulatory requirements were InfoSec investments becoming vocal points of organizations infrastructures (Ribes & Polk, 2014). Top management with clear understandings of IT infrastructure flexibility was able to expediently deploy InfoSec changes as part of their strategic infrastructural change programs (Ribes & Polk, 2014).

SISP Success

SISP success is the successful creation of a SISP within the timeframe and budget set by top management (Ribes & Polk, 2014). Within this section, the critical components of SISP success are discussed, including the metrics by which SISP success is judged, and the conceptual model for SISP success. Also, this section addresses the relationship between IT and SISP. Byrd, Lewis, and Bradley (2006) found there was little SISP success at organizations that did not integrate IS/IT across the entire enterprise. Strategic information system plan success was the successful creation of a SISP that fulfilled the expectations of top management (Hoque et al., 2016). In their research, Byrd et al. (2006) provided a framework that could be deployed by top management to achieve SISP success. The framework includes integrating IS throughout the organization, granting the Chief Information Officer (CIO) more flexibility, and creating an IS/IT advisory board to forecast SISP activities.

The integration of IS throughout an organization needs to give the CIO authorities and a degree of responsibilities, the participation of top management and IT management support, and the creation of an IT advisory committee monitor and forecast SISP activities (Byrd et al., 2006). The CIO, although intimately involved in decision-making procedures with top management, was most likely to produce better SISPs (Byrd et al., 2006). Effective communication between the CIO, top management, and IT management was paramount so that the organization can forecast future IS/IT events to construct specific mitigation strategies to counter each event (Byrd et al., 2006). An IS/IT advisory committee consisting of senior IT management IS/IT personnel and users have a significant effect on SISP success (Byrd et al., 2006). Having a well-placed advisory committee resulted in a better understanding of the different views to incorporate the shared knowledge of committee members into a SISP (Byrd et al., 2006). Also, before executing a SISP, there must be potential for IS/IT applications and supports (Byrd et al., 2006). The research found firms that integrated IS/IT organization-wide with the use of an IS/IT advisory committee, and the supervisory authority of a CIO produced three outcomes vital to

SISP success: technology integration, data integration, and application functionality (Byrd et al., 2006).

Khani, Nor, and Bahrami (2011) provided a conceptual model for SISP success, which considered the inclusion of IT capability, so that top management could further explore environmental and organizational factors that influenced this relationship. Khani et al. (2011) defined IT capability as proficient skills gained through an organization that empowers it to utilize its assets efficiently. IT capability could be used as a subset to enable top management to further the opportunities to obtain further SISP success, and IT capabilities should be exploited as specialized and integrated knowledge of organization-wide IT infrastructure to create SISP success. To assist top management in obtaining a higher valuation, and substantial reinforcement of the SISP success, Khani et al. (2011) believed that allocating an organization's IS/IT resources was paramount. The incorporation and allocation of an organization's IS/IT resources would provide the sustainable long-term competitive advantage of controlling IT costs without affecting the objectives of the business IT implementation (Khani et al., 2011; Jorfi, Nor, & Najjar, 2017).

Synthesis of the Research Findings

Top Management Support

Sharma and Yetton (2011) made a case for top management support as being a critical factor in the successful implementation of IS projects. The authors made their case by proposing a contingency model based on meta structuration and the role of the institutional framework, which uses task-independence to moderate the effect of top management success (Sharma & Yetton, 2011). Because the authors viewed top management success as a critical factor, they developed a rich theory that brought to light modeling and mediating techniques affecting key contingencies, such as scarce resources controls by top management, management commitments symbolic actions, and management decisions (Sharma & Yetton, 2011). In their research, the authors added to the body of knowledge by shaping the intuitional context while identifying the role of top management support, and by making a case for contingency model task independence to shape intuitional context to implement successfully IS projects (Sharma & Yetton, 2011). Top management support becomes critical to the importance of hospitals to achieve SISP benefits (Lee, Elbashir, Mahama, & Sutton, 2014).

Sharma and Yetton (2011) found that task independent, which pertained to moderating the effect of top management support, has become the accepted practice in literature reviews. Further, firms have already developed task-free software such as Comprehensive Meta-Analysis (CMA; Sharma & Yetton, 2011). For instance, in cases where effects vary from one study to the next, CMA combined data from multiple studies to identify reasons for a variation (Sharma & Yetton, 2011; Lee et al., 2014). However, Sharma and Yetton (2011) showed that CMA could also be employed to identify specific effects in the event effect sizes were consistent from one study to the next. Firms consisting of multiple subgroups of top managers may find it useful to utilize the task-independent model to gain the most significant project success with regards to top management support (Sharma & Yetton, 2011; Lee et al., 2014).

Young and Jordan (2008) emphasized top management support as being the most important critical success factor. Top managers can provide or withhold their support voluntarily (Too & Weaver, 2014). However, Young and Jordan (2008) made significant realignment to make a case for convincing top managers of the importance of their support by summarizing a range of behaviors that might constitute top management support such as board-level attention because it consisted of the highest level of investment to project success. Further, high-level involvement made clear of project demands, full awareness of the business processes, and provided standard best practices for high-level decision making to assess risks (Young & Jordan 2008; Too & Weaver, 2014).

Young and Poon (2013) provided further evidence to influence and convince top managers who are reluctant to change due to their views of conventional wisdom. As explained by Young and Poon (2013), conventional wisdom emphasized on misdirecting efforts found during high-level planning made by competent project staff. Further, project governance may hamper IT project success as it may not resolve issues that surface during the life cycle of a project (Young & Poon, 2013). Analysis of top management support showed that high-level planning, project staff, project methodology, and user involvement were the minimum standard factors to measure success (Young & Poon, 2013).

Information Systems Plan

In their 2010 systematic literature search on information systems plan construct, Chen, Mocker, Preston, and Teubner established a framework, which served as a tool that identified three concepts. The first information systems concept viewed IS strategies as support for business strategies. In their established framework regarding IS strategies, Chen et al. (2010) instituted a top management strategy consisting of three subdomains: what was needed, how should it be done, and who needs to do it (Chen et al., 2010). In the second concept, Chen et al. (2010) gathered empirical evidence to suggest that IS strategies were a significant plan for the IS concept. According to Chen et al. (2010), IS strategy became a plan when it aimed to identify essential IS assets such as personnel, monetary resources and technologies, and whenever it began to allocate the existing IS assets in a useful and efficient manner. The last concept that complete their framework showed that IS strategies, once becoming a plan, must be viewed from an organizational perspective (Chen et al., 2010). This perspective made sure that "all members of the organization are heading in the same direction" (Chen et al., 2010, p. 43).

Liu (2015) added more on the usefulness of SISPs by inferring that top managers should develop an IS plan consisting of three general categories, financial systems, operational systems, and strategic systems. Liu (2015) showed that well-directed financial systems and operational systems could become an organization's strategic systems. However, the relationship between IS functions and corporate strategy must be one of the top management's priorities of interest Liu (2015). Failure to connect these two systems could hamper an organization from achieving SISP success. Liu (2015) found that SISP gave organizations a strategic advantage that significantly changed the way management conducts business. A precise definition of SISP is a system that enables firms to change or alter their business strategy and structure (Teubner, 2013). SISP supports and shapes competitive strategies, making the concepts of information system plans essential to top managers. The significance of SISP to top management is beneficial in supporting a variety of strategic objectives, including changes in business processes, and in the creation of innovative applications (Teubner, 2013).

Yang and Tanner (2011) created a model to assist with the usefulness of information systems plan that help described the interrelationship of inhibitors, enablers, and benefits of SISP. Yang and Tanner (2011) drew the model from a case study of a large organization in South Korea. Yang and Tanner (2011) found that there were six information systems plan inhibitors, which included limited knowledge of the planners, lack of top management support and understandings, lack of communication between top management and IT managers, lengthy IS planning, inadequate integration of business objectives, and insufficient understanding of the work needed to deliver and IS project plan. The enablers consisted of top management increasing commitment, business, and IT alignment while integrating strategies and objectives of the organization, and effective communication between top management and IT managers (Yang & Tanner, 2011). The benefits of using Yang and Tanner's (2011) model help with organizational objectives to be accomplished, and ensure capability, collaboration, flexibility, and competency. The information system plan is a critical construct for hospitals to implement as part of their SIS plan to achieve InfoSec benefits.

Infrastructure Flexibility

Furukawa and Minami (2013) proposed a penalty of change concept that could help bridge the gap between top management business strategy and IT. In later research, Furukawa (2013) found that the critical challenge to strategic information system is with environmental changes. A change to the environment requires top managers to maintain a higher level of alignment that could create a higher risk of IT investments. As stated by Furukawa, Hirobayashi, and Misawa (2014), to maintain this alignment, top management must make their IT systems flexible. To allow for IT system flexibility possible top management could make use of penalty of change as a function consisting of cost and time.

The three studies found three strategic gaps that were problematic for top management and IT managers' strategic alignment best practices (Furukawa, 2013; Furukawa et al., 2014; Furukawa & Minami, 2013). Organization strategy is a concern whenever top management fails to accurately calculate for a length of time for implementing new applications, not factoring business needs for the modification, and misallocating tangible and intangible assets to make IT run efficiently (Furukawa et al., 2014; Furukawa & Minami, 2013). Further, the business strategy was a topic of concern when top management failed to factor accrued expenses beyond the scope of a project.

IT strategy was mentioned as an issue when inadequate or unqualified human resources were allocated to a project that was beyond their capabilities to save on costs (Furukawa et al., 2014; Furukawa & Minami, 2013). The three-part empirical research calls for top management and IT managers to combine their efforts when planning for SIS, so changes are recognized quickly, and decisions are made to mitigate these changes in a timely fashion. Moreover, implementation and countermeasures to the identified changes are mitigated promptly (Furukawa, 2013; Furukawa et al., 2014; Furukawa & Minami, 2013).

Kumar and Stilianou (2014) explored IT infrastructure flexibility in further detail and presented a process model consisting of eight steps for managing flexibility. The presented process model includes steps to understand the flexibility as contextual factors by incorporating environmental, organizational, and IS elements. Exhibited in Kumar and Stilianou's (2014) research, the next step was to recognize reasons for the importance of flexibility such as responses to changes in technology, changes in IS/IT business strategies and processes, and changes in the level, locations, and type of available system resources. Kumar and Stilianou (2014) included strategies to evaluate needs for flexibility such as in the allocation of IT investment, personnel assignment, modification of systems, scope and duration of contracted work, and infrastructure standards and scalability. To identify flexibility categories and stakeholders, Kumar and Stilianou (2014) mentioned flexibility in IS operations, flexibility in IS service development, and flexibility in IS management. For diagnosing types of flexibility needs on an organization, Kumar and Stilianou’s (2014) framework presented financials, integration, operation, development, sourcing, staffing, and new technology deployment flexibilities. Infrastructure flexibility is an essential construct for hospitals to implement so that their SISP can achieve InfoSec success (Kumar & Stilianou, 2014).

SISP Success

Ali, Mohamad, and Tretiakov (2013) constructed a theoretical framework consisting of top management commitment and user participation in IS planning to obtain SISP success. Nested within their framework, Ali et al. (2013) constructed a realistic view of top management commitment, explained as awareness, involvement, and proactive advancement at all level of a strategic IS plan. An organization possessing a proactive advancement to top management commitment provided more robust and expedient information relevant to specific organizational strategic goals and objectives and must play a leading role in any strategic IS plan process (Ali et al., 2013; Yeh, Lee & Pai, 2015). Conversely, user participation, which is the degree of involvement of regular employees in strategic IS plans, provided relevant internal and external information pertinent to the SISP process (Ali et al., 2013). Ali et al. (2013) viewed both top management and users as resources allocated to a strategic IS planning process; thus, their involvement significantly enhanced the success of an organization’s strategic IS plan.

To understand synergies and tradeoffs between flexibilities, Kumar and Stilianou (2014) cautioned top management to be aware of the multidimensional nature of flexibility. The reason is that multiple types of flexibility were desirable for top management to address their environmental conditioned so that their organization IT infrastructure flexibility remains aligned with business strategies (Kumar & Stilianou, 2014). Their research prescribed strategies for top management and IT managers aimed at managing IT infrastructure flexibility such as actions aimed at developing IS/IT strategies and IS/IT architectures (Kumar & Stilianou, 2014). Organizations with well-established IT infrastructure flexibilities were found to have created three significant categories of flexibilities such as flexibility in IS operations, flexibility in IS systems, and services development and deployment, flexibility in MIS. These categories were able to expedient and efficiently assist those organizations in becoming flexible (Kumar & Stilianou, 2014). To achieve InfoSec benefits, hospitals should understand the importance of SISP success (Kumar & Stilianou, 2014).

The four constructs established by Lederer and Hannu (1996), top management support, information systems plan, infrastructure flexibility, and SISP success, are critical pillars for hospitals to achieve InfoSec benefits (Ali et al., 2013; Kardan & Akbarnejad, 2014). Hospital IT managers do not fully understand these four constructs, and the lack of knowledge on the four constructs can become a compliance issue in the aftermath of a significant security breach (Clemons, 2015; Kumar & Stilianou, 2014). Understanding the importance of adopting these four constructs in their SISP plans, hospitals could achieve InfoSec success (Clemons, 2015; Furukawa, 2013; Furukawa et al., 2014; Furukawa & Minami, 2013).

Critique of Previous Research Methods

Critiques of previous research methodologies have found a gap in the literature where a limited number of researchers have conducted empirical multiple case studies specifically aimed at assisting Florida hospitals with obtaining the expected InfoSec benefits when implementing SISP (Kardan & Akbarnejad, 2014; Ursacescu, 2014). The Elysee (2012) study, which challenged future researchers to add the SISP bodies of knowledge by qualitatively investigate the relationship of the four constructs to InfoSec, did not explicitly select any of the 18 specific business sectors to conduct further research. However, Elysee (2012) left the opportunity of choosing one of the 18 industry sectors at the discretion of the researcher. Chuang and Inder (2009) suggested that a multiple case study would adequately measure strategic successes of participants because such research would examine participants from a multitude of state-wide hospitals. To resolve potential limitations, critiques of previous research methodologies favor a multiple case study approach, instead of a grounded theory research methodology (Khani et al., 2011; Jorfi et al., 2017). A multiple case study would add rigor and would assure credibility, dependability, bias, transferability, and goodness (Chuang & Inder, 2009).

The inclusion of rigor credibility to a multiple case study methodology is reflected in the comparative examination of existing SISP applications with Florida hospitals' InfoSec strategies while conducting early-stage literature reviews (Khani et al., 2011; Jorfi et al., 2017). The purpose of this qualitative multiple case study was to identify the factors that prevented Florida hospitals from obtaining InfoSec benefits to prevent crypto-malware attacks when implementing SISP. The literature review presented in this chapter has shown the need for this study and how this research could benefit hospitals in containing InfoSec benefits. The literature review presented in this chapter has highlighted a gap in the literature exists regarding InfoSec benefits during the SISP process in hospitals since the need has not been explored in greater empirical depths (Mishra et al., 2014). Therefore, the problem to be addressed within the study is why SISP does not return the expected InfoSec benefits in hospitals in the United States, specifically in Florida (Lee et al., 2015).

Summary

The literature review in this chapter presented the methods of researching, the theoretical orientation for the study, and the review of the literature. The literature review presented primary and current literature of the four SISP constructs, agency theory, and SISP theory. Each construct helped support this multiple case research. The researcher reviewed the foundation of each construct and presented the information in chronological order. Finally, the critique of previous research methods was presented to reinforce the reason for choosing a multiple case study, as opposed to a grounded theory methodology. It was important to look at this in a hospital setting to see what was needed to be done to gain InfoSec success. Chapter 3 presents the methodology for this multiple case study.

CHAPTER 3. METHODOLOGY

The purpose of this qualitative multiple case study was to identify the factors that prevented Florida hospitals from obtaining InfoSec benefits to prevent crypto-malware attacks when implementing SISP. For this research study, the researcher sought to determine the causes of changes that are associated with the observed phenomenon (Hyett, Kenny, & Dickson-Swift, 2014; Maheshwari & Vohra, 2015). This chapter presents the purpose of this research, the research question, and the research design used in this study. Additionally, this chapter presents a description of the targeted population and the methods used to select participants for this study. Furthermore, this chapter provides an in-depth discussion of the procedures used to conduct the study, the strategy used for collecting data, and the known ethical considerations of the study.

Purpose of the Study

The purpose of this qualitative multiple case study was to identify the factors that prevented Florida hospitals from obtaining InfoSec benefits to prevent crypto-malware attacks when implementing SISP. By investigating the four SISP constructs, this study contributes to the body of knowledge in research of information technology in industry and social science research. The research may contribute to hospitals by assisting top management in acquiring InfoSec benefits (Elysee 2012; Lee et al. 2015; Mishra et al. 2014). InfoSec benefits protect organizations from crypto-malware attacks, virus attacks, and spyware and worm attacks, which can cause severe disruptions to organizations (Georg, 2017; Kenyon & McCafferty, 2016; Richards, 2016). InfoSec benefits also protect data from theft by providing confidentiality, integrity, and availability of information to authorized users (Syväjärvi et al., 2017).

Research Questions

To understand better why Florida hospitals fail to obtain the full InfoSec benefits when implementing information systems plans SISP, the researcher developed the following research questions:

RQ 1: How do IT managers describe the process their organization went through to secure top management support before initiating strategic information systems planning as an InfoSec advantage?

RQ 2: How do IT managers describe the usefulness of SISP to obtain InfoSec benefits?

RQ 3: How do IT managers describe the InfoSec benefits to the degree of information technology infrastructure flexibility?

