2017

Strategies to Minimize the Effects of Information Security Threats on Business Performance

Stella Ifeyinwa Okoye
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Stella Okoye

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. Gregory Uche, Committee Chairperson, Doctor of Business Administration Faculty

Dr. John Hannon, Committee Member, Doctor of Business Administration Faculty

Dr. Diane Dusick, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

Strategies to Minimize the Effects of Information Security Threats on Business Performance

by

Stella Ifeyinwa Okoye

MBA, University of Bradford, 2012

MSc, Nnamdi Azikiwe University, Awka, Nigeria, 1992

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

July 2017

Abstract

Business leaders in Nigeria are concerned about the high rates of business failure and economic loss from security incidents and may not understand strategies for reducing the effects of information security threats on business performance. Guided by general systems theory and transformational leadership theory, the focus of this exploratory multiple case study was to explore the strategies small and medium-sized enterprise (SME) leaders use to minimize the effects of information security threats on business performance. Semistructured interviews were conducted with 5 SME leaders who worked in SME firms that support oil and gas industry sector in Port Harcourt, Nigeria, had a minimum of 2 years experience in a leadership role, and had demonstrable strategies for minimizing the effects of information security threats in a SME. The thematic analysis of the interview transcripts revealed 10 strategies for reducing the effects of information security threats: network security, physical security, strong password policy, antivirus protection and software update, information security policy, security education training and awareness, network security monitoring and audit, intrusion detection, data backup, and people management. The findings may contribute to social change by providing SME leaders with more insight about strategies to minimize the effects of information security threats on business performance. The improved business performance can increase the flow of funds into the local economy and allow community leaders to provide social services to residents.

Strategies to Minimize the Effects of Information Security Threats on Business Performance

by

Stella Ifeyinwa Okoye

MBA, University of Bradford, 2012

MSc, Nnamdi Azikiwe University, Awka, Nigeria, 1992

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

July 2017

Dedication

To God be the glory for His abundant grace and mercy throughout my doctoral program. I dedicate my doctoral study to my family: Sylvester, Somtoochukwu, and Adunife. Togetherness in unity and trust, we can weather the storm to attain infinite goals.

Acknowledgments

My sincere gratitude to faculty, family members, and friends who supported and helped me throughout this journey to obtain my doctoral degree. I would like to specially thank my committee chair and mentor, Dr, Gregory Uche, for the guidance, respect, exemplary leadership, and inspiration throughout the doctoral study process. My special thanks to my second committee chair, Dr. John Hannon, and to my URR, Dr. Diane Dusick, for their guidance and support. Your constructive feedback and comments during the doctoral study review process to ensure that my study conform to the standards of Walden University is a hallmark of your professional excellence and I remain grateful for the knowledge share. Special thanks to the program director, Dr. Freda Turner, for the assurance of continued faculty support.

To my husband, Sylvester, who has been of immense support and care; thank you for understanding and I remain indebted to you for the many sacrifices you have made to see that I complete this journey. To my children, Somtoochukwu and Adunife, who believed and cheered me through this doctoral study process, I profess my unconditional love and pray you to reach for the stars. The support from all of you provided me with the strength and encouragement to initiate and accomplish my doctoral goal.

A special thanks to my friends, colleagues, and classmates. Thank you Ngozi Kay Okoro, Chinwe Bello, Amaka Ani, Ebele Anagor, and Ngozi Nnebe for your encouraging words and prayers.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

SMEs face the risk of cyber attack, data fraud, and theft of business information systems, and breakdown of critical information infrastructure (Green, 2015). SME leaders sometimes fail to adjust to the rapidly changing information technology (IT) systems and networks to safeguard business information systems (Bahl & Wali, 2014), resulting in an estimated financial loss of 37% from security incidents (Bojanc & Jerman-Blazic, 2013). Cyber attacks against SMEs in the United States increased from 27% in 2009 to 63% in 2010 (Rahman & Lackey, 2013). Additional research is needed in information security management given the frequent media report of cyber security hacking, loss of company trade secrets, theft of sensitive research and development information, and data loss. To mitigate the increasing threats to information security, SME leaders should understand the strategies needed to minimize the effects of information security threats on business performance.

Background of the Problem

Information is the building block of sustainable business (Cai, Chen, & Bose, 2013). Organizational leaders, including SME leaders, use the Internet for information storage and communication and use the World Wide Web to connect people (Balasubramanian, Jagannathan, & Natarajan, 2014). Enhanced access to data and applications is increasing security threats and opportunities for cyber criminals to exploit the vulnerable and unsuspecting computer users (Vidalis & Angelopoulou, 2013). The high-average cost of security breaches that SMEs experience in the United Kingdom increased from £150,000 in 2014 to £311,000 in 2015 (Department for Business, Innovation & Skills, 2015).

Researchers addressed the preservation of confidentiality, integrity, and availability of information resources to control information security using the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002 (Disterer, 2013; Mesquida & Mas, 2015; VonSolms & VanNiekerk, 2013; Webb, Maynard, Ahmad, & Shanks, 2014). Some researchers (e.g., Chatterjee, Sarker, & Valacich, 2015; Montesdioca & Macada, 2015) related the behavior of users to the business investments in information security training and awareness programs. Gaps exist regarding strategies to reduce the effects of information security threats on business performance. The aim of this qualitative exploratory multiple case study was to explore the strategies SME leaders use to minimize the effects of information security threats on business performance.

Problem Statement

SME leaders face challenges coping with rapidly evolving information security threats (Webb, Maynard, et al., 2014) and lack adequate situation awareness regarding information security management risks (Safa, Von Solms, & Furnell, 2016; Webb, Ahmad, Maynard, & Shanks, 2014). The estimated average total organizational cost of data security breaches in the United States in 2016 was $7.01 million (IBM & Ponemon Institute, 2016). The general business problem was that cybercrime losses can affect the sustainability of a business organization. The specific business problem was that some

SME leaders lack strategies to minimize the effects of information security threats on business performance.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies SME leaders use to minimize the effects of information security threats on business performance. The population for the study consisted of five leaders in SME firms that support the oil and gas industry sector in the city of Port Harcourt, Nigeria who have successfully developed and implemented strategies for minimizing the effects of information security threats in their businesses. The data from this study might provide SME leaders with an in-depth understanding of the strategies that could help reduce the effects of information security threats on business performance. Implications for positive social change include business improvement, which could increase the flow of funds into the local economy and allow community leaders to build schools, health centers, and libraries for residents.

Nature of the Study

The qualitative research method was a viable choice for this study because the goal was to explore strategies that successful SME leaders use to minimize the effect of information security threats. A qualitative approach was appropriate because the method enabled me to use open-ended questions to explore the details of the strategies successful SME leaders use to minimize the effects of information security threats on business performance. Quantitative research method was not appropriate because I did not wish to examine whether a relationship or differences exist among variables (Bahl & Wali, 2014;

Runhaar, ten Brinke, Kuijpers, Wesselink, & Mulder, 2013). Researchers use closed questions and collect statistical data and test hypotheses in quantitative research (Lunde, Heggen, & Strand, 2013). The goal in this study was not to determine a relationship or statistical difference, but to explore successful information security strategies.

Researchers use the qualitative research method to investigate the meaning of a phenomenon (Gioia, Corley, & Hamilton, 2013; Nelson & Evans, 2014; Uluyol & Akci, 2014). The qualitative method was appropriate for this study because the purpose of the investigation was to explore information security strategies. Mixed methods research approach is a combination of qualitative and quantitative methods in one study (Archibald, 2016; Maxwell, 2016). Researchers use the mixed methods approach to examine and explore a business problem.

The fundamental assumption in mixed methods research is that collecting diverse types of data would provide better answers to the research questions (Abro, Khurshid, & Aamir, 2015; Caruth, 2013; Frels & Onwuegbuzie, 2013; Venkatesh, Brown, & Bala, 2013). A mixed methods approach was not appropriate for this study because the intent of the investigation was not to collect diverse types of data but to explore information security strategies. The purpose of this doctoral study was to explore strategies that successful SME leaders use to minimize the effects of information security threats on business performance, which made the qualitative method the most appropriate research method for this study.

Case study research was a useful framework for exploring contemporary phenomena within real-life settings (Cronin, 2014; Dasgupta, 2015; Henry & Foss, 2015;

Morse & McEvoy, 2014). My choice of research design for this study was a multiple case study (Webb, Maynard, et al., 2014). Other qualitative designs I considered for this study included ethnography, narrative, historical, descriptive, and phenomenological. An ethnographic design was not appropriate for this study because the focus of the research was not to characterize the participants' everyday practices in a cultural setting (Cunliffe & Karunanayake, 2013; Lindley, Sharma, & Potts, 2014; Simpson, Slutskaya, Hughes, & Simpson, 2014; Zilber, 2014).

Furthermore, an ethnographic design was not ideal for the study because SME leaders are not all from the same cultural group. The narrative and historical designs were not appropriate for the study because the focus of the investigation was not to obtain the stories about the lives of the SME leaders but to explore successful information security strategies they use (Caine, Estefan, & Clandinin, 2013; Scutt & Hobson, 2013; C. C. Wang & Geale, 2015). A qualitative descriptive approach provides the description of events and their background within specific geographic boundaries (Nelson & Evans, 2014). The descriptive design was not appropriate for the study because the purpose of the investigation was not to describe, but to explore the information security strategies for a small case study population.

Many researchers use the phenomenological design to define the essence of a phenomenon through individuals' lived experiences and perceptions (Hou, Ko, & Shu, 2013; Mohlameane & Ruxwana, 2014). The phenomenological design was not appropriate for the current study because my intent was to explore successful information security strategies, not lived experiences. By using a qualitative case study, I provided useful insights regarding strategies successful SME leaders use to minimize the effects of information security threats on business performance.

Research Question

The overarching research question of the study was this: What strategies do SME leaders use to minimize the effects of information security threats on business performance?

Interview Questions

Participants responded to the following questions:

1. What strategies are you using to reduce the effects of information security threats on business performance?
2. How did you identify and select the strategies for reducing the effects of information security threats to your organization?
3. How did you implement the strategies for minimizing the effects of information security threats in your information security system?
4. What challenges did you encounter in implementing the strategies to reduce the consequences of information security threats?
5. How did you manage the challenges faced in implementing the strategies to minimize the effects of information security threats?
6. What systems do you have in your company to support the implementation of strategies to reduce the consequences of information security threats?
7. What strategies are most effective in reducing the effects of information security threats on business performance?

8. What strategies are less effective in reducing the effects of information security threats on business performance?
9. What factors influence the implementation of strategies to minimize the effects of information security threats on business performance?
10. What additional information, documentation, or processes would you like to share with me that would help in this research study?

Conceptual Framework

The purpose of this investigation was to explore the strategies SME leaders use to reduce the effects of information security threats on business performance. In this study, I integrated two theories: (a) general systems theory (GST) and (b) transformational leadership theory. Von Bertalanffy (1969) developed GST with the focus on complexity and interdependencies.

The fundamental proposition of GST is on the premises that (a) system wholeness, (b) collaborative interactions and continual relationships within system, and (c) the analysis of systems provides a way of viewing and interpreting the interconnected wholes (Von Bertalanffy, 1969). Researchers use GST as the lens to understand the wholeness of organization systems by discussing related functions, including management and leadership. When I applied GST to this study, the propositions of the theory allowed me to explore the concept of system wholeness in strategies SME leaders use to minimize the effects of information security threats on business performance.

Burns (1978) developed transformational leadership theory to explain leadership based on the premise that leaders can inspire followers to change expectations, perceptions, and motivations to work toward common goals. The primary constructs underlying the transformational leadership theory are (a) idealized attributes, (b) idealized behaviors, (c) intellectual stimulation, (d) inspirational motivation, and (e) individualized consideration. When I applied transformational leadership theory to this study, the propositions of the theory enabled me to explore the transformational characteristics of SME leaders who implemented strategies to reduce the effects of information security threats on business performance.

Operational Definitions

Terms used in this study are defined as follows:

Corporate sustainability: Corporate sustainability is a business approach that enhances long-term shareholders' value and improves business performance by removing waste and managing risk (Nowduri, 2014).

Cybersecurity: Cybersecurity refers to an information system used in resisting threats from cyberspace, which may compromise the availability, integrity, or confidentiality of data (Luiijf, Besseling, & De Graaf, 2013).

Information and communication technology (ICT): ICT refers to electronical business processes including Internet and related technologies that enable effective and efficient business activity (P. Jones, Simmons, Packham, Beynon-Davies, & Pickernell, 2014).

Information security: Information security is the preservation of confidentiality, integrity, and availability of information (ISO/IEC 27000, 2014).

Information security strategy: Information security strategy is the art of deciding how to use the most appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defend organization's information infrastructure(s) against internal and external threats (A. Ahmad, Maynard, & Park, 2014).

Information security threats: Information security threats are events that could compromise an information system, which could result in an adverse impact on business operations, business assets, and individuals including disclosure or unauthorized access of confidential information through social engineering and phishing (Ryan, Mazzuchi, Ryan, Cruz, & Cooke, 2012).

Management information system (MIS): MIS is a computer-based system or process that provides support for corporate management for intelligent decision-making with information necessary to manage at all levels in the organization (Nowduri, 2014).

Small and medium-sized enterprises (SMEs): SMEs are businesses with annual sales turnover of not more than $100 million or employing no more than 200 staff (Gupta, Seetharaman, & Raj, 2013).

Assumptions, Limitations, and Delimitations

The critical components of a viable research proposal are assumptions, limitations, and delimitations (Leedy & Ormrod, 2013). Researchers should clearly articulate the research assumptions, limitations, and delimitations to improve the credibility of their study. In this section, I discuss assumptions, limitations, and delimitations of this study on strategies SME leaders use to minimize the effects of information security threats on business performance.

Assumptions

Assumptions are facts that are outside a researcher's control, which the researcher considers to be relevant to the study and seems to be true but without verification. (Collins, Onwuegbuzie, Johnson, & Frels, 2013; Leedy & Ormrod, 2013; Lips-Wiersma & Mills, 2014; Roy & Pacuit, 2013; Semenova & Hassel, 2015). Schoenung and Dikova (2016) opined that assumptions are beliefs that researchers deem to be true but with no adequate facts to support the beliefs. The brief and assumptions of researchers influence the scope of research inquiries and findings (Kirkwood & Price, 2013). Because assumptions serve as the primary foundation of a proposed study, which some researchers neglect, I made some assumptions to help reduce misunderstanding and resistance to this study.

The first assumption of the study was SME leaders would be available and willing to participate voluntarily in the study and provide honest responses, which could help to determine reliability of data and research findings. Second, I assumed the mode of administration of interview questions would not affect the study outcome. Third, I assumed collection of data from a minimum of five participants would represent accurate information to understand the strategies SME leaders use to minimize the effects of information security threats on business performance. Finally, I assumed the patterns and themes emerging from data analysis would be adequate to answer the research question.

Limitations

Limitations are some potential weaknesses or problems that could affect the study that are not within the control of the researcher and might limit the scope of the research findings (Berbary, 2014; Madsen, 2013; Stewart & Gapp, 2014). Some of the factors that could limit a study include potential weaknesses from the geographical location and sample size or data availability (Coffie, 2013). Because limitations could threaten the internal validity of this study, I considered some limitations. The first limitation of the study was that respondents could introduce a certain level of bias. Responses from study participants might be to the best interest of their organization, which could subject their response to the interview questions to bias arising from self-reporting.

The second limitation was the generation of the data from a cross-sectional research design rather than a longitudinal research study. The implication was that duration for data collection would be short and data collected would depend on the prevailing situation during the data collection period. The longitudinal study could provide additional information and the data would enable further testing of the implementation of information security strategies at different times.

The third limitation was limiting of sample size to five SME leaders, which could pose a problem, but during the interview process, the number of interviewees could increase until the point of data saturation. O. C. Robinson (2014) and Royset (2013) noted that using a larger sample size might yield a different result. The fourth limitation was the purposive sampling technique, which was limited to the fact that members of the target population did not have equal chance of being selected. The final limitation was the restriction of the study location to leaders in SME firms that support the oil and gas industry sector in Port Harcourt, Nigeria, and the research findings may not apply to other business sectors and geographical areas.

Delimitations

Research delimitations are critical components of an applied research and refer to the investigation boundary or scope, which researchers should establish before commencing a study (Leedy & Ormrod, 2013; Ody-Brasier & Vermeulen, 2014; Semenova & Hassel, 2015). Researchers state their research delimitations to help readers to understand the factors intentionally excluded from the study (Leedy & Ormrod, 2013). Because research delimitations affect the external validity or generalization of the research findings, I outlined some delimitations of this qualitative multiple case study.

