2015

Best Practices to Minimize Data Security Breaches for Increased Business Performance

Fedinand Jaiventume Kongnso
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Fedinand Kongnso

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Yvette Ghormley, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Denise Land, Committee Member, Doctor of Business Administration Faculty

Dr. Franz Gottleib, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2015

Abstract

Best Practices to Minimize Data Security Breaches for Increased Business Performance

by

Fedinand Jaiventume Kongnso

MISM, Walden University, 2010

BBA, Viterbo University, 2006

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2015

Abstract

In the United States, businesses have reported over 2,800 data compromises of an estimated 543 million records, with security breaches costing firms approximately $7.2 million annually. Scholars and industry practitioners have indicated a significant impact of security breaches on consumers and organizations. However, there are limited data on the best practices for minimizing the impact of security breaches on organizational performance. The purpose of this qualitative multicase study was to explore best practices technology leaders use to minimize data security breaches for increased business performance. Systems theory served as the conceptual framework for this study. Fourteen participants were interviewed, including 2 technology executives and 5 technical staff, each from a banking firm in the Northcentral United States and a local government agency in the Southcentral United States. Data from semistructured interviews, in addition to security and privacy policy statements, were analyzed for methodological triangulation. Four major themes emerged: a need for implementation of security awareness education and training to mitigate insider threats, the necessity of consistent organization security policies and procedures, an organizational culture promoting data security awareness, and an organizational commitment to adopt new technologies and innovative processes. The findings may contribute to the body of knowledge regarding best practices technology leaders can use for securing organizational data and contribute to social change since secure organizational data might reduce consumer identity theft.

Best Practices to Minimize Data Security Breaches for Increased Business Performance

by

Fedinand Jaiventume Kongnso

MISM, Walden University, 2010

BBA, Viterbo University, 2006

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

December 2015

Dedication

This program has been a long journey for me and I want to thank God for the strength he gave me to keep on. I dedicate this study to my beautiful wife, Kimberly A. Kongnso, my daughters Kiara Kongnso and Khloe Kongnso, my parents Erica and Francis Kongnso, and my host parents Ann and Jake Delwiche. The support from my wife and children has been amazing and commendable. My wife made sure I had enough time to focus on my studies, as she took care of the children. My children, especially Kiara let me focus, even when she wanted to spend time with me. My parents instilled in me the importance of hard work and education. My host parents encouraged and motivated me throughout this process.

Acknowledgments

Completing this DBA program was my educational goal. However, this would not have been possible without the help of so many at Walden University. I would like to thank my committee chair Dr. Yvette Ghormley for all the support, patience, respect, and encouragement throughout this process. Dr. Ghormley guided me through challenging times in the program, and I would not be completing this journey without her guidance. Words cannot express how I feel. Thank you! Thank you!

I would like to acknowledge Dr. Denise Land and Dr. Franz Gottleib for their guidance and support. Thank you for your professionalism throughout the review processes. I would also want to acknowledge, Dr. Maurice Dawson for his support and encouragement. Finally, I would like to thank Dr. Freda Turner for being there to listen and assure continued faculty support.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

In the global economy, organizations are finding ways to streamline business operations and processes through the implementation of information technology (IT) systems. Technology systems assist organizations in improving business operations, customer relationships, and stakeholder values (Setia, Venkatesh, & Joglekar, 2013). Computer systems have provided organizations with the ability to complete business processes such as supply chain management, marketing, forecasting, finance, and complying with industry standards and government regulations (Zhang, van Donk, & van der Vaart, 2011). Businesses are adopting technology innovations to drive efficiencies within business operations to increase value (Caniëls, Lenaerts, & Gelderman, 2015). However, despite the positive effects technology has on businesses, IT services have introduced data security and privacy issues (Arlitscha & Edelmanb, 2014).

Background of the Problem

The reliance on IT for daily business activities and competitiveness has increased throughout the past decade (Grant & Royle, 2011). Individuals, corporations, and governments are processing and storing large amounts of sensitive data electronically. This sensitive information is vulnerable to threats and risks of abuse as well as unauthorized access or disclosure (Bisong & Rahman, 2011). According to Susanto, Almunawar, Tuan, Aksoy, and Syam (2011), technological advancements have introduced business risks and security threats that are a serious concern for business leaders. Moreover, 93% of large companies and 87% of small businesses have reported at

least one security incident (Price Waterhouse Cooper, 2013).

Results from a 5-year analysis of data security breaches in the public and private sectors indicated a compromise of more than 200 million consumers' data (Garrison & Ncube, 2011). The National Institute of Standards and Technology (NIST, 2011) indicated that the United States and other developed nations have recognized the significance of information security to economic growth and national security. In addition, the NIST (2011) reported that the number of cyber-attacks and data security breaches against the U.S. government and U.S. corporations have increased in the last 2 decades.

Information is a vital business asset (Susanto, Almunawar, & Tuan, 2012). Therefore, to protect business information assets against internal and external threats, organizations implement controls to monitor, measure, and respond to security vulnerabilities (Carter, Phillips, & Millington, 2012). Corporations, governments, and individuals face numerous data security threats and risks each day (Arlitscha & Edelmanb, 2014). Businesses have increased investments in information security, and dedicate an average of 40% of annual IT budgets to information security initiatives (Lo & Chen, 2012). Studies have also found that data security breaches have an impact on organizational financial performance (Zafar, Ko, & Osei-Bryson, 2012).

Confidentiality of proprietary and consumer information is more than just a business requirement (Reid, 2013). Thompson et al. (2011) illustrated that data protection is an ethical and legal requirement. Approximately 70% of executives responding to a

survey by Ernst and Young (2013) indicated that information security policy oversight is a key responsibility of the board of directors. In response, corporations have recognized the impact of data security breaches on stock prices and financial performance (Chai, Kim, & Rao, 2011). In prior studies researchers have focused on the impact of information security breaches on an organization's financial performance (Chai et al., 2011), and have recommended further research on the effect of security breaches on businesses (Yayla & Hu, 2011). Moreover, White, Hewitt, and Kruck (2013) have noted that most security professionals lack the necessary expertise to combat security threats. Therefore, my objective in this study was to explore the best practices technology leaders use to minimize data security breaches for enhanced business performance.

Problem Statement

Businesses in the United States have reported over 2,800 data security breaches of an estimated 543 million records, which have significantly affected business financial performance (Romanosky, Hoffman, & Acquisti, 2014). Security breaches increase an average of 70% every 3 years, costing U.S. companies approximately $7.2 million annually (Zafar, Ko, & Osei-Bryson, 2015). Combined costs of information security programs within the U.S. government and corporate sectors averages about $15 billion each year (Executive Office of the President of the United States, 2013). The general business problem I sought to address in my study was the increasing cost of protecting confidential data. and how that cost affects business sustainability. The specific business problem this study addressed was that some technology leaders lacked best practices to

minimize data security breaches for increased business performance.

Purpose Statement

The purpose of this qualitative multicase study was to explore best practices technology leaders use to minimize data security breaches for increased business performance. The specific population consisted of technology executives and technical staff at a bank in the Northcentral region of the United States, and a local government agency in the Southcentral region of the United States. The population was comprised of members of computer security incident response teams (CSIRT). Computer security incident response teams handle implementing, enforcing, reviewing, and responding to data security breaches (Wara & Singh, 2015). Data from this research might provide business leaders with best practice measures to protect consumers against identity theft and reduce consumers' costs stemming from security breaches.

Nature of the Study

I selected a qualitative research method for this study. Researchers use a qualitative research method to explore a problem, case, or group through interviews and observations of participants (Bansal & Corley, 2011). The qualitative method was appropriate for this study because I utilized a multicase study design and interviewed participants. Quantitative research methodology is appropriate when examining the relationships between variables and the validation or invalidation of hypotheses (Denzin, 2012). Because I did not test a hypothesis, the quantitative approach was not appropriate for this study. Researchers use the mixed-methods approach when combining the

participants' experiences and empirical data to determine the relationship and differences between identified variables (Yin, 2013). Because I did not examine relationships or differences among variables resulting from participant experiences and empirical data, the mixed-methods methodology was likewise not appropriate for this study.

I chose a multicase study design. Case study researchers investigate a phenomenon in depth within a specific context to address a research question (Yin, 2013). The multicase study design was appropriate because the objective of this study was an in-depth investigation of security best practices within an organization. Researchers utilize grounded theory designs to develop a theory relating to a social process or action (Manuj & Pohlen, 2012). A grounded theory design was not appropriate for this study because I did not seek to develop a theory. An ethnographic design is appropriate when researchers seek to understand cultural groups through observation and interviews (Petty, Thomson, & Stew, 2012). An ethnographic design was not appropriate for this study because I did not observe group cultures. In a phenomenological design, the researcher seeks to explore lived experiences (Hou, Ko, & Shu, 2013). I did not explore lived experiences in this study. A narrative design is suitable when a researcher is exploring participants' reminiscence of life experiences of an event (Petty et al., 2012). Thus, a narrative design was not appropriate for this study because participants' life experiences were not the focus of this research.

Research Question

Data obtained from this study might provide business and technology leaders with

best practices to minimize the impact of data security breaches. The following research question guided this study: What best practices do technology leaders use to minimize data security breaches for increased business performance?

Interview Questions

1. How long have you been involved in the design or implementation of security policies and incident response strategies?
2. What has been your experience dealing with data security challenges?
3. What are some of the challenges when responding to data security breaches?
4. What is the value of incident response strategies for your organization?
5. Why do some technology executives lack the skills needed to minimize data security breaches?
6. What are the management skills needed by technology executives to assist in minimizing a data breach?
7. What are the technical skillsets technology executives need to improve data security prevention within corporations?
8. How can technology executives champion best practice data security policies within corporations?
9. What are some recommendations that may assist leaders in implementing proactive data security measures at organizations?
10. What are some recommendations that might assist a firm to improve incident response after a data security breach?

11. What additional information can you add that would be valuable to the study?

Conceptual Framework

I utilized systems theory for the conceptual framework of this study. In the 1940s, von Bertalanffy introduced systems theory, noting open systems and systems thinking as the fundamentals of the general systems theory (von Bertalanffy, 1968). Researchers von Bertalanffy, Juarrero, and Rubino (2008), expanded on Bertalanffy's work by stating that systems are inputs and outputs working together to achieve objectives of the organism. Furthermore, von Bertalanffy et al. (2008) indicated that *living systems* are open hierarchical systems at the state of equilibrium.

The basis of systems theory is the evolution of complex systems, as well as the interdependence of organisms (systems) and components (Moeller & Valentinov, 2012; von Bertalanffy et al., 2008). The core component of systems theory is the actual system (Hammond, 2010). Ducq, Chen, and Doumeingts (2012) have noted that a system represents a set of elements with attributes and relations with each other, while Hammond (2010) has indicated that a system is *complete* when all the components are working appropriately.

Businesses are complex systems that consist of a diverse array of components such as business units, functions, and activities (Pushkarskaya & Marshall, 2010). The interaction of business components should result in the achievement of organizational objectives. Information security is a critical business component (Sehgal et al., 2011). Therefore, leaders should ensure that security and business objectives align. According to

Mitleton-Kelly (2011), in a complex system, organizational components work together to ensure proper functionality of business units and processes. The multidimensional nature of businesses includes the social, cultural, physical, economic, technical, and political dimensions that influence each other to foster organizational integration (Mitleton-Kelly, 2011).

Understanding how organizations interdepend in a complex and systemic fashion could drive creativity and evolutionary changes for information security enhancement. Systems theory provided me a basis for exploring data security components within organizations such as security policies and procedures, objective organizational alignment, and employee awareness. Following systems theory by von Bertalanffy, (1968), Coole and Brooks (2014) noted the breakdown of security mitigations occur when security components do not function as a system. Exploring the expertise used to minimize data security breaches for business performance might contribute to reducing the gap in business practice between executive leadership's balance of data security and organizational goals. Systems theory formed the basis for the interview questions in this study.

Operational Definitions

Data security: Data security is the protection of information at rest and in transit from unauthorized access, disclosure, and/or modified intentionally or unintentionally (Saidani, Shibani, & Alawadi, 2013).

Data security process: A data security process defines the guidelines and

procedure to ensure data safety (Saidani, Shibani, & Alawadi, 2013).

Information technology leaders: For the purpose of this study, information technology leaders were the chief information officers, chief technology officers, chief information security officers, and/or information security managers of an organization (Ifinedo, 2012).

Information security: Information security is the safeguard and preservation of information and IT systems against vulnerabilities and threats from unauthorized access, use, disclosure, disruption, modification, or destruction in order to maintain availability, integrity, and confidentiality of a system (Fuchs, Pernul, & Sandhu, 2011).

Information security breach (information security incident): An information security breach (information security incident) is the misuse of information, unauthorized access to information and/or IT systems or the loss and theft of systems such as laptops and mobile devices that result in a compromise (Gordon, Loeb, & Zhou, 2011).

Information security threats: Information security threats are the situations that may result in an information system compromise to cause a negative impact on business operations, business assets, and individuals such as disclosure or unauthorized access of confidential information through social engineering and phishing (Ryan, Mazzuchi, Ryan, Cruz, & Cooke, 2012).

Risk: Risk is the measure of the extent to which an exceptional circumstance such as data security breach, business liability, or failure affects business operations. Risk management helps an organization effectively manage exposure to risk (Gupta, 2011).

Social engineering: Social engineering is the unauthorized access to restricted information or systems by deceiving an individual into revealing secure information (Posukhova & Zayats, 2014).

Technical staff: For the purpose of this research, technical staff included security engineers, network engineers, security architects, systems analysts, system administrators, and security administrators within an organization (Slaughter & Rahman, 2011).

Technology vulnerabilities: Technology vulnerabilities are the probability that an asset will be unable to resist the actions of a threat agent (Reddy, Samshabad, Prasanth, & Naik, 2012).

Assumptions, Limitations, and Delimitations

Assumptions

Lips-Wiersma and Mills (2014) noted that research assumptions are elements out of a researcher's control, but considered by the researcher as relevant to the study and true but unverified. Six assumptions were operative in my study. The first assumption was that technology departments at the banking firm and a local government agency dedicated resources towards the design, implementation, and enforcement of security controls to minimize data security breaches. Secondly, I assumed that some leaders lacked the best practices to minimize data breaches for increased business performance. The third assumption was that systems theory was an appropriate method for leaders to understand and incorporate technology operations to prevent data breaches. My fourth

assumption was that interviewing technology executives and technical staff was sufficient to answer the research question. Fifth, I assumed that participants would articulate their understanding of data security effectively and provide honest and truthful responses to the interview questions. Lastly, I assumed that patterns and themes emerging from the data analysis would assist in addressing the research question.

Limitations

Madsen (2013) has noted that limitations are the potential weakness that might limit the scope of the research findings. The first limitation of my research was its restriction to leaders' best practices. The second limitation was the study's targeted small sample size which might limit the ability to generalize the research findings (Pilnick & Swift 2011). Third, my use of a multicase study design might limit insights gained from the study findings, because the research scope is limited to the selected case studies.

Delimitations

According to Becker (2013), delimitations are the boundaries that guide the research study. The first delimitation of the study was the exploration of best practices leaders use to minimize data breaches and increase business performance based on a systems theory perspective. Next, the study was limited to a multicase study approach with technology executives and employees at a bank and a local government agency who were members of CSRITs. Lastly, the use of interviews and archival documents for data gathering excluded information I could gain through other qualitative or quantitative designs. Although organizations outside the selected industries might provide relevant

data to address the central question, the geographical criterion limited participation to CSRIT members of a bank in the Northcentral United States and a local government agency in the Southcentral United States.

Significance of the Study

Contribution to Business Practice

Organizations and individuals utilize technological innovations to improve lives, streamline business processes, and foster human-machine interaction. The integration of technology in business environments introduces new opportunities as well as challenges such as data privacy and security. Mellado and Rosado (2012) have noted that data security is a growing concern affecting all sectors of society including individuals, organizations, and governments. Given the heavy dependence on information systems by organizations, data have become a critical business asset (Mellado & Rosado, 2012). Because of this, technology leaders should possess the skills to protect organizational data effectively. The results of this study might assist business leaders in identifying employee skills for preventing security breaches and unauthorized access to corporate and consumer information.

The findings in this study could assist technology leaders in preventing and addressing the gaps in business practice regarding proactive data security measures and the mitigation of security breach damages. Studies have shown that data security breaches have a significant impact on organizational and financial performance (Chai et al., 2011), and that publicly traded organizations which have experienced a security

breach have seen negative impacts on stock prices (Zafar et al., 2012; Yayla & Hu, 2011). Data from this study might assist business and technology leaders to identify best practices to minimize data security breaches.

According to Chen, Kataria, and Krishnan (2011), businesses have increased information security investments on detection and preventions tools to reduce the effects of the data security breach on an organization's bottom-line. A rise in security investments demonstrates that leaders are aware of the adverse effects of security breaches and the need to reduce the risk of data compromise through investments (Huang, Behara, & Goo, 2014). Identifying skill sets leaders need may reduce the gaps between the investments in data breach detection and prevention, and the leadership best practices needed for mitigation and response.

Implications for Social Change

According to Jewkes and Yar (2011), the defense of digital privacy has become a force for creativity and social change as technology drives community engagement and fosters corporate innovations. Understanding the best practices technology leaders use to minimize data security breaches may assist leaders in limiting the impact on business performance and costs to consumers. Furthermore, given that the performance impact of security-related incidents to U.S. businesses is approximately $67.2 billion a year (Gordon et al., 2011), the findings of this study might assist technology leaders in reducing the cost of protecting confidential data for business sustainability. Finally, because approximately 81% of all data security incidents result from the theft of

consumer data (Lai, Li, & Hsieh, 2012), data from this study may provide companies with best practice security strategies and policy development tools to protect consumers against the costs of identity theft.

A Review of the Professional and Academic Literature

A literature review allows a researcher to present the viewpoints of other researchers and build on existing knowledge (Onwuegbuzie, Leech, & Collins, 2012). Using Google Scholar, ACM Digital Library, IEEE Xplore Digital Library, Science Direct, EBSCOhost, and ProQuest, I reviewed the extant literature relating to *information security*, *information security standards*, *information security investments*, *security awareness*, *security governance*, *information security laws and regulations*, *risk management*, *and systems theory*. I gathered information from 124 resources for the literature review, of which 110 (88.7%) were peer-reviewed articles and 106 (85.5%) of the total references were published between 2011 and 2015. In addition, the literature review included three seminal books (2.4%), seven government publications (5.6%), and four non-peer reviewed articles (3.2%).

My review of the literature established a scholarly foundation for the study and provided a critical analysis of the body of knowledge related to the research question. This literature review had two major categories: information security, and risk management. I subdivided the information security category into the following: (a) information security standards, (b) information security investments, (c) information security awareness, (d) information security governance, (f) information security laws

and regulations, and (g) information security breaches. My detailed review of the literature addressed the basis for the research question.

Information Security

Securing data is a key function of IT and business strategies. According to Ioannidis, Pym, and Williams (2012), information security is the practice of protecting technology systems and data from vulnerabilities, threats, and attacks. The vulnerabilities, threats, and attacks can be an intentional or unintentional exploitation of systems to compromise the availability, integrity, and confidentiality of information (Savola, 2014). Information security vulnerabilities and threats are present in technology innovations; therefore, an analysis of organizational risk should include information security parameters (Ioannidis, Pym, & Williams, 2012). Susanto et al. (2011) noted that information security assessments are essential in every business environment. Security professionals need to develop frameworks to guide the practical and theoretical security practices within the organization (Susanto et al., 2011). The frameworks above may assist business leaders in understanding best practice security models.

The dependence on technology innovations by businesses, governments, and individuals is on the rise (Susanto et al., 2012). Innovations such as the Internet have made business transactions such as banking, job searching, and shopping convenient for many individuals (Kim, Xu, & Gupta, 2011; Lawrence, 2011). Companies are using IT solutions to improve and streamline business processes (Susanto et al., 2012), and technology has become an enabler of organizational agility (Lu & Ramamurthy, 2011). In

recent years, technology has played a vital role in business process improvement through a coordinated effort between organizational interactions and system integration (Lu & Ramamurthy, 2011). Business leaders are seeking innovative solutions to identify new opportunities to reach future consumers and increase market shares.

Technological innovations such as computer systems, smartphones, and the Internet have introduced business opportunities and challenges. Companies in the global marketplace interconnect to streamline business communication. This interconnection has resulted in large data transactions, sharing, and storage of sensitive information on computer systems (Susanto et al., 2012). Businesses need to implement solutions and security measures to protect technology systems against information security threats. Data security has become an essential element of every business strategy (Susanto, Almunawar, & Tuan, 2011).

To protect information and data, security professionals should understand the fundamentals of information security. Computer security is the protection of IT systems, networks, and data from unauthorized access (Fuchs et al., 2011). Moreover, information security deals with the maintenance of confidentiality and data for purity (Ankita, 2012). According to Ankita (2012), data security is a critical and difficult task for businesses because no system is totally secure. Ankita further noted that information security always starts and ends with the secrecy, validity, and accessibility of information. Organizations collect, store, and manage sensitive business and consumer information that needs protection from hackers trying to exploit system vulnerabilities (Ankita, 2012).

For several decades, network security was the main layer of defense for computer systems against malicious software and hackers (Basem, Ghalwash, & Sadek, 2015). According to Dawson, Burrell, Rahim, and Brewster (2010), network security alone has proven to be an inadequate line of defense against security threats and vulnerabilities. Further, following systems theory (von Bertalanffy, 1968), Dawson et al. (2010) noted that application software vulnerabilities pose the most threat to businesses. Therefore, security professionals need to understand how to review software code to identify potential security vulnerabilities. Dawson et al. emphasized the need for software engineers to integrate information security controls in the software development process. Secure software development may help reduce information security vulnerabilities and the cost associated with a security compromise (Dawson et al., 2010). The focus of secure software development, integration, and implementation in the software development lifecycle (SDLC) is to protect the application and data.

The principal objective of information security is to maintain the availability, integrity, and confidentiality of information (Liao & Chueh, 2012). As information security continues to be a problem for organizations, offsetting data security against accessibility has proven to be a prevalent problem. According to Zissis and Lekkas (2012), businesses operate in a technology driven era where information saved on computers and network devices are vulnerable to security attacks. Liao and Chueh (2012) noted that data security breaches are a result of inefficient management of the availability, integrity, and confidentiality of information. The effective management of

information security can alleviate security vulnerabilities for both external and internal entities (Liao & Chueh, 2012). Maintaining the integrity and confidentiality of information, and ensuring data availability to users is a challenge for many organizations.