RQ 4: How do IT managers describe the degree of SISP success to their InfoSec environments?

Research Design

The researcher used a qualitative multiple case methodology and conducted interviews with senior managers, directors, senior directors, and CISOs who work at for-profit and nonprofit hospitals in Florida. Researchers have conducted studies related to different aspects of SISP (Elysee 2012). However, to date only a limited number of qualitative studies have been conducted using a multiple case study approach to assess the alignment of SISP with IT to create an InfoSec benefit in Florida hospitals (Coronado, & Wong, 2014; Jaana et al., 2014; Mishra et al., 2014). To address these gaps in the literature and to add to the body of knowledge of SISP, this study used a multiple case study methodology and sampled participants from a pool of IT

professionals who work for Florida hospitals to investigate a set of research questions derived from the four SISP constructs (Georg, 2017; Richards, 2016; Yin, 2009; Yin 2013).
Elysee (2012) argued that future researchers add to the body of knowledge on SISP through qualitative investigations into the relationship of the four constructs of InfoSec that the relationship of the four constructs in Hartono, et al. (2003) discussed in their seminal work. These four key SISP constructs are top management support, the usefulness of SISPs, the degree of information technology infrastructure flexibility, and the degree of SISP success (Hartono et al., 2003).

Moreover, Chuang and Inder (2009) found that organizations operating in the healthcare sector do not have efficient frameworks to take advantage of SIS with the business to construct inexpensive and expedient strategic plans. The healthcare sector comprises of companies, such as hospitals, which specialize in products and services related to health and medical care (Elysee, 2012; Georg, 2017; Richards, 2016). The lack of efficiency in SIS frameworks is beginning to cause businesses in the healthcare sector to become vulnerable to frequent cyberattacks like malware, crypto-malware, and denial of service attacks (Georg, 2017; Kenyon & McCafferty, 2016; Richards, 2016). Wilkin et al. (2016) expanded on the topic by illustrating that this problem was because of costs associated with running the organization, and local, state, and federal regulatory compliance mandates. Wilkin et al. (2016) found a growing need for healthcare-based firms to produce sound organization-wide SISP to align their SIS with IT to obtain InfoSec benefits.

Target Population and Sample

One responsibility of researchers is to produce reliable samples that generate relevant information on an observed phenomenon (Marshall, Cardon, Poddar, & Fontenot, 2013). Similarly, Denzin and Lincoln (2011) showed that in qualitative studies, researchers must reflect the intended frame they are studying to the scope of the research. Finally, Miles, Huberman and Saldana (2014) underscored the importance of research questions that are consistent with the conceptual framework. To this end, the researcher used a sample size and selection procedures that were consistent with the research question and the theoretical framework.

Population

The researcher conducted this qualitative multiple case study by conducting face-to-face interviews with IT professionals who work at Florida hospitals and who have five years or more of experience in SISP and InfoSec. The population for this study came from the 2015 Directory of Hospitals, published yearly by the Florida Hospital Association (FHA). The Directory of Hospitals consists of all nonprofits and for-profit member hospitals licensed to operate in Florida. The names of licensed hospitals, their locations, and the contact information for the hospitals' top management who run the day-to-day operations of hospitals are listed in the directory (Davis, 2014). The Directory of Hospitals also contains information about the hospitals' top management, their office phone number and address. The FHA advocates on behalf of Florida-licensed member hospitals on issues that assist member hospitals in their community services and patient care missions (Davis, 2014).

Sample

The researcher used a purposive sampling method to select 15 senior executives from hospitals listed in the FHA Directory of Hospitals (Davis, 2014; Orcher, 2005). The purposefully selected, randomly sampled group of top management identified the IT professionals affiliated with their hospitals to be contacted for participation in this study (Davis, 2014; Houghton, Casey, Shaw, & Murphy, 2013; Marshall et al., 2013; Miles et al., 2014; Orcher, 2005; Stewart, 2012; Yin, 2013). All possible participants in the sample were Florida hospital IT professionals with expertise in InfoSec and an extensive SISP background (Gill, Stewart, Treasure, & Chadwick, 2008; Mason, 2010). The researcher excluded those respondents who did not possess five years or more professional experience in SISP and InfoSec. Participants who did not have any experience in SISP and InfoSec were those who had less than five years as a Florida hospital IT professional, less than five years employed at Florida hospitals, less than five years engaged in strategic IS plan and less than five years engaged in InfoSec. The researcher also excluded participants with less than five years of professional experience in SISP and InfoSec. The final sample size was 15 of these professionals.

Procedures

Participant Selection

After obtaining Institutional Review Board (IRB) approval from Capella University, the researcher sent introductory outreach recruitment letters to top management at hospitals licensed to operate in Florida and listed in the FHA 2015 Directory of Hospitals. These introductory outreach and recruitment letters included a personal introduction and asked top management to recommend an IT professional to participate in this qualitative multiple case research. If an introductory outreach and recruitment letter did not reach the intended top management, then a request was made to forward the letter to that person. Once approval was granted by top management, and they provided the names of potential research participants, the researcher sent recruitment emails to these Florida hospital IT professionals. The recruitment email explained that they had been selected by top management to participate in this qualitative multiple case research. Those who responded and showed interest in participating in this study were sent an email containing a participant recruitment screening question, and a copy of the IRB-approved informed consent form, which explained more about the purpose of the study and that their participation was voluntary.

The researcher waited 15 business days for a reply. After the allotted time, if fewer than 30 replies were received, the researcher followed up with other possible participants. The researcher contacted, via a telephone call, those who did not respond to the initial call for recruitment. If there were no replies, then another list of randomly purposive samples was generated, and the cycle began again (Davis, 2014; Marshall et al., 2013; Miles et al., 2014; Orcher, 2005). Additional emails were sent to top management from the original list found in the Directory of Hospitals if fewer participants than anticipated responded (Davis, 2014; Miles et al., 2014).

The participant recruitment screening questions that the researcher sent to potential participants served as a tool to select participants who were engaged in SISP and InfoSec operations in their hospitals. Answers provided by participants from the participant recruitment screening questions provided the inclusion and exclusion criteria for this study and helped identify participants who met the inclusion criteria. Participants were given instructions to answer the participant recruitment screening questions and to submit their answers to the researcher via email. Recruitment question responses were carefully reviewed and classified into two categories. The first category consisted of participants who had professional experience in Florida hospitals SISP and InfoSec. The other category comprised responses from participants who did not have any or had limited, experience in Florida hospitals SISP and InfoSec. Additionally, those selected for this study had more than five years of employment as a Florida hospital IT professional, more than five years employed at their current roles as IT professionals, more than five years engaged in strategic IS plan, and more than five years engaged in InfoSec (Creswell & Creswell, 2017; Yin, 2013).

Protection of Participants

The researcher protected participants’ identities by segregating their interview responses in separate notebooks, and by separating their information in separate folders. The researcher further protected participants, the research questions, and answers by transferring the collected data from notebooks and digital audio recorders to Microsoft Word, Excel, and digital audio recorder software. This method ensured that identifiable information unique to participants were gathered and transferred to a reliable technology format. To further protect participants who volunteered to take part in this research, the researcher provided participants with an IRB-approved informed consent letter, which explained more about the purpose of the study and that their participation was voluntary. The researcher destroyed senior executives and participants' email addresses after the completion of this study (American Psychological Association, 2017; Miles et al., 2014; National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979).

Expert Review

A group of experts consisting of five specialists in the field of ITM, InfoSec, MIS, healthcare-based MIS, and business management, tested the preliminary interview questions. The team of experts gave their assessments, as well as their constructive criticisms on the formatting of follow-up questions based on the four constructs. The expert panel feedback indicated that the research questions would be more useful if each question was broken down into the structure of each construct.

Data Collection

The researcher used an unobtrusive method of data triangulation, which suggests that as soon as a proposal has been established by "two or more independent measurement processes" the improbability of its clarification is significantly reduced, (McDavid, Huse, & Hawthorn, 2012, p. 94). The researcher employed triangulation due to its ability to be the most effective measurement process based on face-to-face interviews. The researcher must depend on a variety of methods to gather data, such as face-to-face interviews, research memos, research notes, and digital voice recorders of participants to contribute to the trustworthiness of collected data. The purpose of using triangulation is to generate research data that is credible, transferable, and valid.

The researcher sent a recruitment email to Florida hospital IT professionals that invited them to participate in this research study. The recruitment email informed participants that the reason for their receipt of the email was because their organization's top manager identified them as a Florida hospital IT professional. This email also explained the purpose of the study, and what would be expected of them if they decided to participate. The recruitment email sought participants' consent to participate in a face-to-face interview at their organization, which took approximately 50 minutes (Creswell & Creswell, 2017; Yin 2009; Yin 2013).

Participants who showed interest in volunteering for this study were encouraged to send a reply to the researcher via email, at which time they were sent the participant recruitment screening questions questionnaire. The participant recruitment screening questionnaire consisted of five questions. These questions served as a tool to aid in selecting participants who were engaged in SISP and InfoSec in their respective Florida hospitals. Accompanying each participant recruitment screening questionnaire was an informed consent form. The inform consent form clearly stated that there were no anticipated risks to the participants, or to their organizations based on their participation in this study, and there were no expected of benefits to them or their organization in participating for this research (Creswell & Creswell, 2017; Yin, 2013).

The researcher gave participants instructions to review the informed consent form and sign it if they consented to participate, to complete the screening questionnaire, and to submit these forms to the researcher via email. The researcher also provided his telephone number for the participants to call if they had further questions about the research and their participation (Creswell & Creswell, 2017; Creswell & Miller 2000; Yin, 2013).

The researcher reviewed all participants' returned answers to the participant recruitment screening questions questionnaire. The researcher emailed those participants who met the study requirements and assured them that they may ask questions while being interviewed and may terminate the interview process at any given time and for any reason. The researcher advised participants that digital recording hardware would be employed for later transcription and that these transcripts would be analyzed using NVIVO 11 Pro Qualitative Data Analysis software. The researcher informed participants that they had the opportunity to review these interview transcripts (Creswell & Creswell, 2017; Creswell & Miller, 2000; Yin, 2013).

This study relied on open-ended questions for the interview protocol. The researcher developed the open-ended questions so that participants could discuss their experiences regarding the success of SISP based on the four selected constructs. The interview protocol made use of well-crafted open-ended face-to-face interview questions following the guidelines established by Creswell & Creswell (2017).

The researcher conducted each face-to-face interview at the participant's work location, or a private place free from distractions and interferences. Participants also had the option to complete the interview via phone, Skype, or WebEx for video conferencing if the need arose. The goal of the face-to-face interviews was to conduct them at locations where there were minimal interferences. The researcher asked each participant a total of 12 questions, grouped in a series of three questions for each of the four constructs. The answers that participants gave were later analyzed and yielded information relevant to SISP and InfoSec success Florida hospitals (Creswell & Creswell, 2017; Yin, 2013).

The researcher used naturalistic observation (i.e., unstructured observation) to study the spontaneous behavior of participants during face-to-face interviews and recorded the reaction of participants while they answered the interview questions. The naturalistic observation allowed the researcher to study the whole situation by observing moods and body languages displayed by participants (Creswell & Creswell, 2017; Yin, 2013). Using this technique enabled the exploration of avenues of inquiry not thought of before in the research (Houghton et al., 2013; Miles et al., 2014; Stewart, 2012; Yin, 2013).

The researcher created a memo for each face-to-face interview participant while conducting the research. These memos captured the opinions of participants' experiences in SISP, took account of participant reactions to SISP successes, and created relations generated from the interviews. These memos also allowed for comparisons between participants' experiences on SISP constructs and InfoSec success (Creswell & Creswell, 2017; Yin, 2013). The researcher wrote research notes during and after each interview. These notes focused on participants' impressions, the use of body language in responding to each research question, and responses to follow-up probing questions (Yin, 2013). The interview research notes examined experiences that participants expressed during the interviews (Yin, 2013).

The researcher used a digital audio recorder in each interview. The digital audio recorder captured the name of the participant, the location of the interview, and its date and time. The researcher employed the digital audio recorder throughout the interview. Before stopping the digital audio recorder, the researcher indicated that the interview had ended and noted the date and time of the end of the interview. Audio recordings were automatically transcribed using the digital audio recorder, which also converted spoken words of participants into text that were saved into a word-processing program. Transcripts were uploaded to NVIVO 11 Pro, a qualitative data analysis software to help identify themes and subthemes for this research.

During the interviews, the researcher asked each participant if there were any additional documents on InfoSec policies, procedures, or guidelines which the researcher could review. The researcher examined each participant's company's website for any publicly available documentation on InfoSec policies, procedures, and guidelines. The researcher kept these documents private per participants' instructions and returned documents if participants requested. These additional documents were deidentified and summarized in Chapter 4 (Creswell & Creswell, 2017; Miles et al., 2014; Stewart, 2012; Yin, 2009; Yin, 2013).

Data Analysis

Braun and Clarke (2006) described six steps of thematic analysis (TA), which the researcher will use to analyze the data from this study. The six steps of TA are described as linear, which means that no one phase can proceed to the next phase without correctly completing the preparatory phase (Braun & Clarke, 2006; 2013; Creswell, 2009; 2013; Creswell & Poth 2018; McDavid et al., 2012). The researcher performs a constant comparison of the data; there is a back-and-forth involved in this analysis as well. During the first phase, familiarization, the researcher became familiar with the data by reading and re-reading the data and making a note of any initial analytic observations (Braun & Clarke, 2006; 2013). In the coding phase, the researcher generated concise labels for the essential features of the collected data and looked for statements relevant to the research questions (Braun & Clarke, 2006; 2013). The researcher coded all data and terminated this phase by organizing all codes and data extracts by order of relevance (Braun & Clarke, 2006; 2013; Creswell & Poth 2018; McDavid et al., 2012).

The researcher then searched for themes from the coded data using NVIVO 11 Pro, a computer-assisted qualitative data analysis (CAQDA) tool that helps researchers organize coded data relevant to each theme to complete step 3. In step 4, the researcher reviewed the themes concerning the extracted data and the full dataset. Each theme’s name helped define the nature of that theme and its thematic relationships (Braun & Clarke, 2006; 2013 Creswell & Poth 2018;

McDavid et al., 2012). During the define and name phase, the researcher conducted and wrote a detailed definition of each theme and identified the essential substance of each theme. The researcher also constructed a concise, effective, and informative name for each theme (Braun & Clarke, 2006; 2013; Creswell & Poth 2018; McDavid et al., 2012). In the last phase, the researcher wrote up the results, putting together the data extracts and the analytic descriptions to convey a coherent and persuasive story about the data, and to contextualize the data in relation to existing literature (Braun & Clarke, 2006; 2013; Creswell & Poth 2018; McDavid et al., 2012).

Instruments

Role of the Researcher

The researcher served as the interviewer who facilitated each interview and analyzed all collected data. For this qualitative multiple case study standardized, open-ended interview questions methods were employed to collect data from the participants (Houghton et al., 2013). Open-ended interviews allow flexibility in case new data emerge during the research process. As the interviewer, the researcher was the listener and employed effective listening skills while being mindful of participants' sensitivities. The researcher analyzed the data for patterns and themes based on the results of the research questions. The researcher also analyzed the data patterns for attributes and perspectives of participants and the goal of the research.

Researcher-Designed Guiding Interview Questions

The researcher developed four guiding interview questions based on the four constructs of SISP for this research study. Within these four guiding questions, there are a series of further probing questions and they are as follows:

Construct 1. Top management support. How would you describe the degree of top management support to high-level IT planning within your organization (Young & Jordan, 2008; Sharma & Yetto, 2011; Young & Poon, 2013). How would you describe the interpersonal interactions of project staff on SISP and InfoSec within your organization (Sharma & Yetto, 2011; Young & Jordan, 2008; Young & Poon, 2013). What type of user involvement do you encounter during a SISP (Sharma & Yetto, 2011; Young & Jordan, 2008; Young & Poon, 2013).

Construct 2. Information systems plan. How would you describe the intensity of communications of top management on business goals (Byrd, Sambamurthy, & Zmud, 1995; Chen et al., 2010; Gottschalk 1999b; Gottschalk 2002; Hann & Weber, 1996, Hemmatfar et al., 2010; Yang & Tanner, 2011). How have the intentions of top management on executing SISP impacted your organization's InfoSec (Byrd, et al., 1995; Chen et al., 2010; Gottschalk 1999b; Gottschalk 2002; Hann & Weber, 1996; Hemmatfar et al., 2010; Yang & Tanner, 2011). What are your agency goals regarding initiation, and planning phases of SISP for InfoSec (Byrd, et al., 1995; Chen et al., 2010; Gottschalk 1999b; Gottschalk 2002; Hann & Weber, 1996; Hemmatfar et al., 2010; Yang & Tanner, 2011).

Construct 3. Infrastructure flexibility. What are the implications for InfoSec of the organizational strategies you are using for information technology (Furukawa, 2013; Furukawa, & Minami, 2013; Furukawa et al., 2014; Kumar & Stylianou, 2014). How does IT management incorporate top management business strategies into the overall business needs at your organization (Furukawa, 2013; Furukawa, & Minami, 2013; Furukawa et al., 2014; Kumar & Stylianou, 2014). What effect on InfoSec of using contract labor for major IT projects have you observed (Furukawa, 2013; Furukawa, & Minami, 2013; Furukawa et al., 2014; Kumar & Stylianou, 2014).

Construct 4. SISP success. What is your experience in participating in SISP processes (Ali et al., 2013; Kumar & Stilianou, 2014). How has the participation of top management affected your organization's SISP to achieve InfoSec success (Ali et al., 2013; Kumar & Stilianou, 2014). How does IT management cope with staffing changes turnover during a SISP, (Ali et al., 2013; Kumar & Stilianou, 2014).