The first delimitation was that SME leaders with at least 2 years of managerial experience in the organization's top management team with knowledge of the organization's information security threats would participate in this study. The research participants were five SME leaders of businesses in Port Harcourt, Nigeria, and might not warrant the generalization to other business units in other geographical areas. The scope of this study included the information security strategies that could help to minimize the effects of information security threats on business performance. The reasons why the SME leaders apply the information security strategies were outside the scope of this study.

Significance of the Study

The purpose of this study was to explore strategies SME leaders use to reduce the effects of information security threats on business performance. SMEs face the risk of cyber-attack, data fraud, theft of enterprise information systems, and breakdowns of critical information infrastructure (Green, 2015). The knowledge gained might assist SME leaders to implement strategies to safeguard businesses against information security threats and breaches and improve business performance (Alegre, Sengupta, & Lapiedra, 2013; Carraher & Van Auken, 2013; Hamann, Smith, Tashman, & Marshall, 2017).

Contribution to Business Practice

Researchers have attributed the high business failure rates of 92% and 71% within 1 and 3 years for small businesses within the United Kingdom to a lack of information system management (P. Jones et al., 2014). In 2013, SMEs experienced a 37% economic loss from security incidents (Bojanc & Jerman-Blazic, 2013). SME leaders seek to understand the strategies to use in minimizing the effects of information security threats on business performance to maximize business success and maintain critical knowledge capital within their organizations. Organizational leaders could gain significant knowledge from this study, which is conducive for maximizing sustainable business growth (Lawal, Ajonbadi, & Otokiti, 2014; Oluga et al., 2014; Valli, Martinus, & Johnstone, 2014). The contributions to professional practice might include providing SME leaders with the strategies needed to minimize the effects of information security threats on business performance.

Implications for Social Change

Servaes and Hoyng (2017) noted that ICTs are techno-centric development tools for social change and suggested the integration of the conceptions of agency and social change with institutions and networks. Small businesses are increasingly experiencing security breaches that negatively affect the company’s turnover, productivity, and profitability (Department for Business, Innovation & Skills, 2015). The potential for effecting positive social change is that business improvement could catalyze a greater flow of funds into the local economy, which would allow community leaders to build schools, health centers, and libraries for Port Harcourt city residents.

A Review of the Professional and Academic Literature

The purpose of this qualitative multiple case study was to explore the strategies successful leaders in SME firms that support the oil and gas industry sector in Port Harcourt, Nigeria use to minimize the effects of information security threats on business performance. Some SME leaders lack the understanding and knowledge of IT security management. The research question underpinning the doctoral study was the following: What strategies do SME leaders use to minimize the effects of information security threats on business performance? In this section, I discuss the strategy for searching the literature, provide a comprehensive overview of the conceptual framework, and critically review the literature about potential themes and phenomenon.

I reviewed the literature in the field of IT, information systems, and information security to collect and systematically organize the findings to identify the relevant themes and patterns that would answer the research question. The specific focus areas are the general systems theory, the transformational leadership theory, SME leaders, information security risks and threats, information technology governance, information security management system, cyber security, and digital technology.

The various sources and contents for the review of literature include peer-reviewed articles and journals, websites, dissertations, books, and corporate and government reports. The primary research libraries and databases included the Walden University Library, Google Scholar, SAGE Premier, EBSCOhost, ProQuest, and Emerald Insight. The strategy for the literature review was to research for recent articles that relate to the doctoral study topic in the business environment sources mentioned above.

The search keywords and terms include *transformational leadership theory*, *general system theory*, *SME*, *information security*, *data security*, and *cybersecurity*. I used the Ulrich's Periodicals Directory to confirm the peer-reviewed status of the articles. Table 1, the reference tracker, shows the distribution of sources of articles to achieve the rule, which requires that in-text citations should consist of 85% of peer-reviewed articles published within 5 years from anticipated graduation date. The literature review includes 112 references with 109 references representing 97.3% of articles published within 5 years from the anticipated graduation date. The literature review contains 97 peer-reviewed articles published within 5 years from expected completion date of July 2017, representing 89.0% of recent references and 86.6% of total sources.

Table 1

The Reference Tracker

Titles	Recent References less than 5 years from anticipated completion date	References older than 5 years from anticipated completion date	Total	% of recent reference (Not less than 85%)
Books	0	2	2	0%
Dissertations	0	0	0	0%
Peer-reviewed Articles	97	1	98	99.0%
Web Pages	1	0	1	100%
Government Report	2	0	2	100%
Other Sources	9	0	9	100%
Total	109	3	112	97.3%
		Percentage of Peer-reviewed		86.6%

GST

The Von Bertalanffy (1969) GST is a trans- and interdisciplinary theoretical framework, which researchers use to study elements of complex systems that act in concert to produce some result in organizations, nature, society, and science. The focus of GST is on complexity and interdependencies of systems. A system is composed of inputs and outputs that interact to achieve the objective of the scheme.

Von Bertalanffy (1969) conceptualized the GST in 1937 and subsequently expanded and introduced the theory in a German language journal in 1949. The systems theory relates to the concept of an organism as an open system with various components working together to complete a task (Von Bertalanffy, 1972). The fundamental propositions of GST include (a) system wholeness, (b) collaborative interactions and continual relationships within systems, and (c) the analysis of systems provides a way of viewing and interpreting the interconnected wholes.

Researchers and scholars use GST as a lens to understand the wholeness of organization systems by discussing related functions, including management and leadership (Ceric, 2015; Yawson, 2013). Ceric (2015) applied cross-impact analysis method, a derivative of the systems theory method, to propose an evaluation model for examining an ICT value creation process. The assessment process focuses on six dimensions of an ICT value creation system that have important implications for managing the system: (a) drivers, (b) outcomes, (c) identity, (d) goals, (e) trends, and (f) its structure (Ceric, 2015). Ceric demonstrated that organizational stakeholders could use the evaluation model as a basis for informed management of their ICT value creation system.

Yawson (2013) studied systems theory and thinking as a foundational discipline or approach in human resource development. The set of constructs includes information and game theory, cybernetics and chaos theory, the theory of autopoiesis, complexity theory, and dynamic systems theory (Yawson, 2013). Sturmberg, Martin, and Katerndahl (2014) analyzed GST and demonstrated the use of systems theories in general practice and family medicine.

The system theory comprises of the following factors: (a) the complexity science, (b) self-organizations, (c) emergence, (d) dynamics in systems, (e) science of network, and (f) evolutions and adaptation (Sturmberg et al., 2014). According to Sturmberg et al. (2014), evolution is a major factor in GST because it led to the development of subsystems with new characteristics and dynamics. Mangal (2013) utilized GST to demonstrate that websites with dysfunctional components provide a less enjoyable experience than a website with cohesive integration of system components. Neumann (2013) developed the "Know Why" thinking approach to describe why certain systems work and why other systems do not, which researchers can utilize to explain the success of systems and motivation of human behavior. Concerning the GST, the integration and collaboration of the elements of information security management within an organization are essential to minimize the effects of information security threats on business performance.

Transformational Leadership Theory

The foundation of leadership studies is the literature on transformational leadership. Burns (1978) developed transformational leadership theory to describe how leaders can inspire followers to change expectations, perceptions, and motivations to work toward common goals. The primary constructs underlying the transformational leadership theory are (a) idealized attributes, (b) idealized behaviors, (c) intellectual stimulation, (d) inspirational motivation, and (e) individualized consideration. Syrek, Apostel, and Antoni (2013) outlined the transformational leadership characteristics to include inspiration of followers to work hard, encouraging members to think creatively and solve problems, and providing followers with personalized attention. The primary focus of transformational leaders is on the overall vision of the organization, providing direction, inspiring and motivating followers to bring about organizational change (Oterkiil & Ertesvag, 2014). Transformational leaders and followers are involved in relationship contracts where a leader connects with the followers in such a way that raises the level of motivation and morality in both the leader and followers for a common goal rather than self-interest (Burns, 1978).

A transformational leader inspires positive change in followers (Carter, 2013). The transformational leader inspires and stimulates followers to achieve positive outcomes, helps followers to develop into leaders, and recognizes and rewards deserving followers (Grigoroudis, Tsitsirisi, & Zopounidis, 2013). Transformational leadership refers to a process where individuals (leaders) engage others (followers) to create connections that results in increased motivation and productivity in both followers and leaders (Garrison & Vaughan, 2013).

Studies on transformational leadership began with the classic work of James MacGregor Burns in 1978, which was expanded by Bass and Avolio in 1991, and further expanded and revised by Bass in 1985 (Tyssen, Wald, & Spieth, 2014; Van Knippenberg & Sitkin, 2013). Meuser et al. (2016) discussed leadership theories and investigated the status of leadership theory integration. The six leadership approaches include (a) transformational leadership, (b) charismatic leadership, (c) strategic direction, (d) leadership and diversity, (e) participative/shared leadership, and (f) trait approach to leadership (Meuser et al., 2016). Meuser et al. posited that concepts of transformational and charismatic leadership are the most researched leadership theory because of the theoretical linkage between them. Transformational leaders influence their followers while followers impact charisma to their leaders (Meuser et al., 2016).

The focus of strategic leadership is contextual theories, information processing and decision making, and cognitions rather than individual followership (Meuser et al., 2016). The focus of leadership and diversity theories is underrepresentation of ethnic minorities and women in leadership roles. In participative/shared leadership, leadership is shared among many individuals rather than an individual. Traits approach to leadership is the oldest leadership theory and holds that leaders emerge because of their traits and possession of skills relevant to the position (Meuser et al., 2016). Meuser et al. (2016) provided 10 additional leadership theory graphs and analysis: (a) leadership in teams and decision groups, (b) leader and follower cognitions, (c) ethical leadership, (d) leadership emergence, (e) leadership development, (f) emotions and leadership, (g) implicit leadership, (h) leader-member exchange, (i) authentic leadership, and (j) identity and identification process theories of leadership.

Effelsberg, Solga, and Gurt (2014) demonstrated that a positive relationship exists between transformational leadership and employees’ willingness to engage in unethical proorganizational follower behavior. Sosik, Chun, Blair, and Fitzgerald (2014) stated that transformational leadership characteristics such as charisma and modeling of high ethical and moral behaviors tend to have an idealized influence on subordinates.

Dinh et al. (2014) explored current theoretical trends and changing perspectives in leadership theory and studies in the 21st century while Yammarino (2013) explored the state of leadership. Ford and Harding (2015) studied the academic theory of followership about leadership theory and introduced a critical approach to followership studies. Dinh et al. conducted a comprehensive qualitative review of leadership theory across 10 top-tier academic publishers to generate an inventory of established and developing leadership theories.

Dinh et al. (2014) explained that leaders determine the fate of their organizations through their decisions, strategies, and influence on others; and presented a review of developments in the leadership field and identified a total of 66 different leadership theory domains. Ford and Harding (2015) posited that leadership theory is separate from practice (that is, from the physical encounters between people in workplaces), and cannot advise leaders on how to govern followers. Yammarino (2013) stated that leadership is a universal and multilevel phenomenon involving many constructs, processes, and entities.

Adeleye (2015) investigated how an established firm in a dynamic market could implement a corporate renewal program successfully in a hypercompetitive business environment. Adeleye noted that transformation is best achieved in an environment when radical changes in design and talent management systems complement process and structural change. The five principles of successful corporate transformation program are (a) leading by vision, (b) putting people first, (c) listening to the voice of customer, (d) competing in technology and innovation, and (e) taking operational risk management and governance serious (Adeleye, 2015). Organizations that adopt the five principles can successfully achieve world-class operations and deliver outstanding results (Adeleye, 2015).

Bronkhorst, Steijn, and Vermeeren (2015) indicated that transformational leadership style has a direct relationship with work motivation because a transformational leader directly inspires people, resulting in a greater work effort. Goal setting is partly mediating the relationship between transformational leadership and work motivation, while an indirect relationship exists between transformational leadership style and the goal-setting process (Bronkhorst et al., 2015). S. Kim and Yoon (2015) posited that climate of creativity through enhancing recognition of employee creativity, flexibility of change, and resources for innovation had a significant association with employees' perceptions of a culture of innovation.

The degree to which an employee perceives a culture of innovation varies among agencies while the supervisor's transformational leadership is essential in fostering a culture of innovation in local government (S. Kim & Yoon, 2015). S. K. Pandey, Davis, Pandey, and Peng (2015) provided empirical evidence of the relationship between transformational leadership and employees' use of normative public values in organizational decisions. Transformational leadership can play a significant role in public organizations because the influence of transformational leadership increases the integration of normative public values in corporate decision-making (S. K. Pandey et al., 2015).

The lack of leadership skills may set back SME development and overall business performance (Alegre et al., 2013; Carraher & Van Auken, 2013). Lawal et al. (2014) studied the relationships between leadership style and organizational effectiveness among SMEs in Nigeria. The Nigerian SMEs have mixed leadership styles but are more autocratic and less participative because of the vast power distance between business owner and employees, and an insignificant relationship exists between leadership style and organizational effectiveness (Lawal et al., 2014). The transformational leadership theory posits that leadership style of organizational leaders is essential to minimize the effects of information security threats on business performance effectively.

SMEs

According to the Small and Medium Enterprises Development Agency of Nigeria (SMEDAN, 2013), companies with 10 to 49 employees and an asset base of NGN5-50 million are termed small businesses, while companies with 50 to 199 employees and an asset base of NGN50-500 million refer to medium enterprises. In 2013, the national population of small businesses was 68,168 small businesses and 4,670 medium companies with 2981small businesses and 41 medium businesses operating in Rivers state respectively (SMEDAN, 2013). Gbandi and Amissah (2014) indicated that Britain, United States, and some European countries also define SMEs by the turnover and number of employees. Holt and Powell (2015) explained the European Commission's definition of SME classified businesses with 10 to 49 employees as small enterprises and businesses with 50 to 249 employees as medium-sized enterprises.

Agwu (2014) indicated that SMEs constitute about 97% of companies in Nigeria. In Portugal, SMEs represent 99.5% of all businesses, generating 74% of employment, and 59.8% of sales (Santos, Barros, Mendes, & Lopes, 2013). Small businesses constitute 99.9% of all businesses in United States (Armstrong, 2013). The important roles of SMEs include (a) job creation, (b) innovation, (c) investments, and (d) economic development

(Hamann et al., 2017; Narteh, 2013; Osei-Assibey, 2013). Uluyol and Akci (2014) pointed out that SME should be competitive at the global level to survive the current competition environment of the global economy.

Uluyol and Akci (2014) indicated that SME experience problems in incapability technological issues. SME leaders face challenges of coping with the rapidly evolving information security threats (Webb, Maynard, et al., 2014) and lack adequate situation awareness on information security risk management (Webb, Ahmad, et al., 2014). Organizational leaders speculate the effect of information security risk rather than conduct information security risk assessment that is negatively affecting the management of information security risks (Webb, Maynard, et al., 2014). SME leaders should pursue competent-based strategies rather than flexibility-based strategies to ensure sustainable business growth (Armstrong, 2013). With globalization and market liberalization, SME leaders are adopting IT for improved business performance (S. Z. Ahmad, 2014). SME leaders with entrepreneurial and innovative capabilities generate higher sales growth than large firms (Bala Subrahmanya, 2015).

Awiagah, Kang, and Lim (2016) studied the factors influencing adoption of electronic commerce by SMEs in four regions (greater Accra, western, northern, and upper west) in Ghana. The factors affecting SMEs' adoption of e-commerce in Ghana include (a) technological factors, (b) organizational factors, (c) environmental factors, and (d) individual constructivism. Awiagah et al. identified government support, managerial support, and influence of enabling and regulatory conditions as the primary factors affecting adoption of e-commerce among SMEs in Ghana.

Osakwe, Chovancova, and Agu (2016) examined the contextual factors that influenced decision-making process of micro-enterprises to adopt corporate website from the perspective of a developing economy like Nigeria. The factors affecting the decision to choose website are (a) technological contexts, (b) organizational contexts, (c) environmental contexts, and (d) demographics of the decision-maker. Osakwe et al. advised micro-enterprise owners in developing economy to embrace digital world. The decision to adopt a website is a strategic marketing tool that micro-enterprises could use to enhance their brand enterprise visibility in the globalized marketplace (Osakwe et al., 2016).

IT Security Risks

With increasing effect of access to data and applications, cybercriminals continually exploit vulnerable and unsuspecting computer users (Vidalis & Angelopoulou, 2013). The frequency and sophistication of information security incidents have increased and concern for information security management has become a significant business problem. The aim of information security is to protect information from unauthorized access, use, disclosure, disruption, modification, and destruction (Mesquida & Mas, 2015).

The process of information security risk management will enable business leaders to focus efforts on using the most efficient and cost-efficient means to protect information assets and resources. Due to growing vulnerability of IT security risk, researchers and scholars have increased attention on some areas of information security. The key sectors include (a) business continuity and disaster recovery, (b) cyber risks and cyber threats, (c) data leakage and data loss prevention, (d) information security transformation, and (e) compliance monitoring (Fazlida & Said, 2015). According to Fazlida and Said (2015), the purpose of information security is to protect and preserve confidentiality, integrity, and availability of information; maintain the authenticity and reliability of information, and ensure that entities are accountable for information.