Information security breaches in recent years have reminded security experts and business leaders of the importance of effective information security strategies. According to Chan (2011), business leaders are now taking data security concerns more seriously than ever, given the effects of information security breaches on business and consumers. Computer viruses, Trojan horses, and worms have evolved, posing significant threats to individual and corporate computer systems (Sung & Su, 2013). After a security incident, information security experts always discover new security threats and vulnerabilities (Chan, 2011). Further, Chan noted that identifying and measuring the impact of information security threats is a concern for any researcher, security expert, and organizations involved in data protection.

Information Security Standards

Businesses keep confidential records of business transactions with consumers and vendors. Business data from sales activities, marketing campaigns, and customer relationships provide new opportunities for business intelligence (Hsinchun, Chiang, & Storey, 2012). Furthermore, Susanto et al. (2011) have noted that information is a key organizational asset. The accuracy, completeness, and availability of information for business leaders is necessary for decision-making processes and business strategy development (Susanto et al., 2011). In addition, the security of technology systems is

vital to the success of businesses; therefore, companies need to implement established industry best practices and standards to protect critical technology assets (Susanto et al., 2011).

Standardization, according to Tsohou, Kokolakis, Lambrinoudakis, and Gritzalis (2010), provides best practice requirements which products and services must meet in the global marketplace. Setting standards also ensures conformity and provides a mechanism for accessing and measuring product and service criteria (Tsohou et al., 2010). Further, enterprise standards established within technology and business environments can provide a wider consensus for adoption (Lou, Andrechak, Riben, & Yong, 2011). System standards strengthen technology interoperability and establish a general agreement for functional/nonfunctional system and software requirements (Tsohou et al., 2010). Moreover, Tsohou et al. (2010) noted that information security standards are gaining acceptance and adoption, but awareness and compliance remain neglected.

Information security standards can be technology or management related (Tofan, 2011). Technology related security standards focus on the logical and physical security of IT systems and technology security specifications. On the other hand, management related standards serve to guide and ensure best practice security measures (Tofan, 2011). In 2005, the International Organization for Standardization (ISO) established the ISO/IEC 27001 standard which specified the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving security management systems and security governance (Alebrahim, Hatebur, Fassbender, Goeke,

& Côté, 2015). ISO 27001 provides security experts and business managers with a framework for information security management that aligns with IT objectives (Susanto et al., 2012).

In the security standard ISO 27001, risks, vulnerabilities, and threats to organizational strategies are the main objectives (Alebrahim et al., 2015). Information security in the ISO 27001 focuses on risk management, which allows experts to implement a flexible security management framework (Susanto et al., 2012). Information security standards such as the ISO27001, the Generally Accepted Information Security Principles (GAISP), the Information Security Forum (ISF), and the Standard of Good Practice for Information Security, guide organizations to develop effective security programs (Liao & Chueh, 2012). The goal of information security programs is to provide a framework for the development and implementation of IT security policies, procedures, and strategies (Susanto et al., 2011). Standards such as the ISO 27001 provide organizations with a blueprint for implementing effective security controls and policies.

Many organizations have implemented strict security controls and policies, however, these security measures may fail to mitigate security threats (Yang, Shieh, & Tzeng, 2013). For instance, the apparel and home fashions retailer, TJX, implemented security controls that failed to stop a data security breach and compromise of customer data at the firm (Goldberg, 2013). The data security breach at TJX affected approximately 45 to 100 million customers, with financial losses estimated at $0.5 to $1.5 billion (Goldberg, 2013). An evaluation of the security at TJX indicated the company

failed to configure network and firewalls to comply with the Payment Card Industry Data Security Standards (Kuhn, Ahuja, & Mueller, 2013). Furthermore, Kuhn et al. (2013) cited inadequate wireless network security, improper data storage, and a lack of data encryption, as key vulnerabilities leading to the data loss. Goldberg (2013) noted that security experts should not just rely on security policies and procedure, rather include consistent maintenance and management of computer systems through security audits to ensure compliance. The data breach at TJX illustrated potential drawbacks of security policies and strategies.

Information security and data access are essential components of information security policies. When developing information security policies, experts take into consideration the storage, safeguards, availability, and accessibility of information. Hripcsak et al. (2013) illustrated the need to find a balance between information security and accessibility during the design and implementation of security procedures and policies. Managing the balance between data security and access is an ongoing challenge for organizations especially in healthcare (Hripcsak et al., 2013). Effective security management strategies are essential to the success of security policy implementations and initiatives (Enescu, Enescu, & Sperdea, 2011). Security frameworks and policies provide business leaders with knowledge regarding effective security controls.

Given the significance of data security to organizations, information security professionals report to a corporate chief executive (Enescu et al., 2011). In most industries, business executives pay close attention to security threats because technology

is a critical part of organizational continuity (Fenz, Ekelhart, & Neubauer, 2011). Executive involvement in security strategy development may ensure business leaders understand technology risks, data requirements and approve security investments.

Information Security Investments

Several organizations have heavily invested in information security tools to protect network infrastructures and IT systems (Chen et al., 2011). Even with an unlimited budget, no business can be completely secure; however, organizations need to understand the right amount of information security investment required before an attempt to initial security programs (Huang, Behara, & Goo, 2014). The return on investment (ROI) of information security is complex and difficult to determine. According to Flores, Sommestad, Holm, and Ekstedt (2011), assessing ROI on security investments before the investments are in place is always a challenge. Investing in information security applications is a significant investment, and the ROI is a leading concern for business executives. However, despite the increased investment in information security by organizations, the effectiveness of security controls is still largely unknown (Lo & Chen, 2012).

According to Shirtz and Elovici (2011), organizations have increased investments in information security tools to preserve the significance of IT assets. Shirtz and Elovici also noted that information security is a cat and mouse game between organizations, security experts, and computer hackers. Shirtz and Elovici proposed that IT professionals should think like a hacker to assist organizations in identifying in advance potential

remedies for dealing with undesired security threats. Thinking like a hacker may assist leaders in understanding the elements affecting and influencing information security assets to justify security investments.

Investments in modern IT infrastructures are essential to effective information security strategies (Ranjan et al., 2012). Ranjan et al. (2012) noted that security vulnerabilities such as cyber-attacks, identity theft, and financial frauds have highlighted the need for organizations to fund and implement secure IT infrastructures. Organizations are investing in intrusion prevention and detection systems, and identity management solutions to control access to information and systems (Courtney, 2011). Threats to information assets have required the development and implementation of effective information security strategies (Ranjan et al., 2012). Organizations take advantage of new technology innovations without understanding the full security risk (Ranjan et al., 2012).

In a global economy, there is a reliance on electronic information to conduct business transactions. According to Btoush et al. (2011), business leaders depend on the availability, confidentiality, and accuracy of information to make decisions, and for corporate governance and sustainability. The amount of electronic data collected, stored, processed, manipulated, and shared by organizations and governments means data security is no longer a matter of just physical security (Jawad et al., 2012). Data security involves the safeguard of data in transit and at rest. Therefore, the effective management of the availability, storage, and accessibility of information is essential to improve system security and privacy.

Attacks on business IT systems have steadily raised despite investments in information security appliances and software (Ryan et al., 2012). Information security is a challenge facing business and technology leaders (Hall, Sarkani, & Mazzuchi, 2011). Improving an executive's perspective on information security is essential to achieve business objectives and implementing sustainable security policies (Ghezal, 2015). Leaders should stay informed on business operations, especially where threats to business continuity exist. Because of the criticality of technology as a tool for competitive advantage, the security of IT assets has become less of a technology problem and more of a business problem (Susanto et al., 2011). Despite the increased number of data security breaches, Ryan et al. (2012) indicated that increased investments in information security provide greater protection and rigidity to security vulnerabilities. Security investments demonstrate the business executive's commitment to improving data security measures.

As organizations strive to minimize technology risk, security audits are critical to ensuring compliance and safeguard of sensitive information. According to Zhao and Zhao (2010), security audits improve accountability and form the backbone of the information security policy. Security audits incorporate areas such as user access levels, safe computing, and the appropriate behavior guidelines communicated to employees on a regular basis. A dilemma for organizations is dealing with information security breaches by employees. Teh, Ahmed, and D'Arcy (2015) noted that 94% of banks breaches were employee related. However, employee related breaches are typically difficult to proof; as a result, security awareness initiatives are critical to the success of security policies (Teh,

Ahmed, & D'Arcy, 2015).

Information Security Awareness

According to Mittal, Roy, and Saxena (2010), information security management is not limited to hardware and software. Mittal et al. noted that organizational security management requires a complete end-to-end solution of systems, policies, and expertise. Information has become a critical business asset, making the security of data assets a top priority for organizations. Therefore, organizations need to establish security measures to deal with both technical and nontechnical vulnerabilities and threats (Btoush et al., 2011). Nontechnical threats such as social engineering should serve as a focal point for security experts during awareness training, given that researchers and technology practitioners agree the lack of security awareness can result in system and data breaches (Mittal et al., 2010).

Analyzes of data security breaches have shown that humans play a major role in breach occurrences. Mittal et al. (2010) indicated that there is a strong relationship between human behavior and information security. Furthermore, Lacey (2010) stated that vulnerabilities such as design flaws, lack of data encryption, social engineering, and human behavior further undermine technology security systems. Organizational culture and human behavior also play a vital role in information security implementations. Lacey noted that end-user awareness programs and information security initiatives fail because of organizational culture and employee behavioral problems (Lacey, 2010). Lacey also claimed that organizations have to review problem areas, set intervention strategies, and

develop themes, education, and notifications to promote recommended policies for change initiatives such as information security to be effective. Security experts should take into consideration human interactions, along with individual and social behaviors when developing and implementing security policies (Lacey, 2010); following systems theory approach (von Bertalanffy, 1968).

According to Knapp and Ferrante (2012), security policies are ideal when the policy assists employees in understanding how an employee's behavior can affect an organization with respect to protecting information and computer systems. Information security policies should establish the foundation and expectations for employee behavior and serve as recommendations when confronted by situations indicated in the policy. Knapp and Ferrante further noted organizational policy development must encompass the same framework as government laws and regulations, which define acceptable and unacceptable behavior. Security awareness programs focus on communicating and enforcing security policies. Therefore, information security policies should include the availability, integrity, and confidentiality of information stored and transmitted between IT systems and the end-users (Knapp & Ferrante, 2012).

Sun, Ahluwalia, and Koong (2011) noted that organizations are facing security challenges because of the large amounts of data stored on Internet-connected devices. Therefore, the security of data depends on user attitudes towards different security measures (Sun et al., 2011). Businesses have found a way to protect critical information to gain a competitive advantage in the marketplace. However, the effectiveness of

information security policies and procedures largely depends on the successful implementation of security solutions and end-user awareness initiatives (Kruger, Drevin, & Steyn, 2010). The human factor and behavior are critical to the success of information security implementations (Kruger et al., 2010).

A company's ability to manage and mitigate security risks, according to Harnesk and Lindström (2011), is a crucial aspect of information security. Harnesk and Lindström focused on the understanding of security behaviors using the concept of discipline and agility by developing a security behavior topology to identify behavioral interpretations of security enactment. Furthermore, Harnesk and Lindström noted that discipline and agility shape the different types of security behavior within an organization. Understanding organizational culture and employee behavior can assist security managers to recognize how different security behaviors affect the outcome of inscribed security procedures (Harnesk & Lindström, 2011).

Data security breaches through intentional, malicious acts, espionage, and sabotage by insiders/employees occur on a daily basis (Posey, Bennett, & Roberts, 2011). Posey, Bennett, and Roberts (2011) noted that organizations do not want to report security breaches, employee sabotage, and espionage because the breaches have a negative impact on the organization. Continuous monitoring and vigilance by security experts is essential in minimizing intentional data security breaches. Posey et al. indicated the need for regular evaluation of internal information security controls as the best practice to reduce internal security threats. Security experts implementing and facilitating

security controls require knowledge of security best practices.

Organizations have developed policies and procedures to protect information assets from security risk and vulnerabilities. Security policies and procedures assist organizations in securing digital assets; however, without widespread acceptance, management involvement, and consequences, security policies are useless (Hu, Dinev, Hart, & Cooke, 2012). Hu, Dinev, Hart, and Cooke (2012) noted that employees remain the weakest link in corporate defenses and information security. Employees who do not obey or comply with information security policies pose a serious threat to an organization (Puhakainen & Siponen, 2010). Mandating employee compliance with security policies is a constant challenge; however, monitoring, auditing, and enforcing security policies may force compliance and reduce internal threats (D'Arcy & Greene, 2014).

Employees play a vital role in ensuring the success of information security strategies, policies, and procedures within organizations (Hagen, Albrechtsen, & Johnsen, 2011). According to Puhakainen and Siponen (2010), when employees understand security vulnerabilities and the impact and severity of security threats to an organization, employees tend to be more compliant with security policies. The need for employee compliance is critical, especially in heavily regulated publicly trading organizations, educational institutions, healthcare settings, government agencies, and the banking industries. Compliance by employees can provide organizations with confidence to focus on mitigating external threats. Puhakainen and Siponen also noted that organizations should establish security plans aimed at encouraging managers to present employees with

real-time recovery practice and the potential impact of security threats.

Organizations are constantly developing creative strategies to protect information assets from both internal and external threats and vulnerabilities. Willison and Warkentin (2013) indicated that organizations may forget about internal security threats when developing security policies and implementing security solutions. Insider threats are becoming a serious security concern and demand attention from security professionals when developing security policies (Willison & Warkentin, 2013). Wolf, Haworth, and Pietron (2011) indicated that end-user awareness programs play a role in mitigating security threats. An evaluation of security awareness initiatives within U.S. federal law enforcement agencies uncovered a relationship between security and end-user behavior (Wolf et al., 2011). According to Wolf et al., for security awareness programs to be effective, everyone must know and obey security policies.

Hu, Xu, Dinev, and Ling (2011) indicated that the compromise of IT systems by hackers is no longer for bragging rights, but financial profit. Hacking is now a profitable endeavor perpetrated by underground entities such as hacktivist groups. Many organizations have developed and implemented security policies, systems, and procedures to mitigate security vulnerabilities. Nevertheless, the effectiveness of security policies depends on employee awareness and the security expertise of the implementer (Hu et al., 2011). Furthermore, Hu et al. noted that the role of humans in information security is critical to the success of security implementations, and any deterrence is not an effective information security strategy.

Given the intrusion of technology in daily business transactions and activities, along with increasing threats to information assets, businesses need security measures, such as user awareness initiatives to help them protect IT assets. According to Kruger et al. (2010), organizations also need to focus on managerial information security awareness and corporate leadership actions toward information security. Effective information security awareness by business managers assists in the process of corporate efficiency to improve business and technology performance (Kruger et al., 2010). Furthermore, Kruger et al. noted that security awareness initiatives influence managerial actions and the subsequent security performance of organizations after a breach. Technology leaders should acquire security awareness skills to assist in mitigating breaches resulting from vulnerable employees.

Information Security Governance

In a hyper-connected economic environment, businesses are frequently under attack by hackers, viruses, Trojan horses, spyware, and other cyber threats (Sharma, 2012). Protecting networks and computer systems are a vital element of organizational success given the rise of cyber crimes (Sharma, 2012). Organizational structure and management actions are a critical part of the organizational success (Khaleghi, Alavi, & Alimiri, 2013). Technology governance sets the strategic directions of information security within an organization. Ali and Green (2012) noted that IT governance provides security experts an implementation framework. According to Whitman and Mattord (2013), the effectiveness of information security governance (ISG) is accessible by

examining an organization's belief, behaviors, capabilities, and actions. Moreover, security governance provides business leaders with data on security implementation, policies, and the processes for safeguarding information assets (Whitman & Mattord, 2013).

Yaokumah (2014) noted that security governance is a challenge for business leaders, as ISG involves adequate risk management, reporting, and accountability. ISG is an essential component of IT governance and as a result, information security has become an integral part of organizational management (Yaokumah, 2014). The establishment of ISG programs begins with risk identification and assessment, also to business and technology risk management (Yaokumah, 2014). Understanding security risks may ensure an ISG team can properly implement ISG initiatives.

Effective ISG teams provide firms with the ability to manage information security at the executive level and bring security to the attention of the board of directors and CEO's (Whitman & Mattord, 2013). Further, Whitman and Mattord (2013) noted that ISG teams assist information security leaders with planning processes to ensure inclusion of desired goals and objectives for organizational security policies. Nevertheless, to maintain an ISG program, security experts, and managers need to be able to quantify the ROI of the program to the organization (Whitman & Mattord, 2013). Given the critical nature of information security, ISG provides organizational leaders with a framework to assist in data breach mitigation.

As organizations work on developing IT strategies to mitigate information

security risk, leaders must ensure effective management of these strategies. Business and technology strategies are effective when the implementation and management are effective (Abbas, Magnusson, Yngstrom, & Hemani, 2011). According to Abbas et al. (2011), a dynamic change of security requirements, externalities caused by a security system, and an obsolete evaluation of security within an organization are security concerns resulting from security management inefficiencies. Security managers should possess the expertise to mitigate and respond to data security threats.

According to Nicollet (2012), advances in targeted security threats have been increasing over the last decade. The increased number of mobile and portal devices means businesses must develop ISG programs that can adapt to evolving threats. Nicollet indicated that in 2015, approximately 80% of all security compromises would exploit well-known security flaws and vulnerabilities detectable by a security monitoring system. Furthermore, Nicollet advocated the need for security experts to work hand-in-hand with technology innovators and professionals to assess security vulnerabilities. This collaboration ensures security programs are up-to-date with information on known and unknown threats.

As technology leaders work on developing ISG programs, incorporation of best practices and integration with business goals are essential. According to Mishra (2015), security governance defines the direction of information security policies and practices with an organization. Business and government leaders are realizing that effective ISG requires securing the availability, integrity, and confidentiality of information assets.

Therefore, investments in security governance can ensure effective security controls and operations (Mishra, 2015). Business managers need to evaluate the positive and negative effects of technology on an organization as a measure of normal business activities (Mishra, 2015). The Internet, for example, has facilitated the development of vast communication networks linking businesses and individuals, as well as introducing new security threats. As a result, governments have ratified information security laws and regulations to increase accountability and protect consumers and proprietary data (Lewis, Campbell, & Baskin, 2015). The number of security breaches in the United States has increased each year, despite additional efforts to safeguard consumer data from compromise. The U.S. government and others entities around the world are focusing on protecting computer networks and data through laws, regulations, and industry technology initiatives.

Information Security Laws and Regulations

The integration of technology in a global economy has proven to be beneficial and sometimes disastrous for businesses. In a global environment, decisions, policies, and regulations by governments such as the United States and the European Union affect the global market (Moshirian, 2011). The standards, rules, and regulations set by developed nations have become the framework for underdeveloped nations. Compliance with government regulations by businesses is an essential element of the security implementation process (Moshirian, 2011).

Maintaining compliance with industry and government security regulations such

as the NIST Special Publication 800-144 is a challenge for most companies (Caytiles & Lee, 2012). U.S. corporations have invested in internal and external security controls, and audit processes to ensure compliance with government and industry regulations (Saini, Rao, & Panda, 2012). U.S. regulations include the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act (FERPA), and the Payment Card Industry Data Security Standard (Family Educational Rights and Privacy Act Amendments of 2008; Gramm-Leach-Bliley Act 1999; Health Insurance Portability and Accountability Act of 1996; PCI Security Standards Council, 2015; Sarbanes-Oxley Act of 2002). The U.S. federal government enacted regulatory frameworks such as HIPAA, GLBA, and SOX to improve the availability, integrity, and confidentiality of information (Mohammed & Mariani, 2014).

After the collapse of Enron and WorldCom, the U.S. Congress ruled that business executives be accountable for all business decisions and actions (Yallapragada, Roe, & Toma, 2012). In 2002, the U.S. Congress passed SOX to protect shareholders and consumers by holding executives accountable by law and increase corporate transparency (Yallapragada et al., 2012). The SOX legislation introduced new data compliance requirements, including organizational implementation of information security measures to improve internal security controls and hold chief financial officers responsible for financial decisions (Wallace, Lin, & Cefaratti, 2011). Continual SOX compliance is a serious challenge for corporate executives and information security experts. However,

Wallace et al. (2011) noted that effective security management strategies could assist businesses with uninterrupted SOX compliance.

For decades, the United Kingdom, like other developed nations, has enacted regulations aimed at dealing with the growing issues of data loss and privacy (Mansell & Steinmueller, 2013). In 2010, the U.K. House of Commons passed the Digital Economy Act (DEA) with the goal to protect individual privacy, copyright infringement, and data loss (Mansell & Steinmueller, 2013); U.K. The National Archives, 2010). Laws and regulations such as DEA provide business and individual's protection.

Many states in the United States have passed data security breach and notification laws. The State of California led the legal battle with one of the toughest notification laws (Romanosky, Telang, & Acquisti, 2011). In 2002, the California state legislature passed the California Security Breach Information Act (SB-1386), which required businesses storing personal information to notify individuals in the event of an information security compromise (Legislative Counsel of California, 2002). The California Security Breach Information Act stated that information such as first and last names, social security numbers, driver's license numbers, bank account numbers, and credit/debit card numbers are personal and confidential information (Legislative Counsel of California, 2002). According to Romanosky, Telang, and Acquisti (2011) California's legislative body considered SB.1386 as a possible remedy for identity theft. The bill empowered consumers seeking damages from businesses in the event of a breach of consumers' personal information, as well as an early notification process to allow consumers to

cancel accounts, and notify the credit bureau to prevent potential fraud. The notification law in California required businesses to implement notification triggers, notification mechanisms, and strategies to enforce, respond, and mitigate security threats.

The globalization of industries has introduced new businesses opportunities and challenges. Transporting, sharing, storing, and transmitting sensitive information, such as banking data, between countries has introduced new concerns for multinational corporations (Popov & Udell, 2012). Terrorism and espionage have resulted in increased security at border entry points (Peres & Pielmus, 2011). The U.S. Customs and Border Patrol agents now have authority over devices and goods entering the United States (Peres & Pielmus, 2011). In addition, border patrol agents have the authority to search and seize any electronic device entering or exiting the United States. This authority given to border agents could be detrimental to employees traveling with devices containing sensitive business information. Organizations requiring employees to travel with laptops containing confidential data should develop policies and implement solutions like encryption to protect the data (Nawafleh, Hasan, Nawafleh, & Fakhouri, 2013). Data has become a critical business asset used to achieve organizational success.