Ethical Considerations

The researcher protected the identity of each participant by segregating their answers in separate notebooks, and by separating their information into separate folders. The researcher further protected participants, the research questions, and answers by transferring the collected data from notebooks and digital audio recorders to Microsoft Word, Excel, and digital audio recorder software (Creswell & Creswell, 2017; Yin, 2013). The abovementioned method ensures that identifiable information unique to participants are gathered and transferred to a reliable technology format. The researcher will destroy top management and participants' email addresses after the completion of this qualitative multiple case study (American Psychological Association, 2017; Miles et al. 2014; National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979).

On July 12, 1974, the National Research Act became law, which created the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (American Psychological Association, 2017; Miles et al., 2014; National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). The Commission identified important ethical principles for conducting behavioral and biomedical research concerning human subjects. The Commission also developed guidelines for those doing studies to follow, so that researchers carried out those policies (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979; Drew & Hardman, 2007; Miles et al., 2014). Based on the guidelines from the Commission, researchers must consider the role of assessing risks of research involving human subjects. Also, a researcher must create appropriate guidelines for the selection of human subjects who will participate in such study, the nature of the study, and have a well-defined of participants' informed consent in various research settings (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979; Drew & Hardman, 2007; Miles et al., 2014).

Based on the guidelines from the Commission, as mentioned earlier principles, the researcher obtained approval from the IRB, before beginning any research activities. The IRB approval process certified that the research conformed to the guidelines for assessing risks associated with conducting behavioral and biomedical research concerning human subjects. Further, the researcher ensured that all participants had a complete understanding of the purpose of the research, the methods that were used to collect data, all associated risks from being involved in this study, and the expectations placed upon them as participants, (Jones & Kottler, 2006). To mitigate risks associated with participating in this study, the researcher obtained third-party consent from Florida hospitals top management before contacting participants for this study. The researcher also received direct consent from participants before sending the participant recruitment screening questions for face-to-face interviews (Miles et al., 2014). The informed consent form contained three elements as follows: capacity, information, and voluntariness (Drew & Hardman, 2007). The researcher used their Capella University email address for all research-related correspondence. Further, this email address was used to correspond with the research study participants, communicate with participants, and generate paper trails that were consistent with, and relevant to, the research.

In 1979, the *Belmont Report* disclosed three essential principles that researchers must abide by when dealing with human subjects, which are benevolence, justice, and respect (U.S. Department of Health and Human Services, National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). These three principles were later cited in Blumberg, Cooper, and Schindler (2008) and again by the American Psychological Association (2017). Recent research by Miles et al. (2014) mentioned that when conducting interviews, further ethical considerations included honesty for the reorganization of other's work and contributions and bracketing when analyzing and reporting findings. Blumberg et al. (2008) also stated that when conducting research, the researcher must ensure the protection of the rights and safety of all willing participants. Researchers must remain within the scope of the study, and examiners must perform and deliver their research using the highest form of the code of ethics.

The researcher protected the identity of each participant by segregating their interview responses in separate notebooks, and by separating their information in separate folders. The researcher further protected participants, the research questions, and answers by transferring the collected data from notebooks and digital audio recorders to Microsoft Word, Excel, and audio recorder software. This method ensured that identifiable information unique to participants were gathered and transferred to a reliable technology format. To further protect participants who volunteer to take part in this research, an IRB-approved informed consent letter, which explained more about the purpose of the study and participation was voluntary. The researcher will destroy senior executives and participants' email addresses after the completion of this study (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979; American Psychological Association, 2017; Miles et al., 2014).

Issues of Trustworthiness

Graneheim and Lundman (2004) reported that establishing credibility in a research study must employ specific interview questioning. These questions helped the researcher gather data based on answers given by participants. The researcher made sure that data collection and data analysis remained within the scope of the research, which allowed credibility in this qualitative multiple case research. The researcher used methodological triangulation with observation to establish further credibility in this study (Graneheim & Lundman, 2004).

In qualitative research, transferability entails transferring results in other contexts, and make results applicable to simulator situations or studies (Trochim, 2006). Further, qualitative researchers must provide precise descriptions of contexts methods of participant selection, must provide detailed procedures used to collect data, and must use accurate data analysis procedures (Trochim, 2006). Qualitative research studies are judged by the consistency of the investigation, the credibility of collected data over some time, and the dependability of the collected data (Trochim, 2006). Houghton, Casey, Shaw, and Murphy (2013) provided examples to researchers pursuing a qualitative multiple case study to follow and illustrated specific strategies used to ensure the credibility of their research, which reinforced and confirmed previously mentioned concepts from (Trochim, 2006). The researcher followed the guidelines of Trochim (2006) and

Houghton, et al. (2013) for data transferability to establish rigor, and to enhance the transferability of the study.

In qualitative research, dependability endorses the predispositions of a researcher, which include being made accountable for methods adapted to conduct the study (Shenton, 2004; Trochim, 2006). Dependability also acknowledges for accountability in the report, gives reasons for preferring one’s approach as opposed to other approaches, and reports weaknesses in the techniques used to conduct the research (Houghton et al., 2013; Miles et al., 2014; Shenton, 2004; Trochim, 2006). Throughout this study, the researcher clearly stated the methods and steps undertaken in the research, the procedures used for data collection and analysis, and the assessments of participants’ answers that led to the formation of recommended best practices.

Shenton (2004) made a case for employing the positivist investigative method, which is preferential for ensuring internal validity, external validity, objectivity, and reliability. The positivist method, known as the Guba Constructs, has been accepted by many qualitative researchers (Shenton, 2004). The researcher employed Guba Constructs to make sure that the study remains trustworthy.

Summary

The purpose of this qualitative multiple case study was to identify the factors that prevented Florida hospitals from obtaining InfoSec benefits to prevent crypto-malware attacks when implementing SISP. The study investigated the four SISP constructs and attempted to contribute to the body of knowledge in the research of SISP. The contribution made from this research may assist hospitals with acquiring the necessary knowledge on how to align SISP with IT to effectively, and efficiently manage their IT departments to obtain InfoSec success. In

Chapter 4, the researcher will discuss the research findings based on the data analysis from this qualitative multiple case study.

CHAPTER 4. PRESENTATION OF THE DATA

The purpose of this qualitative multiple case study was to identify the factors that prevented Florida hospitals from obtaining InfoSec benefits to prevent crypto-malware attacks when implementing SISP. By investigating the four SISP constructs, this study contributes to the body of knowledge in research of information technology in industry and social-science research. This contribution may assist Florida hospitals in acquiring InfoSec benefits (Elysee 2012; Lee et al., 2015; Mishra et al., 2014). InfoSec benefits protect organizations from crypto-malware attacks, virus attacks, and spyware and worm attacks, which can cause severe disruptions to organizations (Georg, 2017; Kenyon & McCafferty, 2016; Richards, 2016). InfoSec benefits also protect data from theft by providing confidentiality, integrity, and availability of information to authorized users (Syväjärvi et al., 2017).

InfoSec benefits also involve policies and procedures that protect users from having their passwords compromised (Kitsios & Kamariotou, 2018). InfoSec benefits increase computer performance and reduce computer failures by monitoring automatic updates of operating systems (Pankratz, & Basten, 2018). InfoSec benefits provide remote privacy to users by allowing users to store data and files anywhere without fear of cyberattacks (Georg, 2017; Kim, 2018). Obtaining InfoSec benefits is vital for Florida hospitals, so that they continue to remain compliant to federal regulations and mandates (Elysee, 2012; Kim, 2018; Lee et al., 2015; Mamonov, & Benbunan-Fich, 2018; Mishra et al., 2014; Pankratz, & Basten, 2018).

Chapter 4 begins with an introduction to the study and description of the role of the researcher. Next, the chapter describes the sample, which includes a table containing the demographics of participants. The chapter also includes a recapitulation of the methodology used to analyze the data. The data and results are then presented in detail, and the chapter concludes with a summary of the results.

Description of the Sample

The sample for this study included 15 participants from for-profit Florida hospitals and four participants who represented nonprofit hospitals in Florida. The researcher chose to investigate this phenomenon because Elysee (2012) suggested adding to the body of SISP knowledge by conducting qualitative research in SISP, as little empirical research has been conducted to assist Florida hospitals to obtain the expected InfoSec benefits when implementing SISP (Kardan, & Akbarnejad, 2014; Ursacescu, 2014; Weech-Maldonado et al., 2018). Furthermore, the researcher is interested in this phenomenon because various researchers have conducted studies related to different aspects of SISP. However, only a limited number of qualitative studies have been conducted using the case study approach to assess the alignment of SISP with IT to create an InfoSec benefit in the healthcare environments (Coronado, & Wong, 2014; Jaana et al., 2014; Mishra et al., 2014).

A set of three questions from each of the four constructs established by Lederer and Hannu (1996) were carefully formulated by the researcher and approved by their mentor. In their seminal work, Lederer and Hannu (1996) identified top management support, the degree of information system plan, the degree of information technology flexibility, and SISP success as the four primary constructs for successfully adapting to an organization-wide SISP. These four constructs were later reinforced by Yang and Tanner (2011) in a comprehensive case study review of SISP in a sizeable Korean firm. The general theory used to understand the phenomenon was Shapiro’s (2005) agency theory because of its use in the study of ITM and

MIS, and it provides guidelines to all parties to behave in their own best interests and contributes to ITM and MIS project success (Mahaney & Lederer, 2011; Sirisomboonsuk et al., 2017).

There are 15 participants included in this research study. Five participants were women, and 10 participants were men. Ten participants were senior directors in their organizations, while two were directors, and one was a senior manager. The other two were CISOs in their organizations. Five participants worked for single hospitals, while the other 10 worked for multiple hospital systems. Finally, four participants worked for nonprofit hospitals, and the other 11 worked for for-profit hospitals. Table 1 displays these participant demographics.

Table 1
Participant Demographics

Participant	Position	Hospital	Profit Status
1	CISO	Multiple	For-profit
2	Director	Single	For-profit
3	Senior Director	Multiple	Nonprofit
4	Senior Director	Single	Nonprofit
5	Senior Director	Multiple	For-profit
6	Director	Multiple	For-profit
7	CISO	Multiple	For-profit
8	Senior Director	Single	Nonprofit
9	Senior Director	Multiple	For-profit
10	Senior Director	Multiple	Nonprofit
11	Senior Director	Multiple	For-profit
12	Senior Director	Multiple	For-profit
13	Senior Director	Multiple	For-profit
14	CISO	Single	For-profit
15	Senior Manager	Single	For-profit

Research Methodology Applied to the Data Analysis

Following the collection of the data, the researcher analyzed the data using Braun and Clarke’s (2006; 2013) six steps of thematic analysis (TA). TA is a robust method of data analysis that does not adhere to one research methodology and is, therefore, flexible for use with several qualitative research designs. The researcher conducted the TA using the first 15 interviews that he conducted during the data collection phase of this research study. The first step of TA is familiarizing oneself with the data, which the researcher accomplished by transcribing the speech-to-text transcripts from the interviews into a word processing document. In the second step of TA, the researcher began coding these data using NVIVO 11 Pro, a computer-assisted qualitative data analysis program designed to assist researchers with the organization and analysis of qualitative data. During this process, this researcher moved from line to line through each interview transcript and highlighted meaningful or significant passages of text that related to the research questions. The researcher coded these passages to nodes in NVIVO 11 Pro, which are like storage buckets containing information of similar type. The researcher gave these coded passages brief, descriptive names based on the information that they conveyed.

In the third step of TA, the researcher examined all codes created in step 2 for similarities and differences and began placing codes that conveyed similar sentiments into the same nodes, creating a short title for each of these new nodes. This third step is where the researcher began to develop themes based on these new nodes containing similar codes. In the fourth step, the researcher examined these initial themes against the initial codes from step 2. Here, the researcher explored all codes within the initial themes to ensure that the placement of the codes made sense and that the theme captured what all codes within it conveyed. The researcher made any adjustments to code placements in the step and reviewed the themes that he developed to ensure that they partially or entirely addressed at least one of the researcher questions. If they did not, the researcher removed the theme. Following this, the researcher finalized the themes and gave them descriptive titles to complete step 5 In step 6, the researcher presented the results of the data analysis. Table 2 presents the relationship between the research questions and the themes that the research created through TA.

Table 2
Relationship Between Research Questions and Themes

Research Question	Theme	Subthemes
RQ 1. How do IT managers describe the process their organization went through to secure top management support before initiating strategic information systems planning as an InfoSec advantage?	Theme 1. Role of Top management support in SISP and InfoSec	Level of involvement, level of support, communication
RQ 2. How do IT managers describe the usefulness of information systems plans to obtain InfoSec benefits?	Theme 2. Planning for InfoSec	Level of detail, goals
RQ 3. How do IT managers describe the InfoSec benefits on the degree of information technology infrastructure flexibility?	Theme 3. Flexibility	Relationship with top management, compliance
RQ 4. How do IT managers describe the degree of SISP success on their InfoSec environments?	Theme 4. Top management support on SISP Success	No discernible subthemes

None of the themes that the researcher created answered RQ 4. To answer that research question, the researcher created a spreadsheet and, using interviews with Participants 1-15, determined if the participants believed that the SISP was successful, unsuccessful, or yielded mixed results. To do this, the researcher examined questions 10-12 on the interview protocol.

The researcher created three columns, successful, unsuccessful, and mixed, and put a check mark in the appropriate column for each participant.

The data analysis was complicated by the fact that the researcher used an unconventional approach to data collection. The researcher conducted face-to-face interviews while using a digital audio recorder that automatically converted responses of participants in a speech-to-text dictation program. The researcher wrote answers of participants on notebooks specifically assigned to each participant. During the interviews, the researcher and participants spoke directly into the digital audio recording program, and as they spoke the speech-to-text dictation program dictated their responses to text. While some interviews were better dictated to text than others, there was no single interview that the software captured with 100% accuracy. Most of the transcripts contained large chunks of dictation error, leading to the unintelligibility of participants' responses and even interviewer questions. The researcher used the passages of data that were intelligible in the data analysis with the understanding that some context was lost and that those passages of data might be inaccurate. To verify the accuracy of any data contained in the transcripts, the researcher matched the spoken words of participants with the notebooks used to write their responses during the interview to recollect the data.

Presentation of Data and Results of the Analysis

Case 1

The first case is Participant 1, who works for multiple for-profit hospital systems. Participant 1 described top management support for SISP for InfoSec planning as well-managed. The project staff receives daily reminders from top management of their goals, and top management is good about holding staff accountable for achieving these strategic goals related to

SISP. Top management incorporates business strategies through monitoring to ensure all servers are running correctly.

Case 2

The second case is Participant 2, who is the IT director at a single for-profit hospital. Participant 2 said that there is top management support for SISP and InfoSec, and attributed the success of SISP for InfoSec, in part, to this support. When there are budgetary concerns, top management addresses those concerns right away. Participant 2 also shared that working closely with the HIT to build an infrastructure that they could all be proud of was important. The project staff at this organization is small, and Participant 2 said that this was helpful because everyone, including top management, could be involved in the development and implementation of SISP for InfoSec. In the planning stages, the owners collaborated with subject matter experts to design the InfoSec infrastructure, which helped achieve the overall goals of creating an infrastructure that was aligned with the organization’s security operations plan and ensuring that it was on time for launch.

Case 3

The third case is Participant 3, an IT senior director at multiple nonprofit hospital systems. Participant 3 attributes the success of their SISP for InfoSec to the support that the board of directors and executive management provided the team. Top management is involved at every level of planning and initiating SISPs. In Participant 3’s multiple nonprofit hospital systems, top management develops the business goals to align with HIT and SISP to ensure uniformity in SISP strategies for InfoSec benefits across all components of the organization. Participant 3 describes top management as aggressive in terms of SISPs that implement strategic goals, feasibility, and risk management based on well-researched frameworks. The frameworks and SISPs that top management develops to ensure alignment with InfoSec and regulatory mandates. Doing this provides greater flexibility. Participant 3 elaborated that this flexibility allows them to respond quickly to predicted and unpredictable changes.

Case 4

The fourth case is Participant 4, who is an IT senior director at a single nonprofit hospital. This participant described the support for SISP from top management as good, including the daily interactions about SISP-related matters. The goals for their organization’s InfoSec infrastructure flexibility are to reduce or eliminate downtime and business interruption. Their business strategies are integrated at all levels so that the processes are all streamlined. Top management has impacted the success of their SISP for InfoSec through reinforcements but also by developing plans that are flexible enough to cope with changes to threat models.

Case 5

The fifth case is Participant 5, an IT senior director at multiple for-profit hospital systems. According to this participant, the success of SISP for InfoSec advantages is because of top management involvement in terms of ensuring that projects are fully developed and initiated while maintaining regulatory compliance so that when executing projects there are no problems. Top management is supportive of high-level IT planning, and everyone on the team is very hands-on. Participant 5 described the importance of ensuring that top management understands the corporate structure of the hospital system, because the hospitals in the system are at multiple sites and locations, including their respective IT departments, and this de-centralization presents its own set of challenges.

Case 6

The sixth case is Participant 6, the IT director at multiple for-profit hospital systems. For a SISP to be successful in achieving InfoSec benefits, the top management must be able to outline the actions it envisions for SISPs and have a clear vision of the organization and its destination. Participant 6 believes that top management has been very supportive of these SISPs, leading to their overall success at achieving InfoSec. The intentions of top management on SISPs for InfoSec benefit have been staying on top of the tools and technologies available for use and retaining operational control over the different divisions. The organizational strategies that this participant’s department has been using have allowed for greater flexibility in finding appropriate solutions to problems.