Montesdioca and Macada (2015) developed a model to measure user satisfaction with information security practices. Nazareth and Choi (2015) examined the effect of investing in different areas of information security. Using the system dynamics model, Nazareth and Choi investigated the financial implications of investment attributable to security decisions on an organization's information asset base.

Wong, Veneziano, and Mahmud (2016) examined related issues and consequences of usability of SAP, a software system for business process management. Wong et al. demonstrated that lack of proper training and communicativeness affect the usability of SAP enterprise resource planning (ERP) software. Organizations should implement well-organized training initiatives for SAP ERP users to avoid project failure (Wong et al., 2016).

Holm, Sommestad, Ekstedt, and Honeth (2014) evaluated the value of three indicative variables (consensus, experience, and self-proclamation) for data collection in four different domains of cyber security. The four areas of cyber security were (a) intrusion detection, (b) denial of service attacks, (c) arbitrary code injection attacks, and (d) software vulnerability discovery. Holm et al. identified census, as a reasonable indicator of calibration while the research findings indicate there is no significant correlation between neither calibration and experience nor calibration and self-proclamation.

Gupta et al. (2013) studied the perception of SMEs toward usage and adoption of cloud computing in Asia-Pacific (APAC) region and benefits thereof. Gupta et al. specifically created a research model, identified existing core variables that formed the theoretical basis for their study, and examined the business community's usage of cloud. The five key variables are (a) ease of use and convenience, (b) security and privacy, (c) cost of reduction, (d) reliability, and (e) sharing and collaboration. The three most dominant factors influencing SMEs' cloud usage are ease of use and convenience, security and privacy, and cost of reduction (Gupta et al., 2013).

P. Jones et al. (2014) studied micro-enterprise owners' attitude and strategic responses in adopting ICT. P. Jones et al. posited that sole-proprietor micro-enterprises' perception of the value of ICT adoption influence their attitude toward ICT adoption. Sole-proprietor micro-enterprises develop strategic responses to drive immediate and attainable benefits with readily available finance rather than leveraging on ICT as an agent of longer-term transformational change to achieve future business growth (P. Jones et al., 2014).

Abualrob and Kang (2016) examined the significant barriers that hinder small businesses in Palestine from adopting electronic commerce (e-commerce). The three major barriers to e-commerce adoption are occupation restrictions, political instability, and logistical obstacles in occupied lands (Abualrob & Kang, 2016). Abualrob and Kang demonstrated that financial losses do not influence e-commerce adoption while perceived uncertainty and complexity has a negative effect on e-commerce adoption in Palestine. Ramdani, Chevers, and Williams (2013) examined technology-organization-environment (TOE) factors influencing SMEs’ adoption of enterprise applications (EA) in northwest of England. Ramdani et al. demonstrated that technology, organization, and environment contexts affect SMEs’ adoption of EA, which implies that TOE model can predict SMEs’ adoption of EA.

Gangwar, Date, and Ramaswamy (2015) identified 12 variables for cloud computing adoption, which include relative advantage, compatibility, complexity, organizational readiness, top management support, and training and education. Others are competitive pressure, trading partner pressure, security, third-party control, perceived ease of use, and perceived usefulness. Carcary, Doherty, and Conway (2014) examined adoption of cloud computing technology among Irish SMEs and noted that most SMEs have not adopted cloud computing. Some SME leaders who adopted cloud computing did not rigorously assess their readiness for cloud computing technology or did not take in-depth approaches for managing their engagement with the cloud (Carcary et al., 2014).

Fu and Chang (2016) studied the factors that affect implementation of a cloud customer relationship management (CRM) service in traditional Taiwanese machine industry. Fu and Chang stated that adoption of cloud CRM service model is an organizational issue rather than a technological issue or environmental issue. The three most important factors influencing the plans to adopt cloud CRM are support of senior managers, corporate strategies, and system security (Fu & Chang, 2016).

Lin (2014) developed a research model to investigate the determinants of electronic supply chain management (e-SCM) adoption. Lin provided a conceptual guideline to explain the important determinants of e-SCM adoption. Technological context is the primary determinant of the decision to adopt e-SCM but does not affect the extent of e-SCM adoption (Lin, 2014). The organizational and environmental contexts determine the scope of e-SCM adoption (Lin, 2014).

Sahdev, Medudula, and Sagar (2014) identified and analyzed the key barriers to adoption of cloud computing in education sector in India. Sahdev et al. demonstrated that data security is the primary barrier influencing the decision to migrate IT services in the education sector to cloud architecture. The top five barriers that influenced adoption of cloud computing in the school sector in India are data security concerns, technology issues, regulatory compliance concerns, lack of return on investment model, and institutional culture (Sahdev et al., 2014). Others include attrition of staff positions, lack of institutional executive support, utilization of contract terms, lack of education and tools, and lack of confidence.

Zhao, Xue, and Whinston (2013) presented the risk management approaches. Zhao et al. explored the risk management strategies of third-party cyber insurance, risk pooling arrangements (RPA), and managed security services. Zhao et al. opined that firms could use an RPA as a complement to cyber insurance to address over investment issue due to negative externalities of security investments.

Firms that adopt RPA do not derive a compatible incentive to suggest that security investment generates positive externalities (Zhao et al., 2013). Mejias and

Balthazard (2014) developed information security awareness (ISA) information system security (ISS) risk assessment model and provided empirical evidence on the positive association between ISA and ISS risk assessment. Mejias and Balthazard posited a positive relationship between technical knowledge, organizational impact, and attacker assessment, and ISA but organizational impact and attacker assessment generated stronger path coefficients with ISA than technical expertise.

Information Security Management System

Information security refers to safeguard of confidentiality, integrity, and availability of information (ISO/IEC 27000, 2014). Confidentiality focus on the property that information is not made available or disclosed to unauthorized individuals, entities, or process - set of interrelated or interacting activities that transforms inputs into outputs. Integrity focus on the property of accuracy and completeness while availability focuses on ownership of accessible and usable of information upon demand by an authorized entity. Other properties include authenticity (assets that an entity is what it claims to be), accountability, non-repudiation (ability to prove occurrence of alleged event or action and its originating entities), and reliability (property of consistent intended behavior and results; ISO/IEC 27000, 2014).

Nazareth and Choi (2015) stated that corporate leaders could achieve effective information security management with the deployment of security resources on multiple fronts including attack prevention, vulnerability reduction, and threat deterrence. Nazareth and Choi advised managers to invest in security detection tools rather than investing in security deterrence.

The alignment of ISO/IEC 15504 international standard with the ISO/IEC 27000 information security management framework will improve information security management system (Mesquida & Mas, 2015). Mesquida and Mas (2015) advised software companies to make some changes to support implementation of related security controls. Organizations can use international standards ISO/IEC 27000, 27001, and 27002 as guideline or framework to establish, implement, and maintain an adequate information security management system (Disterer, 2013).

Gangwar et al. (2015) developed a conceptual model to measure cloud computing in organizations while Jarvelainen (2013) validated theoretical information system continuity management (ISCM) framework. The components of the ISCM framework include (a) external requirements (regulations, customers), (b) management support, (c) organizational alertness and preparedness, (d) embeddedness of continuity practices, and (e) perceived business impacts on ISCM. Jarvelainen demonstrated that embeddedness of continuity practices is directly related to perceived business results on ISCM while no direct linkage exists between organizational alertness and preparedness, and recognized business impacts on ISCM.

Webb, Ahmad, et al. (2014) proposed a situation awareness on the process of information security risk management (SA-ISRM) model to complement the process of information security risk management. The purpose of SA-IRSM process model, a derivative of Endsley's situation awareness model, is to address identified deficiencies in the practice of information security risk assessment which inevitably lead to poor decision-making and inadequate or inappropriate security. Using findings from a case study of United States national security intelligence enterprise, Webb, Ahmad, et al. refined the SA-ISRM process model. Webb, Maynard, et al. (2014) examined how structure and functions of United States national security intelligence enterprise (USNSIE) correspond with Endsley's theoretical model, and how to adopt facets of United States company to improve SA-ISRM process of organizations.

Webb, Maynard, et al. (2014) identified three types of SA deficiencies in information security literature and proposed an enterprise SA model to improve an organization's SA-ISRM process. The three SA deficiencies in the organizational practice of ISRM are (a) not carefully thought risk assessments, (b) estimation of security risks without investigation, and (c) occasional rather than continuous assessment of security risks (Webb, Maynard, et al., 2014). Tondel, Line, and Jaatun (2014) explored the current practice and experiences on information security incident management in a wide variety of organizations. Tondel et al. noted that information security incidents might result in multiple negative impacts, including loss of company reputation and customer confidence, litigations, loss of productivity, and direct financial loss. Tondel et al. posited that current practice and experiences with information security incident management comply with the incident management phases of ISO/IEC 27035.

De Gusmão, e Silva, Silva, Poleto, and Costa (2016) proposed a risk analysis model for information security assessment and illustrated the applicability of the proposed model in a real context. The model is a combination of events tree analysis (ETA) and fuzzy decision theory. De Gusmão et al. analyzed twelve alternatives using two different methods of setting probabilities of occurrence of events and demonstrated that deliberate attack on external database services represent the riskiest alternative. Shameli-Sendi, Aghababaei-Barzegar, and Cheriet (2016) presented the taxonomy of information security risk assessment (ISRA) and identified four categories of ISRA approaches. The ISRA approaches are appraisement, perspectives, resource valuation, and risk measurement. Shameli-Sendi et al. noted that ISRM is composed of four processes, which include framing risk, assessing risk, responding to risk, and monitoring risk.

Silva, de Gusmão, Poleto, e Silva, and Costa (2014) presented a multidimensional approach to ISRM using the failure mode and effects analysis (FMEA) and fuzzy theory. The five dimensions of information security are (a) access to information and systems, (b) communication security, (c) infrastructure, (d) security management, and (e) secure information systems development. Silva et al. demonstrated that communication security is the most important aspect of information security while infrastructure is the next. Perez, Branch, and Kuofie (2014) studied the effect of behavioral and organizational factors on satisfactory implementation of information security. Perez et al. stated that a significant correlation exists between organizational structural factors, balanced security factors, information security awareness, and end-user intentionality toward information security.

Safa et al. (2016) conceptualized the information security policy compliance model and illustrated how compliance with information security organizational policy (ISOP) affects and mitigates risk of employees' behavior. The root causes of user's mistakes are lack of information security awareness, ignorance, negligence, apathy, mischief, and resistance (Safa et al., 2016). Safa et al. demonstrated that information security knowledge sharing, collaboration, intervention, and experience have a significant impact on employees' attitude toward compliance with ISOP while attachment does not have a major effect on employees' attitude toward ISOP. Also, commitment and personal norms affect employees' attitude while employee's attitude toward compliance with ISOP has a significant effect on behavioral intention regarding security compliance (Safa et al., 2016).

Singh, Gupta, and Ojha (2014) explored key frameworks and factors of organizational information management system (IMS) and identified top management factors for addressing organizational information security challenges. The top 10 management factors of corporate IMS are top management support, information security policy, information security training, and information security awareness. Others include information security culture, information security audit, IMS best practices, asset management, information security incident management, and information security regulation compliance (Singh et al., 2014).

Bradshaw, Cragg, and Pulakanam (2013) studied the relationship between SMEs and information systems (IS) consultants to determine whether IS consultants influence SME's IS competencies during a major IS project. Bradshaw et al. demonstrated that SMEs lack many IS skills and capabilities while consultants compensate or enhance six IS skills for SMEs. The six IS competencies that SMEs lack are business and IS strategic thinking, defined IS distribution, defined IS strategy, exploitation, deliver solutions, and supply. Bradshaw et al. concluded that IS consultants influence the six macro competencies by helping SMEs to overcome the lack of IS skills rather than helping them to develop IS competencies.

IT Governance

Bin-Abbas and Bakry (2014) developed and tested an integrated simple approach for assessment of IT governance in organizations and provided direction for future development. Bin-Abbas and Bakry relied on critical IT management methods to develop the theoretical framework of their study. Some of the IT management methods include control objective for information and related technology (COBIT), IT infrastructure library (ITIL), ISO 20000, ISO 38500, and Massachusetts Institute of Technology (MIT) IT governance practice.

The IT governance domain is composed of some management frameworks which organizations use to develop structures and good practice statements to improve their IT governance performance, including ISO 38500 and COBIT (Debreceny, 2013). Debreceny (2013) used strategy, technology, organization, people, and environment (STOPE) model to develop an IT governance assessment approach and illustrated the model using seven senior staff members of IT center of a Saudi organization. Debreceny relied on the six-sigma process to develop an integrated IT governance which is within the scope of STOPE domain and could drive knowledge management. Bin-Abbas and Bakry (2014) provided 50 primary IT governance control elements structured after STOPE domain and identified key strengths and weaknesses of IT management in organizations which could drive the direction of future development. Further development of IT governance requirement controls could enhance knowledge sharing and support business improvement (Bin-Abbas & Bakry, 2014).

Wu, Straub, and Liang (2015) proposed a homological model by consolidating the strategic alignment and IT governance models, to explain how to create organizational value through IT governance mechanisms. Wu et al. drew the research design from resource-based view of the firm and provided guidance on how strategic alliance can mediate the effectiveness of IT governance on organizational performance. Wu et al. posited that significant positive and impactful relationships exist between IT governance mechanisms and strategic alignment and between strategic alignment and organizational performance. Bahl and Wali (2014) studied employee perceptions of information security management and its impact on information security service quality delivered to customers of Indian software service providers.

In an IT outsourcing firm, a highly predictable impactful positive relationship exists between information security governance and information security service quality (Bahl & Wali, 2014). Yaokumah and Brown (2014) examined the relationships and integration between information security governance (ISG) strategic alignment with risk management, value delivery, performance measurement, and resource management in Ghanaian organizations. Yaokumah and Brown mapped the corporate governance theories, namely, agency theory, stakeholder theory, and organizational theory to the strategic alignment, risk management, value delivery, performance measurement, and resource management. ISG strategic alignment practices are predictors of information security risk management, value delivery, performance measurement, and resource management (Yaokumah & Brown, 2014).

Devos and Van de Ginste (2015) implemented a reverse engineering work and attempted to explain the propositions from COBIT 5 as empiricism. Devos and Van de Ginste posited that COBIT 5 holds theoretically supported claims with principal-agent theory (PAT) and stakeholder theory (SHT) contributing most of the theoretical statements. The primary causes of IT governance failure are the imperfect implementation of IT governance and futile IT management policies (Fazlida & Said, 2015). The four perspectives of IT governance are (a) management mechanism, (b) decision-making, (c) strategic alignment of business and IT, and (d) strategic IT planning and control.

The specific objectives of IT management frameworks are IT control structure, protection of IT investment, security and monitoring of IT, protection of information from losses, assuring data integrity, quality of IT services, and quality software. Fazlida and Said (2015) stated that researchers had combined auditing standards and information security organization bylaws to develop customized IT governance frameworks to assure efficient information security management. Fazlida and Said opined that information security complements IT management concerning assurance of confidentiality, integrity, and availability of information, and advised organizations to use IT governance framework such as COBIT and ISO 27001 to implement its ISG system.

Ferguson, Green, Vaswani, and Wu (2013) examined the relationship between overall level of effective IT governance and five commonly advocated individual IT governance mechanisms. Ferguson et al. indicated that a significant association exists between the overall level of effective IT governance and three IT governance mechanisms, namely, IT steering committee, senior management involvement in IT, and corporate performance measurement systems. Heroux and Fortin (2013) explored the relationship between IT governance and control of website content while Suicimezov and Georgescu (2014) examined the literature on IT management and cloud computing. The IT management of most organizations is more developed than their control of website content. The IT governance structures, processes, and relational capabilities could be related to website content control (Heroux & Fortin, 2013).

Suicimezov and Georgescu (2014) recognized the importance and impact of IT governance in evolution of IT system and emphasized the importance of management in cloud computing at the business level. Qassimi and Rusu (2015) analyzed IT governance practices in public agency particularly in a government organization in a developing country. Qassimi and Rusu identified the need to improve the basic elements of IT governance framework to promote accountability of IT projects and contribute to an effective implementation of IT governance in the organization.

Orozco, Tarhini, and Tarhini (2015) developed a framework of IT-business alignment management practices to improve the design of IT governance (ITG) architectures. At tactical and operational levels, the core structural capabilities that can positively improve the process of IS/business alignment are improving the coordination of IT investment management process and enabling structures that strengthen the connection of budgetary controls (Orozco et al., 2015). Rebollo, Mellado, Fernandez-

Medina, and Mouratidis (2015) performed an empirical evaluation of information security governance cloud (ISGcloud) framework. The entire ISGcloud framework enabled the state public organization to establish a security management structure to achieve security governance objectives, minimize security risks of storage services, and increase security awareness among users (Rebollo et al., 2015).