Businesses are required to implement security policies in response to new threats and comply with government and industry regulations (Johnson, Lincke, Imhof, & Lim, 2014). However, document leaks and dumps on sites such as WikiLeaks demonstrate the need for strict government and industry regulations to safeguard state and corporate secrets for homeland security (Hood, 2011). Compliance with industry regulations and

government laws forces organizations to invest in digital information security. Many businesses are spending substantial amounts of resources to ensure compliance. Nevertheless, according to Renaud (2011), there is limited to no evidence indicating data security regulations assist organizations in mitigating information security breaches or data losses.

Information Security Breaches

The dependence on technology innovations by corporations and individuals for critical transactions introduces new security risks. Kesh and Raghupathi (2013) noted that these risks are costly. With approximately 4000 data breaches and over 621 million records compromised between January 1, 2005, through December 31, 2013, security breaches have become a serious problem for organizations (Holtfreter & Harrington, 2014). U.S. businesses spend on average $204 per data record breached (Shackelford, 2012). The average costs of data security breaches increased from $6.65 million in 2008 to $6.75 million in 2009 (Hart et al., 2011). The 2011 Computer Security Institute (CSI) annual security survey confirmed an ongoing rise in the cost of responding to data security breaches. About 22% of security executives surveyed by the CSI and Federal Bureau of Investigation (FBI) indicated their organization had experienced some form of a security breach within the year (Zhao, Xue, & Whinston, 2013). Based on the CSI/FBI survey, exploring the best practices leaders use to minimize data security breaches is a business necessity.

A significant volume of data transactions occurs on the Internet (Einav, Levin,

Popov, & Sundaresan, 2014). However, companies have revealed a compromise of an estimated 543 million records because of over 2,800 data breaches with an associated $13.3 billion in financial loss from identity theft (Romanosky, Hoffman, & Acquisti, 2014). Research by Zafar et al., (2015) also indicated that security incidents result in both financial and reputational impact on the breached organization. Businesses face continual data security threats from unauthorized disclosure of sensitive consumer information (Romanosky et al., 2014).

According to Gatzlaff and McCullough (2012), unidentified data security breaches, publicly announced breaches, government regulations, and security standards have made protecting IT assets a priority. The establishment of security regulations such as SOX, GLBA, PCI DSS, and HIPAA occurred because of data security concerns and increased security threats such as identity theft (Gatzlaff & McCullough, 2012). Lai, Li, and Hsieh (2012) noted a 9.9 million increase in identity theft costing consumers $48 billion. The disconnection that exists between established and accepted security frameworks and the variables of undiscovered security threats could describe the rise in data security breaches.

The increasing number of information security breaches limits the ability of businesses to provide a satisfactory level of service to customers. Chlotia and Ncube (2011) noted that most data security breaches result from stolen data and exposed computer systems. The effects of information security breaches go beyond financial impacts to the breached organization. According to Chlotia and Ncube, information

security breaches affect both the breached firms and consumers. Moreover, a data security breach affects a firm's market share and reputation as well as consumer confidence (Chlotia & Ncube, 2011). Business leaders need to consider the impact on organizational reputation and to brand after a security compromise. As such, consumers need to exercise caution when providing sensitive information online. The monetary losses because of information security breaches can cause disruption to business communications and continuity (Figg & Kam, 2011).

Chai et al. (2011) noted that information security breaches could result in a significant financial impact on organizational performance. As such, business leaders need to understand the extent to which breaches can affect their organization. Business leaders must define information security guidelines to protect a firm's technology assets against internal and external threats (Figg & Kam, 2011). The guidelines should include an impact analysis of a data security breach to understand the effects of the availability, integrity, and confidentiality (AIC) of sensitive information, given that AIC is the foundation of information security. Moreover, Yayla and Hu (2011) indicated that data security breaches pose a long-term impact on organizational performance. However, the impact of data security breaches may depend on the organization's IT and business integration (Chai et al., 2011). According to Chai et al., security breaches on data confidentiality and availability have a long-term impact on businesses performance about physical breaches. For example, denial of service security attacks, have a greater effect on organizations than unauthorized access data breaches (Yayla & Hu, 2011).

A negative reaction by investors after security breaches illustrates an impact on organizational performance. Yayla and Hu (2011) noted a significant change in market valuation after a data security breach as investors react to the announcement of the incident. Information security breaches, technology risk, and vulnerabilities have made information security a serious concern for business and IT executives (Yayla & Hu, 2011). Businesses need to find a balance between the possibilities of a data breach and security investments (Flores et al., 2011). The significance of information security to a firm's strategy means leaders should view security breaches as a threat to organizational success (Fleming & Faye, 2013). The impact of data security breaches depends on the type of attached, organizational factors such as size, and the industry of the breached organization (Das, Mukhopadhyay, & Anand, 2012).

There has been agreement among researchers and security experts regarding the cost of data breaches (Gordon et al., 2011). The expense of mitigating and responding to security breaches is a critical component of IT budgets. The mitigation of security vulnerabilities and threats require investments in security technology and tools, as wells as expertise. Therefore, business and technology leaders need to work closely to provide the necessary resources to protect computer systems, as well as the organization from the implicit costs of potential legal challenges due to data loss or unauthorized access (Gordon et al., 2011). Nevertheless, the financial losses because of a data breach are difficult to assess because businesses are reluctant to disclose security breaches (Saini et al., 2012). The increase in business costs resulting from a data security breach within the

last 4 years is illustrated in Figure 1.

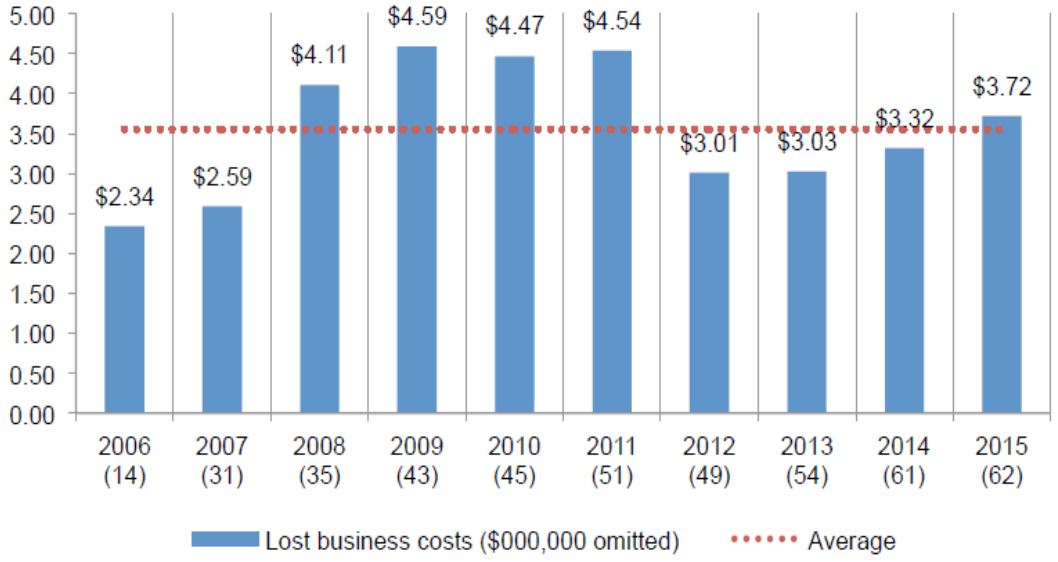


Figure 1. Average business costs over 10 years. Business costs include the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. As shown, business costs increased over the past two years with the current year's cost of $3.72 million represents an increase from $3.32 million. Retrieved from "2015 Cost of Data Breach Study: United States," by IBM & Ponemon Institute, 2015, *Ponemon Institute Research Report*, p. 13. Copyright 2015 by Ponemon Institute. Adapted with permission (Appendix A).

Information security is a complex and essential element for competitive advantage for organizations. The ability to detect and prevent security threats and vulnerabilities alone may provide a competitive edge (Abawajy, 2014). The effective mitigation of security incidents might assist in reducing the overall cost of security. An effective understanding of security attacks provides security experts with best practice measures to protect currents and future systems (Susanto et al., 2011).

There has been a rise in identity theft on the Internet. Developed nations such as the United States face increased security challenges due to the amount of individual

electronic data available on Internet-enabled devices (Hsinchun et al., 2012). Identity theft is becoming a complicated issue for consumers and businesses. According to Kapoor, Pandya, and Sherif (2011), advancements technologies such as e-commerce and social media have resulted in the loss of privacy. Kapoor et al. also noted that the consequence of online transactions such as credit card processing, stock purchasing, and banking data has increased the likelihood of data breaches. These breaches could result in businesses losing billions of dollars in revenues, as well as customers losing confidence in e-commerce (Kapoor et al., 2011).

Given the increased dependence on technology and the number of information security breaches, organizations need to implement strategies to respond to security incidents. According to Ben-Asher and Gonzalez (2015), the protection of enterprise systems from vulnerabilities is the responsibility of security professionals. To develop an effective security response plan, analysts need to detect and analyze security breaches to identify network threats and vulnerabilities that might lead to data compromise (Ben-Asher & Gonzalez, 2015). Moreover, Rahman and Choo (2015) indicated that security incident responses should include containment, eradication, and recovery of the breached data and system.

Risk Management

In a competitive global economy, business leaders focus on sustainable business decisions, as well as a risk management oversight (Ballou, Dan, & Stoel, 2011). Information security risk management provides business leaders with the ability to ensure

business and system risk are part of an organizational strategy (Fenz et al., 2011). Moreover, executive involvement ensures there is managerial support and investment in information security initiatives. Ballou et al. (2011) noted that organizations have not defined the types of risk a business can take. However, a survey of executives illustrated a shift towards an alignment of business risk across departments to ensure effective risk analysis and risk management. Furthermore, Ballou et al. noted business leaders need constant updates and information on emerging risks and risk response management strategies.

Studies have shown that 9 out of 10 businesses fail within the first two years of operation (Patil, Grantham, & Steele, 2012). Starting a new business or launching a new product is a risky proposition; however, how business leaders and innovators assess and manage risk are key factors to the success of the product or service (Patil et al., 2012). Moreover, Patil et al. (2012) noted that diversity and competition in the global marketplace make risk assessment a critical requirement for every business. Business leaders need to identify business mistakes that may lead to failure and develop strategies to avoid a crisis. Executives should take into account all types of business risk such as processes, people, external events, and systems to ensure proper risk management (Patil et al., 2012).

Risk management is a business strategy aimed at developing business environments for a limited probability of events that may cause damage to an organization's assets (Chitakornkijsil, 2010). According to Chitakornkijsil (2010), risk

management is the process through which an organization identifies business risks and losses to developing a strategy to discover, minimize, and respond to future risks. However, the risk is uncertain, and there are different methods for defining and identifying potential business losses. Identifying situations, where the loss is probable, is the objective of risk management. Chitakornkijsil also noted that risk management is complex and adds value to an organization and may promote competitive advantage. According to Zissis and Lekkas (2012), business managers and technology leaders need to understand business risk and information asset vulnerabilities.

Business leaders take risks with the introduction of new products, expansion of new markets, reorganization of executive management, and the acquisition of other firms to increase shareholder wealth (Dai, Maksimov, Gilbert, & Fernhaberd, 2014). However, organizational mismanagement, such as the collapses of Lehman Brothers Holdings and WorldCom, indicated the need for effective risk management within corporate governance (Calandro, 2011). Gendron, Brivot, and Guénin-Paracini (2015) noted that corporate boards and executives are concerned about and proactive towards organizational exposure to risks. High level of organizational risk means governance and strategies need to be flexible, iterative, and inclusionary as well as focus on risk mitigation, avoidance, and acceptance (Renn & Klinke, 2013).

According to Borison and Hamm (2010), an examination of the collapse of firms like Lehman Brothers can assist in evaluating a firm's risk management approach. Borison and Hamm contended that risk management failures at most businesses were

because of managers looking for risk in the wrong places. Many businesses rely on traditional risk management; the higher the risk a company takes, the greater the chances for failure. Borison and Hamm recommended that businesses move towards the Bayesian risk management approach to provide accurate and powerful results. The Bayesian perspective recognizes risk taking involves data analysis and individual judgment. This perspective combines both data and judgment to identify, assess, and manage risk (Borison & Hamm, 2010).

Business risk, like information security risk, is difficult to identify and manage. Avoidance, acceptance, and mitigation of information security risk involve collaboration between all stakeholders within an organization. Executive management, employees, and vendors need to understand the impact of a security risk to a business. The changing business landscape and increased use of technology make identifying every security risk difficult. According to Amancei (2011), efforts by organizations to mitigate information security threats through a risk management approach take into account the strategic value of information assets. An effective management security plan requires both business and technology leaders to accept the possibility of the unknown. In addition, security experts need to have effective risk management skills to ensure proper identification of business risk posed by technological innovations (Amancei, 2011).

Organizations face many types of security threats and vulnerabilities. Information security risk management has become an integral part of firms' business strategies (Bojanc & Jerman-Blažič, 2013). Bojanc and Jerman-Blažič (2013) stated that

organizational security risks include the inadvertent disclosure of sensitive and proprietary business information by employees. Moreover, managing the risks associated with inadvertent disclosure of sensitive information is a concern for organizations, especially with the prevalence of social media (Duncan-Daston, Hunter-Sloan, & Fullmer, 2013).

Systems Theory

Protecting information assets has become an integral part of business and IT strategy (Knapp & Ferrante, 2012). As businesses, governments, and individuals' dependence on technology increases, security threats, vulnerabilities, and risk to confidential information also increase (Susanto et al., 2012). Organizations are allocating between 8% and 10% of their annual IT budgets on information security (Lesk, 2014). To ensure security investment and implementation effectiveness, an alignment must occur between business units and organizational processes.

The conceptual framework for this study is systems theory. Introduced by von Bertalanffy in the 1940s, systems theory relates to the concept of an organism as an open system with various components working together to complete a task (von Bertalanffy, 1968). A system has inputs and outputs working together to achieve the objectives of the system (von Bertalanffy, 1968). Furthermore, von Bertalanffy (1968) indicated that a system is a mechanistically oriented object evaluated solely in terms of mathematics, feedback, and technology. Von Bertalanffy utilized systems theory to demonstrate that living systems are open hierarchical systems aimed at achieving a state of equilibrium.

Hammond (2010) further elaborated on von Bertalanffy's systems theory as the foundation of the open-systems concept stating that all components of an organization must function properly to accomplish business objectives. As business leaders continue to take advantage of technology, they need to ensure organizational components are working together (Hammond, 2010). Further, Mangal (2013) utilized systems theory to predict whether new website features improved user efficiency or improved system functionality. Mangal stated that websites with dysfunctional components were less efficient and affected a user experience, and a cohesive integration of system components provides for an enjoyable experience. In relation to systems theory, the integration and collaboration of all information security elements within an organization is essential to minimize security threats effectively.

In contrast, the constructivist theory states that people construct meaning and knowledge from previous individual experiences (Enonbun, 2010). The constructivism theory assists researchers to create a subjective concept of objective reality with information linked to prior knowledge (Enonbun, 2010). Constructivism offers a new paradigm through which researcher and participants can use a large spectrum of information to construct reason. Research studies contain embedded philosophical worldviews, which are the fundamental beliefs and principles guiding the actions and decision of a researcher (Mostovicz, Kakabadse, & Kakabadse, 2011). A constructivists' worldview in qualitative research provides an in-depth understanding of participants' insights on a particular subject area (Enonbun, 2010).

Similarly, the complexity theory illustrates how entities interrelated in a complex and systemic fashion with the differences that drive creativity, evolution, and change (Cairney, 2012). According to Cairney (2012), the complexity theory presents a view of the world and organizations as components that are systemic and interconnected. In complexity theory, systems are diverse, connected, and open to the environment so systems can evolve (Cairney, 2012). Because businesses are complex systems, Mitleton-Kelly (2011) noted that multi-dimensional nature of complex systems influences how an organization functions.

In summary, as business leaders continue to find new ways to increase shareholder net worth, there is a need to identify best practices to manage business and technology risks effectively. Technology innovations such as the Internet are a driver of social change (Jewkes & Yar, 2011) and an opportunity for communities and businesses to reach new markets. Jewkes and Yar (2011) further noted that the Internet has had profound social and cultural impact in the fields of education, consumerism, political activism, and socialization. However, technology innovations have introduced new information security threats. Therefore, developing strategies and data policies taking into account security concerns may assist leaders in the development of confidential information safeguards on the Internet. Given the growing integration of technology and business processes (Susanto et al., 2011), leaders need to balance the operational necessity for confidentiality, integrity, and availability of data.

In addition, increasing numbers of security breaches cost businesses financially.

According to Ernst and Young (2013), 32% of U.S. companies spend more than $1 million on information security, and 80% indicated a rise in security threats. Gordon et al. (2011) noted increasing threats to data and the approximately $67.2 billion yearly costs for U.S. businesses. Thus, the efforts to minimize security breaches and the associated impact on organizational performance may require technology leaders to gain new skills.

Transition

Section 1 was an illustration of the security threats to IT systems and data. In this section, I emphasized the need for technology leaders to understand best practices for developing IT strategies and policies that address data security concerns. In addition, I included a discussion of the background of the problem, the problem and purpose statements, the nature of the study, assumptions, limitations, delimitations, the research question, conceptual framework, and a definition of terms and review of the literature. An outline of information security standards, investments, security awareness, and governance, information security laws and regulations, and breaches and risk management are in the literature review. Section 2 is an overview of the research project, which includes the purpose statement, my role as a researcher, participants, the research method and design, population and sampling, ethical research, data collection instrument and technique, the data organization technique, analysis, and the reliability and validity of the study. In Section 3, I include an overview of the study, presentation of findings, application to professional practice, implications social change, recommendations for action and future research, a reflection of my experiences conducting this study, and my

research conclusion.

Section 2: The Project

The objective of this study was to explore best practices technology leaders use to minimize data security breaches for increased business performance. In Section 2, I include detailed information on my methodology and research process. This section also contains the purpose statement, the role of the researcher, participants, research method and design, population, sampling, and data collection to include organization and analysis, reliability and validity.

Purpose Statement

The purpose of this qualitative multicase study was to explore best practices technology leaders use to minimize data security breaches for increased business performance. The specific population consisted of technology executives and technical staff at a bank in the Northcentral region of the United States, and a local government agency in the Southcentral region of the United States. The population was comprised of members of computer security incident response teams (CSIRT). Computer security incident response teams handle implementing, enforcing, reviewing, and responding to data security breaches (Wara & Singh, 2015). Data from this research might provide business leaders with best practice measures to protect consumers against identity theft and reduce consumers' costs stemming from security breaches.

Role of the Researcher

As the researcher, I served as the primary instrument for data collection. Pezalla, Pettigrew, and Miller-Day (2012) noted that the researcher is the instrument in qualitative

research interviews. As a technology architect, I possess knowledge in the areas of data security and incident response. However, I had no relationship with the participants. Conversely, as Vaccaro (2012) has indicated, a researcher's expertise in a subject area adds credibility with participants. I avoided bias by not asking leading questions during the interview session in keeping with Onwuegbuzie and Hwang's (2014) suggestion that researchers should refrain from asking leading questions to mitigate bias. I reviewed the Belmont Report, a summary of the ethical principles and guidelines for the protection of human subjects in research (U.S. Department of Health & Human Services, 1979). An understanding of the Belmont report ensures that a researcher respects participants, maximizes the benefits of the study design while minimizing risks, and selects research participants impartially (Fiske & Hauser, 2014). I completed the Protecting Human Research Participants training offered by the National Institutes of Health (NIH) Office of Extramural Research (Certification Number: 801339, Appendix B). Resnik, Miller, Kwok, Engel, and Sandler (2015) noted the NIH participant protection training assisted researchers in the informed consent process, in the protection of participants, and in dealing with ethical challenges in research.

My objective was to conduct the interviews in a manner that allowed the participants to express insights on data security within their organization and industry. Yin (2013) noted that a case study protocol guides a researcher to collect reliable data. Using interviews provided me a deeper understanding of the research topic (Bölte, 2014). My interview protocol (Appendix C) was a guide for the interview format. In my role as

the researcher, I used the interview protocol to ensure that I followed the same protocol with each participant. Utilizing this interview protocol added consistency and reliability to the qualitative research process (Foley & O'Conner, 2013).

Participants

Elo et al. (2014) have indicated that researchers must state the principles and criteria for selecting participants to enable other researchers' to assess the transferability of the research findings. A researcher uses participant selection criteria to establish credibility and to accurately identify and describe participants (Hanson, Balmer, & Giardino, 2011). Following the research criteria closely is essential to protect participants (Damianakis & Woodford, 2012).The participants in this study were two technology executives and five technical staff from each of the two cases (a bank in the Northcentral United States and a local government agency in the Southcentral United States) with experience in information security design and implementation. The participants were members of their respective organization's CSIRT teams which are responsible for implementing, enforcing, reviewing, and responding to security incidents within an organization (Wara & Singh, 2015). Participant requirement also included full-time employment for at least five years within the IT department of the targeted case study. The bank and local government agency for this multicase study had not reported any data security incidents within the past 5 years, per the inclusion criteria.

I located banking institutions in the Northcentral United States and local government agencies in the Southcentral United States via the LinkedIn online public

directory, cross-referencing with the Open Security Foundation's (OSF) DataLossDB online public database, to identify organizations with potential participatnt who met the criteria. The LinkedIn Directory is a searchable public repository of organizations by industry, size, and location (LinkedIn, 2013); while the OSF DataLossDB database contains information on organizations that have experienced a security breach (Garrison & Ncube, 2011; Open Security Foundation, 2014). Adebayo (2012) noted that DataLossDB contains records of reported data breaches and types that provide researchers with valuable information for security research and verification.

After Walden University's Institutional Research Board (IRB) approval, I sent potential participants an introduction letter (Appendix D) via LinkedIn mail service. The letter included a brief description of the study, along with a request to contact me directly via e-mail. Once I had gained acknowledgment of participants' willingness to participate in the study, I established a working relationship with them. Taking cue from Holloway and Wheeler's (2013) observation that the relationship between researcher and participants is one of mutual trust and respect, I established open communication with participants to build trust and confidence. Cachia and Millward (2011) noted that open communication with research participants provides security and confidentiality assurance, which leads to a trustful working environment. Building trust between research participants and the researcher is essential to establishing credibility with participants (Culver, Gilbert, & Sparkes, 2012).