Case 7

Case 7 is Participant 7, who is a CISO at multiple for-profit hospital systems. Participant 7 said that “the organization and the support of top management have been essential in terms of funding and endorsing InfoSec because they are stakeholders for the construction of the categories of SISP.” The role of top management is to “design models and construct a framework for these models to provide a general and comprehensive definition of SISP,” Participant 7 described that they provide support throughout the life cycle of all planning, and said that their support remains unchanged during planning for Health Insurance Portability and Accountability Act (HIPAA) regulatory compliance in their environment. The team works collaboratively to create strong InfoSec plans to mitigate risk. Health Insurance Portability and Accountability Act is a Federal law established in 1996 that restricts access to individuals' medical information (Murphy, 2018).

Top management's intentions are incorporated first by brainstorming several ideas and then reviewing the strategic direction of the HIT. Participant 7 said that their primary goal is InfoSec competency, and for a long time, they only sought to maintain InfoSec. Today, because of new top management intentions for InfoSec success, they have created an oversight committee to include more monitoring and evaluation of third-party contractors and "to routinely evaluate and audit HIT for robust cybersecurity oversight." While older SISPs involved only the project managers, because of regulatory mandates by HIPAA, Participant 7's organization has taken a different approach to planning and "HIT and InfoSec staff are now allowed to exchange any information with any other project between them." The team also follows constructs so that the SISP project staff does not need to defend the SISP, as the SISP follows HIPAA regulatory mandates.

Case 8

The eighth case is Participant 8, an IT senior director at a single nonprofit hospital. Participant 8 describes having strong support from top management, and because this person is only two positions away from the CEO, Participant 8 fast-tracks most projects. Participant 8 credits top management with providing support to make InfoSec benefits a success at their hospital. The intentions of top management on executing these SISPs have impacted the organization positively as they can move projects through quickly. The intent is to enhance and enlarge the hospital's security, particularly in terms of who has access to specific parts of the hospital, but the board of directors must approve all plans.

Case 9

Case 9 is that of Participant 9, an IT senior director at multiple for-profit hospital systems. Participant 9 described top management support as well-balanced, and that the team understands security threats and vulnerabilities unique to hospital settings. This participant described the hospitals' need for understanding "the landscape of cybersecurity," including the rules and regulations for infrastructure implementation. Top management sets a specific agenda for SISPs, and then the team follows up with research and brainstorming on how to implement that into a plan. The approach is fast-paced and consists of regulatory compliance and budgetary constraints. One implication for InfoSec of their organizational strategies is safety and security, and Participant 9 described the need for security when patients enter the hospital and want to connect to the hospital's wireless internet, the IT team has to ensure that other information like patient data is secure.

Case 10

The tenth case is Participant 10, an IT senior director at multiple nonprofit hospital systems. Top management is supportive of the IT team and IT planning, as these are two aspects of their corporate governance. Top management provides the team with rules, regulations, policies, and procedures for following HIPAA regulations. They are centralized within the organization and involved in all aspects of planning and implementation. The intentions of top management on executing the SISP are strict and require that the team stays within budget and regulations. Doing this requires meticulous planning based on much research in the planning phase. In terms of InfoSec benefits, the organizational strategies Participant 10 research previously completed plans to understand steps that worked in the past and identify tools and technologies that have previously worked to make necessary adjustments to the current plan in development.

Case 11

The eleventh case is Participant 11, an IT senior director at multiple for-profit hospital systems. The IT team focuses on information and cybersecurity because of the known threats and vulnerabilities. Top management is strict when it comes to this high-level SISP, with intense levels of communication between the team and top management. Participant 11 reported that there were not many concerns regarding top management and InfoSec in terms of malicious hacking, and this is because the team uses an outside consulting firm with their security expert to assess their environment. Participant 11 said that this provides "additional robustness" when implementing SISPs for InfoSec. The SISP for InfoSec provides flexibility to understand the landscape and how to approach particular objectives within that landscape.

Case 12

Case 12 is that of Participant 12, who is an IT senior director at multiple for-profit hospital systems. Top management provides support in that it is centralized over the decentralized hospitals and IT departments in the system. A considerable amount of planning goes into the SISPs at Participant 12's hospital, and top management provides the most support during initiation and monitoring, but less during the planning stages. In incorporating the business strategies into the overall business needs, once top management provides the details of what needs to be done on a project and the budget for that project, then the team can research and plan for the amount of time that the project will take and what they will need to "control these mechanisms."

Case 13

The thirteenth case is that of Participant 13, an IT senior director at multiple for-profit hospital systems. The team at this hospital has a one-on-one relationship with top management, who starts each project by setting the budget and clear intentions for their SISPs. The goals of this are to implement SISPs for InfoSec on time within budget. The IT team relies on an internal team of auditors to ensure regulatory compliance for SISP.

Case 14

Case 14 is that of Participant 14, who is an IT senior director at a single for-profit hospital. The IT project staff are divided into tiers and work on different aspects of SISPs. They work together with top management to plan and execute projects on time and within budgetary constraints, as well as aligning to regulatory mandates. Top management is aware of the problems that can arise when an IT environment does not have a SISP and so works meticulously during the execution phase of projects. The team also employs value-added metrics, including a tool for which they measure business strategies against risk management. They use this to dissect the risks, protocols, policies, procedures, and regulations by dollar value.

Case 15

The last case is Participant 15, who is an IT senior director at a single for-profit hospital. This participant described great understanding and good cooperation with top management, and top management is very straightforward in their communication of business goals. Everything that the team does goes through a board of directors for approval. Top management support has been instrumental in achieving InfoSec success through SISPs, as Participant 15 described them as proactive, especially with information security.

Cross-Case Analysis

Theme 1. Role of top management support in SISP and InfoSec. Theme 1 addressed Research Question 1, How do IT managers describe the process their organization went through to secure top management support before initiating strategic information systems planning as an InfoSec advantage? There were three subthemes associated with this theme which were as follows: level of involvement, level of support, and communication. Participants shared how top management provide them support in their SISP for InfoSec. Top management support was evident through its level of involvement at all stages of SISP as well as its communication with participants and project staff. Participants did not describe any challenges in securing top management support for SISP processes.

Level of involvement. Participants described high levels of top management involvement in SISP. Participant 5 said, "top management is extremely involved" and described them as "extremely proactive." Participant 7 also said that top management was proactive in SISP. They explained that top management is involved in the project meetings and weekly follow-up meetings, and meeting with the project staff. According to Participant 7, top management was also very involved in regulatory compliance and HIPAA regulations for IT, adjusting its goals to make InfoSec projects a top priority. This participant described how top management was "active in building relationships with the hospital" so that regulatory compliance was a concern shared by everyone and not just HIT. Participant 2 appeared impressed with top management as they described how those in top management "sat down with some subject matter experts and people who were involved with helping to design our infrastructure," as this indicated that top management was willing to listen to the infrastructure needs and incorporate these into the SISP for InfoSec.

Participants also shared how top management was involved in SISP. Some described how top management was involved in some phases more than in others. Participant 14 said that top management was very involved in the first two tiers of SISP, stating, "tier one and tier two are the most visible and the most highly scrutinized projects; those projects require a high level of top management support," but in tiers, three and four top management is much less involved. For others, different people in top management were involved in different SISP phases. Participant 9 shared that the chief executive officer and chief operations officer were involved in some phases of SISP, but did not elaborate on which ones, while the chief technical officer and the chief financial officer were more involved in other phases of SISP.

Three participants shared their positive perceptions of top management and its involvement in SISP overall. Participant 1 stated that top management was "very well-managed." Participant 14 described C-level management, or top management, as wanting results. They said, "[top management] are results-driven individuals." Finally, Participant 4 noted that top management used reinforcements "over and over again" to bring awareness of the plan and to ensure that the SISP provided the flexibility required to handle different threat models.

Participants also described the importance of decision making among top management. Participant 10 described these decisions as "very strict," particularly regarding staying within budgetary and regulatory requirements. Participant 11 noted the sense of urgency that comes with decision-making about SISP. They stated, "we have to get this thing done very quickly so top management can understand the landscape," which in turn meant that top management had to "decide and choose the type of what they need … what solution is best for them" so that everyone involved could start planning.

Level of support. Seven participants felt that top management was supportive of the initiation of SISP and at other phases of the process. As Participant 8 stated, "top management has been very supportive." Participant 10 described the support that they received from top management, especially as their team incorporates HIPAA rules and regulations into their InfoSec. The IT planning is part of top management's corporate governance, according to Participant 10, so this participant has experienced ongoing support from top management. Participant 9 described the support from top management as "well-balanced," particularly in terms of planning. Participant 9 also shared that the management team "understand the other security threats and vulnerabilities that we are facing," which facilitated easier planning and project development. Participant 12 described two tiers at which they received top management support. The first tier was during plan initiation, and the second tier was during plan monitoring. However, Participant 12 experienced less support from top management during the plan execution.

Two participants were themselves part of top management and described their ongoing support for SISP and InfoSec projects. Participant 2 said, "I believe in what they are doing, and I believe in their mission and the challenges that they have had, so they have my support 100%." Similarly, Participant 4 said that because they understand the importance of the systems, they "gives that [my] primary support."

Communication. Seven participants described the importance of communicating with top management and the level of intensity of this communication. Participant 1 and Participant 4 said that communication with top management occurred daily. Other participants reported regular meetings with top management. Participant 13 said that their team relies on quarterly physical meetings with top management, as did Participant 15. In addition to these quarterly meetings to discuss the budget, Participant 15 also stated that there are quarterly forums where staff can provide project input. Participant 15 also has a biweekly meeting with the CEO where they can provide direct input to the CEO.

Participant 10 believed that they had “an effective way of communicating with everyone, especially when it comes to the other senior-level professionals.” This participant’s experience included many meetings and follow-up meetings to ensure proper communication between everyone involved in SISP. Participant 11 was also involved in top management communication, which they described as “pretty intense.” This participant liaised between the consulting firm, the in-house team, and the top management during the SISP. Participant 11 also described their role in maintaining communication with the chief financial officer or chief operations officer to ensure compliance with regulations as well as budgetary requirements during SISP.

Theme 2. Planning for InfoSec. Theme 2 addressed Research Question 2, How do IT managers describe the usefulness of information systems plans to obtain InfoSec benefits? There were two subthemes associated with this theme that were as follows: level of detail and goals. SISP processes were helpful for InfoSec, according to participants. The helpfulness of SISP processes to Infosec was especially the case in terms of the detail that went into SISP, which provided a clear framework for proceeding with such processes. Top management’s clear communication of goals was also useful for SISP, as participants took these goals into account during planning, initiation, and execution phases of securing InfoSec benefits.

Level of detail. The level of detail required in a SISP for InfoSec was of critical importance, as five participants noted. Critical importance reflected top management communication strategies used to communicate with the project teams. Participant 12 described the level of detail required for a SISP as like building a structure. When building that structure, Participant 12 shared, "you need an architect to draft the plans, which are very tedious [but] you want to make sure everything is spelled out." Then, those plans go to the masons, and the electricians and so the plans need to be detailed such that everyone can understand them. To Participant 12, this was precisely how they drafted a SISP and communicated the intention of top management with consideration to InfoSec benefits. Participant 13 echoed this sentiment, stating that they like top management's "intention to be clear" during the SISP.

Equally important was the level of detail in the execution phase. Participant 14 said that when it comes to the execution of a SISP, top management should be "meticulous." Participant 3 described this as "aggressive." they said, "I would characterize top management intentions as being extremely aggressive when it comes to executing SISP, as it consists of strategic goals, risks, impact, feasibility, quality, and are based from a well-researched framework." Compliance with federal and state regulations and mandates were also important details, said Participant 3.

Goals. Four participants described the agency goal of working within its budget when implementing projects. Budget approval fell to Participant 8, who approved the budget very quickly so as not to impede progress on a project. Participant 6 described the importance of developing a sustainable budget and including funds in that to train the staff and project managers. Participant 6 said that making the "right business decision" included implementing new technologies that “make financial sense” for the company and the projects. Participant 13 said that setting the budget for the projects is the “very first thing, bottom line.”

Remaining within budget for an IT project was an important goal, so was working within the time frame set for the development and implementation of the project. As Participant 12 said, “I am going to be expecting a 100% operational at all time anywhere and everywhere,” project implementation. Participant 13 stated that part of their job is “to make sure our strategic information system plan is executed in a timely fashion.” Participant 4 described the team’s focus on the end game and ensuring “the least amount of business interruption,” so the goal was to reduce or eliminate downtime while maintaining infrastructure flexibility in the SISP.

Seven participants spoke of regulatory compliance as a goal of SISP for InfoSec. Participant 10 said that they require a subject matter expert on regulatory mandates is involved in SISP for InfoSec. Participant 14 shared that regulatory compliance was essential for top management. There are fines involved if organizations do not comply with federal regulations but being noncompliant might also mean greater vulnerability to cyberattacks. Participant 14 described the frustration of keeping up with the latest viruses that could hit the organization’s infrastructure and the need to stay steps ahead of hacker organizations. they said, “we need to be at least 10-15 years ahead,” which required attending conferences and renewing certifications and keeping up with training. In large part, HIPAA is the chief federal law that enforces, regulates that hospitals must comply. Participant 2 described the importance of maintaining the privacy of patient data and “limiting access to it so that only [authorized] individuals” have access to these data, and that these data remain behind a protective infrastructure.

Theme 3. Flexibility. Theme 3 addressed Research Question 3, How do IT managers describe InfoSec benefits on the degree of information technology infrastructure flexibility? There were two subthemes associated with this theme: relationship with top management and compliance. Participants believed that by paying attention to the business strategies that top management set for SISP process and obtaining InfoSec advantages, participants and their teams were able to build greater flexibility into their InfoSec environments and infrastructure. This flexibility also assisted them as they sought compliance with regulatory mandates.

Relationship with top management. The relationship with top management is essential for infrastructure flexibility, as seven participants described. The flexibility comes from incorporating top management's business strategies into SISP for InfoSec. Participant 11 and Participant 13 described this relationship as coming from them and the project team. Participant 11 said that "we do our research and tell our upper management about the business strategies that we have and how that is going to be impacted if we do not include certain information security tools." Participant 13 also discussed doing the research and presenting this to top management. Participant 13 stated, "we do the homework for them, we make sure that everything is spelled out, we do all of the research for them" so that they can tell top management what their requirements are.

Participant 3 and Participant 7 both described the five-year strategic plans that their organizations follow to allow for infrastructure flexibility. Participant 3 statement was as follows:

> Our organization has a five-year enterprise strategic plan…We also follow a framework for SISP. We align HIT projects with our operational model, which is

> one of the top management's goals. This does not impact on aspects of core HIT performance at our hospitals, and the fact that we have to compete with other hospital systems to survive in a competitive and rapidly changing healthcare field, the environment compels us to make HIT flexible with top management to quickly respond to predicted and sudden changes.

Similarly, Participant 7 shared their organization, too, aligns HIT projects with the operational model. Doing this means the “inclusion of innovations in business processes, the adaptation of organizational structure, and the success of HIT infrastructure flexibility,” according to Participant 7.

Compliance. Flexibility was also related to regulatory compliance, as six participants shared. According to Participant 7, their organization’s IT infrastructure is flexible if it has the ability “to support and enable responsiveness to regulatory requirements.” This participant also shared that “the state of aligning InfoSec with HIPAA regulations increases the development of communication between HIT departments,” which “results in having a more robust HIT infrastructure as it provides us with greater structural flexibility.”

Other participants spoke about the oversight required for compliance, including oversight committees and auditors. Participant 12 and Participant 5 described the oversight committee the looks at their organizations’ frameworks but were unclear as to whether these were internal or external oversight committees. Participant 13 said that an internal team of auditors helps the IT project team ensure compliance.

Theme 4. Top management support on SISP Success. Theme 4 partially addressed Research Question 4, How do IT managers describe the degree of SISP success on their InfoSec environments? There were no discernible subthemes associated with this theme. Four participants attributed the success of the SISP for InfoSec to the support that they received from top management. As Participant 3 stated, “I think first and foremost the support of our board of directors and executive management were key [to the] success of our program; without that, you really cannot do a lot of things you want to do.” Other participants agreed with this regarding their organizations. Participant 7 shared that the support of top management was “essential in terms of funding and endorsing InfoSec,” especially as it pertained to designing the models and constructing the framework for the models during SISP.

Participant 2 discussed the importance of project buy-in from top management. They described the intensity of the SISP and implementation and execution, which required that everyone on the team “wear many hats,” so this participant valued the involvement of everyone. Participant 2 said that top management buy-in was also crucial regarding budgetary issues because, without that buy-in, the budget for the project would be the first thing cut. This participant said that in the past, this has happened, and projects have been less successful.

Results of analysis of Interview Questions 10-12. The results of the analysis of Interview Questions 10-12 from participants 1-15 partially addressed Research Question 4, How do IT managers describe the degree of SISP success on their InfoSec environments? Based on the fragmented data, as described earlier in this chapter, fourteen participants believed that the SISP for InfoSec was successful. Two participants provided mixed reviews of the InfoSec success. No participants indicated that SISP for InfoSec was unsuccessful. Those participants who believed that SISP for InfoSec was successful attributed this to the support coming from top management.

Two participants shared mixed opinions about InfoSec success. Participant 8 was one of these participants. Though They believed that top management helped provide structure for SISP, this structure slowed the team down in InfoSec implementation and execution. Participant 8 did share, though, the structure top management provided helped the team align with government regulations, which they viewed as positive. Participant 2 was the other participant who believed that the InfoSec success was mixed. Participant 2 believed that success had to be defined at multiple levels and in different ways, and these ways may be incongruent. They shared that having top management support and project buy-in was important, but equally crucial for the success of a project was to have actively engaged employees. Participant 2 believed that InfoSec success measures the individual level of the employee in terms of active employee engagement as well as measured by the overall success of the InfoSec.