Tiwana, Konsynski, and Venkatraman (2013) examined literature on IT governance and expanded the scope of research. The range includes (a) IT-enabled governance of new organizing logics, (b) a symbiotic relationship between IT and organizational management, and (c) the need to foster new theory development at the interface of IT and corporate governance. Tiwana et al. developed the IT management cube framework, which is composed of three dimensions that could guide IT research. The dimensions are *who is governed*, *what is governed*, and *how is it governed*.

Boss, Galletta, Lowry, Moody, and Polak (2015) conducted a detailed literature review in information security using protection motivation theory (PMT). Boss et al. described the theoretical foundation of three opportunities for improving information security using PMT. The three opportunities are (a) using PMT’s core constructs in existing information security studies, (b) including fear-appeal manipulations, which is a fundamental element of PMT, and (c) measuring fear to address the actual security behaviors. Boss et al. demonstrated the efficacy of three identified areas for potential improvements.

Boss et al. (2015) provided evidence for practitioners to use fear appeals and to present users with strong arguments for adhering to behavioral security policy. Yeh, Lee, and Pai (2015) examined the factors that influence e-business IT capability and demonstrated that IT capability significantly influences the implementation of IT strategies. The key factors affecting e-business IT capability are IT maturity, IT infrastructure, support from top management, IT human resources, partnership quality, and competitive pressure (Yeh et al., 2015).

A. Ahmad, Maynard, et al. (2014) explored how organizations develop and implement security strategies to protect their information systems. A. Ahmad, Maynard, et al. outlined nine information security strategies: (a) deterrence, (b) prevention, (c) surveillance, (d) detection, (e) response, (f) deception, (g) perimeter defense, (h) compartmentalization, and (i) layering. A. Ahmad, Maynard, et al. posited that most organizations use a preventive approach derived from the desire to guarantee availability of technology and services, and security managers comparatively ignore the exposure to business security risks.

Organizational leaders deploy strategies in a preventive capacity and use other approaches at the operational level to support the preventive strategy (A. Ahmad, Maynard, et al., 2014). The two fundamental dimensions of information security strategy are time and space. A. Ahmad, Maynard, et al. (2014) stated that most organizations deploy information security strategies in an ad-hoc manner without a formal or systematic approach to addressing risks through a combination of strategies.

Information Security Threats

Nowduri (2014) conducted a detailed review of literature in MIS and outlined a framework for the competency model in MIS among the sustainable corporation. Posey, Roberts, Lowry, Bennett, and Courtney (2013) examined protection-motivated behaviors (PMBs) of organizational insiders to protect organizationally relevant information and computer-based information system from a systematic approach. Posey et al. noted that organizational leaders should recognize the important role of corporate insiders rather than relying on technology to protect the organizations' information resources. The area of IS security can benefit from systematics investigations and researchers could use systematics approach to evaluate PMBs (Posey et al., 2013).

J. Wang, Gupta, and Rao (2015) investigated the risk of insider threats associated with different applications within a financial institution and provided evidence of exposure of various applications to varying levels of risks. A. Ahmad, Maynard, and Shanks (2015) studied how an Australian financial organization, OZFinance, learns from security incident response. A. Ahmad et al. developed the dynamic security learning (DSL) process model to enable organizations to create novel structures and practices for gaining new security insights from any incident response. The DSL process model is composed of six security processes: (a) intuiting, (b) attending, (c) interpreting, (d) experimenting, (e) integrating, and (f) institutionalizing across the key organizational stakeholders (A. Ahmad et al., 2015).

Nowduri (2014) provided a detailed discussion on MIS and its impact of the global organizations and proposed four perspectives that will enable modern businesses to remain sustainable. J. Wang et al. (2015) extended the routine activity theory (RAT). The RAT is based on the assumption that people make a rational decision to commit violations but does not explain why under certain structured situation some people are motivated to commit crime while others are not (J. Wang et al., 2015). With increase in technology and awareness toward corporate sustainability, organizational leaders are implementing MIS as part of their business process (Nowduri, 2014).

Posey et al. (2013) identified and presented how corporate insiders classify 67 different PMBs and homogenous classes comprising of eight taxonomy categories which are logically grouped into 14 clusters. J. Wang et al. (2015) stated that RAT is useful in understanding insider threats and provided evidence of exposure to different applications to varying levels of risks. The focus of the four perspectives of corporate sustainability is prevailing competitive markets, natural environment, changing market technology and its innovation, and active collaboration between employee and employer, corporate rules and government regulations, and suppliers and corporate policies (Nowduri, 2014).

Budzak (2016) explored people issues relating to information security, including threats to information systems (ISs) and risks associated with ISs, and addressing mitigation of the threats through managing roles, responsibilities, relationships, and training. The regular and constant deployment of information security campaigns, training, induction and awareness helps to improve people knowledge and understanding of threats and risks to information security and how to mitigate those threats (Budzak, 2016). Parsons et al. (2015) examined the effect of organizational information security culture, rewards, and punishments on knowledge of policies and procedures, attitude toward policies and procedures, and self-reported behaviors of employees that may increase human-based cyber vulnerabilities. Parsons et al. posited that a significant positive relationship exists between information security decision-making and organization information security culture.

The senior management should consider the necessity of strategic cultural change to improve incorporation and enforcement of information security policy (Parsons et al., 2015). Wilding (2016) explored the move from cyber security to cyber resilience and outlined how an organization could approach preventing, detecting, responding, and recovering from cyber attacks with minimal damage to the company reputation and competitive advantage. Some of the suites for learning include phishing, social engineering, online safety, social media, bring your own device (BYOD), removal media, password safety, personal information, information handling, and remote and mobile working (Wilding, 2016).

Ali, Khan, and Vasilakos (2015) presented security issues from shared, visualized, and public nature of the cloud-computing paradigm. The main problem of legal issue about users' assets and laws governing cloud computing is geographical spread of cloud computing (Ali et al., 2015). Ali et al. noted that cloud security challenges occur at the communication, architectural, contractual, and legal levels. The most appropriate security solutions are development of countermeasures for communication and structural issues in the areas of virtualization, data storage, cloud applications and application programming interfaces (APIs), identity management and control, and contractual and legal (Ali et al., 2015).

Abawajy (2014) evaluated use of various delivery methods to create information security awareness to improve end user's knowledge and behavior on information security. Abawajy opined that video-based delivery method is most preferred delivery method, but combination of delivery methods is better than an individual security awareness delivery method. A. Ahmad, Bosua, and Scheepers (2014) discussed the findings of knowledge leakage mitigation and challenges that organizations face with knowledge leakage.

A. Ahmad, Bosua, et al. (2014) indicated that organizations do not have a formal, systematic, comprehensive, or strategic management approach for identification and protection of knowledge assets. Most businesses employ casual or informal approaches, focus on bottom-up approach, and delegate responsibilities to individuals and knowledge owners. Information security strategy is an art of deciding how to utilize the most appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defend an organization's information infrastructure(s) against internal and external threats.

The strategy involves offering confidentiality, integrity, and availability at the expense of least efforts and costs while aiming to be effective (A. Ahmad, Maynard, et al., 2014). Most senior managers are concerned about the confidentiality of organizations' operational data rather than protecting the firms' knowledge and information assets (A. Ahmad, Bosua, et al., 2014). Astuti and Nasution (2014) noted that 36% of SME leaders adopt IT solutions to minimize the effects of information security threats on company computer systems.

Digital Technology

Researchers discussed varying aspects of digital technology (Abebe, 2014; Alonso-Almeida & Llach, 2013; Colombo, Croce, & Grilli, 2013). Abebe (2014) examined the relationship between e-commerce adoption and SME performance, and whether the degree of entrepreneurial orientation moderates the relationship between e-commerce adoption and SME performance. Alonso-Almeida and Llach (2013) examined the impact of ICTs on the firm's human resources (HR) and organizational performance and analyzed the effect of ICT changes on the company's competitiveness. Colombo et al. (2013) investigated the impact of adoption of broadband Internet technology on productivity performance of SMEs.

Abebe (2014) demonstrated that a significantly positive relationship exists between e-commerce adoption and SME's average sales growth rate and adopters of e-commerce technology have significantly higher average sales growth rate than non-adopters. The significant positive relationship between e-commerce adoption and SME's annual sales growth is actively moderated at higher level of entrepreneurial orientation (Abebe, 2014). Colombo et al. (2013) demonstrated that SMEs operating in service industries resort more to broadband Internet technology than SMEs working in manufacturing sector.

Chairoel, Widyarto, and Pujani (2015) presented a conceptual framework regarding factors that influence ICT adoption and its impact on Indonesian SMEs. The conceptual factors comprised of external and external factors. Internal factor includes technology, organization, and managerial characteristics while external factor is environment. The adoption of ICT impacted an organization’s operational and financial performance, including profitability, time and cost savings, reduced costs, additional sales, productivity, and market value (Chairoel et al., 2015).

SME managers should carefully tailor the proper broadband applications to their industry-specific business needs and implement corresponding strategic and organizational changes (Colombo et al., 2013). Policymakers should design appropriate support schemes to help SME leaders fill the competency gaps to increase productivity of SMEs that adopt advanced broadband applications and support economic development (Colombo et al., 2013). Alonso-Almeida and Llach (2013) demonstrated that a significantly positive relationship exists between ICT and a firm’s competitiveness by enhancing HR and organizational performance.

Abebe (2014) provided empirical evidence of the role of e-commerce adoption and entrepreneurial orientation in SME performance while Alonso-Almeida and Llach (2013) provided useful insights into the positive effect of ICT on company’s competitiveness. Colombo et al. (2013) provided valuable insight into the impact of adopting broadband Internet technology on SMEs’ productivity. Mazzarol (2015) explored the impact of digital technology on small to medium enterprises. Mazzarol reviewed recent literature relating to SME’s adoption and use of digital technologies for e-commerce, e-marketing, and e-business implementation and strategy. Mazzarol demonstrated that SMEs adoption of ICT depend on the perception mindset of their owner-managers and highlighted the need for SME leaders to understand better the costs, risks, and benefits of investing in ICT.

Crossler et al. (2013) explored the challenges in behavioral information security, identified the challenges of behavioral information security research, and presented approaches that managers could utilize to address them. The behavioral information security research includes technical, behavioral, managerial, philosophical, and organizational strategies that address the protection and mitigation of risks to information assets (Crossler et al., 2013). K. H. Guo (2013) proposed a framework for conceptualizing security-related behavior.

The proposed conceptual framework for defining security-related behavior is composed of security assurance behavior (SAB), security compliant behavior (SCB), security risk-taking behavior (SRB), and security damaging behavior (SDB). K. H. Guo (2013) demonstrated that differences exist between these four types of security assurance behaviors. Hao and Song (2016) constructed a conceptual framework to examine how technology-driven strategic capabilities facilitate the development of strategic capabilities which may enhance firm performance. Hao and Song demonstrated that technology-driven strategy is positively related to technology capabilities and IT capabilities but negatively related to marketing skills and market-linking capabilities.

All types of strategic capabilities are positively related to firm performance. Hao and Song (2016) provided evidence that strategic skills play a mediating role between technology-driven strategy and corporate performance by facilitating the conversion of technology-driven strategy into superior firm performance. Understanding security behaviors of individuals will assist managers to improve positive security behaviors and decrease negative security behaviors, and provide researchers with insight into the design and implementation of security subsystems (Crossler et al., 2013).

Al-Ansari, Pervan, and Xu (2013) explored innovative characteristics of SMEs and link between innovation and business performance in an emerging economy. A significantly positive relationship exists between innovation and business performance (Al-Ansari et al., 2013). Al-Ansari et al. provided empirical evidence to support the positive impact of innovation on business performance. Cheng, Yang, and Sheu (2014) used the resource based theory to investigate inter-relationships between three types of eco-innovations and business performance. Cheng et al. demonstrated the direct and indirect effects of eco-organizational, eco-process, and eco-product innovations on business performance. IT capability is rare, difficult to imitate or substitute, firm specific, and a major source of differentiation and competitive advantage (Chae, Koh, & Prybutok, 2014). Chae et al. (2014) posited that no significant relationship exists between IT capability and firm financial performance.

Cyber security

Luiijf et al. (2013) noted that organizational leaders adopt cyber security to resist likely events from cyberspace that may compromise availability, integrity, or confidentiality of data stored, processed, or transmitted and of related services that ICT systems offer. According to Valli et al. (2014), 75% of SME leaders believe that their businesses are not target for cybercrime. Cyber attack against SMEs increased from 27% in 2009 to 63% in 2010 in United States (Rahman & Lackey, 2013) and from 60% in 2014 to 74% in 2015 in United Kingdom (Department for Business, Innovation & Skills, 2015). The four domains of cyber security include (a) intrusion detection, (b) denial of service attacks, (c) arbitrary code injection attacks, and (d) software vulnerability discovery (Holm et al., 2014).

Burton (2015) explored the type of challenges small states face in enhancing cyber security. Burton noted the growing cyber attack on private sector and public in New Zealand. With emergence of national cyber security strategies, New Zealand is struggling to formulate sustainable balance between privacy and safety in responding to cyber security issues (Burton, 2015).

Ali et al. (2015) presented security issues arising from shared, visualized, and public nature of cloud-computing paradigm. Ali et al. noted that cloud security challenges include problems at communication, architectural, contractual, and legal levels. The security solutions in literature involve developing countermeasures for communication and structural issues in the areas of virtualization, data storage, cloud applications and application programming interfaces (APIs), identity management and control, and contractual and legal (Ali et al., 2015).

Arlitsch and Edelman (2014) studied the steps and tools to minimize the impact of cyber security on people and organizations. Arlitsch and Edelman advised individuals and organizations to follow simple best practices to protect themselves from being the route of least resistance to potential hackers and limit danger and damage that can occur. Some of the best practices to reduce the risk of cyber attack and growing list of victims include thoughtful online transactions, cautious handling of own and others’ personal information, and diligence in management of information infrastructure. Other practices include timely application of device updates, proper data stewardship, password vault software, effective organizational responsibility, and proactive security practices in credit cards (Arlitsch & Edelman, 2014).

Ben-Asher and Gonzalez (2015) investigated the effect of knowledge in network operations and information security on the detection of intrusions in a simple system. Ben-Asher and Gonzalez demonstrated that an individual's level of awareness in cyber security supports correct detection of malicious events and decrease false classification of good events as malicious. Cyber security professionals can distinguish between different types of cyberattacks while a novice in cyber security is not sensitive to the various kinds of cyberattack (Ben-Asher & Gonzalez, 2015). Oluga et al. (2014) explored fundamental activities of the cyberspace and explained that cyber criminals perpetuate different forms of cybercrimes, which pose great threats to the cyberspace.

Some cyberspace activities include (a) cyber gaming, (b) cyber journalism, (c) cyber broadcasting, (d) cyber advertising, (e) cyber politics, (f) cyber medicine, (g) cyber governance, (h) cyber tourism, (i) cyber evangelism, (j) cyber mobilization, (k) cyber commerce, (l) cyber learning, (m) cyber entertainment, and (n) cyber socialization. The major contemporary cyberspace crimes and threats are (a) cyber harassment, (b) cyber defamation, (c) cyber impersonation, (d) cyber prostitution, (e) cyber child porno, (f) cyber gambling, (g) cyber fraud, and (h) cyber murder. Other cyberspace crimes and threats include (a) cyber warfare, (b) cyber espionage, (c) cyber terrorism, (d) cyber spoofing, (e) cyber service denial, (f) cyber piracy, (g) cyber-jacking, (h) cyber malware, (i) illicit cyber business, and (j) cyber blackmail (Oluga et al., 2014). Oluga et al. (2014)

noted that cyber criminals build networks and collaborate to organize some cyber havocs and pointed out that war against cybercrime should involve collaborative strategies at the individual, organizational, societal, national, and international levels.

M. Robinson, Jones, and Janice (2015) provided an analytical survey of the current state of research into the area of cyber warfare. M. Robinson et al. identified the challenging areas to cyber warfare research community. The areas are (a) early warning systems, (b) ethics of cyber warfare, (c) applying existing laws to cyber warfare, (d) conducting cyber warfare, (e) cyber weapons, (f) attribution problems, (g) cyber defense and deterrence, (h) conceptualizing cyber warfare, and (i) nation's perspectives. M. Robinson et al. noted that multi-disciplinary method is most appropriate approach for future research into cyber war or cyber warfare.

Transition

In Section 1, I introduced the proposed research study on strategies successful SME leaders use to minimize the effects of information security threats on business performance. Section 1 contains the background to the problem, problem and purpose statements, nature of the study, research question, and interview questions. Other contents include (a) conceptual framework, (b) operational definitions, (c) assumptions, limitations, and delimitations, (d) significance of the study, and (e) review of the academic and professional literature. The conceptual framework contains narrative on the use of GST and transformational leadership theory as lenses for this study. The potential for effecting positive social change is that business improvement could increase the flow of funds into the local economy and allow community leaders to build schools, health centers, and libraries for Port Harcourt city residents.