Research Method and Design

Research Method

I chose a qualitative method for this study. Qualitative research is an exploratory method for understanding human behavior, phenomena, groups, or individuals (Hoe & Hoare, 2012; Yin, 2013). A qualitative researcher uses an interpretive approach to collect, analyze, and interpret research data (Yin, 2013). According to Yin (2013), a qualitative researcher explores the *how* and *why*, rather than the *what*, *when*, and *where*, in research. Furthermore, Cambra-Fierro and Wilson (2011) have noted that qualitative studies produce tangible results through a well-documented data collection and analysis process. Tracy (2012) indicated that qualitative research is a result of (a) a worthy topic, (b) rich rigor, (c) sincerity, (d) credibility, (e) resonance, (f) a significant contribution, (g) ethics, and (h) meaningful coherence. Thus, a qualitative method was appropriate for my study because I utilized a multicase study design and interviewed participants to explore data security best practices to address the research question.

Prior to initiating my research, I considered two other methodologies: quantitative and mixed-methods. Quantitative researchers examine relationships between variables and test hypotheses (Denzin, 2012). The success of quantitative research depends on the analysis of statistical data and the extent to which the findings are generalizable (Allwood, 2012). Goertz and Mahoney (2013) indicated that probability and statistics are the fundamental components of quantitative research. Because I did not test hypotheses and did not seek statistical data, a quantitative method was not appropriate for my study.

In the mixed-methods approach, a researcher seeks to combine, congregate, enhance, and illustrate research results using both qualitative and quantitative methods (Denzin, 2012; Muskat, Blackman, & Muskat, 2012). Venkatesh, Brown, and Bala (2013) have noted that mixed methods researchers design, build, and test theories, as well as complete inductive and deductive analysis within studies utilizing a central research question and hypotheses. Mixed-methods provide researchers the ability to combine participants' experiences and empirical data to determine the relationships among specific variables (Yin, 2013). In this study, I focused exclusively on participants' insights. Therefore, examining a combination of experiences, hypotheses, and relationships among variables was not appropriate.

Research Design

Grounded theory, phenomenology, ethnography, narrative, and case study are qualitative designs (Petty et al., 2012); that each design has strengths and limitations. According to Yin (2013), a rigorous research design is essential to guide a researcher throughout a study. For this study, I chose a multicase study design. Wynn and Williams (2012) noted that case study researchers explore, describe, and depict a setting, an individual, or a situation. Yin (2013) indicated that in a case study, a researcher illustrates the viewpoints of participants utilizing multiple data sources to determine how participants make decisions and gain knowledge about an event. A multicase study design was appropriate for this study since I utilized multiple sources of data to explore the best practices.

A researcher uses a grounded theory design for an inductive development of theories to evaluate a social process or action (Manuj & Pohlen, 2012). Researchers utilizing a grounded theory design recognize that establishing a theory guides the research questions, data analysis, and understanding of results (Berge, Loth, Hanson, Croll, & Neumark-Sztainer, 2012). Grounded theory researchers develop new theories based on first-hand data collected in the field (Dunne, 2011). Since, I was not developing a theory, a grounded theory design was not appropriate for this study.

Researchers utilize a phenomenological design to explore experiences based on the meaning participants associate with a phenomenon (Hou, Ko, & Shu, 2013). The objective of phenomenological studies is to describe participants lived experiences (Roberts, 2013), and a researcher uses a phenomenological design to depict structures of experiences in order to reach a more profound understanding of a phenomenon (Cigdemoglu, Arslan, & Akay, 2011). A phenomenological design was not appropriate because I explored participants' security mitigation skills as opposed to lived experiences with the phenomenon.

Ethnographical researchers seek to understand cultural groups through observation and interviews (Petty et al., 2012). A researcher uses an ethnographic design to observe a cultural group for a prolonged period (Cruz & Higginbottom, 2013). Researchers utilize ethnography to explore participants' behavior in a natural rather than artificial setting to interpret and describe behaviors in the context of a culture (Williamson, Twelvetree, Thompson, & Beaver, 2012). An ethnographic design was not

appropriate for this study because I explored best practices as opposed to a culture.

A narrative researcher explores participants' recollection of life experiences on an event or a series of events (Petty et al., 2012). A researcher utilizes the narrative design when conducting a biographical study following the life of individuals (Tamboukou, 2011). Wattanasuwan (2012) noted that narrative study researchers explore how participants view themselves and their experience in an event. I did not select the narrative design for this study because participants' understanding of specific practices was the focus, rather than a reminiscence of an event.

Higginbottom, Rivers, and Story (2014) indicated that a researcher achieves data saturation when interviews with research participants do not yield new themes. According to Kwong et al. (2014), qualitative researchers should continue interviewing more participants until achieving data saturation. Bristowe et al. (2014) noted that qualitative researchers might cease interviewing additional participants when further interviews no longer provide new information on the research topic for data saturation. No new themes emerged (data saturation) after I conducted interviews with eight participants at the bank and seven participants at the government agency.

Population and Sampling

I utilized purposive sampling for this study. Sangestani and Khatiban (2013) noted that using purposive sampling allows the researcher to select participants deliberately based on unique individual characteristics regarding the subject matter under study. Furthermore, Sangestani and Khatiban indicated that purposive sampling is a

nonprobability sampling technique in which the researcher uses *best judgment* to select participants. Ishak and Bakar (2014) noted that purposive sampling is suitable for case study research. Smith, Colombi, and Wirthlin (2013) indicated that purposive sampling enables a researcher to identify the participants who will provide the data to answer the research question. Utilizing purposive sampling enabled me to select participants with an understanding of the research subject area.

According to Hanson, Balmer, and Giardino (2011), a sample size of 10 to 20 participants is adequate to confirm themes in qualitative research. In qualitative research, a researcher uses the sample size to assure the richness of the information, and the number of participants depends on the topic and availability of resources (O'Reilly & Parker, 2012). Orser, Elliott, and Leck (2011) noted that there is a point in qualitative research (data saturation) in which continuing data collection only serves to confirm emerging themes. Palinkas et al. (2013) noted that the goal of an appropriate sample is to provide a detailed and thorough analysis of a phenomenon through the selection of the appropriate cases or individual. Sampling two technology executives and five technical staff in each case was appropriate for this study and provided enough data to achieve data saturation.

Technology executives and technical staff are key stakeholders' in the design, implementation, and enforcement of data security policies, as well as recommend security investments (Naseri & Azmoon, 2012). Furthermore, technology executives and technical staff are responsible and accountable for the security of organization data (Wara

& Singh, 2015). I selected a bank as one of the cases because banks' executives face significant data security threats and an increased adoption of online and mobile banking technologies (Martins, Oliveira, & Popovič, 2014). The selection of a local government agency was because most government agencies now provide online services. The focus of online government services is streamlining communication, improving community engagement, and easing access to facilities (Sandoval-Almazan & Gil-Garcia, 2012).

Ethical Research

Upon IRB approval (08-01-14-0084492), I selected the targeted organization cases and invited potential participants to participate in the study. I e-mailed an informed consent form (Appendix E) to volunteering participants. The informed consent form detailed (a) the study purpose, (b) participation criteria, (c) my role as the researcher, (d) withdrawal process, (e) the disclosure of incentives, (f) data safeguard, and (g) publication intent of the findings. Nishimura et al. (2013) noted that informed consent is a critical component of every research study. I also informed participants that participation in the study was voluntary, and participants had the right to withdraw from the study at any time prior to data analysis without cause by notifying me via e-mail.

Chiumento, Khan, Rahman, and Frith (2015) indicated that the informed consent process should protect and respect the rights of participants to ensure the study follows ethical standards. I followed the Walden University IRB ethical and legal requirements to ensure no harm or risks came to the participants associated with my research. Phelan and Kinsella (2013) indicated that how a researcher balances participant interaction in their

study is a critical element of ethical practices in qualitative research. Ensuring the safety, dignity, and voice of research participants is essential to conducting research ethically (Phelan & Kinsella, 2013). Research participants did not receive any incentives, payments, or rewards for participating in the study. Interviewees acknowledged that participation was voluntary.

Protecting the confidentiality of participants is critical in maintaining the integrity of a study (Damianakis & Woodford, 2012). Yin (2013) noted that using unique identifiers to represent participants protects the safety and professional status of participants. I assigned numbers and letters to each participant to assure participant confidentiality. The letter *P* and a number represented participants while the letters *X* and *Y* represented the two cases, the banking institution, and local government agency respectively. I maintain sole access to all data, on a password protected external drive and locked in a fireproof safe for 5 years to protect the confidentiality of participants.

Data Collection Instruments

As the researcher, I was the primary data collection instrument. Pezalla et al. (2012) noted that researchers are the primary data collection instruments in qualitative studies. As the primary data collection instrument, the researcher collects data in a natural setting, which assists in performing data analysis that is inductive and deductive to establish patterns and themes (Marshall & Rossman, 2010). Qualitative data collection involves building trust with participants, thus as the data collection instrument, a researcher must establish a strategy for developing credibility with participants (Culver et

al., 2012).

Qualitative researchers utilize semistructured interviews for data collection (Pezalla, Pettigrew, & Miller-Day, 2012). I utilized 11 open-ended questions (Appendix C) within the data collection instrument. Cachia and Millward (2011) noted that semistructured interviews are a valid data collection instrument. In addition, the interview questions were open-ended to allow for greater interaction with the participants. Yin (2011) noted that open-ended questions provide the ability for a case study researcher to collect insights on the specific case under study.

Yin (2013) noted that asking the same interview questions to different participants allows for a diverse range of answers and interaction. According to Qu and Dumay (2011), semistructured interview formats allow participants to provide an in-depth understanding of a research topic. Furthermore, Qu and Dumay noted that using semistructured interviews enable a flexible, accessible, and intelligible approach to data collection. Miner-Romanoff (2012) used semistructured interviews to describe an interpretative model for illustrating the effectiveness of qualitative studies. Utilizing semistructured interviews, researchers can disclose hidden facets of human and organizational behavior because participants respond in a way they can best answer the interview question (Qu & Dumay, 2011).

To ensure credibility and reliability, I posed the same interview questions to each participant, and I avoided bias by not asking leading questions. Hermanowicz (2013) noted that posing the same interview questions to participants helps in identifying

themes. Asking the same questions in a sequence allows for efficient data analysis and response comparison (Brédart, Marrel, Abetz-Webb, Lasch, & Acquadro, 2014). According to Onwuegbuzie and Hwang (2014), researchers should refrain from asking leading questions in research interviews in other to avoid any bias.

I also utilized available security and privacy policy statements from each of the institution's Internet website for methodological triangulation. The use of multiple data sources for methodological triangulation increases the credibility, reliability, and validity of the study (Yin, 2013). Snyder (2012) noted that the combination of participant interviews and archived data allows for a highly robust research study. Langen et al. (2014) indicated that archived date such as documents and recordings provide valuable qualitative research data. When a researcher analyzes data from archival documents together with interviews and observations, they reveal research themes (Lee et al., 2014).

According to Denzin (2012), utilizing multiple forms of data (methodological triangulation) provides a researcher with an in-depth understanding of the phenomenon in the study. Bekhet and Zauszniewski (2012) noted that the use of two data collection methods increases the comprehensive validity of data and enriched understanding of a case. Moreover, Wierenga, Engbers, van Empelen, Hildebrandt, and van Mechelen (2012) noted that methodological triangulation enables a researcher to probe for patterns in the data to develop an overall interpretation using multiple perspectives. The use of methodological triangulation increases confidence in the study findings as the researcher uses of multiple sources in mitigating research biases (Harrison, Banks, Pollack,

O'Boyle, & Short, 2014).

I applied member checking during the interview process as a method of achieving research validity and reducing bias. Houghton, Casey, Shaw, and Murphy (2013) noted that member checking assures rigor in case studies. I provided participants an e-mail summary of my interpretation of their interview responses to ensure I captured the participants' responses accurately. All participants confirmed my interpretation. Member checking provides an opportunity for a researcher to seek participants' verification of the accuracy of interview response (Culver et al., 2012). In addition, researchers utilize member checking as a quality control process to confirm, clarify, and augment data collected during qualitative research interviews (Harper & Cole, 2012).

Data Collection Technique

Data collection commenced following IRB approval. Participants who met the research criteria received an invitation (Appendix D) to participate in the study and contacted me via e-mail. Once a participant agreed to participate in the research, the participant received, reviewed and provided consent to participate in the study. The consent form (Appendix E) detailed the withdrawal process, the disclosure of incentives, and data safeguard. When I received consent via e-mail, I requested a convenient date and time for a telephone interview. All participants received a copy of the interview questions (Appendix C) via e-mail prior to the interview.

Interviews, which lasted approximately 45-minutes, were the primary data collection technique. I used open-ended questions (Appendix C) to capture the necessary

data to address the research question. According to Cachia and Millward (2011), semistructured interviews are a viable method of collecting qualitative research data. Researchers using semistructured interviews may elicit in-depth responses to the questions and an understanding of the subject (Qu & Dumay, 2011). Qu and Dumay (2011) further noted that semistructured interviews allow for flexibility and increases the accuracy of the data collection. However, interviews can be very time consuming as well as can result in different interpretations because interviewers may not understand and transcribe interviews in the same way (Edmunds & Brown, 2012).

I recorded all interviews using a handheld voice-to-text digital recorder and had a smartphone recorder available as a backup. Interview recordings assist a researcher in the data analysis process (Al-Yateem, 2012). Recording interviews helps researchers identify any unrecognized thoughts, feelings, and impressions, which might lead to bias in research if unchecked (Chenail, 2011). Rabionet (2011) noted that researchers use audio recordings to validate responses. After the interviews, I transcribed the recordings using Dragon NaturallySpeaking™. I reviewed the transcribed text while listening to the audio recording to ensure accuracy and to summarize my interpretation of the responses for member checking.

According to Denzin (2012), methodological triangulation involves utilizing multiple sources of data. I used methodological triangulation by integrating publicly available security and privacy policy statements as archival documents to collaborate and validate interview responses by participants. Perkmann and Schildt (2015) noted that

methodological triangulation with archival documents enables a researcher to control any potential self-reporting and retroactive bias from the interview data. The combination of security and privacy statements and participants' responses provides detailed information needed to answer a research question effectively (Trenholm & Ferlie, 2013). Utilizing multiple sources of evidence such as archival data and interviews allows for comparison in the research study, which assists in data validation (Canales, 2015).

I utilized the process of member checking for assuring response validity. Harper and Cole (2012) indicated that member checking is a quality control process implemented in qualitative research, which enables a researcher to confirm, clarify, or augment the accuracy of data collected during interviews. According to Marshall and Rossman (2011), member checking assures adequate verification of data collected during interviews. Member checking allows participants to verify response portrayal (Harper & Cole, 2012). I summarized each interview response for thematic analysis and developed a summary for member checking, illustrating themes emerging from individual responses. Galletta (2013) noted that member checking provides researchers with a means to test and fit their interpretation in relation to participants' responses. Each participant received an individual summary of my interpretation of their transcript for review to ensure accurate representation and validity. The participants were also asked to edit, clarify, elaborate, and comment on the narrative summary to ensure I understood their viewpoint. In the data analysis, I incorporated feedback received from each participant and confirmed themes that emerged in the study.

Data Organization Technique

Researchers utilize data organization techniques to manage data, thus increasing the reliability and validity of the study (Martins & Meyer, 2012). After the transcription of the interviews using Dragon NaturallySpeaking™, I organized each transcript in a Microsoft Word document. I organized each transcript in a Microsoft Word document, removed participant personal and identifiable information, and uploaded the document into QSR NVivo. The member-checked transcripts, research log, and the archival documents were stored in a folder labeled for each case study. Next, I organized all collected and reviewed data into categories, which later became nodes in QSR NVivo for thematic analysis. Merriam (2014) indicated that in qualitative studies, organizing data into categories assists researchers in identifying themes during data analysis. In addition, Yin (2011) noted that identifying emerging themes, patterns, and trends from interviews is the focus of data organization.

Yin (2013) indicated that transcriptions, notes, and logs allow researchers to discover themes, patterns and draw meanings from participants' responses to ensure reliability and validity in a study. I took interview notes in a research log to contribute to the conformability, reliability, and validity of my study. According to Wagstaff, Hanton, and Fletcher (2013), a researcher utilizes a research log to capture data to examine assumptions and actions thematic in a study. Moreover, a research log provides a valuable audit trail for conformability enabling the researcher to identify and reflect on challenges that might occur during the study (Georgiou, Marks, Braithwaite, &

Westbrook, 2013). In addition, Greene (2014) noted that keeping a log assists a researcher in minimizing potential bias throughout a study.

Themes and patterns emerged as I uploaded interview transcripts and external data into QSR NVivo for data analysis. QSR NVivo enables researchers to input data and identify themes and trends (Lane & Arnold, 2011). Gibson, Webb, and Lehn, (2014) indicated that researchers utilize software to assist in keeping track of and to organize data. In addition, Myers and Lampropoulou (2013) noted that researchers use computer programs for organizing and categorizing interview responses and data from other sources. Scholars utilize computer software to assist in transcription, data organization, journaling, and data analysis (Wilkerson, Iantaffi, Grey, Bockting, & Simon Rosser, 2014).

I utilized letters and numbers to identify participants on transcripts and my research log. The letters X and Y represented the two cases, the banking institution, and local government agency respectively, the letter P and a number represented each participant. Killawi et al. (2014) noted that researchers should protect identifiable information about participants in research studies. The utilization of letters and numbers protects the confidentiality and privacy of the participants (Yin, 2013). In addition, Muddyman, Smee, Griffin, and Kaye (2013) indicated that using unique identifiers provides participants with confidence that the researcher will not share personal information in the study. I will store the interview recordings, transcripts, and all notes on an encrypted hard drive solely accessible only by me for 5 years.

Data Analysis

The data analysis stage involves thematic exploration of data collected through observations, interviews, and other qualitative data collection techniques (Yin, 2013). According to Tracy (2012), in qualitative research, rigor in data analysis is achievable through the process of transforming and organizing raw data. Data analysis involves applying a common set of principles such as interviews transcription, in-depth analysis of phenomenon explored, data coding development, and identifying links to themes (Smith & Firth, 2011).

The objective of the data analysis process is an in-depth evaluation of themes and patterns that emerge during the interviews (Yin, 2013). I uploaded, organized, and analyzed the transcribed interviews data utilizing QSR NVivo. QSR NVivo is a computer-assisted qualitative data analysis software (CAQDAS) for data collection, management, and analysis of qualitative data such as audio and written data (QSR International, 2014). Researchers utilize QSR NVivo qualitative software to identify meaningful units, develop emergent themes, organize data, and for triangulation (Lane & Arnold, 2011).

I loaded the security and privacy statements into QSR NVivo for methodological triangulation. Methodological triangulation provides a researcher with an opportunity to utilize multiple forms of qualitative research data sources (Denzin, 2012). Case study researchers utilize methodological triangulation for flexibility in finding trends during data analysis (Guion, Diehl, & McDonald, 2013). Hanson et al. (2011) noted

methodological triangulation enables researchers to collect multiple types of data to construct a credible case for the validity of research findings, conclusions and recommendations.

Researchers utilize data coding as a framework to simplify the process of comparing and identifying patterns (Houghton et al., 2013). Zamawe (2015) noted that coding qualitative data involves exploring study data for common categories, themes, and ideas. Coding enables analysis, organization and comparison of data to extract meaningful information (Gale, Heath, Cameron, Rashid, & Redwood, 2013). I applied a coding process for categorizing data by source types such as interviews and achieved documents, to identify emerging themes.

Coding data in QSR NVivo involves the creation of nodes (Bergin, 2011). Furthermore, Bergin (2011) indicated that a node represents a collection of references to a particular theme, place, person, or another area of interest. I created nodes during the coding process by reviewing the interview transcripts and archived data. The nodes represented the data source types, and the following categories for data analysis: (a) risk management, (b) data security governance, (c) information security policies, (e) incident response strategies, (f) business performance, and (g) data security breaches. These categories represent successful business components, as related to complex systems based on the conceptual framework (systems theory) for this study. Pushkarskaya and Marshall (2010) noted that as a system, businesses rely on departments, operations, and employees to work together to achieve organizational objectives.

Reliability and Validity

According to Yin (2013), reliability in research ensures that another researcher who is investigating a similar case and utilizing the same research method would arrive at the same conclusion. The objective of reliability and validity is to eliminate bias and minimize errors in qualitative research (Podsakoff, MacKenzie, & Podsakoff, 2012). Yin further noted that the quality, credibility, conformability, and data dependability of findings guide qualitative research. The accurate interpretation of research data leads to valid and reliable findings (Tracy, 2012). The objective of a qualitative researcher is to establish credibility.

I used methodological triangulation, and member checking to assure accuracy, dependability, and credibility for this study. According to Guion et al. (2013), methodological triangulation requires coalescing data from different sources to reinforce validity and reliability. Methodological triangulation increases confidence in research findings through the utilization of multiple data sources to reduce bias (Harrison et al., 2014). Moreover, Hanson et al. (2011) stated that researchers should collect enough detailed data to construct a credible case for the findings, conclusions, and recommendations of a study. I triangulated semistructured interviews with organization security and privacy policy statements as the archival documents, from the selected institutions, to address validity. Yin (2013) indicated that methodological triangulation addresses potential issues of construct validity in case study research.

To ensure the credibility of this study, I adhered to the research method, design,

data collection, and analysis. Participants responded to identical interview questions. In addition, I employed member checking by reviewing my interpretation of individual interview responses with each interviewee for accuracy. Member checking enables participants to confirm, clarify, or improve the accuracy of the data collected during the interview (Marshall & Rossman, 2011). Moreover, in qualitative research, member checking provides a quality control process (Harper & Cole, 2012). Member checking also provides sufficient verification of the primary interview data to answer the research question (Marshall & Rossman, 2011). Furthermore, Houghton et al. (2013) indicated that verification through member checking could assure accuracy and establish credibility.

Data saturation is a key element in ensuring credibility in qualitative research (White, Oelke, & Friesen, 2012). According to Orser et al. (2011), data saturation is a point in qualitative research in which data collection does not yield new information. After interviews with eight participants at the bank and seven participants at the government agency, no new information emerged in relation to the research topic. Palinkas et al. (2013) noted an appropriate sample provides an effective analysis of a research topic to achieve data saturation. In addition, I achieved data saturation using a purposive sample size for the study. The utilization of purposive sampling supported data saturation through the identification of participants with rich and detailed experiences in data security within each case study. Moreover, I achieved data saturation since I continued the interviews until no new themes emerged.