Summary

The researcher presented the results of this multiple case study data analysis in this chapter. Following Braun and Clarke's TA (2006; 2013), the researcher developed four themes to address the research questions. Participants described an easy process for securing top management support for SISP and InfoSec. Top management was supportive of SISP processes and showed this through the intensity of the communications with participants and their teams, the heavy degree of involvement in SISP processes, and the quick approval of budgets. Participants also believed that SISP for InfoSec was useful and highlighted the importance of the level of detail of the planning and goals of SISP processes for InfoSec, particularly. Participants agreed that top management communication of detailed planning was helpful for SISP processes. They also found it helpful when top management communicated the goals for SISP and InfoSec clearly with them. According to participants, InfoSec provided greater infrastructure flexibility, especially as this pertained to regulatory compliance. Participants indicated that they had greater infrastructure flexibility, which allowed them to maintain regulatory compliance as well as face emerging cybersecurity threats. Finally, participants overall believed that SISP for InfoSec was successful within their organizations and that this success came in large part from the amount of support that they received from top management.

In Chapter 5, the researcher will discuss the results of this chapter in greater detail. Chapter 5 will include an interpretation of the findings, and a discussion of the limitations of this research study, as outlined briefly in this chapter. The researcher will also provide recommendations for future research based on the findings as well as applications.

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

Chapter 5 consists of nine sections, which begins with a summary of the results. Part 2 pertains to a discussion of the outcome, which further elaborates on the analyzed data obtained by answers given by selected eligible participants. Section three provides a conclusion based on the results from data analyzed using NVIVO 11 Pro, NVIVO 11 Pro, a computer-assisted qualitative data analysis (CAQDA) tool that helps researchers organize coded data relevant to themes and subthemes. Part four begins with a comparison based on the results. Section five gives interpretations of the findings, which allows the researcher to draw conclusions based on the results. Chapter 5 continues with section six illustration of the limitations of the research, and section seven that includes the implication for the practice. The final sections include recommendations for further study and the conclusion based on the results of these research findings.

Summary of the Results

While there are ongoing interests on InfoSec benefits to address for the reason SISP does not return the expected InfoSec benefits in for-profit and nonprofit hospitals in the United States, there has been no new research added to SISP (Kisekka, & Giboney. 2018; Lee et al., 2015; Mishra et al., 2014; Nicho 2018; Shoufan & Damiani, 2017). The significance of this qualitative multiple case study is in its review of practices that Florida hospitals use to adopt SISP successfully. The researcher investigates the four SISP constructs as they contain lessons learned that may be applied to help construct better procedures in future SISP implementations for Florida Hospitals.

While the research was being completed new findings regarding the agency theory found that litigation actions may be taken against HIT contractors in the event one or more parties involved do not act by the terms and conditions of the agreed-upon contract (Sirisomboonsuk et al., 2017). There was also a new finding regarding SISP theory that found the inclusion of the four constructs, which were identified by Hartono et al. (2003), was vital to SISP success (Landaeta Olivo et al., 2016). The latest review on top management support by Kitsios and Kamariotou (2018) maintained that the information systems plan document must focus on the business. Otherwise, the plan may not reflect the goals of the corporation adequately (Kitsios and Kamariotou (2018). New findings on information systems plan Kitsios, and Kamariotou (2018) maintained that the information systems plan document must focus on the business. A new study on infrastructure flexibility found the inclusion of efficiency to IT infrastructure flexibility respond well to new market conditions to assist organizations with future integration (Byrd & Turner, 2000; Li et al., 2017).

Other recent researchers have worked on Hartono et al.'s (2003) extended theory and have included further constructs such as complexity risk (Liu, 2015), hybrid approaches for allocating resources (Hoque et al., 2016), and strategy execution (Srivastava & Sushil, 2015). New research on SISP plans provided a conceptual model for SISP success, which considered the inclusion of IT capability, so top management could further explore environmental and organizational factors that influenced this relationship (Jorfi et al., 2017).

The researcher used a qualitative multiple case methodology and conducted interviews with senior managers, directors, senior directors, and CISOs who work at for-profit and nonprofit hospitals in Florida. The researcher analyzed the data using Braun and Clarke's (2006; 2013) six steps of thematic analysis (TA). TA is a robust method of data analysis that does not adhere to one research methodology and is, therefore, flexible for use with several qualitative research designs. Analysis of the data yielded four themes: the role of top management support in SISP and InfoSec, planning for InfoSec, flexibility, and top management support in SISP success. Practical implications include directors developing SISP plans based on obtaining InfoSec benefits and allowing top management to monitor the execution phases of SISPs. These findings depicted areas Florida hospitals should include when designing SISP to assist their organization with obtaining InfoSec success. These findings will enable managers with understanding the four SISP constructs and allowing them to achieve expedient success in plans.

Discussion of the Results

Data were analyzed and yielded four themes: The role of top management support in SISP and InfoSec, Planning for InfoSec, Flexibility, and Top management support in SISP Success. Within each central theme, the data yielded several subthemes. For example, within Theme 1, The role of top management support in SISP and InfoSec, the subthemes are as follows: Level of involvement, level of support, and communication. Theme 2, Planning for InfoSec, consists of two subthemes, level of details and goals. Theme 3, Flexibility, includes the subthemes, relationship with top management, and compliance. Theme 4, Top management support on SISP success, did not yield any noticeable subthemes. However, to answer that research question, the researcher created a spreadsheet and, using interviews with Participants 1-15, to determine whether the participants believed that the SISP was successful, unsuccessful, or yielded mixed results.

Theme 1. The role of top management support in SISP and InfoSec. The first research question investigated how managers in IT described the process their organizations went through to secure top management support before initiating strategic information systems planning as an InfoSec advantage (Sharma & Yetto, 2011; Young & Jordan, 2008; Yeh et al., 2015; Young & Poon, 2013;). The research question yielded three subthemes: level of involvement, level of support, and communication. For a project to be successful in an organization, it must be supported directly by top management (Sharma & Yetto, 2011; Young & Jordan, 2008; Young & Poon, 2013; Yeh et al., 2015).

Level of involvement. Level of involvement is expressed as a logical measurement created to determine what top management support should be (Clegg, Killen, Biesenthal, & Sankaran. 2018). Therefore, Sull, Turconi, Sull, & Yoder (2017) sighted in their research that one factor must express the level of top management support, which the researcher elaborated on from RQ 1 theme and sub theme. Participants 11, 10, 14, 4, 2, 7, 5, and 9 described high levels of top management involvement in SISP. The research shows that after the level of involvement constitute top management to be proactive, which is a motion that was highlighted by Clegg et al. (2018) in their research. Participant 5 mentioned that in their environment, top management was "extremely involved" and "extremely proactive." Clegg et al. found that most projects were completed successfully with the proactivity of top management by hosting project meetings, weekly meetings, and follow-up meetings, which is a sentiment shared by Participant 7 to illustrate the length to which top management goes to be proactive in InfoSec-related projects. While hosting these meetings, Clegg et al. found that subject matter experts helped management remain within the scope of the project, readjust goals and objectives, and redesign the organizational infrastructure to stay compliant. The results of the present study showed that Participant 2 and Participant 7 attested to the abovementioned top management practices and helped their environment with compliance issues, especially in auditing events.

Level of support. Levels of support are the traditional means for securing electronic records used in hospitals to maintain data confidentiality, data availability, and data integrity only to authorized users (Henfridsson & Lind, 2014). Hospital IT is increasingly concerned with cybersecurity, which involves the security of electronic records used in hospitals by maintaining data confidentiality, data availability, and data integrity that leaves the confines of hospital databases by way of the internet (Kim, 2018). Sending data outside of the hospital using the internet becomes paramount (Pankratz, & Basten, 2018).

Recent research has shown that Six Sigma is used to manage hospitals, but the practice encompasses the management of the entire hospital (Lee, McFadden, Gowen, & Charles, 2018). However, within a hospital, there are many departments, with IT being one of such, and ITM and MIS require the use of project management as the primary discipline (McGivern et al. 2018; Lee et al., 2018). Research suggests that using project management as a central discipline best explained the significance and type of the level of support top management needs to enforce to obtain InfoSec success (Pankratz, & Basten, 2018). Lean Six Sigma is the primary driver in terms of process improvement in hospitals (McGivern et al., 2018). However, because of the role of technology, hospitals are heavily dependent on project management practices (Weech-Maldonado et al., 2018).

Participant 9 described the support from top management as “well-balanced.” Recent studies suggest that the use of a well-balanced level of support consists of understanding the security threats and vulnerabilities faced by hospitals (Babatunde, Taiwo, & Dada 2018; Kisekka, & Giboney, 2018). Participant 12 described two tiers at which they received top management support. The first tier was during plan initiation, and the second tier was during plan monitoring. Plan initiation and plan monitoring are two of the six phases found in project management (Weech-Maldonado et al., 2018).

***Communication*.** Communication involves both in-person and remote communication (Dahm, Georgiou & Westbrook, 2017). The finding on communication revealed that participants referred to in-person communication, and this research is limited to in-person communication. Participants mentioned that with regards to communication, it means that there must be a level of intensity. Level of intensity was observed to indicate daily communication, regular meetings, follow up meetings, biweekly meetings, and quarterly meetings (Sull et al., 2017). Participants described the importance of communicating with top management and the level of intensity of this communication as being very high. Participant 1 and Participant 4 said that communication with top management occurred daily. Other participants reported regular meetings with top management. Participants 13 noted that their team relies on quarterly physical meetings with top management, as did Participant 15. In addition to these quarterly meetings to discuss the budget, Participant 15 also stated that there are quarterly forums where staff can provide project input. Participant 15 also has a biweekly meeting with the CEO, where they can provide direct information to top management. Participant 11 also described their role in maintaining communication with top management to ensure compliance with regulations as well as budgetary requirements during SISP to obtain InfoSec benefits.

Theme 2. Planning for InfoSec. The second research question was designed to collect information on how IT managers describe the usefulness of information systems plans to obtain InfoSec benefits (Sharma & Yetto, 2011; Young & Jordan, 2008; Young & Poon, 2013). Analysis of data revealed the theme, Planning for InfoSec, which consists of two subthemes, level of details and goals. Having a clear plan for InfoSec once there is sufficient top management support for a project can result in SISP success (Ragu-Nathan et al., 2004).

***Level of details*.** Subtheme 1, level of details, suggests that the intentions of top management are clear, and plans detailing intentions are specific (Shoufan, & Damiani, 2017). Five participants noted details as essential. Participant 12 described the level of detail required for a SISP like building a structure. Participant 13 echoed this sentiment, stating that it is essential for top management's "intention to be clear" during the SISP. The level of detail at the execution phase of a SISP project is critical and should be meticulous and aggressive. Participant 14 noted that when it comes to the execution of a SISP, top management should be "meticulous." Participant 3 described this as "aggressive," which involves detailing strategic goals, risks, impact, feasibility, quality, which are from a well-researched framework (Safa, Maple, Watson, & Von Solms, 2018). An aggressive level of detail from top management can also help determine how well the organization remains compliant with federal and state regulations and mandates (Safa et al., 2018).

***Goals*.** Achieving goals entails remaining within budget when implementing projects, working within the timeframe for the completion of a SISP project, and, if over budget, getting a budget extension approval from top management (Mamonov, & Benbunan-Fich, 2018;

Weishäupl, Yasasin, & Schryen. 2018). Four participants described that the goal of their organization is to remain within a budget when implementing InfoSec-related projects. Participant 8 expressed that in the event a project goes over budget, top management approved an extension to the budget quickly, so as not to impede progress on a project. Participant 6 mentioned that it was essential to develop a sustainable budget that includes staff and project managers training funds. Weishäupl et al. (2018) and Mamonov and Benbunan-Fich (2018) found that InfoSec training and awareness were paramount and that firms that trained their staff in InfoSec were less likely to fall victims of cyberattacks than those that did not. Participant 13 emphasized that creating a budget for a SISP project remains a top management priority. Participant 6 and Participant 12 expressed that the goal was to reduce or eliminate downtime while maintaining infrastructure flexibility in the SISP.

New empirical revealed that another goal was a return on investment in InfoSec to create InfoSec training and awareness, which can aid organizations in becoming InfoSec compliant (Weishäupl et al., 2018; Mamonov, & Benbunan-Fich, 2018). Analysis of RQ 2 subthemes found that compliance to include HIPAA mandates, which governs the state of patience data privacy and access to data for authorized individuals. Seven participants of the present study spoke of regulatory compliance as a goal of SISP for InfoSec success. Participant 10 said that top management requires a subject matter expert on regulatory mandates to obtain InfoSec success. Participant 14 shared that regulatory compliance was a priority for top management. Fines are involved if organizations are noncompliant and being noncompliant might also mean greater vulnerability to cyberattacks (Georg, 2017). Regulatory fines are in the millions, and top management could face prison terms if found to be at fault for noncompliance (Dahm et al., 2017). Participant 14 mentioned that their organization must remain ahead of hacker organizations -by attending InfoSec-related conferences, renewing InfoSec-related certifications, and keeping up with InfoSec training. Participant 2 described the importance of staying compliant as maintaining the privacy of patient data and limiting access to healthcare data to authorized individuals only.

Theme 3. Flexibility. The third research question investigated how do IT managers describe InfoSec benefits on the degree of information technology infrastructure flexibility (Antal, Debucquet, & Frémeaux, 2017; Furukawa, 2013; Furukawa, & Minami, 2013; Furukawa et al., 2014; Kumar & Stylianou, 2014). There were two subthemes associated with this theme: relationship with top management and compliance. Relationship with top management consists of including ideas from project members (Shao, Feng, & Hu, 2017). Relationship with top management also includes flexibility, which is having a clear plan to incorporate top management business strategies into SISP for InfoSec (Antal et al., 2017; Furukawa, 2013; Furukawa, & Minami, 2013; Furukawa et al., 2013; Kumar & Stylianou, 2014).

Relationship with top management. The idea of having a relationship with top management suggests the need to include ideas from project members. However, these ideas must be from the body of empirical research that can show a negative InfoSec impact on the organization in the long term. Participant 11 and Participant 13 described this relationship as coming from them and the project team. Participant 11 said that "we do our research and tell our upper management about the business strategies that we have and how that is going to be impacted if we do not include certain information security tools." Participant 13 also discussed doing the research and presenting this to top management. Participant 13 stated, "we do the homework for them, we make sure that everything is spelled out, we do all of the research for them" so that they can tell top management what their requirements are.

Having a clear flexibility plan to incorporate top management business strategies into SISP for InfoSec is also imperative (Antal et al., 2017; Furukawa, 2013; Ridge, & Ingram, 2017). The relationship with top management is essential for infrastructure flexibility, as seven participants described. The flexibility comes from incorporating top management's business strategies into SISP for InfoSec. Participant 3 and Participant 7 described the five-year strategic plans that their organizations follow to allow for infrastructure flexibility. The finding also revealed that top management goals should include an alignment of HIT projects with the operational model of the organization. An alignment of the HIT project with SISP should not harm aspects of core HIT performance hospitals. Flexibility should aid top management to respond to predicted and sudden changes quickly.

Compliance. Compliance involves meeting regulatory standards (Kim & Kim, 2017). The compliance subtheme suggests that participants feel that organizations should abide by all federal and state regulations, have an oversight committee, and have internal and external audits in place (Lee, Lee, & Kim, 2016). Participant 7 stated that the organization's IT infrastructure is flexible if it has the ability "to support and enable responsiveness to regulatory requirements." Participant 7 also shared that "the state of aligning InfoSec with HIPAA regulations increases the development of communication between HIT departments," which "results in having a more robust HIT infrastructure as it provides us with greater structural flexibility." Participant 12 and participant 14 also spoke about the oversight required for compliance, including oversight committees and auditors. Participant 12 and Participant 5 reported that the oversight committee looks at their organization frameworks. Participant 13 said that an internal team of auditors helps the IT project team ensure compliance.

Theme 4. Top management support on SISP success. The fourth research question was designed to collect information on how IT managers describe the degree of SISP success on their InfoSec environments. The fourth question also helped give insight into the extent SISP goals have been achieved in InfoSec using goal-centered judgments. There are two categories to be considered when assessing SISP success regarding InfoSec: internal and external (Kisekka & Giboney, 2018; Krishna, Khan, & Pandey, 2017). Internal factor refers to mitigating strategies aimed at minimizing risks associated with employees, staff, and contractors (Kisekka & Giboney, 2018). These risks can be mitigated by policies and procedures to include elements if human resources to create a vetting system that provides for periodic background checks on all personnel (Kisekka & Giboney, 2018). To mitigate the external factor top management can invest in InfoSec using the latest security measures and tools to safeguard their organizations, recertification of IT and IS staff, and create organization-wide security awareness policies and procedures (Kisekka & Giboney. 2018; Nicho, 2018).

Recent research shows an organization that manages an IT department is deemed unsuccessful with regards to SISP success in producing InfoSec benefits if there is a breach of data either externally or internally (Kosseff, 2018). There are strict regulatory mandates that organizations must follow, and the consequences of noncompliance to federal regulations can be severe and financially catastrophic for organizations (Kim, 2018). Noncompliance may include paying a hefty fine, reorganizing IT/IS infrastructure, and being assigned a compliance officer to ensure that the organization redoubles its efforts to adhere to federal regulatory mandates (Kosseff, 2018; Kim, 2018; Kisekka, & Giboney, 2018).