In Section 2, I discuss my role as the researcher, participants, research method and design, population and sampling techniques, ethical research, data collection, organization, and analysis; and reliability and validity. In Section 3, I present the study findings, discuss application to professional practice, implications to social change; and provide recommendations for action and further study, reflections, and a concluding statement.

Section 2: The Project

The purpose of this qualitative multiple case study was to explore strategies SME leaders use to minimize the effects of information security threats on business performance. I conducted semistructured interviews with five SME leaders to gain an in-depth understanding about the problem regarding lack of strategies to minimize the effects of information security threats on business performance. The focus of this section is purpose statement, role of the researcher, participants, research method and design, population and sampling, ethical research, data collection instrument, data collection technique, data organization technique, data analysis, and reliability and validity.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies SME leaders use to minimize the effects of information security threats on business performance. The population for the study consisted of five leaders in SME firms that support the oil and gas industry sector in the city of Port Harcourt, Nigeria, who have successfully developed and implemented strategies for minimizing the effects of information security threats in their businesses. The data from this study might provide SME leaders with an in-depth understanding of strategies that could help reduce the effects of information security threats on business performance. Implications for positive social change include business improvement, which can catalyze a greater flow of funds into the local economy, and could allow community leaders to build schools, health centers, and libraries for residents.

Role of the Researcher

The researcher is the primary instrument for data collection and analysis in qualitative research (Chan, Fung, & Chien, 2013). As the researcher in this qualitative multiple case study, my major role was to serve as the primary instrument for data collection to achieve the purpose of the research study. Other responsibilities of a qualitative researcher include (a) the review of available information, (b) identification and engagement of participants, (c) data collection, (d) data organization, (e) data analysis, (f) data interpretation, and (g) data storage and security (Yin, 2013).

The review of available literature was useful in establishing the appropriateness of the interview instrument for data collection. I identified and qualified prospective participants for the study against established criteria before engaging a minimum of five participants in the study. Purposive sampling technique was a useful tool for selection of participants from the population for face-to-face semistructured interviews. I organized the data collected and used the coding process to identify concurrent themes, analyze, and interpret the data from the interview questions to answer the central research question of the study.

As a certified protection professional of American Society of Industrial Securities, I have knowledge of information security risks and management systems. The motivation to carry out the study stemmed from my familiarity with the research topic and the desire to conduct a detailed literature review on the subject. I did not have any previous relationship with the participants. The semistructured interview involved five SME leaders in Port Harcourt.

My role as a researcher also involved adhering to the research ethics and Belmont research protocol. The aim of Belmont Report is to ensure that researchers adhere to three principles essential for ethical conduct of research: (a) respect for participants, (b) beneficence, and (c) justice (National Institutes of Health [NIH], 2015). Fiske and Hauser (2014) noted that Belmont Report enables researchers to respect respondents, minimize risks, maximize study benefits, and avoid impartial selection of participants. I adhered to the Belmont Report by respecting respondents, minimizing risks, maximizing study benefits, and avoiding impartial selection of participants.

I have attended the online NIH training course on protecting human research participants (Certificate Number: 1796019). The scanned copy of NIH certificate is attached in Appendix A and listed in the Table of Contents. Researchers attend NIH participant protection training to understand the informed consent process, protection of participants, benefit element of engagement, and how to manage ethical concerns in their research (Lantos & Spertus, 2014; Resnik, Miller, Kwok, Engel, & Sandler, 2015). Walden University (2010) maintains the ethical standards for research. Before commencing on the doctoral study, I applied for and obtained Walden University Institutional Review Board (IRB) approval (01-31-2017-0570167).

During the face-to-face data collection, I made efforts to collect data in a trustworthy manner and mitigate bias. Lamb (2013a) noted that writing memos and maintaining a reflective journal could help researchers discern the presence of a personal lens and reduce personal bias. I wrote notes and kept a reflective journal to help eliminate personal bias and enable me to interpret the behavior and reflections of the respondents.

By establishing rapport with the participants, I sought to engender honesty, trust, and respect. Onwuegbuzie and Hwang (2014) noted that qualitative researchers should ask open-ended questions and avoid asking leading and closed questions. By responding to open-ended questions, participants will provide useful insights on the strategies they use to minimize the effects of information security threats on their organizations. I asked open-ended questions to gather information from the participants.

Some strategies researchers use to mitigate their personal lens during data collection process include (a) careful construction of interview questions, (b) use of interview protocol, (c) transcript validation and review, (d) member checking, and (e) reaching data saturation (Cope, 2014; Foley & O'Connor, 2013; Thomas, 2015). Thomas (2015) used expert validation to ensure alignment of interview questions with research question and mitigate personal bias. I asked doctoral study committee members to validate the interview questions.

Foley and O'Connor (2013) noted that researchers develop and use interview protocol as a guide during interview to ensure collection of reliable data and consistency of the interview with each participant. I developed and used interview protocol to collect reliable data and ensured consistent interview process. Cope (2014) pointed out that some qualitative researchers request participants to validate and review the interview transcript to ensure they capture accurate interpretation of their perception of a phenomenon.

Researchers use member checking to verify, clarify, and augment interview data collected to mitigate personal bias (Houghton, Casey, Shaw, & Murphy, 2013; J. M. Jones & Sherr, 2014). I undertook member checking to validate interview data. To ensure data saturation, researchers collect data until no new information is available and themes are similar, which will also mitigate personal bias (Fusch & Ness, 2015). I collected data until no new information was available to achieve data saturation.

Participants

Elo et al. (2014) noted that researchers should state the criteria for selecting research participants to enable other researchers to evaluate the transferability of the research findings. Ketokivi and Choi (2014) noted that researchers establish a list of essential attributes to the study before identifying members of the target population who met the criteria. Most researchers select study participants with personal experience or knowledge of the research topic (Cleary, Horsfall, & Hayter, 2014; Hayes, Bonner, & Douglas, 2013).

Liu, Tang, Wang, and Lee (2013) outlined the criteria for selecting research participants. In this qualitative multiple case study, the research participants met certain criteria to qualify for selection from the target population. The criteria for selecting the study participants included (a) leadership in an SME firm that supported the oil and gas industry sector, (b) above 18 years of age, (c) knowledge of information security management, and (d) awareness of strategies for reducing the effect of information security threats on business performance. The criteria for selecting the research participants were appropriate for the current study because I chose only business leaders who had the competency and extensive knowledge to provide answers to the research question.

Some of the challenges associated with interviews include barriers to access to participants, power dynamics between researcher and participants, and differing culture and language (Drew, 2014). Researchers use calling, e-mailing, and face-to-face techniques to get access to research participants (Abrams, Wang, Song, & Galindo-Gonzalez, 2014; Bowden & Galindo-Gonzalez, 2015; Deakin & Wakefield, 2014; Synnot, Hill, Summers, & Taylor, 2014). I obtained a letter of corporation from an information security professional association and attended their meeting to identify potential participants. The scanned copy of the letter of corporation is attached in Appendix B and listed in the Table of Contents. Some of the values of e-mailing technique include (a) elimination of boundaries of time and space, (b) reduction of research cost, and (c) prioritization of participants' comfortability (Abrams et al., 2014; Bowden & Galindo-Gonzalez, 2015; Synnot et al., 2014). The strategies I used to gain access to potential participants included telephone call, e-mail, or face-to-face visit.

Siu, Hung, Lam, and Cheng (2013) advised researchers to establish a good relationship with participants. According to S. Gibson, Benson, and Brand (2013), the success of research depends on the relationship between researcher and participants. Cleary et al. (2014) noted the importance of building relationships and interactions between interviewers and interviewees, including verbal fluency and clarity, to gather in-depth information. Researchers and participants should have mutual respect and trust for each other, and researchers should use open communication to build trust and confidence of the study participants (S. Gibson et al., 2013; Siu et al., 2013).

My primary strategy for developing a good working relationship with the study participants was to use open communication to build their trust and confidence. Another strategy was to use informed consent forms. Other plans include assuring the study participants that (a) the research was for educational purposes, (b) they could withdraw at any time, and (c) I will uphold their confidentiality and anonymity.

Research Method and Design

In this section, I discuss the need to adopt appropriate research method and design to explore strategies SME leaders use to minimize the effects of information security threats on business performance. The rationale for selecting research method and design is to choose the most appropriate approach to answer the central research question (Hayes et al., 2013; Yin, 2014). I selected qualitative method and case study design for this study. In a similar study, Kongnso (2015) justified the use of qualitative multiple case study to explore the best practices to minimize data security breaches for increased business performance.

Research Method

I used qualitative research method for this study because of the exploratory nature of the research question: What strategies do SME leaders use to minimize the effects of information security threats on business performance? The choice of a research method depends on the research question, purpose, and context of the study (Venkatesh et al., 2013). Researchers use qualitative method, quantitative method, or mixed methods (Nelson & Evans, 2014; Runhaar et al., 2013; Venkatesh et al., 2013).

In a quantitative research method, researchers use close-ended questions to examine whether a relationship exists between variables and to test the study hypotheses by measuring specified study variables (Bahl & Wali, 2014; Runhaar et al., 2013). The fundamental components of a quantitative research are probability and statistics (Goertz & Mahoney, 2013). Quantitative researchers use numerical data to prove or disprove a hypothesis and to generate trends (Aykol & Leonidou, 2014). The quantitative method was not ideal for the study because I did not have specific variables, and the purpose of the research was not to examine trends or relations between variables but to explore successful information security strategies.

Researchers use a qualitative research method to explore meaning of an unknown event from the perspective of the participants to develop themes from the participants' experiences (Gioia et al., 2013; Nelson & Evans, 2014; Uluyol & Akci, 2014). The focus of qualitative research is to explore individual experiences, describe the phenomenon, or develop a theory (Cope, 2014). Qualitative researchers use dialogue to collect data from participants, which enables them to ask the *how* rather than the *how many* questions required in understanding the phenomenon to answer the research question (Cronin, 2014; Dasgupta, 2015). Qualitative researchers use written texts, transcribe individual or focused group interviews, and seek to understand meaning of experience and contribute to knowledge about people's lived experience (Grossoehme, 2014). Cope (2014) noted that qualitative research (a) is subjective, anecdotal, and subject to researcher bias, (b) involves findings from a sample that cannot be generalized to a population, and (c) lacks scientific rigor compared to quantitative research.

Researchers studying similar issues used qualitative research method to explain complex phenomena (P. Jones et al., 2014; Kongnso, 2015; Thomas, 2015; Webb, Ahmad, et al., 2014). Thomas (2015) used a qualitative method to explore retention strategies IT leaders use to retain IT professionals. Also, Kongnso (2015) used a qualitative method to investigate best practices to minimize data security breaches for increased business performance.

The qualitative method is useful in explaining phenomenon rather than predicting or measuring phenomenon (Houghton et al., 2013). The focus of the doctoral study was to explore strategies SME leaders use to minimize the effects of information security threats on business performance. The qualitative method was the most appropriate research method for this study because I established a working relationship with SME leaders and asked open-ended questions during the interview to explore information security strategies.

Mixed method research combines qualitative and quantitative research methods into one single study, which researchers use to examine and explore an issue (Archibald, 2016; Maxwell, 2016). Researchers assume that collecting diverse types of data will provide a better understanding of the research problem (Abro et al., 2015; Caruth, 2013; Frels & Onwuegbuzie, 2013; Venkatesh et al., 2013). Researchers use mixed methods when neither quantitative nor qualitative methods can provide adequate data to answer the research question, or if the research study requires one method to inform or clarify the other method (Abro et al., 2015; Venkatesh et al., 2013). The mixed method approach was not appropriate for this study because my intent for the research was not to examine but to explore information security strategies, which could be appropriate using qualitative method.

The focus of the doctoral study was to explore strategies SME leaders use to minimize the effects of information security threats on business performance. The choice of qualitative method was important because I served as an instrument for data collection and employed multiple methods of data collection to gather information to answer the research question. Researchers use qualitative methods to explain a phenomenon and provide useful insight to respond to research question. The qualitative approach was the most appropriate research method for this study.

Research Design

A case study research is a useful framework for exploring contemporary phenomenon within real-life settings (Cronin, 2014; Dasgupta, 2015; Morse & McEvoy, 2014). Yin (2014) posited that case study approach involves an in-depth exploration of a bounded area of process, activities, programs, or events of several individuals. I used qualitative multiple case study design in this study. Other qualitative designs I considered for this study include (a) ethnography, (b) narrative, (c) historical, (d) descriptive, and (e) phenomenology, but their attributes were not ideal for this study. The focus of this study was to explore strategies SME leaders use to minimize the effects of information security threats on business performance, which made qualitative multiple case study design the most appropriate research design for the study.

An ethnography design is the most basic form of social research for understanding the beliefs, behaviors, and issues of a culture-sharing group (Lopez-Dicastillo &

Belintxon, 2014). The ethnography researcher collects data through in-depth interview, archival research, and continuous observation of participants for a prolonged period (Cruz & Higginbottom, 2013). Ethnography researcher dwells with participants and use a strong theoretical orientation that shapes the study (Lindley et al., 2014; Zilber, 2014).

The ethnography design was a viable consideration, but I did not select the design because the purpose of the study was not to characterize the participants' everyday practices (Cunliffe & Karunanayake, 2013; Simpson et al., 2014). Furthermore, I did not select an ethnography design because SME leaders are not all from the same cultural group and I do not intend to dwell with the participants over a prolonged time. The ethnography design was not ideal for the study because the focus of my study was to gain an in-depth understanding of information security strategies rather than cultural beliefs of SME leaders.

Researchers use narrative or historical design to describe the experiences or the life of one or several individuals in chronological order (Beattie, 2014; Caine et al., 2013; Scutt & Hobson, 2013; C. C. Wang & Geale, 2015). The focus of narrative design is to tell the story of an individual or several individuals rather than exploring an in-depth understanding of business processes and practices. The narrative design was not ideal for the study because the focus of my study was not to compile the stories about the experiences or lives of SME leaders, but to explore successful information security strategies they use.

The qualitative descriptive design is a useful investigative analytical process for gathering information that may be lacking among business practitioners (Vaismoradi, Turunen, & Bondas, 2013). Researchers use descriptive design to provide the description of events and their background within specific geographic boundaries (Killam & Heerschap, 2013; Nelson & Evans, 2014). Blackburn (2014) used the descriptive design approach to investigate a subject matter in its change process. The descriptive design was not ideal for this study because the purpose of the research was not to describe events and its background in a location, but to explore information security strategies for a selected small case study population.

Many researchers use a phenomenological design to describe the essence of a phenomenon through individuals' lived experience and perceptions of the event (Cibangu & Hepworth, 2016; Hou et al., 2013; Mohlameane & Ruxwana, 2014). Researchers use phenomenological approach to understand an individual's lived experiences and perceptions rather than practices, processes, and programs (Roberts, 2013). The phenomenological design was not appropriate for this study because the purpose of the study was to explore useful information security strategies, and not lived experiences and perceptions of individuals.

In a case study analysis, a researcher explores an in-depth analysis of complex social and technical case or multiple cases to gain an understanding of the case or cases aimed at improving business practice (Yin, 2014). The other qualitative designs may provide better control than case study approach, but they are more limited in context or ability to find alternative explanations than case study approach (Cao, Thompson, & Triche, 2013). Researchers use case study designs to focus on a case and retain a holistic and real world perspective; such as in studying individual life cycles, small group behavior, and organizational and managerial processes (Henry & Foss, 2015; Yin, 2014). Researchers studying similar issues on strategies corporate leaders use to improve business performance also used qualitative case study design (P. Jones et al., 2014; Thomas, 2015; Webb, Ahmad, et al., 2014; Webb, Maynard, et al., 2014). The case study approach enabled me to ask the *how* and *what* questions required in understanding strategies SME leaders use to minimize the effects of information security threats, which made case study the most appropriate design for this study.

Yin (2014) outlined three types of case studies: (a) descriptive, (b) explanatory, and (c) exploratory. De Massis and Kotlar (2014) noted that exploratory case study is most appropriate if the researcher's aim is to understand how and why a phenomenon takes place. Yin posited that investigators use exploratory case study to analyze data from the interview. Researchers conduct descriptive case study to explain to readers the relevance of an event (De Massis & Kotlar, 2014). The exploratory case was most appropriate for this study because the purpose of the research was to explore in depth the meaning and understanding of strategies SME leaders use to minimize the effects of information security threats on business performance.

De Massis and Kotlar (2014) indicated that case study research is the most adopted qualitative method in organizational studies because researchers have significant opportunities to advance the theoretical understanding of firms and contribute to business literature. Researchers could conduct either a single case study involving an organization and location or a multiple case study involving multiple organizations and locations (Yin, 2014). The rationale for single-case designs includes critical, unusual, common, revelatory, and longitudinal reasons while the justification for multiple-case designs is the understanding of literal and theoretical replications of the study (Yin, 2014).