Utilizing transferability, confirmability, and dependability assists in establishing trustworthiness and improves the quality of a study (Thomas & Magilvy, 2011). The research structure included purposeful sampling and a detailed outline of the research assumptions, limitations, and delimitations, and provided sufficient context for determining transferability of this study by other researchers. Marshall and Rossman (2011) indicated that transferability is the ability to generalize the research findings to a wider population. A qualitative researcher achieves transferability when the research findings have meaning for a person not involved in the study (Cope, 2014). Furthermore, Liu, Tang, Wang, and Lee (2013) noted that using purposive sampling could enhance transferability. I achieved confirmability and dependability in this study by recording and reviewing transcripts, member checking, and note taking during the interview process. Dependability refers to the constancy of the research data over similar conditions (Houghton et al., 2013). Liu et al. (2013) indicated that researchers utilize a reflexive journal as an audit trail to ensure confirmability and dependability in qualitative research. In addition, Cope (2014) indicated that confirmability ensures that the researcher represents participants' response and not the researcher's bias.

Transition and Summary

In Section 2, I outlined (a)my role as the researcher, (b) the participants, (c) research method and design, (d) population sampling, (e) ethical guidelines for the research, (f) data collection instruments, (g) techniques, (h) organization, (i) analysis, and (j) reliability and validity of the study. Section 3 is a presentation of the detailed findings

and the application to professional practice. In addition, I elaborate on the (a) implications for social change, (b) recommendations for action, (c) recommendation for future research, (d) a reflection of my experiences conducting this study, and (f) research conclusion.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multicase study was to explore best practices technology leaders use to minimize data security breaches for increased business performance. Two technology executives and five technical staff from each of two case studies, a bank in the Northcentral United States and a local government agency in the Southcentral United States, participated in this study. Participant interview responses and security and privacy statements (archival data) provided me the data with which to address the research question. Several themes emerged. Technology executives emphasized the need for skills in areas such as personnel management, communication skills, industry and government regulations, incident response, as well as gaining knowledge on current data security threats and risks to businesses. Technical staff indicated that acquiring and maintaining technical skills in areas such as (a) computer networking, (b) programming, (c) intrusion detection and prevention, (d) web technologies, (e) operating systems, (f) threat analyses, and (g) computer hardware were essential to respond effectively to security breaches. The technical staff voiced that leaders with good technical skills are in a better position to effectively respond to data security breaches. In both cases, participants indicated that technology executives within their organizations need technical and non-technical expertise to minimize data security breaches for increased business performance.

Presentation of Findings

The central research question for this study was: What best practices do technology leaders use to minimize data security breaches for increased business performance? I utilized semistructured interviews with open-ended questions (Appendix C), and organization security and privacy policy statements as the archival documents to collect data for this study. I analyzed the data for this study using QSR NVivo. The four themes that emerged from my analysis were: (a) a need for implementation of security awareness education and training to mitigate insider threats, (b) the necessity of consistent organization security policies and procedures, (c) an organizational culture promoting data security awareness, and (d) organizational commitment to adopting new technologies and innovative processes.

Theme 1: Security Awareness

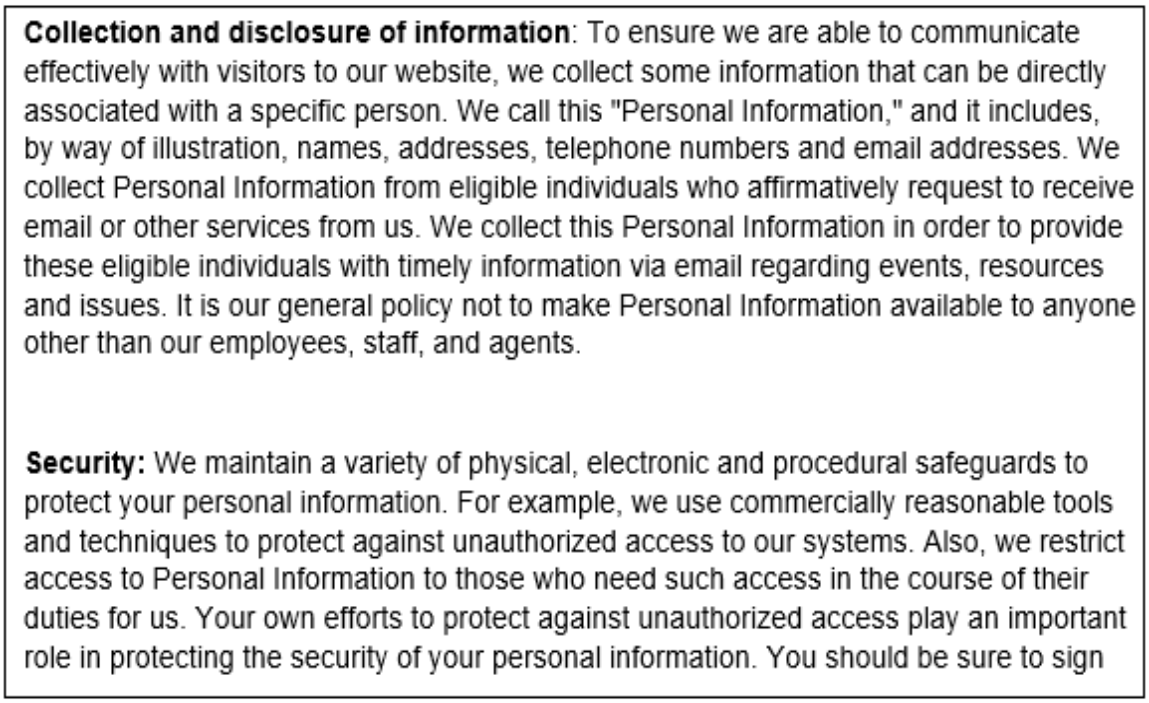
Mishra, Caputo, Leone, Kohun, and Draus (2014) indicated that creating awareness about security issues is imperative for an organization's overall objective to implement an effective security program. Education and training are effective methods of creating awareness about security vulnerabilities within an organization because these make employees aware of the risks and responsibilities of protecting information technology assets (Mishra et al., 2014). About 90% of the research participants echoed Mishra et al., stating that security lapses within their organizations resulted from a lack of security awareness.

Participant responses to interview question 2, 3, 4, and 8, as well as security and

privacy statements (Figure 2 and 3) from both cases indicated that each organization provided annual employee training on protecting the privacy and confidentiality of information, which is a best practice that might assist in identifying and mitigating breaches. Participants from the bank noted that the firm's fraud protection statement outlined the measures used to protect consumer information, educate consumers on how to detect fraudulent activities, and identify where to go for help in case of a security breach.

To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. All of our employees are trained annually and are bound by c Code of Conduct to maintain the privacy and confidentiality of your information.
We collect your personal information, for examples when you ▪ open an account or seek advice about your investments ▪ apply for loan or provide account information ▪ make deposits or withdrawals from you account We also collect your personal information from others, such as credit bureaus, affiliates or other companies.
Federal laws gives you're the right to limit only ▪ sharing for affiliates' everyday business purpose – information about your creditworthiness ▪ affiliates from using your information to market you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing.

Figure 2. Privacy policy, what we do. A direct excerpt from the security and privacy policy of the banking institution that illustrates what the bank does to protect consumer data, which includes annual employee training, what type of personal information is collected, and consumer rights under federal law.



Collection and disclosure of information: To ensure we are able to communicate effectively with visitors to our website, we collect some information that can be directly associated with a specific person. We call this "Personal Information," and it includes, by way of illustration, names, addresses, telephone numbers and email addresses. We collect Personal Information from eligible individuals who affirmatively request to receive email or other services from us. We collect this Personal Information in order to provide these eligible individuals with timely information via email regarding events, resources and issues. It is our general policy not to make Personal Information available to anyone other than our employees, staff, and agents.

Security: We maintain a variety of physical, electronic and procedural safeguards to protect your personal information. For example, we use commercially reasonable tools and techniques to protect against unauthorized access to our systems. Also, we restrict access to Personal Information to those who need such access in the course of their duties for us. Your own efforts to protect against unauthorized access play an important role in protecting the security of your personal information. You should be sure to sign

Figure 3. Privacy policy, collection and disclosure of information, security. An excerpt from the privacy policy of a local government agency that indicated how and what type of data the agency collects and discloses, and the security measures in place to protect consumer data.

A banking executive (P1X) noted that social engineering phone calls have become prevalent in the banking sector and that making employees and consumers aware of such activities has been a good practice for their firm. Conversely, participants from the local government agency did not indicate the agency provides any detailed security or fraud preventions information to their consumers. However, participant P4Y noted the government agency needed to improve consumer engagement and education efforts concerning data security.

Participants from the banking institution indicated that leaders struggle with consumer communication regarding security essentials such as creating strong passwords,

using secure surfing, and protecting sensitive data. French (2012) noted that the complex security measures implemented by most banks to protect consumer information are contributing to poor security behaviors by users. Participant P3X indicated that banks focused more on technology and security measures to protect systems and do not take into account the users who will access a system. However, two executive participants from the bank noted that news events on large security breaches, such as the Target Corporation data breach in 2014 (Gray & Ladig, 2015), resulted in an increase in the number of consumers attending their in-house consumer security education sessions. Participants from the local government agency indicated that executives reinforced the importance of improving security protocols after a major breach was reported on the news. Participant P2Y indicated the importance for businesses to implement protocols and procedures which encourage and reinforce data security responsibilities of each member of the organization. The ability to keep teams informed and educated on how to identify and respond to security threats is critical (P4Y).

Participants' responses to the interview questions aligned with Mishra et al.'s (2014) statement that security awareness through education and training assists in developing a more positive mindset and behavior towards security. Approximately 85% of the participants indicated that their perceptions of information security changed after their organizations mandated yearly awareness training session. Kim (2014) identified the same perception among college students who took security awareness training, noting that students' attitudes towards information security changed significantly after

awareness training. However, participants, specifically those from the local government agency, indicated a decline in the vigilance and use of best practice security measures weeks after security training. In Table 1, I illustrate the frequency at which participants mentioned the need for security awareness.

Table 1

Need for Security Awareness (Frequency)

Participant	Interview questions	Total number of references
P1X	2,3,4,8,10,11	8
P2X	8,10,11	4
P3X	4,8,10	3
P4X	3,8,10	4
P5X	3,4,8,10	6
P1Y	8	2
P2Y	8	1
P4Y	8,10	2
P5Y	3,10	2

Theme 2: Security Policy and Procedure Implementation

Information security policies are essential tools for technology management, as a security policy states in writing how a company plans to protect its physical and IT assets (Allassani, 2014). Security policies provide guidelines, requirements, implementation approaches, and consequences for violating a policy (Safa et al., 2015). Seventy-five

percent of the participants indicated that from previous experiences, one of the challenges of responding to a security breach was the lack of consistent security policies between the breach organization and vendors. Participant P1X indicated that dealing with third party vendors that have ineffective security policies and procedures exposes an organization to unforeseen threats. The participant further noted that the organization has a clause in every contract with external vendors requiring an annual review of the vendor's security policy and procedures by the bank's security officer.

Knapp and Ferrante (2012) noted that to reduce expenses resulting from security incidents, organizations should communicate, enforce, and maintain security policies. Approximately 86% of the participants indicated that as part of security awareness their organization sent a security newsletter and/or e-mail to employees to remind them of common security threats and to review organizational security policies. Banking participants indicated a quarterly alert for security threats while the local government participants indicated sporadic alerts throughout the year. Also, participants agreed that technology leaders' effective communication of security policy could assist employees in minimizing threats and vulnerabilities. Technology executive participants at the bank indicated a growing number of security threats which are forcing the organization to review security policies more frequently to ensure compliance and evolving with new threats.

Participants within the banking institution indicated that the communication of security policies should go beyond internal employees and vendors. They suggested that

banking customers need consumer education regarding security policies and procedures and the role each customer plays in securing banking data. Posey, Roberts, Lowry, and Hightower (2014) noted that banks are prone to lawsuits when consumer information is shared with unauthorized users. As such, providing consumers with a copy of the bank's privacy and security policy statements might increase awareness. However, participants from the local government agency did not indicate the existence of any initiatives to educate consumers on data protection policies. In Table 2, I illustrated the frequency participants mentioned the necessity of security policies and procedures during the interviews.

Table 2

Necessity of Consistent Security Policies and Procedures (Frequency)

Participant	Interview questions	Total number of references
P1X	1,3,5,6,7,8	10
P2X	1,5,6,7	5
P3X	1,3,5,10	8
P4X	1,5,6,7,8	6
P5X	1,3,8,10	5
P6X,	3,8,10	3
P1Y	3,8	3
P2Y, P3Y	1	1
P4Y, P6Y	1,3,8,10	6

P5Y	1,3,8	3

Theme 3: Organization Culture

Questions 2 through 9 of the interview allowed participants to provide a detailed description of their security knowledge and the data challenges within their organizations. A theme that emerged from the data was the impact of organizational culture on the participants' data security perspective. Participants from the bank indicated a stricter and aggressive organizational cultural on data security, citing government and industry regulations and sensitive consumer data. While participants from the local government agency indicated a more passive approach to data security, citing the organization stored limited sensitive consumer data. However, most of the local government agency data are publicly available to constituents.

The need to protect information systems and data, the increasing number of security breaches, and the requirement to comply with industry and government regulations have forced organizations to establish information security programs (Chen, Ramamurthy, & Wen, 2015). Participants from the bank indicated that an organizational culture that ensured compliance with government regulations assisted technology leaders in implementing best practices. For example, participants P1X and P2X noted that government regulations force security compliance in the banking industry. According to participant P5X, compliance to government and industry regulations has assisted bank executives in championing a culture that ensures the protection of confidential data.

Participants from the local government entity illustrated regulatory compliance

and standard organizational policies and procedures aligned to the services provided by the agency. Participant P4Y said the local government agency's focus was to provide constituents secure access to public services online. Participant P2Y noted the local government agency's Director of Information Technology encouraged behaviors and application development practices to promote effective data security management. The participant further indicated that a culture of responsibility and accountability assists in effective data security.

According to Chen et al. (2015), an organization's culture is a strong force that can affect business goals, lead to more accountability and less monitoring, and higher efficiency of data security-related investments within organizations. The participants from each case study illustrated different organization cultures shaped their perspective of information security. The participants from the local government agency illustrated a security culture of dependence on top leadership for directions and decision making, while participants from the banking firm demonstrated an independent and proactive approach to security that results from the bank's culture of accountability to consumers and regulators.

Knorst, Vanti, Andrade, and Johann (2011) indicated a failure to recognize the foundation or culture within an organization, such as shared values, beliefs, and behaviors drive the success of the organization when developing a security program, could lead to security lapses that might affect the identification and mitigation of security threats. As mentioned in Knorst et al., I identified similar viewpoints in my review of

participants' responses. Ninety-five percent of the participants' responses to interview question 10 indicated an alignment with the type of services their organization provided to consumers. Table 3, contains a summary of how often participants' responded regarding the need for an organizational culture promoting data security awareness

Table 3

Organization Culture Promoting Data Security Awareness (Frequency)

Participant	Interview questions	Total number of references
P1X	2,4,10	6
P2X, PX4	10	3
P3X	2,6,10	5
P5X	2,6,8,10	4
P1Y, P3Y	10	2
P2Y	2,10	2
P4Y	2,3,8,10	4
P5Y	2,6,10	4

Participants (P1X, P2X, and P3X) from the bank recommended that organizations incorporate security awareness campaigns as part corporate events to reinforce the need to protect sensitive information. Approximately 85% of the participants from the local government agency recommended a focus on a secure and open government and the implementation of essential security measure to protect classified information. Nevertheless, despite the different recommendations, all participants from both cases

illustrated throughout the interview that their organizational culture played a crucial role in data security perspectives within the organization.

Theme 4: New Technology and Innovative Process Adoption

Technology innovations and business processes are constantly evolving to meet organizational objectives. Programs such as Bring Your Own Device (BYOD) have rapidly changed operational business models in an attempt to improve efficiency and productivity (Garbaa, Armaregoa, Murraya, & Kenworthya, 2015). The constant changes in the technology landscape mean organizations need to be proactive and up-to-date on latest trends, threats, vulnerabilities, and confidentiality breaches (Yang, Lee, Park, & Eom, 2015). Figure 4 provides a high-level view of current technology trends that organizations need to account for within their network architecture.

Figure 4. Top 10 Technology Trends for 2015. A high-level illustration of the top 10 technology trends of 2015. Retrieved from "The Top 10 Strategic Technology Trends for

2015," by M. J. Walker and D. W. Cearley, 2015, *Research Guide*. Copyright by Gratner, Inc. Adapted with permission (Appendix F).

Participants (P1X, P2X, P3X, P4X, and P4Y) acknowledged new technology innovations and trends were a security concern particularly around the *Internet of Things* and *cloud computing*. All the participants from the bank focused more on online and mobile banking trends that expose consumer information and unknown threats while 80% of the participants from the local government agency focused on the pressures around providing services online. Approximately 75% of the participants from each case indicated the need for their organization to invest in training employees on new technology innovations and trends that might affect the organization's' security. Participants from the bank indicated that services such as mobile pay provided by Apple and Google were an area in which their organization needed to invest more training dollar for employee and consumer education. Participant P1X stated that "… an 80-year-old grandma that just got an iPad …" does not consider data security when using the iPad to access banking information. Participant P3X also noted that advances in technology are creating difficulties for individuals and organizations to keep up with emerging threats.

Participants from the local government agency did not focus on any specific technology innovation or trend. However, approximately 50% of the local government agency's participants indicated that technology leaders needed to stay informed of innovations that might affect network security. Participant P4Y noted that understanding how current information security threats might affect an organization assists government agency security professional in developing better incident response strategies. Participant

P1Y stated that technology executives need to pay attention to daily operational activities for risk identification, and stay current in their knowledge of emerging technology trends to ultimately combat security vulnerabilities. In Table 4, I outlined the frequency participants indicated the need for organizational commitment to adopt new technologies and innovative processes.

Table 4

Organizational Commitment to Adopt New Technologies and Innovative Processes (Frequency)

Participant	Interview questions	Total number of references
P1X	3,7	4
P2X	6,7	2
P3X	3,7,8	4
P5X	6,7	3
P1Y	6,8	2
P4Y	3,7	2

Ninety-eight percent of the technology executives interviewed from both cases illustrated a need to stay informed on trending technologies, threats, and vulnerabilities. In addition, participants suggested the need for leaders to gain technical expertise in the areas of computer networking, system security, and application vulnerabilities for effective communication during a breach. According to participant P2X, technology leaders, and security professionals need to understand the challenges of new technology

trends to ensure organization security policies and procedures detect and prevent threats effectively.

Findings Related to Systems Theory

As noted by Moeller and Valentinov (2012) and von Bertalanffy et al. (2008), the foundation of systems theory is the evolution of systems or organisms and the interdependence of a system with another and their components. All participants agreed information security was a critical component to the success of an organization. Also, participants illustrated that most lapses in data security are because security policies, tools, employees, and business objectives are not in alignment. Coole and Brooks (2014) noted failures in information security occur when all components are not functioning or working as one unified entity.

Tsohoua, Karydab, and Kokolakis (2015) indicated security awareness programs focus more on content and processes rather than on how employees approach security decision-making and understand security information. Therefore, based on my research findings, the success of security awareness initiatives within organizations depends on how well technology leaders consider all the components of the organization. In addition, Chandrashekhar, Gupta, and Shivaraj (2015) noted that information security awareness is a critical component of a successful organization. From the lens of systems theory, an effective security awareness program may result in information security efficiencies within organizations.

Parsons et al. (2015) indicated that a security-aware organizational culture, such

as incorporating security compliance into employees' work activities, assists employees in developing behaviors in line with effective security policy and procedures. As illustrated in my research findings, organizational culture might influence participants' perspectives towards information security. Since culture is a component of an organization (Ahamed & Mahmood, 2015), in relation to systems theory, all employees must be diligent for effective data security.

The identified themes illustrate there is no one best practice measure that can minimize data security breaches for increased business performance. Following the concepts of systems theory, technology leaders may implement the actions outlined below, together with the best practices identified in the study to protect technology assets, data, people, and property effectively. The participants' answers to the interview questions supported the premise of systems theory, which was the conceptual framework for this study.

Applications to Professional Practice

Identifying the best practices technology leaders use to minimize data security breaches is imperative to addressing an organization's goal towards a secured business and technology environment. Based on the study findings, the most significant contribution may be the development of potential best practices to assist in minimizing data security breaches for increased business performance. Study findings may assist business leaders to reduce costs associated with responding to a data breach. The cost of responding to data security breaches in the United States has been on the rise, with an

estimated increase of 11% ($6.5 million) in the average cost of data breaches in 2014 (IBM & Ponemon Institute, 2015).

In my findings, I introduced potential applications to professional practice by identifying the gap that existed between technology adoption and data security best practices to address the impact of data breaches on business performance. Herath et al. (2014) noted that security designs and technology adoptions have implications on an organization's privacy best practices and awareness initiatives. Furthermore, Atienza et al. (2015) indicated that the adoption of new technology innovations has prompted discussions about privacy and security within organizations. Aligning the need to adopt new technologies and perceived threats provides an organization with options to mitigate security risk effectively (Min, Lim, & Park, 2015). Several of the participants illustrated the need to develop a common strategy for responding to data breaches that align with organizational objectives, technology adoptions, and information security.

Ninety percent of the participant responses to interview questions 8 through 10 indicated a necessity to balance organizational culture and information security. Safa et al. (2015) noted that security awareness initiatives should be an integral part of organizational culture, since organization consistency is a key success factor of information security awareness. Organizations that adopt high moral standards and self-control encourage a security culture of deterrence (Ahmad, Maynard, & Park, 2014). A corporate culture that supports effective security policies, procedures, and responsibilities makes information security a natural aspect of employee's activities (Alnatheer, 2014).

The results from this study might provide additional material for information security leaders use in championing data protection initiatives within their organization. Globally, governments and corporations face cyber threats from entities; implementing best practices would assist in mitigating cyber threats (Choucri, Madnick, & Ferwerda, 2014). The findings of this study might assist technology leaders in reducing the cost of protecting confidential data for business sustainability. Given the negative impact data breaches have on stockholders and stakeholders, business leaders need to protect consumer data, intellectual property, and other confidential information (Modi, Wiles, & Mishra, 2015).