Recent research shows an organization that manages an IT department is deemed unsuccessful with regards to SISP success in producing InfoSec benefits if there is a breach of data either externally or internally (Kosseff, 2018). There are strict regulatory mandates that organizations must follow, and the consequences of noncompliance to Federal regulations can be severe and financially catastrophic for organizations (Kim, 2018). Noncompliance may include paying a hefty fine, reorganizing IT/IS infrastructure, and being assigned a compliance officer to ensure that the organization redoubles its efforts to adhere to federal regulatory mandates (Kim, 2018; Kisekka, & Giboney, 2018; Kosseff, 2018).

The results of the analysis of Interview Questions 10-12 from Participants 1-15 partially addressed RQ 4. Fourteen participants believed that the SISP for InfoSec was successful. Two participants provided mixed reviews of InfoSec success. No participants indicated that SISP for InfoSec was unsuccessful. Participants who believed that SISP for InfoSec was successful attributed this to support from top management.

Two participants shared mixed opinions on InfoSec success. Participant 8 was one of these participants and believed that top management helped provide structure for SISP, but this structure slowed the team down in InfoSec implementation and execution. Participant 8 did share positive views in their answers with the thought that the structure top management provided helped the team align with government regulations. Participant 2 was the other participant who believed that the success of InfoSec was mixed. Participant 2 thought that success had to be defined at multiple levels and in different ways, and these ways may be incongruent. Participant

2 shared that having top management support and project buy-in was essential but equally important for the success of a project was to have actively engaged employees. Participant 2 believed that success should be measured at the individual level of the employee in terms of active employee engagement as well as measured by the overall success of the InfoSec.

Conclusions Based on the Results

The research first began by extrapolating four constructs based on Lederer and Hannu’s (1996) seminal work, which described these constructs as being the pillars to having a sound SISP to obtain InfoSec benefits. The researcher developed 12 questions based on the constructs to identify InfoSec benefits. Florida hospitals, both for-profit and nonprofit, were then selected because Elysee (2012) recommended that future researchers should conduct a multiple case study in the healthcare sector to add to the SISP body of knowledge. The healthcare sector comprises of companies, such as hospitals, which specialize in products and services related to health and medical care (Elysee, 2012; Georg. 2017; Richards, 2016).

Data suggest that the notion of top management support consists of three subthemes: level of involvement, level of support, and communication. For top management to give their support, they must consider these three elements. For the level of involvement, top management should be proactive with showing their support, and they should involve subject-matter experts to add rigor. Having subject-matter experts or having expertise in the subject at hand showed that top management support could add more weight to projects. Participants also mentioned the level of support as consisting of ensuring data confidentiality, integrity, and availability to authorized individuals. Hospitals should employ Lean Six Sigma with their project management practices along with a strong emphasis on communication is also essential, which data showed that communication is either face-to-face or remote. There must also be a level of interaction between top management and the rest of the staff that should include a high level of intensity, including regular meetings, follow-up meetings, bi-weekly meetings, and quarterly meeting.

Findings also revealed the importance of infrastructure flexibility, relationship with top management, and compliance. Relationship with top management includes incorporating the ideas from project members based on their empirical research relevant to SISP and InfoSec. Relationship with top management also consists of the element of flexibility, which data showed as top management having a well-defined plan that can incorporate their strategies in SISP for InfoSec benefits. There are three considerations associated with compliance: federal and state regulatory mandates, the establishment of an oversight committee, and the creation or use of internal or external audits.

For Construct 4, SISP success, it either successful, unsuccessful, or mixed. Participants who understand and practice most of the categories identified in the subthemes from the four constructs seemed to report SISP success more than other participants who did not consider most of these subthemes in their environments. The research also revealed that no organization was unsuccessful with regards to SISP success in producing InfoSec benefits. Participants reported that they all follow strict regulatory mandates, and the consequences of noncompliance to federal regulations are severe and financially catastrophic. Consequences of noncompliance may include paying fines, reorganizing IT/IS infrastructures, and being assigned a federally-appointed compliance regulator to ensure organizations redouble their efforts to remain compliant.

Comparison of Findings With Theoretical Framework and Previous Literature

Four Comparisons Based on the Result

Table 3 is organized by using (Lederer & Hannu, 1996) four constructs, which was the bases of the theoretical framework. Table 3 illustrates the attributes contributed by participants to obtain InfoSec benefits. (Lederer & Hannu, 1996) identified top management support, information system plan, infrastructure flexibility, and SISP success as the four constructs of SISP. (Lederer & Hannu, 1996) limited their research by leaving to future research to further investigate the relevance of the three constructs as they pertain to SISP success. (Lederer & Hannu, 1996) did not explain if there were InfoSec benefits to SISP success. However, Elysee (2012) suggested that future researchers add to the SISP body of knowledge by investigating InfoSec benefits to SISP success.

There are three challenges to this qualitative multiple case research. Challenge 1 was to provide relevance to (Lederer and Hannu 1996) four SISP constructs. The second challenge was to classify and interpret the responses of participants with relevance to the Agency theory and the SISP theory. The third challenge was to provide a proper interpretation of SISP success based on the results of data gathered by interviewing participants. Table 3 shows the four constructs along with their associated themes and subthemes based on the interpretation of responses from participants.

Table 3

Comparison of the Findings With the Theoretical Framework and Previous Literature

Constructs	Theme	Subthemes
Top Management Support	1. Role of Top management support in SISP and InfoSec	Level of involvement *Proactive support with hosting meetings *Inviting Subject-matter Expertise level of support *Secure electronic record *Six Sigma Practices *Project management practices Communication *Face-to-face *Remote *Regular Meeting *Follow-up meeting *Bi-weekly meeting *Quarterly meeting
Information Systems Plan	2. Planning for InfoSec	Level of detail *Intentions of top management are clear *Plans of top management are detailed Goals *Working with a budget *Obtain budget approval *Remain within compliance
Infrastructure Flexibility	3. Flexibility	Relationship with top management *Include ideas from project members based on their research *Have a well-defined plan to incorporate top management business strategies in SISP for InfoSec benefits

Table 3 continued

Constructs	Theme	Subthemes
		Compliance *Federal, state regulations *Have an oversight committee *Have an audit team
SISP Success	4. Top management support on SISP Success	No discernible subthemes *Successful - Fourteen participants believed that the SISP for InfoSec was successful. Those participants who believed that SISP for InfoSec was successful attributed this to the support coming from top management. *Unsuccessful - No participants indicated that SISP for InfoSec was unsuccessful. *Mix - Two participants provided mixed reviews of the InfoSec success

Interpretation of the Findings

From the responses of participants, the findings indicated that participants were aware of the four constructs and their significance or roles they play at their organizations when creating SISP. Participants gave a wealth of information that helps to understand how using the four constructs can help with obtaining InfoSec benefits. Top management support was investigated to see if there are other subthemes equally important for top management to understand so that their support is adequately given and measured.

Top Management Support

Using agency theory in which case the principals are top management, and the agents are the participants, top management involvement means that top management support in SISP in InfoSec involves the need to be proactive by hosting meetings. Top management support also includes inviting subject-matter experts in meetings about SISP. Top management level support needs to include ways to measure electronic records as mandated by HIPAA regulations (Murphy, 2018; Pullin, 2018). Having consistent Six Sigma practices and incorporating Project Management practices would also assist in support. Top management needs to communicate with participants, agents, using face-to-face meetings, remote meetings, and regular meetings. Top management also needs to host or hold follow-up meetings, bi-weekly meetings, and quarterly meetings. These trends were observed by investigating participants, who are senior managers, males, and females, employed at for-profit and nonprofit hospitals in Florida.

Information Systems Plan

Construct 2, Information System Plan, consists of planning for InfoSec, and data shows that the level of details for such a plan needs clear intentions of top management. Top management also needs a detailed plan to ensure SISP success to obtain InfoSec benefits. Top management is the principals (Shapiro 2005; Pouryousefi & Frooman, 2017). As principals of their firm, data show that participants understood the role of top management. Data showed that top management needs to align their goals with the financial standards of their firms as well, and top management need to comply with federal and state regulatory mandates. Data show that participants expressed that the goal of top management with regards to MIS and ITM for the adaptation of a SISP top management need to work within a budget. Top management needs to obtain approval of a budget, and make sure that the SISP remains within federal and state compliance mandates.

Infrastructure Flexibility

Analyzed data from Construct 3 show that participants agree that top management needs to have flexibility within their infrastructure. Participants mention that flexibility means that there is a relationship with top management. For this relationship to occur between top management and participants data show that top management needs to incorporate ideas from project members based from results obtained from their empirical research, so that ideas presented by project team members are included in the project plan. Data also show that flexibility also means having a clear plan that incorporates top management business strategies in SISP for InfoSec benefits.

SISP Success

Construct 4 findings indicated that participants mentioned compliance to include federal and state regulatory mandates. Hospitals fall within the purview of the United States' healthcare regulations such as HIPAA. As a result, top management should create an oversight committee so that the organization is kept current with new changes on regulatory mandates. Participants mentioned that having an audit team helps to make sure that the organization abides by all federal and state regulatory mandates. However, participants did not elaborate on whether audit teams are internal, external, or a mix of internal and external. Future researchers should investigate the significance of having an internal, external, or both, the audit team, and its connection to SISP success with regards to InfoSec benefits.

Limitations

Huang (2012) discussed how SISP could be used to enhance organization-wide operational governance, which assists firms in setting goals and objectives. Conversely, some researchers have discussed limitations linking SISP with the implementation of SISP. For instance, SISP helps corporate strategies, which are associated with existing technological limitations (Kardan, & Akbarnejad, 2014; Kosseff, 2018). The implementation of SISP provides robust structure-based methods which organizations use to audit policies and procedures concerning InfoSec and information technology (IT) outsourcing (Chen et al., 2010; Kosseff, 2018). An organization that uses different IS strategies can vary in their planning practices. Therefore, SISP enables organizations to apply InfoSec best practices and methodologies to help firms comply with federal mandates. This study was limited to Florida hospitals' IT departments. The introductory outreach and recruitment letters are limited to top management who work at licensed for-profit and licensed nonprofit hospitals listed on the 2015 Directory of Hospitals. The sample size was limited to Florida hospital IT professionals who possessed over five years of experience in SISP and InfoSec. The sample frame was limited to Florida hospital IT professionals with experiences in SISP and InfoSec. The source of the data for this study was the perspectives of Florida hospital IT professionals who have experiences in the phenomenon of SISP and InfoSec.

Another limitation was that it was difficult for participants to determine the state of their SISP for obtaining InfoSec benefits. Eleven participants mentioned that they preferred not to rate their organization SISP concerning construct four. However, data showed a pattern with the expression of a successful SISP with regards to InfoSec success as being either successful, unsuccessful, or mix. The researcher completed a further investigation of current empirical research to investigate what constitutes SISP success. The researcher found the presence of federal regulatory mandates as being the central theme for having SISP success. Participants believed their organizations experienced SISP success as long as organizations were compliant.

Implications for Practice

The theoretical underpinning of the study is Shapiro’s (2005) agency theory. Agency theory comprises of two main parties, owners (principals) and directors (agents), and revolves around employees work for owners (Shapiro, 2005). In their 2014 research, Bosse and Phillips described principals and agents as being equivalent to top management and directors, respectively. Principals, top management, have more vested interests in making sure that their involvement leads to InfoSec success. Collected data from participants 11, 10, and 14 suggest that there is a clear understanding in roles of top management (principals) and directors (agents), which aligned with Shapiro’s explanation of agency theory as it applies to organizations. Agency theory consists of two key assumptions. The first assumption is that agents behave or make decisions that benefit their self-interests, while principals similarly work to their advantage (Shapiro, 2005). The second assumption is that agents in a position of power have access to sensitive information but make decisions that work to their advantage (Shapiro, 2005). Participants 4, 2, and 5 expressed that in their top managers (principals) made sure that they remained proactive and involved at all levels in SISP projects to make sure that completing projects results to InfoSec benefits.

Agency theory explained that support involves the use of principals and the usefulness of agents (Shapiro, 2005). The usefulness of principals translates to maximizing profit (Shapiro, 2005; Bosse, & Phillips, 2014). For agents, usefulness is converted to direct compensation, which can be in forms of salary increase, long-term or short-term incentive plans, or paid expenses (Bosse, & Phillips, 2014; Shapiro, 2005; Toivonen & Toivonen, 2014). Using the discipline of project management enabled top management to initiate a SISP project by inviting third-party subject matter experts to guide them in understanding current threats and vulnerabilities that they must address to remain compliant (Toivonen & Toivonen, 2014). Directors can begin constructing a SISP plan based on obtaining InfoSec benefits and leave top managers the task of monitoring the execution phase of such SISP (Evans, & Tourish, 2017). The usefulness of principals and the usefulness of agents help maintain a level of support for the benefit of InfoSec while maintaining constant communication through meetings and follow up meetings either weekly or biweekly (Shapiro 2005; Steinle et al., 2014). Segars and Grover (1998) introduced SISP theory as involving activities requiring substantial resources from top management in term of time and budget. The process, according to SISP theory, must deliver benefits outside the resources necessary to sustain and contribute positively to InfoSec success (Segars & Grover, 1998). There are benefits, the intellectual dimension of top management alignment between SISP plans and business plans, and the long-term and short-term social dimension of alignment in keeping with the conceptualization of the four SISP constructs (Maharaj & Brown, 2015; Tunuguntla, Tunuguntla, & Tunuguntla, 2014). Participant 2 appeared impressed with top management and described how those in top management "sat down with some subject matter experts and people who were involved with helping to design our infrastructure.” This indicated that top management was willing to listen to the infrastructure needs and incorporate these into the SISP for InfoSec benefits. According to Participant 7, top management was also involved in regulatory compliance and HIPAA regulations for IT, adjusting its goals to make InfoSec projects a top priority.

Agency theory provides insights into principals’ approaches for coordinating hospital decision making with agents (Collin et al., 2015). Top management intentions should have clear and detailed SISP plans and should understand the importance of strategic goals, risks, and impact feasibility, based on the agency theory framework. The most successful hospital systems enable principals to formulate strategies that offer the best partnership balance with agents and facilitating technological innovations for constructing SISP (Evans, & Tourish, 2017; Pepper & Gore, 2015). There must be a partnership created between principals and agents to develop effective SISP plans that meet the needs of regulatory requirement and controls to licensed hospitals (Bendickson et al., 2016). The agency theory framework enables principals and agents working with a budget when implementing projects to remain within budget while maintaining HIPAA regulatory compliance for data confidentiality, integrity, and availability (Murphy, 2018; Pullin, 2018).

One of SISP theory’s benefits includes the creation of SISP frameworks such as that developed by (Lederer & Hannu, 1996), which is an essential beginning for measuring InfoSec success. A SISP framework allows for developing a measure for organizations’ MIS and ITM systems’ SISP success. Furthermore, a SISP framework helps in the development of measures and contemporary statistical techniques of organizations’ effectiveness, aimed at the use and operational structures or construct space for factors indicative of InfoSec success (Segars & Grover, 1998).

An effective SISP plan focuses on directing SISP processes to organizational characteristics, which can impact top management business justifications to provide the company effectiveness measures of scales (Peppard et al., 2014). Level of details subtheme can be used with different theoretical definitions to constitute the measurement space of SISP to obtain InfoSec success (Hung et al., 2016). Infrastructure flexibility consists of implementing projects, obtaining budget approval, and maintaining regulatory requirements (Ledered & Hannu 1996; Hermano, & Martín-Cruz, 2016).

Recommendations for Further Research

Findings from RQ 1 revealed three subthemes based top management support. The three subthemes are level of involvement, level of support, and communication. With regards to the level of involvement, this study revealed that top management must be proactive but is limited to the degree of top management involvement. Therefore, future research should focus on identifying the steps needed for top management to remain involved and on developing a mathematical formula to determine the level of involvement needed.

There are also types of communication, such as remote communication and in-person communication (Sull et al., 2017). Within remote communication, there may be different modes such as text, email, and voicemail (Sull et al., 2017). In person, communication may encompass in-person meetings consisting of short briefs or after-action reviews (Sull et al., 2017). Future researchers should concentrate on adding to the SISP body of knowledge by investigating how efficient top management remote communication compares to that of in-person communication.

Future researchers should attempt to investigate, using the quantitative methods, whether top management remote communication is more effective than in-person communication during a SISP project. Future researchers should also investigate the length of time a meeting should last before participants become disinterested in the topic at hand and whether projects involving short meetings complete on time as compared to projects requiring more extended meetings.

The analysis of data from this research showed that Construct 2, Infrastructure Flexibility, consists of two subthemes: level of details and goals. Further, the data noted that subtheme one, level of support, suggests that the intentions of top management must be clear, and plans detailing the intentions of top management must also be unambiguous (Shoufan & Damiani, 2017). Subtheme 2, goals, entails budges, and compliance measurements; however, these two subthemes were analyzed using multiple cased studies of hospitals while adapting the agency theory. Therefore, future researchers should concentrate on a different industry sector other than healthcare and adapt the stakeholder theory to compare if construct two, Infrastructure Flexibility, involves themes other than the level of details and goals that future researchers can explore.