Qualitative researchers prefer multiple-case design to single-case design because of the substantial analytical benefits from two or more cases which include induction of productive and reliable models (Vohra, 2014; Yin, 2013). Creswell (2013) advised researchers to conduct not more than four to five cases. The multiple case study approach is a more effective strategy than single case study approach because numerous cases add external validity and resist observer bias (Landers & Behrend, 2015; Newman, Joseph, & Feitosa, 2015). I used multiple case study approach for this study.

Fusch and Ness (2015) posited that researchers ensure data saturation by collecting data until no new information is available and themes are similar. Data saturation occurs when a researcher reaches a point when additional sampling will not yield new information to answer the research question (Kornbluh, 2015; Morse, 2015). I collected data until no new information is available to achieve data saturation.

The multiple case study approach was the most appropriate research design because the purpose of the doctoral study was to explore strategies SME leaders use to minimize the effects of information security threats on business performance. In a similar study, Kongnso (2015) used qualitative multiple case study to explore the best practices to reduce data security breaches for increased business performance. This study involved a multiple-case design of five case organizations.

I adopted myself as the instrument for the qualitative study and personally, used open-ended questions, emerging approaches, and text or image data to understand information security strategies. The targeted population are SME leaders who adopted strategies that successfully reduced the effects of information security threats on their business performance. By using a qualitative multiple case study, I obtained useful insight to answer the research question on what strategies SME leaders use to minimize the effects of information security threats on business performance.

Population and Sampling

In this section, I discuss the population from which to select the study samples. The focus was to describe and justify the sampling methods and number of participants, identify how to ensure data saturation, and explain how the criteria for selecting participants and interview setting are appropriate to the study. The overall success and acceptability of a study depends on the sampling technique the researcher uses to determine the sample size of the research participants (Guetterman, 2015).

Qualitative researchers use purposive sampling to select and gather appropriate information from the sample population who have relevant experience and qualification required to answer the research questions (Yin, 2014). Moss, Gibson, and Dollarhide (2014) posited that purposeful sampling is the most appropriate method for identifying participants with expert knowledge of a subject matter. Awiagah et al. (2016) pointed out that purposive sampling is a non-probability sampling technique that researchers use to select participants regarding their knowledge and professional judgment. Guetterman (2015) opined that qualitative sampling is a matter of information richness rather than a question of representative opinions because the appropriateness and adequacy of the sampling technique are paramount in qualitative sampling.

Smith, Colombi, and Wirthlin (2013) explained that researchers use purposive sampling to identify the study participants with knowledge of the business problem and will provide the data needed to answer the research question. Ishak and Bakar (2014) stated that purposive sampling is appropriate for case study research while Guetterman (2015) used purposive sampling to select information-rich case studies. Sangestani and Khatiban (2013) explained that researchers use purposive sampling to select deliberately research participants that meet established criteria which the researcher assumed to be a representative of the study population.

Palinkas et al. (2015) indicated that qualitative researchers widely use purposive sampling to identify and select information-rich cases relevant to the phenomenon of interest. The four-point approach to sampling in qualitative interview-based research are (a) defining the sample universe, (b) deciding upon the sample size, (c) selecting the sample size, and (d) sample sourcing (O. C. Robinson, 2014). I used the purposive sampling technique to select the research participants.

The purposive sampling is the most appropriate sampling technique that enabled me to select the participants with adequate knowledge and understanding of the area of research (Sangestani & Khatiban, 2013; Smith et al., 2013). Gentles, Charles, Ploeg, and McKibbon (2015) posited that purposeful sampling is the most common means of sampling in qualitative research. Wara and Singh (2015) used the purposive sampling technique to select participants that were members of the organizations’ teams, who are responsible for managing security incidents in their organizations. I used the purposive sampling technique to select the research participants who fit the criteria for this study on strategies SME leaders use to minimize the effects of information security threats on business performance**.**

The non-probabilistic snowball sampling is a viable sampling technique to identify the initial study participant who will assist to provide the names of potential participants for the study to make a homogenous sampling of participants. Jarvelainen (2013) stated that homogenous sampling would enable a researcher to identify research participants with similar features relevant to the research question. O. C. Robinson (2014) explained that researchers maintain a measure of sample homogeneity to remain contextualized within a defined setting and are cautious in generalizing the study finding, but could localize the study finding to the sample universe. The snowball sampling technique was not appropriate for the proposed study because the purpose of the research is to select participants with extensive expertise in information security strategies.

The target sample size for the doctoral study was five research participants. The sample size is the number of study participants required to achieve data saturation. Researchers achieve data saturation at the point when no new information is available and the codes, themes, or theory are similar (Fusch & Ness, 2015). Guetterman (2015) noted that methodologists advocated the use of grounded theory concept of theoretical saturation as the indicator of a sufficient sample size, but argued that data saturation might not be the best marker of an adequate sample size. Marshall, Cardon, Poddar, and Fontenot (2013) examined IS qualitative studies and posited that most researchers showed little or no rigor to justify their sample size.

The sample size in qualitative studies is contingent to many considerations. Halverson, Graham, Spring, Drysdale, and Henrie (2014) opined that sample size depends on the experience and available publications in methodological and topical trends about the depth of data collected. The sample size in qualitative studies also depends on resource availability (Guetterman, 2015).

The estimation of sample size is important to research process because researchers use sample size to confirm the validity and reliability of their study (Guetterman, 2015). In qualitative research, the quality of data is more important than the quantity of data (Cleary et al., 2014). While researchers use data saturation to obtain accurate and valid data, using too large a small or too little a sample may not ensure data saturation (Fusch & Ness, 2015). The use of small sample size could result in biased results and inability to attend data saturation while large sample size could lead to extensive resources.

Halverson et al. (2014) noted that researchers could justify the use of sample size through maximum participation and monitoring of responses to identify the data saturation point. Yin (2014) stated that three research participants could produce reliable and valuable data, which is adequate to answer the research question without relying on large sample size. Guetterman (2015) pointed out that researchers might determine the sample size using judgment and experience to evaluate the quality of information against its intended uses. Boddy (2016) opined that researchers could justify the use of samples sizes as low as one.

Researchers studying similar issues reported using a varying number of research participants to collect data for their studies. Sangestani and Khatiban (2013) noted that researchers use the best judgment to select the study participants. Most qualitative researchers justify their sample size through counting of themes (Emmel, 2015). I used a sample size of five research participants from five case organizations.

Guetterman (2015) posited that qualitative sampling is an iterative series of decisions throughout the process of research rather than a single planning decision. I maintained iterative series of actions with the study participants throughout the research process. Data saturation is reached when no new information is available and the themes are similar (Fusch & Ness, 2015). I collected data until no new information was available to achieve data saturation. The purposive sampling of five SME leaders was appropriate to attain data saturation.

Qualitative researchers select study participants with personal experience or knowledge of the research topic (Cleary et al., 2014; Hayes et al., 2013). I selected a sample of SME leaders who met either of the following criteria: (a) serves in leadership role in a SME such as Chief Executive Officer (CEO) or Managing Director (MD) or (b) knowledge of information security management such as Chief Information Officer (CIO) or IT Manager. All participants were working in Port Harcourt, Nigeria.

The selected participants have extensive knowledge in information security management to answer the research question. The venue for the face-to-face semistructured interview was at the participant's office. The criteria for selecting participants and location for the interview were appropriate for the study.

Ethical Research

The success of a research study depends on how researchers treat research participants. Before data collection, I applied for and obtained Walden University IRB approval (01-31-2017-0570167), and included the IRB approval number in the final doctoral study manuscript. The purpose of an IRB approval is to assure that (a) potential benefits outweigh potential risks from the combined view of stakeholders, researcher, and university, and (b) researchers are in full compliance with United States (US) federal regulations. The IRB approval decisions depend on the three philosophical principles of the Belmont Report: (a) justice, (b) beneficence, and (c) respect for persons. The purpose of the signed informed consent forms is to provide evidence that participants understand the purpose of the study, the withdrawal process, the disclosure of incentive, and security of data.

Upon receipt of IRB approval (01-31-2017-0570167), I adopted the following process to achieve the informed consent of the research participants:

1. Attended information security professional association meeting to identify potential participants who met the study criteria.
2. Spoke or sent an e-mail or text message to prospective study participants to secure commitment.
3. Sent letter of introduction to potential participants to explain the purpose of the study, the criteria for selection, and the benefits of the research and request for their cooperation. I attached a sample of the introduction letter in Appendix B and listed the introduction letter in the table of contents.

4. Sent the consent form to each participant through electronic mail or face-to-face communication to read and sign to obtain their informed consent.
5. Ensured the respondents are aware of their right to withdraw at any point and the Walden University contact person to correspond with if in need for further clarifications.
6. Ensured the participants have a full understanding of their roles in the study.

To comply with ethical research, I adopted the principles entrenched in the Walden IRB approval as a guide in conducting the study on strategies to minimize the effects of information security threats on business performance. The critical component of every research study is the informed consent form (Nishimura et al., 2013). Vanclay, Baines, and Taylor (2013) identified some ethical principles, which include (a) respect for participants, (b) informed consent, and (c) presumption and preservation of anonymity. Baines, Taylor, and Vanclay (2013) recommended the use of signed consent forms and ethical approval for projects.

The aim of the informed consent form is for researchers to protect the confidentiality and privacy of the participants (Baines et al., 2013; Nishimura et al., 2013; Vanclay et al., 2013). Researchers use the informed consent form to inform participants of their right to participate voluntarily in the study, and the liberty to withdraw at any time they wish during the study (S. Gibson et al., 2013). Participants who want to participate in the study will evidence their consent by completing and signing the consent form (S. Gibson et al., 2013; Lihong & Miguel, 2013; Newington & Metcalfe, 2014).

Newington and Metcalfe (2014) stated that researchers provide participants with the informed consent form to acknowledge confidentiality and protect their rights during the data collection process. Lihong and Miguel (2013) posited that respondents sign the informed consent form to acknowledge their willingness to participate in the study. The aim of the informed consent form is to ensure adherence to ethical standards while protecting and respecting the rights of the participants (Chiumento, Khan, Rahman, & Frith, 2016). I requested all respondents to sign the informed consent form before commencing on the data collection process.

The research study was voluntary, and research participants were free to withdraw from the research at any time from the pre-interview question, through stopping the interview before completion, to not member checking the transcript. The participant can inform me of their intention to withdrawal from the research study by face-to-face contact, or telephone, or e-mail, or text message. The research participant will not suffer a penalty for withdrawing from the study. The interview was at the respondent's convenient date and time, with strict adherence to all protocols in conducting an interview.

Guetterman (2015) posited that offering incentive could increase the response rate of a study. K. Chen, Lei, Li, Huang, and Mu (2014) asserted that using incentive or reward increased the turnout of their face-to-face survey. The use of incentives often implies the bribery of the research participants (Guetterman, 2015). Some researchers do not give incentives to study participants due to ethical concerns and the financial constraints of the investigators (K. Chen et al., 2014). The participants did not receive any form of compensation for participating in this study.

Killawi et al. (2014) explained the need for researchers to protect identifiable information about participants in their studies. To ensure confidentiality, the identities of the participants will remain anonymous. I will keep the research data anonymous and confidential to assure adequate ethical protection of the respondents. The names of the research participants and the case organizations will be anonymous to ensure confidentiality.

I did not disclose the names or identifiable information of the respondents or the case organizations in the consent form, interview protocol, or anywhere in the study document. Yin (2014) pointed out that coding of participants with letters and numbers protects the confidentiality and privacy of the participants. I used fictional letters and figures to identify the respondents to protect the confidentiality and privacy of the participants.

To maintain confidentiality and privacy of the participants, I used the letters A through E to represent the case organizations, and numbers 1 through 5 to describe the study participants on the transcripts and research log. For example, the first respondent was coded A1, while the second respondent and third respondent were coded B2 and C3 respectively. By using unique and pseudo identifiers, the study participants are confident that I will not share their personal information in the study. I am the only person that analyzed and had access to all raw data collection files containing the interview recordings, transcripts, and notes.

I maintain the electronic research data in hard drive password-protected file storage and laptop computer for a minimum of 5 years to protect the confidentiality of study participants. I save and store the signed informed consent forms and all raw data collected in a secure fireproof locker for 5 years from my expected completion date. No person will have access to the personal information of the research participants. The names of individuals and organizations will remain anonymous to ensure the confidentiality of the participants and their companies. After 5 years of completion of the study, I will destroy all data associated with the research by permanently deleting all the electronic data and burning all raw data.

Data Collection Instruments

The primary data collection instrument in qualitative research is the researcher (Chan et al., 2013; Sarma, 2015; Yin, 2014). The goal of this qualitative exploratory multiple case study was to explore strategies SME leaders use to minimize the effects of information security threats on business performance. As the primary data collection instrument, I developed and used the interview protocol to conduct an in-depth semistructured face-to-face interview with the participants.

I attached a sample of interview protocol (see Appendix D) and listed in table of contents. The duration of the interview was 45-60 minutes at participant’s convenient date and time. I augmented the interview data with observations and evaluation of the company data from documents and archival records.

Researchers review business records to obtain valuable qualitative data, which when analyzed together with interviews and observations, can reveal research themes

(Langen et al., 2014; Yin, 2014). Qualitative researchers triangulate interview data with multiple data sources to increase the credibility, reliability, and validity of their study (Yin, 2014). Harrison, Banks, Pollack, O'Boyle, and Short (2017) noted that researchers use triangulation approach to mitigate research biases and increase the confidence in the study findings. Dasgupta (2015) demonstrated that interview method provides in-depth information about an organization's idiosyncrasies.

Qualitative researchers use interviews, observation, and document review methods for data collection (Awiagah et al., 2016; Cao et al., 2013; Dasgupta, 2015; P. Jones et al., 2014). Qualitative researchers use interviews, observation, and documents review methods to understand the phenomenon within a real-world setting by identifying *how* and *why* of the phenomenon (Cao et al., 2013). In this study, I used the following data collection methods: (a) interview, (b) observations, and (c) assessment of official papers such as company documents, archival records, and external sources including business magazines, sector sources, and Internet websites.

The semistructured interview is a valid data collection instrument that qualitative researchers use to collect data from participants (Doody & Noonan, 2013; Yin, 2014). De Massis and Kotlar (2014) noted that researchers use semistructured interviews to gather data to guide against bias. Doody and Noonan (2013) stated that researchers use interviews to uncover details behind a participant's experience. Mealer and Jones (2014) found that researchers use face-to-face interviews to establish rapport and connect with participants while non-verbal communication was essential in fostering trust and compassion. Using interview technique provides participants the opportunity to express their experiences and perceptions freely (Johnson & Bibbo, 2014; S. Pandey & Chawla, 2016).

I conducted a face-to-face semistructured interview with each participant. The semistructured interview will enable the participants to provide an in-depth understanding of the topic (Cao et al., 2013). Building trust with participant is important in qualitative data collection (Fjellström & Guttormsen, 2016; S. Gibson et al., 2013; Siu et al., 2013). The use of open-ended questions will enable respondents to discourse on the topic in their own terms (P. Jones et al., 2014; S. Pandey & Chawla, 2016).

As the data collection instrument, my primary strategy was to develop credibility and trust with participants through the use of open-ended questions. Each participant was expected to answer 10 open-ended interview questions freely. By asking open-ended questions, a researcher interacts with respondents, allowing them to expand their responses, and obtains useful insights to answer the research question (O'Keeffe, Buytaert, Mijic, Brozovic, & Sinha, 2015; S. Pandey & Chawla, 2016).

P. Jones et al. (2014) noted the need to ask related questions that will prompt responses to ensure a more reliable link to the research themes. Researchers ask the same probing questions to participants to obtain a diverse range of answers and interactions to achieve data saturation (Newington & Metcalfe, 2014). I asked the same questions to the participants to obtain diverse answers and achieve data saturation.

Qualitative researchers derive interview questions from central research question to ensure the interview questions align with the research question. The interview technique composed of detailed and organized open-ended questions that engaged the participants to provide comprehensive responses. Thomas (2015) used expert panel to validate the interview questions and enhance the reliability of the instrument. The doctoral study committee provided the external evaluation of the research process. I presented interview questions to follow DBA students and doctoral study committee for expert review to ensure the research instrument is reliable before administering the research tool to research participants.

Qualitative researchers ask the same interview questions to each participant to gain information about the topic or further explore responses (Doody & Noonan, 2013). Researchers guide against researcher bias by avoiding asking leading questions to ensure credibility and reliability (Onwuegbuzie & Hwang, 2014). By using the interview protocol, I posed the same question in the same sequence to each participant.