The findings of the study may contribute to the industry and educational research by reinforcing the role of employees in the protection of confidential data within organizations. The findings in my study are in agreement on the basis of systems theory in that each employee may play an integral role in data protection. Employees can play a critical part in the success of information security initiatives (Cavusoglu, Cavusoglu, Son, & Benbasat, 2015). Research participants recommended best practices that would promote effective communication of security policies and procedures, and increase end-user security awareness through continuous employee education.

Implications for Social Change

The majority of corporate data breaches, approximately 81%, result in the theft of consumer data (Lai, Li, & Hsieh, 2012). Since customer data are a valuable corporate asset (Chen, 2015), organizations need to implement best practices to minimize the

exposure of data to threats. The implementation of security awareness best practices, as illustrated in my findings, may increase employee awareness of potential security threats, vulnerabilities, and responsibility. Business leaders could implement best practices for protecting the consumer and corporate data against threats and vulnerabilities; and thereby decrease the financial burden on consumers to monitor financial and credit information after a security breach.

According to Hille, Walsh, and Cleveland (2015), more than 4% of the United States population in 2012 was a victim of identity theft with damages of approximately $12 billion. Therefore, based on my findings, limiting the negative effects of data breaches on consumers resulting from identity theft may affect society as a whole. In addition, because security breaches have a negative impact on stock prices (Hinz, Nofer, Schiereck, & Trillig, 2015), adopting best practices could impact organizational market value, affecting employee retirement and pension plans as well as employee stock ownership and economic value.

Recommendations for Action

The protection of information technology assets from internal and external threats is critical to the success of organizations (Carter et al., 2012). Organizational leaders are constantly searching for best practices that minimize their exposure to threats and reduce the cost of responding to a data security breach (Caldwell, 2012). Based on the research findings, I recommend the following actions:

- Technology leaders need to take a holistic approach to data security that

effectively integrates all the components such as people, processes, and systems.

- Technology leaders should champion the implementation and audit of security policies and procedures through interactive methods to engage employees.
- Technology leaders should require employees to participate in information security training and awareness forums, quarterly or twice a year, to explore security challenges facing the organization and current data breach trends.
- Technology leaders should stay up-to-date on current security threats and vulnerabilities that might affect the organization.
- Technology leaders need to stay current on technology innovations and trends to ensure the organization is taking advantage of these innovations as well as the security impact.
- Technology leaders should strive to build a work environment that aligns with the organizational culture and information security realities.
- Technology leaders must champion an organizational culture that fosters a positive attitude towards information security.
- Technology leaders should work on improving the relationship between business managers and IT managers to encourage protection of technology assets.

I will seek to disseminate my research findings through industry publications, academic journals, and conferences focused on information security. The essence of research is publication, therefore, the dissemination of research findings via other sources is an essential element of the research process (Saracho, 2013). Moreover, after

reviewing the intended derivative publications, business leader can integrate my study findings into corporate training, employee manuals, and organizational security initiatives. The incorporation of academic research findings into organization documents and publications provides new insights and adds to research productivity (Aydın, 2012).

Recommendations for Further Research

The findings, conclusions, and recommendations stemming from this study may contribute to existing, and future research and gaps in business practice regarding best practices technology leaders could use to minimize data security breaches and increase business performance. The protection of computer systems, confidential and sensitive data is critical to business success (Teh et al., 2015). Secure and safe working environments, security awareness, implementation of security procedures and tools are essential in preventing data security breaches (Btoush et al., 2011). In addition, understanding the effects of data security on consumer habits and finances could assist organizations minimize threats effectively (Safa et al., 2015).

A limitation of the study was that I solely focused on best practices. Future researchers may explore leadership styles and behaviors in relation to information security. Another limitation was the small sample size of the case studies, a banking firm in the Northcentral United States and a local government agency in the Southcentral United States. Future researchers might consider expanding the sample size to other industries and regions of the United States. An additional limitation was the multicase study research design. Utilizing a different research design such as phenomenological,

might provide an opportunity for a larger sample size and cross-industry research. The last limitation was my limited skills as a researcher in data collection. Further studies might involve several experienced researchers with a diverse background in conducting qualitative research.

Quantitative researchers may examine the extent and nature of the relationship between technology leadership styles and the adoption of information security initiatives. Thematically, my study findings showed a need for technology leaders to be champions of their organizations' security initiatives and promote a positive outlook on systems and data security. Moreover, researchers could expand my studying findings by examining the effect of organization culture on information security governance. By developing policies that align with organizational culture, promoting security awareness, and adapting organizational operations based on technological trends and innovations, technology leaders might develop further strategies to minimize data security breaches for increased business performance and consumer protection.

Reflections

Using a qualitative multicase study, I focused on the exploration of best practices technology leaders use to minimize data security breaches for increased business performance. Reflecting on my experiences throughout this research process, I found the adoption of industry best practices varied from industry to industry, as well as from company to company. The participants in this study elaborated on the unique nature of their business and the influence of the organization's culture on their view and adoption

of data security measures. I was pleased to hear participants from both organizations indicate technology leaders needed to play a critical role in championing data security and awareness.

My doctoral study experience enhanced my scholarly knowledge on data security best practices. The insight I gained interacting with participants at the two organizations under study will benefit my current and future career development. Using open-ended questions in this study offered an opportunity for an in-depth discussion with participants, which improved my communications and interpersonal skills. The timing of my research was coincidentally aligned with recent data security breaches within major U.S. corporations, and further enhanced my awareness of the need for effective incident response. I gained personal knowledge on how these breaches affected organizations especially those in my case studies.

Summary and Study Conclusions

The objective of this qualitative multicase study was to explore the best practices technology leaders use to minimize data security breaches for increased business performance. The two cases selected for this study were a banking firm in the Northcentral United States and a local government agency in the Southcentral United States. Utilizing open-ended questions and security and privacy policy statements as the archival documents, I collected and triangulated data to answer the research question. Four themes emerged during data analysis illustrating the best practices technology leaders use to minimize data security breaches for increased business performance. The

themes involved (a) security awareness, (b) security policies, (c) organization culture, and (d) technology and innovation trends. My findings indicated a need for technology leaders to champion security awareness initiatives and utilize business activities in security training programs to illustrate the critical nature of information security. Leaders need to become proactive in their efforts to champion the adoption of industry best practices within their organizations, as well as align the best practices to the organizational culture. Also, technology leaders should ensure their staff are up-to-date on current technology and security trends, as well as threats. Several of the research participants noted that staying connected with recent security events, threads, and vulnerabilities provided an invaluable opportunity for technology leaders and staff to evaluate their organizations' state of data and information security.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*, 237-248. doi:10.1080/0144929X .2012.708787

Abbas, H., Magnusson, C., Yngstrom, L., & Hemani, A. (2011). Addressing dynamic issues in information security management. *Information Management & Computer Security*, *19*, 5-24. doi:10.1108/09685221111115836

Adebayo, A. O. (2012). A foundation for breach data analysis. *Journal of Information Engineering and Applications*, *2*(4), 17-23. Retrieved from http://iiste.org /Journals/index.php/JIEA/index

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

Ahamed, M., & Mahmood, R. (2015). Impact of organizational culture on job satisfaction: A study on Banglalion Communication Ltd, Bangladesh. *European Journal of Business and Management*,*7*(10), 160-174. Retrieved from http://iiste .org/Journals/index.php/EJBM/index

Al-Yateem, N. (2012). The effect of interview recording on quality of data obtained: A methodological reflection. *Nurse Researcher*, *19*(4), 31-35. doi:10.7748/nr2012 .07.19.4.31.c9222

Alebrahim, A., Hatebur, D., Fassbender, S., Goeke, L., & Côté, I. (2015). A pattern-based

and tool-supported risk analysis method compliant to ISO 27001 for cloud systems. *International Journal of Secure Software Engineering*, *6*(1), 24-46. doi:10.4018/ijsse.2015010102

Ali, S., & Green, P. (2012). Effective information technology (IT) governance mechanisms: An IT outsourcing perspective. *Information Systems Frontiers*, *14*, 179-193. doi:10.1007/s10796-009-9183-y

Allassani, W. (2014). Determining factors determinants of bank employees' reading habits of information security policies. *Journal of Information Systems and Technology Management*, *11*, 533-548. doi:10.4301/S1807-17752014000300002

Allwood, M. C. (2012). The distinction between qualitative and quantitative research methods is problematic. *Qual Quant*, *46*, 1417-1429. doi:10.1007/s11135-011-9455-8

Alnatheer, M. A. (2014). A conceptual model to understand information security culture. *International Journal of Social Science and Humanity*, *4*, 104-107. doi:10.7763/IJSSH.2014.V4.327

Amancei, C. (2011). Practical methods for information security risk management. *Informatica Economica*, *15*(1), 151-159. Retrieved from http://revistaie.ase.ro/

Ankita, L. (2012). Odyssey of data security with a new perception. *International Journal of Computer Science Issues, 9*, 303-311. Retrieved from http://ijcsi.org/

Arlitscha, K., & Edelmanb, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration, 54*, 46-56. doi:10.1080

/01930826.2014.893116

Atienza, A. A., Zarcadoolas, C., Vaughon, W., Hughes, P., Patel, V., Chou, W. Y. S., & Pritts, J. (2015). Consumer attitudes and perceptions on mHealth privacy and security: Findings from a mixed-methods study. *Journal of Health Communication*, *20*, 673-679. doi:10.1080/10810730.2015.1018560

Aydın, O. T. (2012). The impact of motivation and hygiene factors on research performance: An empirical study from a Turkish university. *International Review of Management and Marketing*, *2*, 106-111. Retrieved from http://www .ilhanozturk.com/index.php/irmm/index

Ballou, B., Dan, L. H., & Stoel, D. (2011). How boards of directors perceive risk management information. *Management Accounting Quarterly*, *12*(4), 14-22. Retrieved from http://www.imanet.org/resources_and_publications/management _accounting_quarterly.aspx

Bansal, P., & Corley, K. (2011). The coming of age for qualitative research: Embracing the diversity of qualitative methods. *Academy of Management Journal*, *54*, 233-237. doi:10.5465/AMJ.2011.60262792

Basem, B., Ghalwash, A., Z., & Sadek, R., A. (2015). Multilayer secured SIP based VoIP architecture. *International Journal of Computer Theory and Engineering*, *7*, 453-462. doi:10.7763/IJCTE.2015.V7.1002

Becker, J. (2013). *Examining relationships between hospital inpatient expectations and satisfaction for maximum Medicare reimbursement* (Doctoral dissertation).

Available from ProQuest Dissertations and Theses database. (UMI No. 3601243)

Bekhet, A. K., & Zauszniewski, J. A. (2012). Methodological triangulation: an approach to understanding data. *Nurse Researcher, 20*(2), 40-43. doi:10.7748/nr2012.11.20.2.40.c9442

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51-61. doi:10.1016/j.chb.2015.01.039

Berge, J. M., Loth, K., Hanson, C., Croll, J., & Neumark-Sztainer, D. (2012). Family life cycle transitions and the onset of eating disorders: A retrospective grounded theory approach. *Journal of Clinical Nursing, 21*, 1355–1363. doi:10.1111/j.1365-2702.2011.03762.x

Bergin, M. (2011). NVivo 8 and consistency in data analysis: Reflecting on the use of a qualitative data analysis program. *Nurse Researcher, 18*(3), 6-12. doi:10.7748/nr2011.04.18.3.6.c8457

Bisong, A., & Rahman, M. S. (2011). An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security & Its Applications, 3*(1), 30-45. doi:10.5121/ijnsa.2011.3103

Bölte, S. (2014). The power of words: Is qualitative research as important as quantitative research in the study of autism? *Autism, 18*(2), 67-68. doi:10.1177/1362361313517367

Bojanc, R., & Jerman-Blažič, B. (2013). A Quantitative model for information-security

risk management. *Engineering Management Journal*, *25*(2), 25-37. Retrieved from http://www.asem.org/asemweb-emj.html

Borison, A., & Hamm, G. (2010). How to manage risk after the risk-management collapse? *MIT Sloan Management Review*, *52*(1), 51-57. Retrieved from http://sloanreview.mit.edu/

Brédart, A., Marrel, A., Abetz-Webb, L., Lasch, K., & Acquadro, C. (2014). Interviewing to develop patient-reported outcome (PRO) measures for clinical research: eliciting patients' experience. *Health and Quality of Life Outcomes*, *12*(1), 1-10. doi:10.1186/1477-7525-12-15

Bristowe, K., Horsley, H. K., Shepherd, K., Brown, H., Carey, I., Matthews, B., ...Murtagh, F. E. (2014). Thinking ahead – the need for early advance care planning for people on haemodialysis: A qualitative interview study. *Palliative Medicine*, 1-8. doi:10.1177/0269216314560209

Btoush, M., Alarabeyat, A., Zboon, M., Ryati, O., Hassan, M., & Ahmad, S. (2011). Increasing information security inside organizations through awareness learning for employees. *Journal of Theoretical & Applied Information Technology*, *24*, 79–85. Retrieved from http://www.jatit.org

Cachia, M., & Millward, L. (2011). The telephone medium and semistructured interviews: A complementary fit. *Qualitative Research in Organizations and Management: An International Journal*, *6*, 265-277. doi:10.1108 /17465641111188420

Cairney, P. (2012). Complexity theory in political science and public policy. *Political Studies Review*, *10*, 346-358. doi:10.1111/j.1478-9302.2012.00270.x

Calandro, J. (2011). The margin of safety principle and corporate strategy. *Strategy & Leadership*, *39*(5), 38-45. doi:10.1108/10878571111161516

Caldwell, T. (2012). Prepare to fail: creating an incident management plan. *Computer Fraud & Security*, *2012*(11), 10-15. doi:10.1016/S1361-3723(12)70114-8

Cambra-Fierro, J., & Wilson, A. (2011). Qualitative data analysis software: Will it ever become mainstream? Evidence from Spain. *International Journal of Market Research*, *53*(1), 17-24. doi:10.2501/IJMR-53-1-017-024

Canales, J. I. (2015). Sources of selection in strategy making. *Journal of Management Studies*, *52*(1), 1-31. doi:10.1111/joms.12101

Caniëls, M. C., Lenaerts, H. K., & Gelderman, C. J. (2015). Explaining the internet usage of SMEs: the impact of market orientation, behavioural norms, motivation and technology acceptance. *Internet Research*, *25*, 358-377. doi:10.1108/IntR-12-2013-0266

Carter, D. L., Phillips, B., & Millington, P. (2012). The impact of information technology internal controls on firm performance. *Journal of Organizational and End User Computing*, *24*(2), 39-49. doi:10.4018/joeuc.2012040103

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, *52*, 385-

400. doi:10.1016/j.im.2014.12.004

Caytiles, D. R., & Lee, S. (2012). Security considerations for public mobile cloud computing. *International Journal of Advanced Science and Technology*, *44*, 81-88. Retrieved from http://www.sersc.org/journals/IJAST/

Chai, S., Kim, M., & Rao, R. H. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems, 50*, 651-661. doi:10.1016/j.dss.2010.08.017

Chan, C. (2011). Information security risk modeling using Bayesian index. *The Computer Journal*, *54*, 628-638. doi:10.1093/comjnl/bxq059

Chandrashekhar, A. M., Gupta, R. K., & Shivaraj, H. P. (2015). Role of information security awareness in success of an organization. *International Journal of Research*, *2*(6), 15-22. Retrieved from http://internationaljournalofresearch.org/

Chen, S. C. (2015). Customer value and customer loyalty: Is competition a missing link. *Journal of Retailing and Consumer Services*, *22*, 107-116. doi:10.1016/j.jretconser.2014.10.007

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly*, *35*, 397-422. Retrieved from http://misq.org/

Chen, Y., Ramamurthy, K., & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems*, *55*(3), 11-19. Retrieved from http://www.iacis.org/jcis

/jcis.php

Chenail, R. J. (2011). Interviewing the investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research. *The Qualitative Report, 16*, 255-262. Retrieved from http://nsuworks.nova.edu /tqr/vol16/iss1/16

Chitakornkijsil, P. (2010). Enterprise risk management. *International Journal of Organizational Innovation*, *3*, 309-337. Retrieved from http://www.ijoi-online.org/

Chiumento, A., Khan, M. N., Rahman, A., & Frith, L. (2015). Managing ethical challenges to mental health research in post‐conflict settings. *Developing World Bioethics*. doi:10.1111/dewb.12076

Chlotia, P. G., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, *19*, 216-230. doi:10.1108 /09685221111173049

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. *Information Technology for Development, 20*, 96-121. doi:10.1080/02681102.2013.836699

Cigdemoglu, C., Arslan, H. O., & Akay, H. (2011). A phenomenological study of instructors' experiences on an open source learning management system. *Procedia-Social and Behavioral Sciences*, *28*, 790-795. doi:10.1016/j.sbspro .2011.11.144

Coole, M., & Brooks, D. J. (2014). Do security systems fail because of entropy? *Journal of Physical Security*, *7*(2), 50-76. Retrieved from http://www.anl.gov/

Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum*, *41*, 89-91. doi:10.1188/14.ONF.89-91

Cruz, E. V., & Higginbottom, G. (2013). The use of focused ethnography in nursing research. *Nurse Researcher, 20*(4), 36-43. doi:10.7748/nr2013.03.20.4.36.e305

Culver, D. M., Gilbert, W., & Sparkes, A. (2012). Qualitative research in sport psychology journals: The next decade 2000-2009 and beyond. *Sport Psychologist, 26,* 261-281. Retrieved from http://journals.humankinetics.com/tsp

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*, 474-489. doi:10.1108/IMCS-08-2013-0057

Dai, L., Maksimov, V., Gilbert, A. B., & Fernhaberd, A. S. (2014). Entrepreneurial orientation and international scope: The differential roles of innovativeness, proactiveness, and risk-taking. *Journal of Business Venturing*, 29, 511-524. doi:10.1016/j.jbusvent.2013.07.004

Damianakis, T., & Woodford, M. R. (2012). Qualitative research with small connected communities generating new knowledge while upholding research ethics. *Qualitative Health Research*, *22,* 708-718. doi:10.1177 /1049732311431444

Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information

security breach: A study using firm and attack characteristics. *Journal of Information Privacy and Security*, *8*(4), 27-55. doi:10.1080/15536548.2012.10845665

Dawson, M., Burrell, D., Rahim, E., & Brewster, S. (2010). Integrating software assurance into the software development life cycle. *Journal of Information Systems Technology & Planning*, *3*(6), 49-53. Retrieved from http://www.intellectbase.org/journals.php#JISTP

Dawson Jr., E. M., Crespo, M., & Brewster, S. (2013). DoD cyber technology policies to secure automated information systems. *International Journal of Business Continuity and Risk Management*, *4*, 1-22. doi:10.1504/IJBCRM.2013.053089

Denzin, K. N. (2012). Triangulation 2.0. *Journal of Mixed Methods Research, 6*, 80-88. doi:10.1177/1558689812437186

Ducq, Y., Chen, D., & Doumeingts, G. (2012). A contribution of system theory to sustainable enterprise interoperability science base. *Computers in Industry, 63*, 844-857. doi:10.1016/j.compind.2012.08.005

Duncan-Daston, R., Hunter-Sloan, M., & Fullmer, E. (2013). Considering the ethical implications of social media in social work education. *Ethics and Information Technology*, *15*, 35-43. doi:10.1007/s10676-013-9312-7

Edmunds, S., & Brown, G. (2012). Doing qualitative research in dentistry and dental education. *European Journal of Dental Education, 16*, 110-117. doi:10.1111/j.1600-0579.2011.00734.x

Einav, L., Levin, J., Popov, I., & Sundaresan, N. (2014). Growth, Adoption, and Use of Mobile E-Commerce. *The American economic review*, *104*, 489-494. doi:10.1257/aer.104.5.489

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative Content Analysis. *SAGE Open*, *4*(1), 1-10. doi:10.1177 /2158244014522633

Enescu, M., Enescu, M., & Sperdea, N. M. (2011). The specifics of security management: The function of information security required by organizations. *Economics, Management & Financial Markets*, *6*, 200–205. Retrieved from http://www.addletonacademicpublishers.com/economics-management-and-financial-markets

Enonbun, O. (2010). Constructivism and web 2.0 in the emerging learning era: A global perspective. *Journal of Strategic Innovation and Sustainability*, *6*(4), 17-27. Retrieved from http://www.na-businesspress.com/jsisopen.html

Erlingsson, C., & Brysiewicz, P. (2013). Orientation among multiple truths: An introduction to qualitative research. *African Journal of Emergency Medicine*, *3*, 92-99. doi:10.1016/j.afjem.2012.04.005

Ernst & Young. (2013). *Under cyber-attack: EY's global information security survey 2013*. Retrieved from http://www.ey.com/Publication/

Executive Office of the President of the United States. (2013). *Fiscal year 2012 report to congress on the implementation of the federal information security management*

act of 2002. Retrieved from http://www.whitehouse.gov/sites/default/files/omb /assets/egov_docs/fy12_fisma.pdf

Family Educational Rights and Privacy Act Amendments of 2008, S.2859. (2008). Retrieved from http://beta.congress.gov/110/bills/s2859/BILLS-110s2859is.pdf

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing? *Communications of the Association for Information Systems*, *28*, 329–356. Retrieved from http://aisel.aisnet.org/cais/

Figg, C. W., & Kam, J. H. (2011). Medical information security. *International Journal of Security*, *5*, 22-34. Retrieved from http://www.cscjournals.org/journals/IJS /description.php

Fiske, S. T., & Hauser, R. M. (2014). Protecting human research participants in the age of big data. *Proceedings of the National Academy of Sciences*, *111*, 13675-13676. doi:10.1073/pnas.1414626111

Fleming, R. S., & Faye X., Z. (2013). Meeting service level challenges through proactive strategies. *Business Renaissance Quarterly*, *8*, 77-88. Retrieved from http://www .brqjournal.com/

Flores, W. R., Sommestad, T., Holm, H., & Ekstedt, M. (2011). Assessing future value of investments in security-related IT governance control objectives - surveying IT professionals. *Electronic Journal of Information Systems Evaluation*, *14*, 216-227. Retrieved from http://www.ejise.com

Foley, D., & O'Connor, A. J. (2013). Social capital and networking practices of

indigenous entrepreneurs. *Journal of Small Business Management, 51,* 276-296. doi:10.1111/jsbm.12017

French, A. M. (2012). A case study on e-banking security–When security becomes too sophisticated for the user to access their information. *Journal of Internet Banking and Commerce, 17*(2), 1-14. Retrieved from http://www.arraydev.com/commerce/jibc/

Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security – A survey and classification of the research area. *Computers & Security, 30,* 748-769. doi:10.1016/j.cose.2011.08.002

Gale, N. K., Heath, G., Cameron, E., Rashid, S., & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology*, *13*(1), 1-8. doi:10.1186/1471-2288-13-117

Galletta, A. (2013). *Mastering the semi-structured interview and beyond: From research design to analysis and publication*. New York, NY: New York University Press.