Current research suggests that concerning construct four, SISP success; the central theme involves compliance (Kim, 2018; Kisekka, & Giboney, 2018; Kosseff, 2018). Collected data to complete this research showed a pattern with the expression of a successful SISP with regards to InfoSec benefit as being either successful, unsuccessful, or mixed. The researcher completed a further investigation of current empirical research to investigate what constitutes SISP success. The researcher found that the presence of federal regulatory mandates was the central theme for SISP success. SISP success also includes two categories of measurement, which are internal and external (Krishna et al. 2017; Kisekka, & Giboney, 2018). The internal factor refers to mitigating strategies aimed at minimizing risks associated with employees, staff, and contractors within the organization (Kisekka, & Giboney, 2018). The external factor refers to threats that exist beyond the physical confines of the organization (Kisekka, & Giboney. 2018; Nicho 2018). Therefore, to add to the SISP body of knowledge, future researchers can further investigate how useful the theme of regulatory compliance has been in assisting organizations to address internal and external threats.

Future researchers using a qualitative multiple case study design should attempt to duplicate this study at hospitals in other geographic areas to compare findings with those presented in this research. Future researchers should also consider focusing on other organizations within the healthcare sector, to compare their findings with those from this research. The healthcare sector comprises of companies, such as hospitals, which specialize in products and services related to health and medical care (Elysee, 2012; Georg 2017; Richards, 2016). Researchers who are already familiar with government-sponsored hospitals, such as hospitals within the guidelines of the United States Department of Veterans Affairs, should conduct qualitative multiple case research on the four constructs and compare their results with those presented in this research.

Conclusion

The purpose of this qualitative multiple case study was to identify the factors that prevented Florida hospitals from obtaining InfoSec benefits to prevent crypto-malware attacks when implementing SISP. The study was designed to investigate the four SISP constructs of Lederer and Hannu (1996) to identify the traits that impact SISP and prevent InfoSec benefits at

Florida hospital IT environments. To investigate the phenomenon, the researcher developed four questions, one from each of the four SISP constructs. RQ 1 investigated how do IT managers describe the process their organization went through to secure top management support before initiating strategic information systems planning as an InfoSec advantage? RQ 2 looked at how do IT managers describe the usefulness of SISP to obtain InfoSec benefits? RQ 3 examined how do IT managers describe the InfoSec benefits on the degree of information technology infrastructure flexibility? RQ 4 studied how do IT managers describe the degree of SISP success on their InfoSec environments? The research contributes to the body of knowledge in research of information technology in industry and social science research. This contribution may assist healthcare-based entities in acquiring InfoSec benefits, which is to comply with federal regulations (Elysee, 2012; Lee et al., 2015; Mishra et al., 2014).

The qualitative research methodology was used to discover participants' understanding of how their experiences with SISP enable their ability to obtain InfoSec success. Data analysis was completed using the unobtrusive method of data triangulation with codes and themes and later transcribed using the NVIVO 11 Pro. The themes adequately answered the research questions. The theoretical framework for the study was the Two-Tiered theoretical framework based on Ragu-Nathan et al. (2004) quantitative research survey. The Two-Tiered theoretical orientation examined existing direct or indirect top management support relationships, resulting in SISP success. The use of the agency theory provided guidelines for the SISP theory, which enabled the researcher to conduct a meta-analysis of the four constructs, which are top management support, the usefulness of information systems plans, the degree of information technology infrastructure flexibility, and the degree of SISP success. The study's findings emerged from the participants' understanding of their experiences based on the four constructs. These findings depicted areas Florida hospitals should include when designing SISP to assist their organization with obtaining InfoSec success. These findings will enable managers with understanding the four SISP constructs and allowing them to achieve expedient success in plans.

REFERENCES

Abbasi, A., Sarker, S., & Chiang, R. H. (2016). Big data research in information systems: Toward an inclusive research agenda. *Journal of the Association for Information Systems, 17*(2), 1-25. https://doi.org/I-XXXII. doi:10.17705/1jais.00423

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 357-370. https://doi.org/10.1007/s10845-012-0683-0

Ali, A. (2017). Ransomware: A research and a personal case study of dealing with this nasty malware. *Informing Science & Information Technology, 14,* 87-99. https://doi.org/10.28945/3707

Ali, R. H. R. M., Mohamad, R., & Tretiakov, A. (2013). The determinants of strategic information system planning (SISP) success: A proposed framework for small and medium-sized enterprises (SMEs). *Journal of Innovation Management in Small & Medium Enterprises, 2013,* 1-9. https://doi.org /10.5171/2013.348197

Alobaidly, S., Wainwright, D., & Waring, T. (2014). Practical framework for evaluating and implementing information system alignment in developing countries' organizations. *International Journal of Business and Management Studies*, *6*(1), 54-65. Retrieved from https://pdfs.semanticscholar.org/865f/d48989ddf186bae835d16c2af3804db9b97c.pdf

American Psychological Association. (2017). *Ethical principles of psychologists and code of conduct*. Retrieve from http://www.apa.org/ethics/code

Arvidsson, V., Holmström, J., & Lyytinen, K. (2014). Information systems use as strategy practice: A multi-dimensional view of strategic information system implementation and use. *The Journal of Strategic Information Systems*, *23*(1), 45-61. https://doi.org/10.1016/j.jsis.2014.01.004

Babatunde, A. O., Taiwo, A. J., & Dada, E. G. (2018). Information security in health care centre using cryptography and steganography. *Arid Zone Journal of Engineering, Technology and Environment*, *14*(2), 172-182. Retrieved from https://arxiv.org/ftp/arxiv/papers/1803/1803.05593.pdf

Bajwa, D. S., Rai, A., & Brennan, I. (1998). Key antecedents of executive information system success: A path analytic approach. *Decision Support Systems, 22*(1), 31-43. https://doi.org/10.1016/S0167-9236(97)00032-8

Bendickson, J., Muldoon, J., Liguori, E., & Davis, P. (2016). Agency theory: Background and epistemology. *Journal of Management History, 22*(4). 437-449. https://doi.org/10.1108/JMH-06-2016-0028

Blumberg, B., Cooper, D. R., & Schindler, P. S. (2008) *Business research methods*. London England: McGraw Hill.

Braun, V., & Clarke. V. (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The Psychologist*, *26*(2), 120-123. Retrieved from http://eprints.uwe.ac.uk/21155/3/Teaching%20thematic%20analysis%20 Research%20Repository%20version.pdf

Bøe, T., Gulbrandsen, B., & Sørebø, Ø. (2015). How to stimulate the continued use of ICT in higher education: Integrating information systems continuance theory and agency theory. *Computers in Human Behavior*, *50*, 375-384. https://doi.org/10.1016/j.chb.2015.03.084

Bosse D., & Phillips R. (2014). Agency theory and bounded self-interest. *Academy of Management Review*, *41*(2), 276-297. https://doi.org/10.5465/amr.2013.0420

Brown, I. T. J. (2004). Testing and extending theory in strategic information systems planning through literature analysis. *Information Resources Management Journal*, *17*(4), 20-48. https://doi.org/10.4018/irmj.2004100102

Byrd, T. A., Lewis, B. R., & Bradley, R. V. (2006). IS infrastructure: The influence of senior IT leadership and strategic information systems planning. *The Journal of Computer Information Systems, 47*(1), 101-113. https://doi.org/10.1080/08874417.2006.11645944

Byrd, T. A., Sambamurthy, V., & Zmud, R. W. (1995). An examination of IT planning in a large, diversified public. *Decision Sciences, 26*(1), 49-73. https://doi.org/10.1111/j.1540-5915.1995.tb00837.x

Byrd, T. A., & Turner, D. E. (2000). Measuring the flexibility of information technology infrastructure: Exploratory analysis of a construct. *Journal of Management Information Systems*, *17*(1), 168-208. https://doi.org/10.1080/07421222.2000.11045632

Chanopas, A., Krairit, D., & Khang, D. B. (2006). Managing information technology infrastructure: A flexibility framework. *Management Research News, 29*(10), 632-651. https://doi.org/10.1108/0409170610712335

Chen, D. Q., Mocker, M., Preston, D. S., & Teubner, A. (2010). Information systems strategy: Reconceptualization, measurement, and implications. *MIS Quarterly*, *34*(2), 233-A8. https://doi.org/10.2307/20721426

Chen, Y., Wang, Y., Nevo, S., Jin, J., Wang, L., & Chow, W. S. (2014). IT capability and organizational performance: The roles of business process agility and environmental factors. *European Journal of Information Systems*, *23*(3), 326-342. https://doi.org/ 10.1057/ejis.2013.4

Chuang, S., & Inder, K. (2009). An effectiveness analysis of healthcare systems using a systems theoretic approach. *BMC Health Services Research*, *9*, 1-11. https://doi.org/10.1186/1472-6963-9-195

Clegg, S., Killen, C. P., Biesenthal, C., & Sankaran, S. (2018). Practices, projects and portfolios: Current research trends and new directions. *International Journal of Project Management*. *36*(5), 762-772. https://doi.org/10.1016/j.ijproman.2018.03.008

Clemons, R. (2015). *Relationships: Strategic information systems planning factors and customer relationship management implementation success/failure* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. (Order No. 3718620)

Collin, K., Paloniemi, S., & Vähäsantanen, K. (2015). Multiple forms of professional agency for non-crafting of work: Practices in a hospital organization. *Nordic Journal of Working Life Studies, 5,* 63-83. https://doi.org/10.19154/njwls.v5i3a.4834

Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Los Angeles, CA: Sage.

Creswell, J. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Los Angeles, CA: Sage.

Creswell, J., & Creswell, D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches.* Los Angeles, CA: Sage.

Creswell, J., & Miller, D. (2000). Determining validity in qualitative inquiry. *Theory Into Practice*, *39*(3), 124–30. https://doi.org/10.1207/s15430421tip3903_2

Creswell, J., & Poth, N. (2018). *Qualitative inquiry and research design: Choosing among five approaches.* Los Angeles, CA: Sage.

Dahm, M. R., Georgiou A, & Westbrook J. I. (2017). Delivering safe and effective test-result communication, management and follow-up: A mixed-methods study protocol. *BMJ Open, 8,* 1-10. https://doi.org/10.1136/bmjopen-2017-020235

Davis, C. (Ed.). (2014). *2015 directory of hospitals*. Gainsville, FL: Florida Hospital Association Retrieved from the Florida Hospital Association website: http://www.nxtbook.com/ naylor/FHAD/FHAD0014/index.php#/1

Drew, C. J., & Hardman, M. L. (2007). *Intellectual disabilities across the lifespan* (9th ed.). Upper Saddle River, NJ: Merrill.

Dubey, R., Gunasekaran, A., Papadopoulos, T., Childe, S. J., Shibin, K. T., & Wamba, S. F. (2017). Sustainable supply chain management: Framework and further research directions. *Journal of Cleaner Production*, *142*, 1119-1130. https://doi.org/10.1016/j.jclepro.2016.03.117

Duncan, N. B. (1995). Capturing flexibility of information technology infrastructure: A study of resource characteristics and their measure. *Journal of Management Information Systems*, *12*(2), 37-57. https://doi.org/10.1080/07421222.1995.11518080

Elysee, G. (2012). *The effects of top management support on strategic information systems planning success*. (Doctoral dissertation). Retrieved from ERIC database. (Accession No: ED549812)

Esteves, J. M. (2014). An empirical identification and categorisation of training best practices for ERP implementation projects. *Enterprise Information Systems*, *8*(6), 665-683. https://doi.org/10.1080/17517575.2013.771411

Evans, S., & Tourish, D. (2017). Agency theory and performance appraisal: how bad theory damages learning and contributes to bad management practice. *Management Learning, 48*(3), 271-291. https://doi.org/10.1177/1350507616672736

Foss, N., & Stea, D. (2014). Putting a realistic theory of mind into agency theory: Implications for reward design and management in principal-agent relations. *European Management Review*, *11*(1), 101-116. https://doi.org/10.1111/emre.12026

Furukawa, M. (2013). A study on the “flexibility” of information systems (Part 2): How can we make them flexible? *International Journal of Business and Management*, *8*(19), 73–89. https://doi.org/10.5539/ijbm.v8n19p73

Furukawa, M., Hirobayashi, S., & Misawa, T. (2014). A study on the “flexibility” of information systems (Part 3): MIS flexibility planning scheme for IT/Business strategy alignment. *International Journal of Business and Management*, *9*(6), 88-97. https://doi.org/ 10.5539/ijbm.v9n6p88

Furukawa, M., & Minami, A. (2013). A study on the “flexibility” of information systems (Part 1): Why do they need to be flexible? *International Journal of Business and Management, 8*(20), 48–61. https://doi.org/10.5539/ijbm.v8n20p48

Gabriel, M. H., Jones, E. B., Samy, L., & King, J. (2014). Progress and challenges: Implementation and use of health information technology among critical-access hospitals. *Health Affairs, 33*(7), 1262-1270. https:// doi.org/10.1377/hlthaff.2014

Georg, L. (2017). Information security governance: Pending legal responsibilities of non-executive boards. *Journal of Management & Governance, 21*(4), 793-814. https://doi.org/10.1007/s10997-016-9358-0

Gerow, J. E., Grover, V., Thatcher, J. B., & Roth, P. L. (2014). Looking toward the future of IT-business strategic alignment through the past: A meta-analysis 1. *MIS Quarterly*, *38*(4), 1059-1085. Retrieved from https://cpb-us-e1.wpmucdn.com/sites.uark.edu/dist/c/1/files /2017/06/2014-MISQ.pdf

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal, 204*(6), 291-295. https://doi.org/10.1038/bdj.2008.192

Glinkowska, B, & Kaczmarek B. (2016). Classical and modern concepts of corporate governance: Stewardship theory and agency theory. *The Journal of University of Zielona Gora, 19*(2), 84-92. https://doi.org/10.1515/manment-2015-0015

Coronado A. J., & Wong T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical Instrumentation & Technology, 48*(1), 26-30. https://doi.org/10.2345/0899-8205-48.s1.26

Gorla, N., & Somers, T. M. (2014). The impact of IT outsourcing on information systems success. *Information & Management, 51*(3), 320-335. https://doi.org/10.1016/j.im.2013.12.002

Gottschalk, P. (1999a). Implementation predictors of strategic information systems plans. *Information & Management, 36*(2), 77-91. https://doi:10.1016/S0378-7206(99)00008-7

Gottschalk, P. (1999b). Strategic information systems planning: The IT strategy implementation matrix. *European Journal of Information Systems, 8*(2), 107-118. https://doi.org/ 10.1057/palgrave.ejis.3000324

Gottschalk, P. (2002). The role of the chief information officer in formal strategic information systems planning. *International Journal of Technology, Policy and Management*, *2*(2), 93-101.

Grabara, J., Kolcun, M., & Kot, S. (2014). The role of information systems in transport logistics. *International Journal of Education and Research*, *2*(2), 1-8. Retrieved from http://www.ijern.com/journal/February-2014/25.pdf

Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today, 24*(2), 105-112. https://doi.org/10.1016/j.nedt.2003.10.001

Hartono, E., Lederer, A. L., Sethi, V., & Zhuang, Y. (2003). Key predictors of the implementation of strategic information systems plans. *Database for Advances in Information Systems, 34*(3), 41-53. https://doi.org/10.1145/937742.937747

Henfridsson, O., & Lind, M. (2014). Information systems strategizing, organizational sub-communities, and the emergence of a sustainability strategy. *The Journal of Strategic Information Systems, 23*(1), 11-28. https://doi.org/10.1016/j.jsis.2013.11.001

Hermano, V., & Martín-Cruz, N. (2016). The role of top management involvement in firms performing projects: A dynamic capabilities approach. *Journal of Business Research, 69,* 3447-3458. https://doi.org/10.1016/j.jbusres.2016.01.041

Hoenen, A. K., & Kostova, T. (2015). Utilizing the broader agency perspective for studying headquarters–subsidiary relations in multinational companies. *Journal of International Business Studies*, *46*(1), 104-113. https://doi.org/10.1057/jibs.2014.31

Hoque, M. R., Hossin, M. E., & Khan, W. (2016). Strategic information systems planning (SISP) practices in health care sectors of Bangladesh*. European Scientific Journal*, *12*(6), 307-321. https://doi.org/10.19044/esj.2016.v12n6p307

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher*, *20*(4), 12-17. https://doi.org/10.7748/nr2013.03.20.4.12.e326

Huang, L. K. (2012). The impact of IT management sophistication on perceived it importance in strategic alignment. *The Journal of Computer Information Systems, 53*(2), 50-64. https://doi.org/ doi:10.1080/08874417.2012.11645614

Hung, S. Y., Huang, W. M., Yen, D. C., Chang, S. I., & Lu, C. C. (2016). Effect of information service competence and contextual factors on the effectiveness of strategic information systems planning in hospitals. *Journal of Global Information Management (JGIM), 24*(1), 14-36. https://doi.org/10.4018/JGIM.2016010102

Hyett, N., Kenny, A. J., & Dickson-Swift, V. A. (2014). Methodology or method? A critical review of qualitative case study reports. *International Journal of Qualitative Studies on Health and Well-Being, 9*(1), 1-12. https://doi.org/10.3402/qhw.v9.23606

Jaana, M., Teitelbaum, M., & Roffey, T. (2014). IT strategic planning in hospitals: From theory to practice. *International Journal of Technology Assessment in Health Care, 30*(3), 289-297. https://doi.org/10.1017/S0266462314000269

Jemal, H., Kechaou, Z., Ayed, M. B., & Alimi, A. M. (2015). A multi agent system for hospital organization. *International Journal of Machine Learning and Computing*, *5*(1), 51-56. https://doi.org/10.7763/IJMLC.2015.V5.482

Jorfi, S., Nor, K. M., & Najjar, L. (2017). An empirical study of the role of IT flexibility and IT capability in IT-business strategic alignment. *Journal of Systems and Information Technology*, *19*(1/2), 2-21. https://doi.org/10.1108/JSIT-10-2016-0067