By posting the same question in the same series to the participants, researchers can identify themes (Hermanowicz, 2013) and efficient data analysis and comparison (Bredart, Marrel, Abetz-Webb, Lasch, & Acquadro, 2014). By answering the questions, the participants discussed the strategies they use to minimize the effects of information security threats on their businesses. I used the interview protocol to ensure a consistent interview process and guide against personal bias.

Many researchers use member checking to verify the accuracy of the interview response with the participant (Houghton et al., 2013). Houghton et al. (2013) noted that researchers use member checking to assure rigor in case studies. After the interview, I transcribed the recorded interview and shared the interview interpretation with participants through e-mail for transcript validation and review and member checking.

Throughout the study process, I kept participants abreast with information on the study. The study participants confirmed that interpreted interview transcript represent what they intend to say, and clarified any ambiguous or unintended responses.

Member checking is a useful quality control process to verify, clarify, and augment data collected through an interview in a qualitative study (J. M. Jones & Sherr, 2014). Harvey (2015) developed the dialogic qualitative interview design to address the limitations of member-checking. Harvey demonstrated that the dialogic qualitative interview model is a more collaborative and ethical alternative to member-checking. I did not conduct a pilot study of the interview protocol because the accurate recording of participant’s responses and member checking were adequate to verify the effectiveness of the interview protocol.

Data Collection Technique

Data collection technique depends on the research design approach that will most appropriately answer the research question (Yin, 2014). The most appropriate research approach that I used to answer the research question was multiple case study design. O. C. Robinson (2014) presented four-point approach to qualitative sampling integrated theory and process. The four-point approach are (a) defining a sample universe, (b) deciding on sample size, (c) selecting sampling strategy, and (d) sourcing sample cases including matters of advertising, incentivizing, avoidance of bias, and ethical concerns about the informed consent form. I used the four-point approach to collect data.

Yin (2014) identified six sources of data collection techniques in a case study inquiry. These include (a) interview, (b) documentation, (c) direct observation, (d) archival records, (e) participant-observation, and (f) physical artifacts. Researchers use data source triangulation, the collection of data from different types of people, to gain multiple perspectives and broaden their understanding of the phenomenon of interest and validation of data (N. Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). I used qualitative multiple case study approach and interview, observation, documents review, and audiotape for data collection.

Interviews constituted the primary source of data while the secondary sources of evidence include observations and records. The research design, data collection techniques, and implementation of data collection methods were appropriate to answer the research question. Before commencing on data collection, I applied for and obtained the IRB approval from the University (01-31-2017-0570167) and the signed informed consent forms from the participants.

N. Carter et al. (2014) explained that selection of the type of interview depends on the purpose of the study and availability of resources. The purpose for this study was to explore strategies business leaders use to minimize the effects of information security threats, which made the semistructured interview with open-ended questions the most appropriate data collection technique. Doody and Noonan (2013) advised researchers to develop an interview guide before collecting data.

I used the interview protocol during the interview with each participant. The sample of the interview protocol is attached in Appendix D and listed in the Table of Contents. I used semistructured interview as the data collection method and member checking process to verify the accuracy of interpretation of the interview transcript. The use of semistructured interview was helpful in asking probing questions that will instigate expanded answers. At the instance of the participants, I rephrased the interview questions to ensure clarity.

The audio-recorded interview is helpful in ensuring accurate rendition because researchers could re-listen to all or parts of the interview (Gale, Heath, Cameron, Rashid, & Redwood, 2013). I recorded the interview using a high-quality audio recorder and a backup with a Smartphone recorder. During the interview meetings, I took notes of my observations, feelings, and thoughts, and the facial expressions, voice tones, and body language of the participants. Member checking is a useful quality control process to verify, clarify, and augment data collected through a meeting in a qualitative study to improve credibility, transferability, and validity of recorded interviews (Cope, 2014; Houghton et al., 2013; J. M. Jones & Sherr, 2014).

I produced word-for-word transcription and interpretation of the interview including detailed notes and shared with participants to verify accurate capturing of their responses to the interview questions. Houghton et al. (2013) noted that member checking is an important strategy for assuring rigor of qualitative study. I conducted the member verification process within 48 hours from the interview date to ensure that participants still remember their original responses to the interview questions.

Some researchers use transcriptions, notes, and research logs to discover themes, patterns, and trends to draw meaning from the participants' responses to ensure reliability and validity of the study (Yin, 2014). The research journal is a useful quality control tool researchers use during fieldwork to record personal thoughts and observations in a systematic manner (Lamb, 2013a, 2013b). Researchers use research log to (a) minimize potential biases throughout the study, (b) provide a valuable audit trail for conformability, and (c) identify and reflect on challenges that might occur during the study (Houghton et al., 2013). I took interview notes in a research log to contribute to the reliability and validity of the research.

The second source of data include documents on company's information security management practices including but not limited to plans, e-mails, risk assessment reports, incident reports, backup reports, budget, patches, application updates, and other internal records. The third source of data include documents from archival records such as previous information security budgets, risk assessments, and incidents. The goal of reviewing the company data is to explore information regarding strategies they are using to minimize the effects of information security threats. The fourth source of data was observations of the firms' information security practices.

Harrison et al. (2017) opined that researchers use triangulation approach to mitigate research biases and increase the confidence in the study findings. Cope (2014) and Houghton et al. (2013) explained that researchers use method triangulation to enhance credibility and trustworthiness in qualitative research. I augmented interview data with observations, company documents, and archival records to achieve methodological triangulation.

An important factor to consider in qualitative research is whether to conduct pilot study of the interview protocol (Cleary et al., 2014). Awiagah et al. (2016) conducted a pilot study with members of study population to assess the easiness of comprehending the study questions. Thomas (2015) used experts to validate the interview questions. I did not conduct a pilot study but used expert validation strategy to obtain the views of the doctoral study committee experts on the interview questions.

Data Organization Technique

Researchers use various techniques in the data organization phase to identify the empirical material collected in the field (Soares & de Oliveira, 2016). The sources of data include interview, company documents, and observation. In this section, I discuss the techniques for organizing all the data collected, safe storage of data (electronic and hard copies), and destruction of data after 5 years.

The focus of data organization is to identify the emerging themes, patterns, and trends from the interview (Yin, 2014). Researchers code data and organize data into categories to support identification of themes and ideas during data analysis (Gale et al., 2013; Houghton et al., 2013; Zamawe, 2015). Researchers and scholars use computer-assisted qualitative data analysis software (CAQDAS) or programs for the data organization of interview responses and data from other sources (Myers & Lampropoulou, 2013; Thomas, 2015; Woods, Paulus, Atkins, & Macklin, 2016).

The key CAQDAS are ATLAS.ti and NVivo software (Woods et al., 2016). Most qualitative researchers use CAQDAS in the data organization process to identify emerging themes, patterns, trends, and dominant topics from the interview (Guo, Porschitz, & Alves, 2013; Woods et al., 2016). I used the NVivo software for data storage and organization.

Researchers code qualitative data to enable analysis, organization, and comparison of data to extract meaningful information (Gale et al., 2013). Houghton et al. (2013) stated that researchers use data coding to simplify the process of comparing and identifying patterns. After each interview, I coded and organized the raw data, documents, and observations with notes taken during the meeting in a folder labeled for each participant. I created a case study database to track the research evidence to ensure efficient development of the case histories, reliability, and consistency.

The case study database comprised of written and electronic notes on each participant, organized and categorized in alphabetical order. I also maintained a documentary system of research logs, reflective journals, and cataloging or labeling systems. I converted all the recorded interviews with study participants to text using Microsoft Word document and securely stored the interview transcript. The research participants are aware of the process for safe storage of research data.

I was the only person who analyzed and had access to all raw data collection files containing the participants' signed informed consent forms, the interview recordings, transcripts, and notes. I stored and saved all electronic data in files in a password-protected folder and stored all raw data in a fireproof locked locker for 5 years from my expected completion date. After 5 years, I will permanently delete all the electronic data and burn all raw data associated with the study.

Data Analysis

The analysis of qualitative data involves the thematic exploration of the data collected through observation, interview, and other qualitative data collection technique

(Yin, 2014). Researchers identified four types of triangulation: (a) data source triangulation, (b) analysis triangulation, (c) theoretical or perspective triangulation, and (d) methods triangulation (Carter et al., 2014; Yin, 2013). Data source triangulation involves the collection of data from different types of people to gain multiple perspectives and validation of data (Carter et al., 2014; Cope, 2014; Houghton et al., 2013). Analysis triangulation involves the participation of two or more researchers in a study to provide multiple observations and conclusions (Carter et al., 2014).

Theoretical or perspective triangulation involves the use of different theories to analyze and interpret data (Carter et al., 2014). Method triangulation involves the use multiple methods to collect research data about the same phenomenon (Carter et al., 2014; Cope, 2014; Houghton et al., 2013). Researchers use method triangulation as the primary strategy to enhance credibility and trustworthiness in qualitative research (Carter et al., 2014; Houghton et al., 2013).

Heale and Forbes (2013) noted that qualitative researchers use methodological triangulation to attain a higher comprehensive picture of a phenomenon than using a single type of data. The data source triangulation and method triangulation can strengthen the validity of case study evaluations (Yin, 2013). I used method triangulation strategy to obtain research data through interview, observation, company documents, and journal articles.

The four primary strategies researchers use to analyze case study evidence include (a) rely on theoretical propositions, (b) work with quantitative and qualitative data, (c) develop a case description, and (d) examine plausible rival explanations (Yin, 2014). I used qualitative data for data analysis. The five analytical techniques researchers use to implement the strategies for analyzing case study evidence include (a) pattern matching, (b) time-series analysis, (c) explanation building, (d) logic models, and (e) cross-case synthesis (Yin, 2014). I used the pattern matching technique to identify themes during data analysis.

Gale et al. (2013) presented a step-by-step guide on the application of a framework method for the management and analysis of qualitative data. The framework method involves the thematic analysis of textual data to identify commonalities and differences, before focusing on relationships between different parts of data and drawing a descriptive or an explanatory conclusion that clustered around themes (Gale et al., 2013). I used the thematic analysis method to apply and ascribe meaning to the transcribed interview recordings including notes and observations, and company documents.

Gale et al. (2013) presented a seven-stage approach for the analysis of qualitative data: (a) transcription, (b) formalization with the interview, (c) coding, (d) develop a working analytical framework, (e) apply the analytical framework, (f) chart data into the matrix, and (g) interpret the data. I adopted the seven stages of analysis outlined in the framework method during the analysis of the qualitative data. The first step is to transcribe the audiotaped interviews, interview questions, and interview notes into Microsoft Word document. The second phase is to become familiar with the interview using the audio recording and transcript and contextual or reflective notes to identify and remove irrelevant data that does not conform to the search criteria (Gale et al., 2013).

The third step is coding, which involves the classification of all the data for systematic comparison with other parts of the data set (Gale et al., 2013). The NVivo tool is a beneficial data management tool that can provide a comprehensive audit trail to depict decisions made during the research process (W. Gibson, Webb, & Lehn, 2014; Houghton et al., 2013; Myers & Lampropoulou, 2013). During data analysis, I uploaded the interview transcripts and external documents into the NVivo tool and identified the emerging themes, trends, and patterns.

Yin (2014) suggested that researchers should note conflicting participants' interpretations, alternative perspectives, and critiques. I took note of the discrepancies in the participants' interpretations, perspectives, and evaluations to the interview questions. During the coding of the interview transcript, researchers look for common patterns, themes, and categories that relate to the research question to identify new additional codes that may emerge (Yin, 2014). Digital coding using NVivo software is useful in automatically keeping track of new codes (Gale et al., 2013).

Houghton et al. (2013) noted that NVivo software is beneficial as a data management tool that can provide a comprehensive audit trail to depict decisions made during the research process. Edwards-Jones (2014) noted that NVivo software is a useful tool for data management and analysis of a complex multi-data source, and involves planning, storing, managing, collating, analyzing, visualizing, and presenting data. Thomas (2015) used auto-coding feature in the NVivo software to code qualitative data. I used the NVivo software for coding of the interview transcript, documents, and observations to identify the prominent words the respondents use frequently during the interview.

The fourth step is to group the codes into categories to form the working analytical framework (Gale et al., 2013). In the fifth step, I applied the working practical framework to the NVivo software tool to identify themes emerging from the interview data, company documents, and observations. The sixth step involve the use a spreadsheet to generate a matrix and chart data into the model (Gale et al., 2013). Researchers use the charting process to summarize the data by category from each transcript including references to interesting or illustrative quotations.

The focus is to achieve the study purpose by extrapolating the key themes and address the research question. The final step involves the interpretation of data to identify the characteristics of and differences between the data (Gale et al., 2013). My focus at this stage was to correlate the key themes emerging from the interviews with the recent literature and conceptual frameworks. I used the NVivo software to input, store, code, explore themes and patterns, and align collected data with recent literature.

The conceptual framework connects the literature, methodology, and study findings (Borrego, Foster, & Froyd, 2014). I analyzed data in view of GST and transformational leadership theory. Researchers use GST as lens to understand the wholeness of organization systems by emphasizing on related functions, including management and leadership (Von Bertalanffy, 1969).

By correlating the key themes with the propositions of the GST, I explored strategies SME leaders use regarding the concept of the wholeness to minimize the effects of information security threats on business performance. Researchers use the transformational leadership theory as lens to understand leadership on the premise that leaders can inspire followers to change expectations, perceptions, and motivations to work toward common goals (Burns, 1978). I used the propositions of the transformational leadership theory to explore the transformational characteristics SME leaders use to implement strategies that reduce the effects of information security threats on business performance.

Reliability and Validity

The criteria for evaluating the quality of qualitative research study include (a) validity, (b) reliability, and (c) generalizability (Leung, 2015; Loh, 2013). Birt, Scott, Cavers, Campbell, and Walter (2016) posited that trustworthiness of research findings underpins high quality qualitative research. In this section, I discuss the criteria for establishing reliability and validity in this qualitative multiple case study.

Reliability

Researchers should establish the reliability of the research tool to ensure the instrument contains set of items that most strongly relate to the construct of interest and will answer the research question (Cope, 2014; Houghton et al., 2013). The objective of establishing reliability is to minimize errors and eliminate bias in the research study (Cope, 2014; Noble & Smith, 2015). Fan (2013) pointed out that reliability does not refer to the measurement instrument but to the consistency of results obtained. Yin (2014) noted that reliability is one of the criteria for judging the quality of research designs while data dependability of findings is a logical test that guides qualitative research.

Researchers establish reliability in research to demonstrate the consistency of their analytical procedures to repeat with the same results (Cope, 2014; Houghton et al., 2013; Noble & Smith, 2015). To establish reliability, qualitative researchers use dependability to focus on the measurement within a construct (Carter et al., 2014; Cope, 2014; Houghton et al., 2013). In this section, I discussed how to establish dependability of the study findings.

Dependability. The single term researchers use to determine reliability in qualitative case studies is dependability (Fusch & Ness, 2015). Dependability refers to the consistency of the data over similar conditions (Cope, 2014). To determine reliability, researchers audit the research process to ensure the results will not be subject to change and instability.

I ascertained the reliability of the doctoral study by documenting the sequence of processes from data collection through data analysis to data interpretation. I also provided a detailed explanation of the structure and strategies of the doctoral study and state the criteria for selecting research participants. Finally, I recognized the important role of the researcher and researcher-participant relationship, documented the process of data analysis, and clarified the approach for generating data.

The strategies researchers use to determine dependability are audit trail and reflexivity (Houghton et al., 2013). Audit trail approach involves the detailed description of the decisions made throughout the research process to provide the reader with the rationales for the investigation methodology and interpretative judgments of the researcher (Loh, 2013). Using an audit trail enables a reader to discern how the researcher interpreted the study findings.

The reflexivity strategy ensures that decision trials do not suppress the personal contributions of the scholar and the recording of individual responses (Houghton et al., 2013). Researchers use reflective journal to achieve reflexivity (Houghton et al., 2013). To ensure dependability of this study, I used the audit trail and reflexivity strategies.

Validity

Researchers use validity to establish the effectiveness and efficiency of measuring instrument in achieving the intended goal (Gregor & Hevner, 2013). The objective of validity is to minimize errors and eliminate bias in the research study, establish the integrity and applicability of methods, and determine the precision in which the findings accurately reflect the data (Noble & Smith, 2015). Most researchers seek to establish the validity of the research tool to ensure the instrument contains set of items that most strongly relate to the construct of interest and will answer the research question.

To establish validity, researchers focus on the measurements between constructs (Yin, 2014). Yin (2014) noted that trustworthiness, credibility, and conformability of findings are logical tests that guide qualitative research. The three criteria for judging the quality of research designs are construct validity, internal validity, and external validity (Yin, 2014). In a qualitative study, similar criteria for establishing validity are creditability, transferability, confirmability, and authenticity (Carter et al., 2014; Cope, 2014; Houghton et al., 2013). In this section, I discuss how to establish creditability, transferability, and confirmability of the study findings; and data saturation.