Garbaa, B. A., Armaregoa, J., Murraya, D., & Kenworthya, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy and Security, 11,* 38-35. doi:10.1080/15536548.2015.1010985

Garrison, P. C., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security, 19,* 216-230.

doi:10.1108/09685221111173049

Gatzlaff, K. M., & McCullough, K. A. (2012). Implications of Privacy Breaches for Insurers. *Journal of Insurance Regulation, 31,* 197-216. Retrieved from http://www.naic.org/store_jir.htm

Gendron, Y., Brivot, M., & Guénin-Paracini, H. (2015). The construction of risk management credibility within corporate boardrooms. *European Accounting Review*, (ahead-of-print), 1-30. doi:10.1080/09638180.2015.1064008

Georgiou, A., Marks, A., Braithwaite, J., & Westbrook, J. I. (2013). Gaps, disconnections, and discontinuities - The role of information exchange in the delivery of quality long-term care. *The Gerontologist*, *53,* 770-779. doi:10 .1093/geront/gns127

Ghezal, S. (2015). Performance impacts of information assurance strategic alignment in the context of small business. *Mustang Journal of Management and Marketing, 6,* 45-69. Retrieved from http://mustangjournals.com/MJMM/index.htm

Gibson, W., Webb, H., & Lehn, V. D. (2014). Analytic affordance: Transcripts as conventionalised systems in discourse studies. *Sociology, 48,* 780-794. doi:10.1177/0038038514532876

Goertz, G., & Mahoney, J. (2013). Methodological Rorschach tests: Contrasting interpretations in qualitative and quantitative research. *Comparative Political Studies, 46,* 236 –251. doi:10.1177/0010414012466376

Goldberg, E. (2013). Preventing a data breach from becoming a disaster. *Journal of*

Business Continuity & Emergency Planning, *6*, 295-303. Retrieved from http://www.henrystewartpublications.com/jbcep

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*, 33–56. doi:10.3233/JCS-2009-0398

Gramm-Leach-Bliley Act, S.900. (1999). Retrieved from http://beta.congress.gov/106/plaws/publ102/PLAW-106publ102.pdf

Grant, L. G., & Royle, T. M. (2011). Information technology and its role in creating sustainable competitive advantage. *Journal of International Management Studies*, *6*(1), 1-7. Retrieved from http://www.jimsjournal.org/pi.html

Gray, D., & Ladig, J. (2015). The implementation of EMV chip card technology to improve cyber Security accelerates in the US following Target Corporation's data breach. *International Journal of Business Administration*, *6*, 60-67. doi:10.5430/ijba.v6n2p60

Guion, A. L., Diehl, C. D., & McDonald, D. (2013). Triangulation: Establishing the validity of qualitative studies. *University of Florida, The Institute of Food and Agricultural Sciences*. Retrieved from http://edis.ifas.ufl.edu/fy394

Gupta, P. K. (2011). Risk management in Indian companies: EWRM concerns and issues. *The Journal of Risk Finance*, *12*, 121-139. doi:10.1108/15265941111112848

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities

in information security. *Information Management & Computer Security, 19*, 155–176. doi:10.1108/09685221111153546

Hagen, J., Albrechtsen, E., & Johnsen, S. O. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security, 19*, 140-154. doi:10.1108/09685221111153537

Hammond, D. (2010). *Science of synthesis: Exploring the social implications of general systems theory.* Boulder, CO: University Press of Colorado.

Hanson, J. L., Balmer, D. F., & Giardino, A. P. (2011). Qualitative research methods for medical educators. *Academic Pediatrics, 11*, 375-386. doi:10.1016/j.acap.2011.05.001

Harrison, J. S., Banks, G. C., Pollack, J. M., O'Boyle, E. H., & Short, J. (2014). Publication bias in strategic management research. *Journal of Management (Online)*. doi:10.1177/0149206314535438

Harnesk, D., & Lindström, J. (2011). Shaping security behaviour through discipline and agility: Implications for information security management. *Information Management & Computer Security, 19*, 262-276. doi:10.1108/09685221111173076

Harper, M., & Cole, P. (2012). Member checking: Can benefits be gained similar to group therapy? *The Qualitative Report*, *17*, 510-517. Retrieved from http://www.nova.edu/ssss/QR/

Hart, M., Manadhata, P., & Johnson, R. (2011). Text classification for data loss

prevention. *Lecture Notes in Computer Science,* 18-37. doi:10.1007/978-3-642-22263-4_2

Health Insurance Portability and Accountability Act of 1996, H.R.3103. (1996). Retrieved from http://beta.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal*, *24*, 61-84. doi:10.1111/j.1365-2575.2012.00420.x

Hermanowicz, J. C. (2013). The longitudinal qualitative interview. *Qualitative Sociology*, *36*, 189-208. doi:10.1007/s11133-013-9247-7

Higginbottom, G., Rivers, K., & Story, R. (2014). Health and social care needs of Somali refugees with visual impairment (VIP) living in the United Kingdom: A focused ethnography with Somali people with VIP, their caregivers, service providers, and members of the Horn of Africa Blind Society. *Journal of Transcultural Nursing*, *25*, 192-201. doi:10.1177/1043659613515715

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing*, *30*, 1-19. doi:10.1016/j.intmar.2014.10.001

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information*

& Management, 52, 337-347. doi:10.1016/j.im.2014.12.006

Hoe, J., & Hoare, Z. (2012). Understanding quantitative research: Part 1. *Nursing Standard*, *27*, 52-57. Retrieved from http://nursingstandard.rcnpublishing.co.uk/

Holloway, I., & Wheeler, S. (2013). *Qualitative research in nursing and healthcare* (3rd ed.). Oxford, United Kingdom: John Wiley & Sons

Holtfreter, R. E., & Harrington, A. (2014). Towards a model for data breaches: A universal problem for the public. *International Journal of Public Information Systems*, *10*(1). 40-58. Retrieved from http://www.ijpis.net/ojs/index.php/IJPIS/index

Hood, C. (2011). From FOI world to WikiLeaks world: A new chapter in the transparency story*? Governance*, *24*, 635-638. doi:10.1111/j.1468-0491.2011.01546.x

Hou, W. L., Ko, N. Y., & Shu, B. C. (2013). Recovery experiences of Taiwanese women after terminating abusive relationships: A phenomenology study. *Journal of Interpersonal Violence, 28*, 157-175. doi:10.1177/0886260512448851

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

Hripcsak, G., Bloomrosen, M., FlatelyBrennan, P., Chute, G. C., Cimino, J., Detmer, E. D., . . . Wilcox, B. A. (2013). Health data use, stewardship, and governance: ongoing gaps and challenges: A report from AMIA's 2012 health policy meeting.

Journal of the American Medical Informatics Association, 21, 204-211. doi:10.1136/amiajnl-2013-002117

Hsinchun, C., Chiang, R. L., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly*, *36*, 1165-1188. Retrieved from http://misq.org/

Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a healthcare information exchange: An economic analysis. *Decision Support Systems*, *61*, 1-11. doi:10.1016/j.dss.2013.10.011

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*, 615-660. doi:10.1111/j.1540-5915.2012.00361.x

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54–60. doi:10.1145/1953122.1953142

IBM & Ponemon Institute (2015). *2015 cost of data breach study: United States.* Retrieved from http://www-03.ibm.com/security/data-breach/

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*, 83-95. doi:10.1016/j.cose.2011.10.007

Ioannidis, C., Pym, D., & Williams, J. (2012). Information security trade-offs and

optimal patching policies. *European Journal of Operational Research, 216,* 434-444. doi:10.1016/j.ejor.2011.05.050

Ishak, N. M., & Bakar, A. Y. A. (2014). Developing sampling frame for case study: challenges and conditions. *World Journal of Education*, *4*(3), 29-35. doi:10.5430/wje.v4n3p29

Jawad, M., Butrous, E., Faber, B., Gupta, C., Haggart, C., & Patel, S. (2012). A study to define the international guidelines of ethics concerning electronic medical data. *European Journal of Law and Technology*, *3*(1). Retrieved from http://ejlt.org/article/view/121/206

Jewkes, Y., & Yar, M. (2011). *Handbook of Internet crime*. New York, NY: Routledge.

Johnson, J., Lincke, S. J., Imhof, R., & Lim, C. (2014). A comparison of international information security regulations. *Interdisciplinary Journal of Information, Knowledge, and Management*, *9*, 89-116. Retrieved from http://www.informingscience.org/Journals/IJIKM/Overview

Kapoor, B., Pandya, P., & Sherif, S. J. (2011). Cryptography: A security pillar of privacy, integrity and authenticity of data communication. *Kybernetes, 40,* 1422-1439. doi:10.1108/03684921111169468

Kesh, S., & Raghupathi, W. (2013). Managing information security risks: An examination of multiple risk perspectives. *Journal of American Business Review, Cambridge*, *2*(1), 35-41. Retrieved from http://www.jaabc.com/jabrc.html

Khaleghi, D., Alavi, H. A., & Alimiri, M. (2013). A study on the effects of organizational

structure on success of performance measurement. *Management Science Letters*, *3*, 1611-1614. doi:10.5267/j.msl.2013.05.028

Killawi, A., Khidir, A., Elnashar, M., Abdelrahim, H., Hammoud, M., Elliott, H., ... & Fetters, M. D. (2014). Procedures of recruiting, obtaining informed consent, and compensating research participants in Qatar: findings from a qualitative investigation. *BMC medical ethics*, *15*(1). doi:10.1186/1472-6939-15-9

Kim, B. E. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, *22*(1), 115-126. doi:10.1108/IMCS-01-2013-0005

Kim, H., Xu, Y., & Gupta, S. (2011). Which is more important in Internet shopping, perceived price or trust? *Electronic Commerce Research and Applications*, *11*, 241–252. doi:10.1016/j.elerap.2011.06.003

Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement, and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy & Practice, 13*(5), 66-80. Retrieved from http://www.na-businesspress.com/jmppopen.html

Knorst, A. M., Vanti, A. A., Andrade, R. A. E., & Johann, S. L. (2011). Aligning Information Security with the Image of the Organization and Prioritization Based on Fuzzy Logic for the Industrial Automation Sector. *Journal of Information Systems and Technology Management, 8*, 555-580. doi:10.4301/S1807-17752011000300003

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security, 18*, 316-327. doi:10.1108/09685221011095236

Kuhn, R. J., Ahuja, M., & Mueller, J. (2013). An examination of the relationship of IT control weakness to company financial performance and health. *International Journal of Accounting and Information Management*, *21*, 227-240. doi:10.1108 /IJAIM-12-2011-0042

Kwong, J. P , Kwong, E. J., Posluns, E. C., Fitch, M. I., McAndrew, A., & Vandenbussche, K. A. (2014). The experiences of patients with advanced head and neck cancer with a percutaneous endoscopic gastrostomy tube: A qualitative descriptive study. *Nutrition in Clinical Practice*, *29*, 526-533. doi:10.1177 /088453361453269

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*, 4-13. doi:10.1108 /09685221011035223

Lai, F., Li, D., & Hsieh, C. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*, 353–363. doi:10.1016/j.dss.2011.09.002

Lane, S., & Arnold, E. (2011). Qualitative research: A valuable tool for transfusion medicine. *Transfusion*, *51*, 1150–1153. doi:10.1111/j.1537-2995.2011.03112.x

Langen, T. A., Mourad, T., Grant, B. W., Gram, W. K., Abraham, B. J., Fernandez, D. S., ... & Hampton, S. E. (2014). Using large public datasets in the undergraduate

ecology classroom. *Frontiers in Ecology and the Environment, 12*, 362-363. Retrieved from http://www.frontiersinecology.org/fron/

Lawrence, E. J. (2011). The growth of e-Commerce in developing countries: An exploratory study of opportunities and challenges for SMEs. *International Journal of ICT Research and Development in Africa, 2*(1), 15-28. doi:10.4018 /jictrda.2011010102

Legislative Counsel of California. (2002). *Senate bill no. 1386*. Retrieved from http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill _20020926_chaptered.pdf

Lesk, M. (2014). Staffing for security: Don't optimize. *Security & Privacy, IEEE, 12*(4), 71-73. doi:10.1109/MSP.2014.78

Lewis, N., Campbell, M. J., & Baskin, C. R. (2015). Information security for compliance with select agent regulations. *Health security, 13*, 207-218. doi:10.1089/hs.2014 .0090.

Liao, K., & Chueh, H. (2012). Medical organization information security management based on ISO27001 information security standard. *Journal of Software, 7*, 792-797. doi:10.4304/jsw.7.4.792-797

LinkedIn. (2013). *Company directory*. Retrieved from http://www.linkedin.com/directory /companies

Lips-Wiersma, M., & Mills, A. J. (2014). Understanding the basic assumptions about human nature in workplace spirituality beyond the critical versus positive

divide. *Journal of Management Inquiry, 23*, 148-161. doi:10.1177/1056492613501227

Liu, C. H., Tang, W. R., Wang, H. M., & Lee, K. C. (2013). How cancer patients build trust in traditional Chinese medicine. *European Journal of Integrative Medicine, 5*, 495-500. doi:10.1016/j.eujim.2013.08.003

Liu, Y., Sarabi, A., Zhang, J., Naghizadeh, P., Karir, M., Bailey, M., & Liu, M. (2015). Cloudy with a chance of breach: Forecasting cyber security incidents. In *USENIX Security Symposium*. Retrieved from http://web.eecs.umich.edu/~mingyan/pub/usenix15.pdf

Lo, C. C., & Chen, W. J. (2012). A hybrid information security risk assessment procedure considering interdependences between controls. *Expert Systems with Applications, 39*, 247-257. doi:10.1016/j.eswa.2011.07.015

Lou, J. J., Andrechak, G., Riben, M., & Yong, H. W. (2011). A review of radio frequency identification technology for the anatomic pathology or biorepository laboratory: Much promise, some progress, and more work needed. *Journal of Pathology Informatics, 2*(1), 34. doi:10.4103/2153-3539.83738

Lu, Y. & Ramamurthy, K. (2011). Understanding the link between information technology capability and organizational agility: An empirical examination. *MIS Quarterly, 35*, 931-954. Retrieved from http://www.misq.org/

Madsen, A. K. (2013). Virtual acts of balance: Virtual technologies of knowledge management as co-produced by social intentions and technical limitations.

Electronic Journal of E-Government, 11, 183-197. Retrieved from http://www.ejeg.com/main.html

Mangal, V. (2013). Systems theory and social networking: Investigation of systems theory principles in web 2.0 social network systems. *International Journal of Business and Commerce*, *3,* 117-135. Retrieved from www.ijbcnet.com

Mansell, R., & Steinmueller, W. E. (2013). Copyright infringement online: The case of the Digital Economy Act judicial review in the United Kingdom. *New Media & Society*, *15,* 1312-1328. doi:10.1177/1461444812470429

Manuj, I., & Pohlen, T. L. (2012). A reviewer's guide to the grounded theory methodology in logistics and supply chain management research. *International Journal of Physical Distribution & Logistics Management*, *42*, 784-803. doi:10.1108/09600031211269758

Marshall, C., & Rossman, B. G. (2010). *Designing qualitative research.* Thousand Oaks, CA: Sage Publications, Inc.

Martin, C. E., & Meyer, W. J. H. (2012). Organizational and behavioral factors that influence knowledge retention. *Journal of Knowledge Management*, *16*, 77-96. doi:10.1108/13673271211198954

Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, *34*, 1-13. doi:10 .1016/j.ijinfomgt.2013.06.002

Mellado, D., & Rosado, G. D. (2012). An overview of current information systems security challenges and innovations. *Journal of Universal Computer Science, 18*, 1598-1607. Retrieved from http://www.jucs.org

Merriam, S. B. (2014). *Qualitative research: A guide to design and implementation*. San Francisco, CA: John Wiley & Sons.

Miner-Romanoff, K. (2012). Interpretive and critical phenomenological crime studies: A model design. *The Qualitative Report*, *17*, 1-32. Retrieved from http://www.nova.edu/ssss/QR/

Mishra, S. (2015). Organizational objectives for information security governance: A value focused assessment. *Information & Computer Security*, *23*, 122-144. doi:10.1108/ICS-02-2014-0016

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*, 139-138. Retrieved from http://cluteinstitute.com/ojs/index.php/IJMIS

Mitleton-Kelly, E. (2011). A complexity theory approach to sustainability. *The Learning Organization*, *18*, 45-53. doi:10.1108/09696471111095993

Mittal, Y., Roy, D., & Saxena, D. (2010). A knowledge management model to improve information security. *International Journal of Computer Science Issues*, *7*(6), 105-108. Retrieved from http://ijcsi.org/

Min, H., Lim, Y. K., & Park, J. W. (2015). Integrating X-ray technologies with intelligent transportation systems for enhancing the international maritime security. *International Journal of Logistics Systems and Management*, *22*, 1-14. doi:10.1504/IJLSM.2015.070888

Modi, S. B., Wiles, M. A., & Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management*, *35*, 21-39. doi:10.1016/j .jom.2014.10.003

Moeller, L., & Valentinov, V. (2012). The commercialization of the nonprofit sector: A general systems theory perspective. *Systemic Practice & Action Research*, *25*, 365-370. doi:10.1007/s11213-011-9226-4

Mohammed, D., & Mariani, R. (2014). An evaluation of the cybersecurity policies for the United States health & human services department: Criteria, regulations, and improvements. *International Journal of Business and Social Research*, *4*(4), 1-7. Retrieved from http://thejournalofbusiness.org/index.php/site

Moshirian, F. (2011). The global financial crisis and the evolution of markets, institutions and regulation. *Journal of Banking & Finance 35*, 502–511. doi:10.1016/j .jbankfin.2010.08.010

Mostovicz, E. I., Kakabadse, A., & Kakabadse, N. (2011). The four pillars of corporate responsibility: Ethics, leadership, personal responsibility and trust. *Emerald Group Publishing Limited*, *11*, 489-500. doi:10.1108/14720701111159307

Muskat, M., Blackman, D., & Muskat, B. (2012). Mixed methods: Combining expert interviews, cross-impact analysis and scenario development. *The Electronic Journal of Business Research Methods*, *10*, 9-21. Retrieved from http://www .ejbrm.com/main.html

Myers, G., & Lampropoulou, S. (2013). What place references can do in social research interviews. *Discourse Studies*, *15*, 333-351. doi:10.1177/1461445613480589

National Institute of Standards Technology. (2011). *2010 computer security division annual report.* Retrieved from http://csrc.nist.gov/publications/nistir/ir7751/nistir-7751_2010-csd-annual-report.pdf

Naseri, A., & Azmoon, O. (2012). Proposition of model for CSIRT: Case study of telecommunication company in a province of Iran. *International Journal of Computer Science Issues*, *9*, 156-160. Retrieved from www.ijcsi.org

Nawafleh, S. A., Hasan, M. Y., Nawafleh, Y., & Fakhouri, S. A. A. R. (2013). Protection and defense against sensitive data leakage problem within organizations. *European Journal of Business and Management*, 5(23), 87-95. Retrieved from www.iiste.org

Nishimura, A., Carey, J., Erwin, P. J., Tilburt, J. C., Murad, M. H., & McCormick, J. B. (2013). Improving understanding in the research informed consent process: a systematic review of 54 interventions tested in randomized control trials. *BMC Medical Ethics*, *14*. doi:10.1186/1472-6939-14-28

Onwuegbuzie, A. J., & Hwang, E. (2014). Interviewing successfully for academic

positions: A framework for candidates for asking questions during the interview process. *International Journal of Education, 6*, 98-113. doi:10.5296/ije.v6i2.4424

Onwuegbuzie, J. A., Leech, L. N., & Collins, T. M. K. (2012). Qualitative analysis techniques for the review of the literature. *The Qualitative Report, 17*, 1-28. Retrieved from http://www.nova.edu/ssss/QR/

Open Security Foundation. (2014). *Datalossdb*. Retrieved from http://datalossdb.org/

Orser, B. J., Elliott, C., & Leck, J. (2011). Feminist attributes and entrepreneurial identity. *Gender in Management: An International Journal*, 26, 561-589. doi:10.1108/17542411111183884

O'Reilly, M., & Parker, N. (2012). Unsatisfactory saturation: a critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, *13*, 190–197. doi:10.1177/1468794112446106

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2013). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*. doi:10.1007/s10488-013-0528-y

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*, 117-129. doi:10.1177/1555343415575152

Patil, R., Grantham, K., & Steele, D. (2012). Business risk in early design: A business

risk assessment approach. *Engineering Management Journal*, *24*(1), 35-46. Retrieved from http://www.asem.org/asemweb-emj.html

PCI Security Standards Council. (2015). *Payment card industry (PCI) data security standard*. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Petty, N. J., Thomson, O. P., & Stew, G. (2012). Ready for a paradigm shift? Part 2: Introducing qualitative research methodologies and methods, *Manual Therapy*, *17*, 378-384. doi:10.1016/j.math.2012.03.004

Peres, G., & Pielmus, C. (2011). The USA immigration policy, border surveillance and control. *Journal of Criminal Investigation*, *4*(1), 99-105. Retrieved from http://www.cij.ro/arhiva_eng.html

Perkmann, M., & Schildt, H. (2015). Open data partnerships between firms and universities: The role of boundary organizations. *Research Policy*, *44*, 1133-1143. doi:10.1016/j.respol.2014.12.006

Pezalla, A. E., Pettigrew, J., & Miller-Day, M. (2012). Researching the researcher-as-instrument: an exercise in interviewer self-reflexivity. *Qualitative Research*, *12*(2), 165-185. doi:10.1177/1468794111422107

Phelan, S. K., & Kinsella, E. A. (2013). Picture this... safety, dignity, and voice - ethical research with children practical considerations for the reflexive researcher. *Qualitative Inquiry*, *19*, 81-90. doi:10.1177/1077800412462987

Pilnick, A., & Swift, J. A. (2011). Qualitative research in nutrition and dietetics:

assessing quality. *Journal of Human nutrition and Dietetics*, *24*, 209-214. doi:10.1111/j.1365-277X.2010.01120.x