Karahanna, E., & Preston, D. S. (2013). The effect of social capital of the relationship between the CIO and top management team on firm performance. *Journal of Management Information Systems, 30*(1), 15-56. https://doi.org/10.2753/MIS0742-1222300101

Kardan, A., & Akbarnejad, A. (2014). An investigation of the processes of IT management. *Kuwait Chapter of the Arabian Journal of Business and Management Review, 3*(7), 117-140. https://doi.org/10.12816/0018277

Kearns, G. S. (2006). The effect of top management support of SISP on strategic IS management: Insights from the US electric power industry. *Omega*, *34*(3), 236-253. https://doi.org/10.1016/j.omega.2004.10.008

Kenyon, B., & McCafferty, J. (2016). Ransomware recovery. *ITNOW, 58*(4), 32-33. https://doi.org/10.1093/itnow/bww103

Khani, N., Nor, K. M., & Bahrami, M. (2011). IS/IT capability and strategic information system planning (SISP) success. *International Journal of Managing Information Technology (IJMIT), 3*(3), 28-37. https://doi.org/10.5121/ijmit.2011.3303

Kim, L. (2018). Cybersecurity matters. *Nursing Management*, *49*(2), 16-22. https://doi.org/10.1097/01.NUMA.0000529921.97762.be

Kim, S. S., & Kim, Y. J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. *Journal of Knowledge Management*, *21*(4), 986-1010. https://doi.org/10.1108/JKM-08-2016-0353

Kisekka, V., & Giboney, J. S. (2018). The effectiveness of health care information technologies: Evaluation of trust, security beliefs, and privacy as determinants of health care outcomes. *Journal of Medical Internet Research*, *20*(4), 1-11. https://doi.org/10.2196/jmir.9014

Kitsios F., & Kamariotou M. (2018). Decision support systems for strategic information systems planning: An approach for logistics strategic management. *International Journal of Decision Support Systems, 3*(4), 207-221. https:// doi.org/10.1504/IJDSS.2018.100188

Kosseff, J. (2018). Defining cybersecurity law. *Iowa Law Review, 103*(3), 985-1031. Retrieved from https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law/

Krishna, A., Khan, S. R. A., & Pandey, C. M. (2017). Security issues, challenges and success factors of hospital information system. *I-Manager's Journal on Information Technology, 6*(3), 30-35. https://doi.org/10.26634/jit.6.3.13782

Kumar, R. L., & Stilianou, A. C. (2014). A process model for analyzing and managing flexibility in information systems. *European Journal of Information Systems*, *23*(2), 151-184. https://doi.org/10.1057/ejis.2012.53

Landaeta Olivo, J. F., García Guzmán, J., Colomo-Palacios, R., & Stantchev, V. (2016). IT innovation strategy: Managing the implementation communication and its generated knowledge through the use of an ICT tool. *Journal of Knowledge Management*, *20*(3), 512-533. https://doi.org/10.1108/JKM-06-2015-0217

Lederer, A. L., & Hannu, S. (1996). Toward a theory of strategic information systems planning. *The Journal of Strategic Information Systems*, *5*(3), 237-253. https://doi.org/10.1016/S0963-8687(96)80005-9

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, *59*, 60-70. https://doi.org/10.1016/j.cose.2016.02.004

Lee, J., Elbashir, M. Z., Mahama, H., & Sutton, S. G. (2014). Enablers of top management team support for integrated management control systems innovations. *International Journal of Accounting Information Systems*, *15*(1), 1-25. https://doi.org/10.1016/j.accinf.2013.07.001

Lee, J. Y., McFadden, K. L., & Gowen, C. R. (2018). An exploratory analysis for lean and six sigma implementation in hospitals: Together is better? *Health Care Management Review*, *43*(3), 182-192. https://doi.org/10.1097/HMR.0000000000000140

Lee, T., Ghapanchi, A. H., Talaei-Khoei, A., & Ray, P. (2015). Strategic information system planning in healthcare organizations. *Journal of Organizational and End User Computing (JOEUC)*, *27*(2), 1-31. https://doi.org/10.4018/joeuc.2015040101

Li, Y., Shepherd, M., Liu, J. Y., & Klein, G. (2017). Enhancing development team flexibility in IS projects. *Information Technology and Management*, *18*(1), 83-96. https://doi.org/10.1007/s10799-016-0258-4

Liu, S. (2015). Effects of control on the performance of information systems projects: The moderating role of complexity risk. *Journal of Operations Management*, *36*, 46-62. https://doi.org/10.1016/j.jom.2015.03.003

Mahaney, R. C., & Lederer, A. L. (2011). An agency theory explanation of project success. *Journal of Computer Information Systems, 51*(4), 102-113. https://doi.org/10.1080/08874417.2011.11645506

Maharaj, S., & Brown, I. C. (2015). The impact of shared domain knowledge on strategic information systems planning and alignment. *South African Journal of Information Management, 17*(1), 1-12. https://doi.org/10.4102/sajim.v17i1.608

Maheshwari, S., & Vohra, V. (2015). Identifying critical HR practices impacting employee perception and commitment during organizational change. *Journal of Organizational Change Management, 28*(5), 872-894. https://doi.org/10.1108/JOCM-03-2014-0066

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior, 83*, 32-44. https://doi.org/10.1016/j.chb.2018.01.028

Marshall, B., Cardon, P. W., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? A review of qualitative interviews in IS research. *Journal of Computer Information Systems, 54*, 11-22. https://doi.org/10.1080/08874417.2013.11645667

Mason, M. (2010). Sample size and saturation in PhD studies using qualitative interviews. *Forum: Qualitative Social Research, 11*(3), 1-19. https://doi.org/10.17169/fqs-11.3.1428

McDavid, J. C., Huse, I., &. Hawthorn, L., R. L. (2012). *Program evaluation and performance measurement: An introduction to practice.* (2nd ed.). London, England: Sage.

McGivern, G., Dopson, S., Ferlie, E., Fischer, M., Fitzgerald, L., Ledger, J., & Bennett, C. (2018). The silent politics of temporal work: A case study of a management consultancy project to redesign public health care. *Organization Studies, 39*(8), 1007-1030. https://doi.org/10.1177/0170840617708004

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis.* (2nd ed.). London, England: Sage.

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative data analysis* (3rd ed.). London, England: Sage.

Mishra, S., Caputo, D. J., Leone, G. J., Kohun, F. G., & Draus, P. J. (2014). The role of awareness and communications in information security management: A health care information systems perspective. *International Journal of Management & Information Systems (Online), 18*(2), 139-138. https://doi.org/10.19030/ijmis.v18i2.8495

Mullaly, M. (2014). The role of agency in project initiation decisions. *International Journal of Managing Projects in Business, 7(*3), 518-535. https://doi.org/10.1108/IJMPB-09-2013-0043

Murphy, S. (2018). A holistic approach to cybersecurity starts at the top. *Frontiers of Health Services Management, 35*(1). 30-36. https://doi.org/10.1097/HAP.0000000000000041

U.S. Department of Health and Human Services, National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research* (45 CFR 46. Retrieved from http://www.hhs.gov/ohrp/regulations-and-polocy/belmont-report/

Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security, 26*(1), 10-38. https://doi.org/10.1108/ICS-07-2016-0061

Orcher, L. T. (2005). *Conducting research: Social and behavioral science methods*. Gendale, CA: Pyrczak.

Pankratz, O., & Basten, D. (2018). Opening the black box: Managers' perceptions of IS project success mechanisms. *Information & Management*, *55*(3), 381-395. https://doi.org/10.1016/j.im.2017.09.005

Peppard, J., Galliers, R. D., & Thorogood, A. (2014). Information systems strategy as practice: Micro strategy and strategizing for IS. *Journal of Strategic Information Systems*, *23*(1), 1-10. https://doi.org/10.1016/j.jsis.2014.01.002

Pepper, A., & Gore, J. (2015). Behavioral agency theory: new foundations for theorizing about executive compensation. *Journal of Management*, *41*(4), 1045-1068. https://doi.org/10.1177/0149206312461054

Pouryousefi, S., & Frooman, J. (2017). The problem of unilateralism in agency theory: Towards a bilateral formulation. *Business Ethics Quarterly*, *27*(2), 163-182. https://doi.org/10.1017/beq.2016.77

Premkumar, G., & King, W. R. (1994). Organizational characteristics and information systems planning: An empirical study. *Information Systems Research*, *5*(2), 75-109. https://doi.org/10.1287/isre.5.2.75

Pullin, D. W.(2018). Cybersecurity: Positive changes through processes and team culture. *Frontiers of Health Services Management*, *35*(1), 3-12. https://doi.org/10.1097/HAP.0000000000000038

Ragu-Nathan, B. S., Apigian, C. H., Ragu-Nathan, T. S., & Tu, Q. (2004). A path analytic study of the effect of top management support for information systems performance. *Omega*, *32*(6), 459-471. https://doi.org/10.1016/j.omega.2004.03.001

Rahimi, F., Møller, C., & Hvam, L. (2016). Business process management and IT management: The missing integration. *International Journal of Information Management*, *36*(1), 142-154. https://doi.org/10.1016/j.ijinfomgt.2015.10.004

Ribes, D., & Polk, J. B. (2014). Flexibility relative to what? change to research infrastructure. *Journal of the Association for Information Systems*, *15*, 287-305. https://doi.org/ 10.17705/1jais.00360

Richards, J. (2016). Cyber crime:An evolutionary arms race. *Itnow*, *58*(3), 38-39. https://doi.org/10.1093/itnow/bww075

Ridge, J. W., & Ingram, A. (2017). Modesty in the top management team: Investor reaction and performance implications. *Journal of Management*, *43*(4), 1283-1306. https://doi.org/10.1177/0149206314551796

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity-based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*, *40*, 247-257. https://doi.org/10.1016/j.jisa.2017.11.001

Saldaña, J. (2015). *The coding manual for qualitative researchers*. London, England: Sage.

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. https://doi.org/10.2307/249393

Shao, Z., Feng, Y., & Hu, Q. (2017). Impact of top management leadership styles on ERP assimilation and the role of organizational learning. *Information & Management*, *54*(7), 902-919. https://doi.org/10.1016/j.im.2017.01.005

Shapiro, S. P. (2005). Agency theory. *Annual Review of Sociology*, *31*, 263–84. https://doi.org/10.1146/annurev.soc.31.041304.122159

Sharma, R., & Yetton, P. (2011). The contingent effect of management support and task independence on successful information systems implementation. *MIS Quarterly*, *27*(4), 533-556. https://doi.org/ 10.2307/30036548

Silvius, A. J., & Stoop, J. (2013). The relationship between the process of strategic information systems planning and its success: An explorative study. *2013 46th Hawaii International Conference on System Sciences*, 4495-4501. https://doi.org/10.1109/hicss.2013.536

Singh, R., Mindel, V., & Mathiassen, L. (2017). IT-enabled revenue cycle transformation in resource-constrained hospitals: A collaborative digital options inquiry. *Journal of Management Information Systems, 34*(3), 695-726. https://doi.org/10.1080/07421222.2017.1373005

Sirisomboonsuk, P., Gu, V. C., Cao, R. Q., & Burns, J. R. (2017). Relationships between project governance and information technology governance and their impact on project performance. *International Journal of Project Management*. https://doi.org/10.1016/j.ijproman.2017.10.003

Shenton, A. K., (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information 22,* 63-75. https://doi.org/10.3233/EFI-2004-22201

Shoufan, A., & Damiani, E. (2017). On inter-rater reliability of information security experts. *Journal of Information Security and Applications, 37*, 101-111. https://doi.org/10.1016/j.jisa.2017.10.006

Srivastava, A. K., & Sushil. (2015). Modeling organizational and information systems for effective strategy execution. *Journal of Enterprise Information Management*, *28*(4), 556-578. https://doi.org/10.1108/JEIM-09-2013-0071

Steinle, C., Schiele, H., & Ernst, T. (2014). Information asymmetries as antecedents of opportunism in buyer-supplier relationships: Testing principal-agent theory. *Journal of Business-to-Business Marketing, 21*(2), 123-140. https://doi.org/10.1080/1051712X.2014.903457

Stewart, J. (2012). Multi-case study methods in governance-related research. *Public Management Review, 14*(1), 67-82. https://doi.org/1080/14719037.2011.589618

Sull, D., Turconi, S., Sull, C., & Yoder, J. (2017). Turning strategy into results. *MIT Sloan Management, 59*(3). Retrieved from https://sloanreview.mit.edu/article/turning-strategy-into-results/

Syväjärvi, A., Leinonen, J., Kivivirta, V., & Kesti, M. (2017). The latitude of information management in local government: Views of local government managers. *International Journal of Electronic Government Research (IJEGR)*, *13*(1), 69-85. https://doi.org/10.4018/IJEGR.2017010105

Tawaha, M. S. H. (2015). The effect of alignment strategy on organizational performance in Jordanian banks registered in Amman stock exchange up to 2012. *International Journal of Business Administration*, *6*(3), 94. https://doi.org/10.5430/ijba.v6n3p94

Teo, T. S. H., & Ang, J. S. K. (2001). An examination of major IS planning problems. *International Journal of Information Management, 21*(6), 457-470. https://doi.org/10.1016/S0268-4012(01)00036-6

Teubner, R. A. (2013). Information systems strategy. *Business & Information Systems Engineering, 5*(4), 243-257. https://doi.org/10.1007/s12599-013-0279-z

Toivonen, A., & Toivonen, P. U. (2014). The transformative effect of top management governance choices on project team identity and relationship with the organization—An agency and stewardship approach. *International Journal of Project Management*, *32*(8), 1358-1370. https://doi.org/10.1016/j.ijproman.2014.07.001

Too, E. G., & Weaver, P. (2014). The management of project management: A conceptual framework for project governance. *International Journal of Project Management*, *32*(8), 1382-1394. https://doi.org/10.1016/j.ijproman.2013.07.006

Trivedi, A., & Rajawat, S. (2015). An effective analysis of healthcare systems using a systems theoretic approach. In V. Vijay, S. Yadav, B. Adhikari, H. Seshadri, & D. Fulwani (Eds.), *Systems thinking approach for social problems* (pp. 221-230). https://doi.org/10.1007/978-81-322-2141-8_19

Trochim, W. (2006). *The research method knowledgebase* (2nd ed.). Cincinnati, OH: Atomic Dog.

Tunuguntla, P. C., Tunuguntla, V., & Tunuguntla, L. V. M. (2014). Impact of social factors on business-IT alignment. *The International Journal of Interdisciplinary Organizational Studies, 8*(1). 15-32. https://doi.org/10.18848/2324-7649/CGP/v08i01/53417

Ursacescu, M. (2014). Assessing the maturity level of information technology management process in a Romanian company. *International Journal of Management & Information Systems (Online), 18*(3), 201. https://doi.org/10.19030/ijmis.v18i3.8706

Vähäsantanen, K., Paloniemi, S., Hökkä, P., & Eteläpelto, A. (2017). Agentic perspective on fostering work-related learning. *Studies in Continuing Education, 39*(3), 251-267. https://doi.org/10.1080/0158037X.2017.1310097

Ward, K. (2012). A proposed measure of IT infrastructure flexibility in the global networked firm: Extending the IT infrastructure measure of reach and range. *International Journal of Management & Information Systems (Online), 16*(1), 39-44. Retrieved from https://clutejournals.com/index.php/IJMIS/article/view/6720/6795

Weech-Maldonado, R., Dreachslin, J. L., Epané, J. P., Gail, J., Gupta, S., & Wainio, J. A. (2018). Hospital cultural competency as a systematic organizational intervention: Key findings from the National Center for Healthcare Leadership Diversity Demonstration Project. *Health Care Management Review*, *43*(1), 30-41. https://doi.org/10.1097/HMR.0000000000000128

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security, 77*, 807-823. https://doi.org/10.1016/j.cose.2018.02.001

Wilkin, C. L., Couchman, P. K., Sohal, A., & Zutshi, A. (2016). Exploring differences between smaller and large organizations' corporate governance of information technology. *International Journal of Accounting Information Systems*, *22*, 6-25. https://doi.org/10.1016/j.accinf.2016.07.002

Yang, J., & Tanner, K. (2011). Enablers and inhibitors of SISP: A case study of a Korean large corporation. *Communications of the IBIMA, 2011*, 1-16. https://doi.org/10.5171/2011.922957

Yang, J., & Pita, Z. (2014). Research instrument of the measurement of facilitators for enhancing SISP success and dynamic capabilities. *PACIS 2014 Proceedings*, 314. Retrieved from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1073&context=pacis2014

Yeh, C. H., Lee, G. G., & Pai, J. C. (2015). Using a technology-organization-environment framework to investigate the factors influencing e-business information technology capabilities. *Information Development*, *31*(5), 435-450. https://doi.org/10.1177/0266666913516027

Yin, R. K. (2009). *Case study research*: *Design and methods* (4th ed.). Thousand Oaks, CA:

Sage.

Yin, R. K. (2013). *Case study research: Design and methods* (5th ed.). Los Angeles, CA: Sage.

Yoshikuni, A.C., & Albertin, A. (2018). The effects of strategic IS on firm performance: An empirical study of the three-way interaction investigation of turbulent scenario. *Journal of Public Administration and Governance*, *8*(4), 20-43. https://doi.org/10.5296/jpag.v8i4.13767

Young, R., & Jordan, S. (2008). Top management support: Mantra or necessary? *International Journal of Project Management*, *26*(7), 713-725. https://doi.org/10.1016/j.ijproman.2008.06.001

Young, R., & Poon, S. (2013). Top management support–Almost always necessary and sometimes sufficient for success: Findings from a fuzzy set analysis. *International Journal of Project Management, 31*(7), 943-957. https://doi.org/10.1016/j.ijproman.2012.11.013