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, *63*, 539-569. doi:10.1146/annurev-psych-120710-100452

Popov, A., & Udell, G. F. (2012). Cross-border banking, credit access, and the financial crisis. *Journal of International Economics*, *87*(1), 147-161. doi:10.1016/j.jinteco .2012.01.008

Posey, C., Bennett, J. R., & Roberts, L. T. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, *30*, 486–497. doi:10.1016/j.cose.2011 .05.002

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, *51*, 551-567. doi:10.1016/j.im.2014.03.009

Posukhova, O., & Zayats, P. (2014). Social engineering as a mechanism of optimization of human resources management in Rostov region. *Middle-East Journal of Scientific Research*, *19*, 424-428. doi:10.5829/idosi.mejsr.2014.19.3.13688

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*,

34, 757-778. Retrieved from http://www.misq.org

Pushkarskaya, H., & Marshall, I. M. (2010). Family structure, policy shocks, and family business adjustment choices. *Journal of Family and Economic Issues, 31*, 414-426. doi:10.1007/s10834-010-9231-2

Price Waterhouse Cooper. (2013). *2013 information security breaches survey*. Retrieved from www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf

QSR International. (2014). *NVivo10.* Retrieved from http://www.qsrinternational.com/

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management, 8,* 238-264. doi:10.1108/11766091111162070

Rabionet, S. E. (2011). How I learned to design and conduct semi-structured interviews: An ongoing and continuous journey. *Qualitative Report, 16*, 563-566. Retrieved from http://www.nova.edu/ssss/QR/QR16-2/rabionet.pdf

Rahman, N. H. B., & Choo, K. K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security, 49*, 45-69. doi:10.1016/j.cose.2014.11.006

Ranjan, S., Maurya, M., Malviya, A., Yadav, R., Gupta, R., Mishra, M., & Rai, S. (2012). Building an information security infrastructure - A comprehensive framework towards a robust, resilient, and dependable infrastructure. *International Journal of Computer Science Issues*, *9*, 414-419. Retrieved from http://ijcsi.org/

Reddy, C. K. K., Samshabad, R. R., Prasanth, S. K., & Naik, S. L. (2012). Cloud specific issues and vulnerabilities solutions. *International Journal of Scientific and*

Engineering Research, 3(7), 1-6. Retrieved from http://www.ijser.org/

Reid, B. (2013). A business review of the ethics and law of non-disclosure agreements. *Mustang Journal of Business and Ethics*, *4*, 72-85. Retrieved from http://mustangjournals.com/index.html

Renn, O., & Klinke, A. (2013). A framework of adaptive risk governance for urban planning. *Sustainability*, *5*, 2036-2059. doi:10.3390/su5052036

Resnik, D. B., Miller, A. K., Kwok, R. K., Engel, L. S., & Sandler, D. P. (2015). Ethical issues in environmental health research related to public health emergencies: reflections on the GuLF study. *Environmental health perspectives*, *123,* A227–A231. doi:10.1289/ehp.1509889

Roberts, T. (2013). Understanding the research methodology of interpretative phenomenological analysis. *British Journal of Midwifery*, *21*, 215-218. Retrieved from http://www.britishjournalofmidwifery.com

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, *11*, 74-104. doi:10.1111/jels.12035

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management, 30*, 256-286. doi:10 .1002/pam.20567

Ryan, J. C. H. J., Mazzuchi, A. T., Ryan, J. D., Cruz, J. L., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research, 39*, 774–784. doi:10.1016/j.cor.2010.11.013

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78. doi:10.1016/j.cose.2015.05.012

Saidani, M., Shibani, A., & Alawadi, K. (2013). Managing data security in the United Arab Emirates. *Prime Research on Education*, *3*, 458- 464. Retrieved from http://www.primejournal.org/PRE/

Saini, H., Rao, S. Y., & Panda, C. T. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209. Retrieved from http://www.ijera.com/

Sandoval-Almazan, R., & Gil-Garcia, J. R. (2012). Are government internet portals evolving towards more interaction, participation, and collaboration? Revisiting the rhetoric of e-government among municipalities. *Government Information Quarterly*, *29*, S72-S81. doi:10.1016/j.giq.2011.09.004

Sangestani, G., & Khatiban, M. (2013). Comparison of problem-based learning and lecture-based learning in midwifery. *Nurse education today*, *33*, 791-795. doi:10.1016/j.nedt.2012.03.010

Saracho, O. N. (2013). Writing research articles for publication in early childhood education. *Early Childhood Education Journal*, *41*, 45-54. doi:10.1007/s10643-012-0564-3

Sarbanes-Oxley Act of 2002, H.R.3763. (2002). Retrieved from http://beta.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf

Savola, M. J. (2014). Towards measurement of security effectiveness enabling factors in software intensive systems. *Lecture Notes on Software Engineering*, *2*, 104-109. doi:10.7763/LNSE.2014.V2.104

Sehgal, K. N., Sohoni, S., Xiong, Y., Fritz, D., Mulia, W, & Acken, M. J. (2011). A cross section of the issues and research activities related to both information security and cloud computing, *IETE Technical Review*, *28*, 279-291. doi:10.4103/0256-4602.83549

Setia, P., Venkatesh, V., & Joglekar, S. (2013). Leveraging digital technologies: How information quality leads to localized capabilities and customer service performance. *MIS Quarterly, 37*, 565-590. Retrieved from http://misq.org/

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, 55, 349-356.doi:10.1016/j.bushor.2012.02.004

Shirtz, D., & Elovici, Y. (2011). Optimizing investment decisions in selecting information security remedies. *Information Management & Computer Security, 19*, 95-112. doi:10.1108/09685221111143042

Slaughter, J., & Rahman, M. S. (2011). Information security plan for flight simulator applications. *International Journal of Computer Science & Information Technology*, *3*(3), 1-15. doi:10.5121/ijcsit.2011.3301

Smith, J., & Firth, J. (2011). Qualitative data analysis: the framework approach. *Nurse researcher, 18*, 52-62. doi:10.7748/nr2011.01.18.2.52.c8284

Smith, R. A., Colombi, M. J., & Wirthlin, R. W. (2013). Rapid development: A content

analysis comparison of literature and purposive sampling of rapid reaction projects. *Procedia Computer Science, 16*, 475-482. doi:10.1016/j.procs.2013.01.050

Snyder, C. (2012). A case study of a case study: Analysis of a robust qualitative Research methodology. *Qualitative Report, 17*, 1-21. Retrieved from http://www.nova.edu/ssss/QR/QR17/snyder.pdf

Sun, J., Ahluwalia, P., & Koong, S., K (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems, 111*, 570–588. doi:10.1108/02635571111133551

Sung, P., & Su, C. (2013). Using system dynamics to investigate the effect of the information medium contact policy on the information security management. *International Journal of Business and Management, 8*(12), 83-96. doi:10.5539/ijbm.v8n12p83

Susanto, H., Almunawar, M. N., & Tuan, C. Y. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences, 11*, 23–29. Retrieved from http://www.ijens.org/

Susanto, H., Almunawar, M. N., & Tuan, C. Y. (2012). Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology, 2*(1), 67-75. Retrieved from http://www.sciencepubco.com/index.php/IJET

Susanto, H., Almunawar, N. M, Tuan, C. Y., Aksoy, S. M., & Syam, P. W. (2011).

Integrated solution modeling software: A new paradigm on information security review and assessment. *International Journal of Science and Advanced Technology*, *1*(10), 90-99. Retrieved from http://www.ijsat.com/

Tamboukou, M. (2011). 'Portraits of moments': Visual and textual entanglements in narrative research. *Current Narratives*, *3*, 3-13. Retrieved from http://ro.uow.edu .au/currentnarratives/

Teh, P. L., Ahmed, P. K., & D'Arcy, J. (2015). What drives information security policy violations among banking employees: Insights from neutralization and social exchange theory. *Journal of Global Information Management*, *23*(1), 44-64. doi:10.4018/jgim.2015010103

Thomas, E., & Magilvy, K., J. (2011). Qualitative rigor or research validity in qualitative research. *Journal for Specialists in Pediatric Nursing*, *16*, 151–155. doi:10.1111/j.1744-6155.2011.00283.x

Thompson, A. L., Black, E., Duff, W. P., Black, P. N., Saliba, H., & Dawson, K. (2011). Protected health information on social networking sites: Ethical and legal Considerations. *Journal of Medical Internet Research*, *13*(1), 8. doi:10.2196 /jmir.1590

Tofan, C. D. (2011). Information security standards. *Journal of Mobile, Embedded and Distributed Systems, 3*, 128-145. Retrieved from http://jmeds.eu/

Tracy, S. J. (2012). The toxic and mythical combination of a deductive writing logic for inductive qualitative research. *Qualitative Communication Research*, *1*(1), 109-

141. doi:10.1525/qcr.2012.1.1.109

Trenholm, S., & Ferlie, E. (2013). Using complexity theory to analyse the organisational response to resurgent tuberculosis across London. *Social Science & Medicine*, *93*, 229-237. doi:10.1016/j.socscimed.2012.08.001

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness Programs. *Computers & Security*, *52*, 128–141. doi:10.1016/j.cose.2015.04.006

Tsohou, A., Kokolakis, S., Lambrinoudakis, C., & Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. *Information Management & Computer Security*, *18*, 350-365. doi:10.1108/09685221011095263

U.K. The National Archives. (2010). *Digital economy act 2010*. Retrieved from http://www.legislation.gov.uk/ukpga/2010/24/notes/contents

U.S. Department of Health & Human Services. (1979, April). Ethical principles and guidelines for the protection of human subjects of research. *Human Subjects Research (45 CFR 46). The Belmont Report.* Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Vaccaro, A. (2012). Campus microclimates for LGBT faculty, staff, and students: An exploration of the intersections of social identity and campus roles. *Journal of Student Affairs Research and Practice, 49*, 429-446. doi:10.1515/jsarp-2012-6473

Venkatesh, V., Brown, A. S., & Bala, H. (2013). Bridging the qualitative–quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*, 25-54. Retrieved from http://www.misq.org/

von Bertalanffy, L., Juarrero, A., & Rubino, A., C. (2008). An outline of general system theory. *Emergence: Complexity & Organization*, *10*, 103-123. Retrieved from http://www.isce.edu/index-2.html

von Bertalanffy, L. (1968). *General systems theory: Foundations*, *development*, *application* (Revised ed.). New York, NY: George Braziller.

Wagstaff, C. R., Hanton, S., & Fletcher, D. (2013). Developing emotion abilities and regulation strategies in a sport organization: An action research intervention. *Psychology of Sport and Exercise*, *14*, 476-487. doi:10.1016/j.psychsport.2013.01.006

Wallace, L., Lin, H., & Cefaratti, M. A. (2011). Information security and Sarbanes-Oxley compliance: An exploratory study. *Journal of Information Systems, 25*(1), 185–211. doi:10.2308/jis.2011.25.1.185

Wara, Y. M., & Singh, D. (2015). A guide to establishing computer security incident response team (CSIRT) for national research and education network (NREN). *African Journal of Computing & ICT*, *8*(2), 1-8. Retrieved from http://www.ajocict.net/

Wattanasuwan, K. (2012). Narrative: An alternative way to gain consumer insights. *Journal of American Academy of Business, Cambridge*, *18*(1), 130-136. Retrieved

from http://www.jaabc.com

White, G. L., Hewitt, B., & Kruck, S. E. (2013). Incorporating global information security and assurance in I.S. education. *Journal of Information Systems Education*, *24*, 11-16. Retrieved from http://jise.org/

Whitman, E. M., & Mattord, J., H. (2012). Information security governance for the non-security business executive. *Journal of Executive Education, 11*, 97-111. Retrieved from http://digitalcommons.kennesaw.edu/jee/

White, D. E., Oelke, N. D., & Friesen, S. (2012). Management of a large qualitative data set: Establishing trustworthiness of the data. *International Journal of Qualitative Methods, 11*, 244-258. Retrieved from http://socialiststudies.com/index.php/IJQM/index

Wierenga, D., Engbers, H. L, van Empelen, P., Hildebrandt, H. V., & van Mechelen, W. (2012). The design of a real-time formative evaluation of the implementation process of lifestyle interventions at two worksites using a 7-step strategy. *BMC Public Health*, *12*, 1-11. doi:10.1186/1471-2458-12-619

Wilkerson, M. J., Iantaffi, A., Grey, J. A., Bockting, W. O., & Simon Rosser, B. R. (2014). Recommendations for internet-based qualitative health research with hard-to-reach populations. *Advancing Qualitative Methods, 24*, 561-574. doi:10.1177/1049732314524635

Williamson, S., Twelvetree, T., Thompson, J., & Beaver, K. (2012). An ethnographic study exploring the role of ward based advanced nurse practitioners in an acute

medical setting. *Journal of Advanced Nursing, 68,* 1579-1588. doi:10.1111/j.1365-2648.2012.05970.x

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1–20. Retrieved from http://misq.org/

Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring an information security awareness program. *The Review of Business Information Systems, 15,* 9-21. Retrieved from http://journals.cluteonline.com/index.php/RBIS

Wynn, J., & Williams, C. K. (2012). Principles for conducting critical realist case study research in information systems. *MIS Quarterly, 36,* 787-810. Retrieved from http://www.misq.org

Yallapragada, R. R., Roe, C. W., & Toma, A. G. (2012). Accounting fraud, and white-collar crimes in the United States. *Journal of Business Case Studies, 8,* 187-192. Retrieved from http://cluteonline.com/journals/index.php/JBCS/index

Yang, J. S., Lee, H. J., Park, M. W., & Eom, J. H. (2015). Security threats on national defense ICT based on IoT. *Advanced Science and Technology Letters, 97,* 94-98. doi:10.14257/astl.205.97.16

Yang, O. Y., Shieh, H., & Tzeng, G. (2013). A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. *Information Sciences, 232,* 482-500. doi:10.1016/j.ins.2011.09.012

Yaokumah, W. (2014). Information security governance implementation within Ghanaian

industry sectors: An empirical study. *Information Management & Computer Security*, *22*, 235-250. doi:10.1108/IMCS-06-2013-0044

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: the effect of contingency factors. *Journal of Information Technology*, *26*, 60–77. doi:10.1057/jit.2010.4

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

Yin, K. R. (2011). *Qualitative research from start to finish*. New York, NY: The Guilford Press.

Zafar, H., Ko, M. S., & Osei-Bryson, K. M. (2015). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers*, 1-11. doi:10.1007/s10796-015-9562-5

Zafar, H., Ko, M., & Osei-Bryson, K. (2012). Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal*, *25*(1), 21-37. doi:10.4018/irmj.2012010102

Zamawe, F. C. (2015). The Implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, *27*, 13-15. doi:10.4314/mmj.v27i1.4

Zhang, X., van Donk, P. D., & van der Vaart, T. (2011). Does ICT influence supply chain management and performance? A review of survey-based research. *International Journal of Operations & Production Management*, *31*, 1215-1247. doi:10.1108

/01443571111178501

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems*, *30*, 123-152. Retrieved from http://www.jmis-web.org/issues

Zhao, J. J., & Zhao, Y. S. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, *27*, 49-56. doi:10.1016/j.giq.2009.07.004

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*, 583–592. doi:10.1016/j.future.2010.12.006

Appendix A: Ponemon Copyright Permission

Betsy Froling <blabonte@ponemon.org> Tue, Sep 15, 2015 at 6:55 PM
To: Fedinand Kongnso <fedinand.kongnso@waldenu.edu>
Cc: Susan Jayson <research@ponemon.org>

Hello Fedinand,

Thank you for your interest in our research. You have permission to quote with proper attribution. In your attribution, please identify IBM as the sponsor of the study.

Kind regards,

Betsy Froling
2308 U.S. 31 North
Traverse City, MI 49686
231.938.9900

On Sep 15, 2015, at 7:37 PM, Fedinand Kongnso <fedinand.kongnso@waldenu.edu> wrote:

Hello,

I am just writing to follow-up on my request below.

Best Regards,
Fedinand Kongnso

On Fri, Sep 11, 2015 at 4:05 PM, Fedinand Kongnso <fedinand.kongnso@waldenu.edu> wrote:
To whom this may concern,

My name is Fedinand Kongnso and I am completing my doctoral studies at Walden University. I am writing to obtain permission to quote/reuse Figure 14, in the 2015 Cost of Data Breach Study: United States report, in my doctoral dissertation.

Sincerely,
Fedinand Kongnso

Appendix B: Human Subject Research Certificate of Completion

Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Fedinand Kongnso** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 11/12/2011

Certification Number: 801339

Appendix C: Interview Protocol and Questions

Interview Protocol

A. Introduce self to participant.

B. Verified receipt and/or responds to consent form, answer for any questions and/or concerns of participant.

C. Get confirmation and acknowledgement that interview is being recorded.

D. Turn on recording device.

E. Thank participant for accepting to participate in the study.

F. Start interview with question #1; follow through to final question.

G. End interview and discuss member checking with participant.

H. Thank the participant for partaking in the study. Confirm the participant has contact information for follow up questions and concerns.

I. End protocol.

Interview Questions

1. How long have you been involved in the design or implementation of security policies and incident response strategies?
2. What has been your experience dealing with data security challenges?
3. What are some of the challenges when responding to data security breaches?
4. What is the value of incident response strategies for your organization?
5. Why do some technology executives lack the skills needed to minimize data

security breaches?

6. What are the management skills needed by technology executives to assist in minimizing a data breach?
7. What are the technical skillsets technology executives need to improve data security prevention within corporations?
8. How can technology executives champion best practice data security policies within corporations?
9. What are some recommendations that may assist leaders in implementing proactive data security measures at organizations?
10. What are some recommendations that might assist a firm to improve incident response after a data security breach?
11. What additional information can you add that would be valuable to the study?

Appendix D: Invitation Letter

Dear _____,

My name is Fedinand Kongnso, and I am a doctoral candidate at Walden University working on completing my Doctor of Business Administration degree. I am conducting a research study on what best practices technology leaders need to minimize data breaches for increased business performance.

I am inviting technology executives and technical staff within an organization to participate in this study. I am aware of the time constraints in doing interviews, and I will be asking only about 45 minutes of your time. I believe your participation and knowledge on information security and data breaches will contribute significantly to this research and available literature.

If you agree to participant in the study, you will receive a summary of the findings, which will allow you to learn about some of the best practices utilized by organizations to minimize data security breaches.

Your confidentiality will be protected throughout this study. I will provide you with a consent form via e-mail that contains additional information about the study and interview questions prior to the interview. If interested in participating in the study, please let me know of a convenient date/time and contact information for a phone interview.

Please contact me at (608) 498-4122 or via e-mail fedinand.kongnso@waldenu.edu with any questions.

Sincerely,
Fedinand Kongnso

Appendix E: Consent Form

CONSENT FORM

You are invited to take part in a research study of what best practices do technology leaders use to minimize data security breaches for increased business performance. The researcher is inviting technology executives and technical staff, who are members of a computer security incident response teams (CSIRT) at a banking firm in Northcentral United States and a local government agency in Southcentral United States to participate in the study. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part.

A researcher named Fedinand J. Kongnso is conducting this study. Fedinand is a doctoral student at Walden University.

Background Information:

The purpose of this study is to explore best practices needed by technology leaders to minimize data security breaches for increased business performance.

Procedures:

If you agree to be in this study, you will:

- Select a time and date convenient for an interview.
- Be interviewed via telephone, for approximately 45 minutes.
- The researcher will provide a summary of your responses to interview questions to ensure accurate interpretation.

Here are some sample questions:

- What are some of the challenges when responding to data security breaches?
- What is the value of incident response strategies for your organization?
- Why do some technology executives lack the skills needed to minimize data security breaches?
- What are the management skills needed by technology executives to assist in minimizing a data breach?

Voluntary Nature of the Study:

This study is voluntary. The researcher will respect your decision of whether or not you choose to be in the study. No one at your firm will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind during or after the study. You may stop at any time. You will also not waive any legal rights.

Risks and Benefits of Being in the Study:

As part of this type of study, you may encounter minor discomforts, same as with your daily activities, such as stress. Being in this study would not pose any risk to your safety or wellbeing. Due to the sensitive nature of the interview questions, the researcher will not disclose any participant information and their responses to anyone.

The findings in this study might benefit organizations in implementing best practice security strategies and policy development tools to protect consumer information against identity theft or unknown threats.

Payment:

Participants will not receive any financial incentives to participate in this study.

Privacy:

All information you provide be confidential. The researcher will not use your personal information for any purposes outside of this study, and your name will not be included, as well. All interviews will be audio-recorded and stored on an encrypted drive securely kept in a safety box. The researcher will be the only one with access to the safe. Data collected during this study will be kept for 5 years, as required by the university. After 5 years, all data will be permanently destroyed.

Contacts and Questions:

If you any questions or concerns later, you may contact the researcher at (XXX) XXX-XXXX or XXXXX@XXXXXXX. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 1-800-925-3368, extension 3121210. Walden University's approval number for this study is **08-01-14-0084492** and it expires on **July 31, 2015.**

You may print or keep a copy of this consent form for your records.

Statement of Consent:

I have read the above information, and I feel I understand the study well enough to make a decision about my involvement. By replying to the e-mail with the words 'I Consent', I am agreeing to the terms described above.

Appendix F: Gartner Copyright Permission

On Wed, Aug 12, 2015 at 4:13 PM, Pettey,Christy <Christy.Pettey@gartner.com> wrote:

Hi Ferdinand,
I was forwarded your request. You have permission to cite and use Figure 1 Gartner's Top 10 Technology Trends for 2015 in my doctoral study.

Thanks,
Christy

Christy Pettey
Director, Public Relations
Gartner
Tel: 1 408 709 8124
Press Hotline: 1 408 709 8220
E-mail: christy.pettey@gartner.com
Web site: http://www.gartner.com

From: Fedinand Kongnso [mailto:fedinand.kongnso@waldenu.edu]
Sent: Monday, August 10, 2015 9:57 PM
To: Quote Requests
Subject: Copyright permission

Hello,

Thanks for the call this afternoon about my request for copyright permission.

The publication I am looking at is the Research Guide: The Top 10 Strategic Technology Trends for 2015, https://www.gartner.com/doc/2966917?srcId=1-3132930191.

I would like to cite and use Figure 1. Gartner's Top 10 Technology Trends for 2015 in my doctoral study.

Best Regards,
Fedinand Kongnso