Creditability. Creditability is the term used rather than validity in qualitative research. Creditability refers to the truth of the data or participants' views (Cope, 2014). To establish creditability, researchers evaluate the fit between the data and research findings (Cuthbert & Moules, 2014). Because qualitative researchers are the research instruments, the creditability of the study depends on procedures implemented and investigator's self-awareness throughout the research process.

Noble and Smith (2015) noted that qualitative researchers design and incorporate methodological strategies to enhance the creditability of their findings. The methodological strategies are (a) reflection and reflexivity on own perceptions, (b) representativeness of sample about the phenomenon, (c) achieving audit ability, and (d) application of conclusions to other contexts (Noble & Smith, 2015). Others include (a) detailed and thick verbatim description of participants' accounts to support findings, (b) respondent validation, and (c) data triangulation (Noble & Smith, 2015). Maree, Parker, Kaplan, and Oosthuizen (2016) maintained creditability by using appropriate research method, peer scrutiny, member checking, and early familiarization with data.

Other strategies researchers use to determine the creditability of their study findings include (a) prolonged engagement and persistent observation, (b) triangulation, (c) peer debriefing, (d) negative case analysis, (e) referential adequacy, and (f) member checking (Houghton et al., 2013; Loh, 2013). In prolonged engagement and persistent observation strategy, the researcher spends sufficient time in the case study site to obtain a full knowledge of the phenomenon under investigation until no new emerging data, which indicates data saturation. I did not use prolonged engagement and persistent observation strategy because the purpose of the study is not to observe the participants over an extended period but to explore information security strategy.

Triangulation refers to the use of numerous sources of data for confirmation of data and ensures completeness of data. Confirmation of data includes comparing data from multiple sources for consistency, which will increase the creditability of the findings (Houghton et al., 2013). Integrity of data includes gathering multiple perspectives of a variety of sources to portray a complete picture of the phenomenon (Houghton et al., 2013).

Peer debriefing requires the use of external colleague or expert to support the creditability of the finding (Loh, 2013). Member checking is the use of participants to verify the interview transcript to ensure accurate recording and support reliability of the research outcome (Loh, 2013). Researchers use member checking to ensure the capturing of meanings as the participants' want. I used triangulation approach and member checking to ensure the creditability of the study findings.

Transferability. In qualitative research, researchers provide the detailed description of the research process and reader and future researchers have the responsibility to determine the transferability of the study. Transferability refers to the application of findings to other settings or groups (Cope, 2014). Researchers use methodological triangulation to confirm the similarities found in different data collection sources and document detailed and transparent description of the research process, which another researcher can replicate (Cope, 2014).

Maree et al. (2016) stated that purposive sampling enhances transferability of findings. Researchers state the criteria for selecting research participants to enable other researchers to evaluate the transferability of their research findings (Elo et al., 2014). The most appropriate strategy to determine transferability is thick verbatim description of the research process (Houghton et al., 2013; Loh, 2013; Maree et al., 2016).

Researchers should provide rich and thick verbatim descriptions of the participants' response to enable the reader to make informed decisions about the transferability of specific contexts of the study and interpretations of the study findings (Noble & Smith, 2015). Houghton et al. (2013) noted that researchers could enhance portability through a detailed presentation of research results, with appropriate academic citations. I used the purposive sampling method and provided a detailed description of the research process, findings, and academic citations to enhance the transferability of the study results.

Confirmability. The focus of confirmability is to ensure the researcher demonstrates that data represent participant's responses and not figments of own viewpoint or biases (Cope, 2014; Cuthbert & Moules, 2014). Maree et al. (2016) noted that recognition of limitations of the study and audit trail enhanced confirmability. The strategies researchers use to determine confirmability are the audit trail and reflexivity (Houghton et al., 2013; Loh, 2013). The audit trail approach involves the detailed description of decisions the researcher made throughout the research process to provide the reader with justifications for investigation methodological and interpretative judgments of the researcher (Houghton et al., 2013).

Using an audit trail enables a reader to understand how the researcher interpreted the data. Researchers use reflexivity strategy to ensure that decision trials do not suppress the personal contributions of the scholar and the recording of individual responses. Houghton et al. (2013) noted that researchers achieve reflexivity through the use of a reflective diary. To address confirmability of this study, I used the audit trail and reflexivity strategies.

Data saturation. Researchers attain data saturation when the participants have thoroughly explored the interview questions in detail, and no new concepts or themes are emerging in subsequent interviews (Cleary et al., 2014; Fusch & Ness, 2015; Kornbluh, 2015). J. M. Morse (2015) noted that adequate and appropriate qualitative samples facilitate the building of detailed and useful data on the scope and replication within the process of inquiry to achieve data saturation. Data saturation is a useful for enhancing the reliability of investigation results, and the failure to reach data saturation might negatively affect the quality of the research study because it hampers content validity (Fusch & Ness, 2015).

Scholars can achieve data saturation through methodological triangulation using multiple sources of data and member checking to verify the accuracy of the interview data (Cope, 2014; Houghton et al., 2013; P. Jones et al., 2014). The general principles to reach data saturation include (a) no new information, (b) no new coding, (c) no new themes, and (d) ability to replicate the study (Fusch & Ness, 2015). I used method triangulation and member checking to ensure data saturation.

Transition and Summary

Section 2 of this study contains an overview of the steps for conducting the proposed research study. The focus areas include (a) purpose statement, (b) role of the researcher, (c) participants, (d) research method and design, (e) population and sampling, (f) ethical research, (g) data collection, (h) data organization, (i) data analysis, and (j) reliability and validity. My role as a researcher include sampling and data collection, organization, and analysis.

Furthermore, Section 2 contains justification relating to decisions to use qualitative exploratory multiple case study design, purposive criterion sampling technique, sample size of five SMEs, interview protocol, and open-ended questions during interviews. Another focus area in this section was the description of how to enhance reliability and validity of the research instruments and findings. In Section 3, I explain the presentation of findings, application to professional practice, implications to social change, recommendations for action and further study, and reflections and a concluding statement.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore the strategies SME leaders use to minimize the effects of information security threats on business performance. Five SME leaders from five firms that support oil and gas industry sector in the city Port Harcourt, Nigeria participated in this study. Based on data from participant interview responses, company documents on information security policies (archival data), and observations, I identified 10 themes. These include network security, physical security, strong password policy, antivirus protection and software update, information security policy, security education, training and awareness, network security monitoring and audit, intrusion detection, data backup, and people management. The SME leaders confirmed that an ability to be proactive in implementing a combination of information security strategies was essential in minimizing the effects of information security threats on business performance. Section 3 includes the presentation of findings, application to professional practice, implications to social change, recommendations for action and further study, and reflections and a concluding statement.

Presentation of the Findings

The overarching research question of the study was the following: What strategies do SME leaders use to minimize the effects of information security threats on business performance? I collected the data for this study from five participants using semistructured interviews with open-ended questions (Appendix C), observations, and archival documents on the organizations’ information security policy statements. Table 2, the demographic information of participants, shows the respondents by current job position, experience in a leadership role and information security, highest education, gender, and age group.

Table 2

The Demographic Information of Participants

Participant	Current job position	Experience in leadership role	Experience Information security	Highest education qualification	Gender	Age group (years)
A1	IT Manager	Four years	Six years	BSc	Male	31-40
B2	Information Security Analyst	Five years	10 years	BSc	Male	51-60
C3	Head, Engineering	10 years	Six years	MSc	Male	41-50
D4	Director	15 years	13 years	BSc	Male	41-50
E5	Principal Partner	Five years	Seven years	MBA	Male	41-50

I used the QSR NVivo to analyze the data for this study. Ten themes emerged from my analysis of interview responses, observations, and company documents. The 10 themes were (a) network security, (b) physical security, (c) strong password policy, (d) antivirus protection and software update, (e) information security policy, (f) security education, training and awareness, (g) network security monitoring and audit, (h) intrusion detection, (i) data backup, and (j) people management. In Table 3, I present the development of themes about the interview questions and participants.

Table 3

The Development of Themes

Theme	Interview Question Numbers	Participants
Network security	1, 6, 7	A1, C3
Physical security	1, 3	C3, E5
Strong password policy	1, 6	C3, E5
Antivirus protection and software update	1, 6	A1, B2, E5
Information security policy	1-4	B2, C3, E5
Information security education, training, and awareness	1, 3-7	All
Network security monitoring and audit	1-3, 6, 7	A1, B2, D4
Intrusion detection	1, 6, 7	A1, B2, D4
Data backup	1, 4, 6	A1, B2, C3, E5
People management	3-5, 7	A1, B2, C3, D4

Theme 1: Network Security

Information security experts utilized a firewall mechanism to assure essential protection of information systems and the baseline for advanced protection techniques (Bingman, 2016; Iacob, 2015; Iacob & Defta, 2015). Firewalls were the primary method that firms use to keep a computer secure from intruders (Ference & Graf, 2016). Security technologies, such as a firewall alone, are inadequate to manage the security challenges (Gangwar & Date, 2016). Bingman (2016) noted that information security experts utilized the firewall and other layers of detection and protection mechanism to protect networks and achieve defense-in-depth means of cyber security. Iacob (2015) demonstrated the use of the firewall to enhance data security on e-learning platforms while Iacob and Defta (2015) configured a Layer 3 firewall to improve network security and minimize information security threats on e-learning platforms. Brown (2015) noted that firewall is an effective information security strategy.

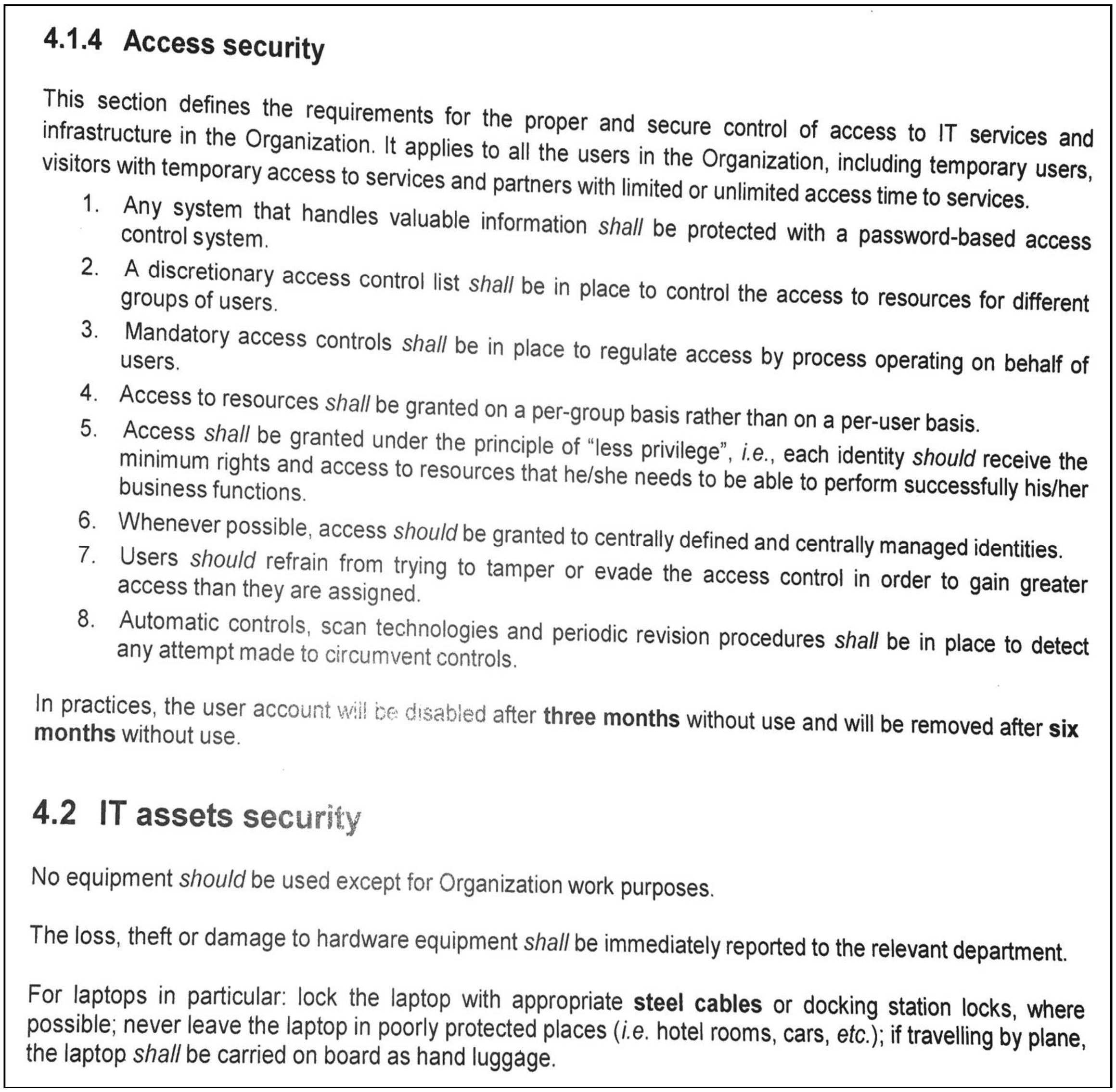
The theme network security involving firewall and logical security emerged from Interview Questions 1, 6, and 7. Participants A1 and C3 discussed the use of the firewall to minimize the effects of information security threats on their business performance. In response to Interview Question 1, Participant A1 responded, “One of the things we have done physically is the firewall,” while C3 stated, “One of the strategies that we use is what we call firewall.” In response to Interview Question 6, Participant AI responded, “We have a firewall. The firewall is set up in a way that it does not allow an intruder from outside and to filter what we are doing.” Responding to Interview Question 7, C3 stated that “the firewall we have put in place” is the second strategy, following access restriction in reducing the effects of information security threats on business performance. The participants’ responses to the interview questions aligned with Bingman’s (2016) statement that firewall is a useful tool for enhancing network security in contested cyberspace environments and Iacob’s (2015) assertion that firewall improved data security in e-learning platforms.

Theme 2: Physical Security of Information Assets

Organizational leaders used not only physical control systems to secure information security infrastructure but also integrated physical control systems into IT network (McCreight & Leece, 2016). The first line of defense against any information security threat is physical security (Brown, 2015). McCreight and Leece (2016) noted that physical security involves restricting unauthorized access to assets, which are visibly evidenced through card access receivers. Brown (2015) noted organization should consider designing physical and technological security in their prevention strategy.

An important area of concern for organizations toward ensuring the safety of their information systems is access controls (Bélanger, Collignon, Enget, & Negangard, 2017). Yang and Ye (2015) noted that access control is a major security strategy that information security experts use to ensure that only authorized users have access to certain information security assets and data. The access control could involve the use of access card, Kensington key, or secured cabinets. Ference and Graf (2016) posited that firms use a lock or access code to restrict access to areas in which the companies keep their information assets.

The theme physical security involving the use of access control and padlock to safeguard information assets emerged from Interview Questions 1 and 3. Participants C3 and E5 highlighted using the physical security of information assets as a strategy to minimize the effects of information security threats on their business performance. In response to Interview Question 1, Participants C3 and E5 explained that physical security measures were in place to safeguard information infrastructures. Participant C3 stated, "You have to have a clock card before you can have access to data center environment." Participant E5 noted, "My staff ensure that there are good padlocks and keys in their cabinet section so that after use of any of the tools especially laptop, you ensure you lock it up." Responding to Interview Question 3, E5 stated, "We make sure every staff locks up any system after each and every use" to explain how they implement the strategy regarding the physical security of their equipment systems. I observed the use of Kensington lock to physically secure laptops. The participants' responses, company documents, and my observation aligned with Brown's (2015) statement that organizations should consider the physical security of employee workstations and devices. The IT and security policies (Figures 1 and 2) from two SME firms indicated that SME leaders implemented physical security measures to reduce threats to information security.



4.1.4 Access security

This section defines the requirements for the proper and secure control of access to IT services and infrastructure in the Organization. It applies to all the users in the Organization, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

1. Any system that handles valuable information *shall* be protected with a password-based access control system.
2. A discretionary access control list *shall* be in place to control the access to resources for different groups of users.
3. Mandatory access controls *shall* be in place to regulate access by process operating on behalf of users.
4. Access to resources *shall* be granted on a per-group basis rather than on a per-user basis.
5. Access *shall* be granted under the principle of "less privilege", *i.e.*, each identity *should* receive the minimum rights and access to resources that he/she needs to be able to perform successfully his/her business functions.
6. Whenever possible, access *should* be granted to centrally defined and centrally managed identities.
7. Users *should* refrain from trying to tamper or evade the access control in order to gain greater access than they are assigned.
8. Automatic controls, scan technologies and periodic revision procedures *shall* be in place to detect any attempt made to circumvent controls.

In practices, the user account will be disabled after **three months** without use and will be removed after **six months** without use.

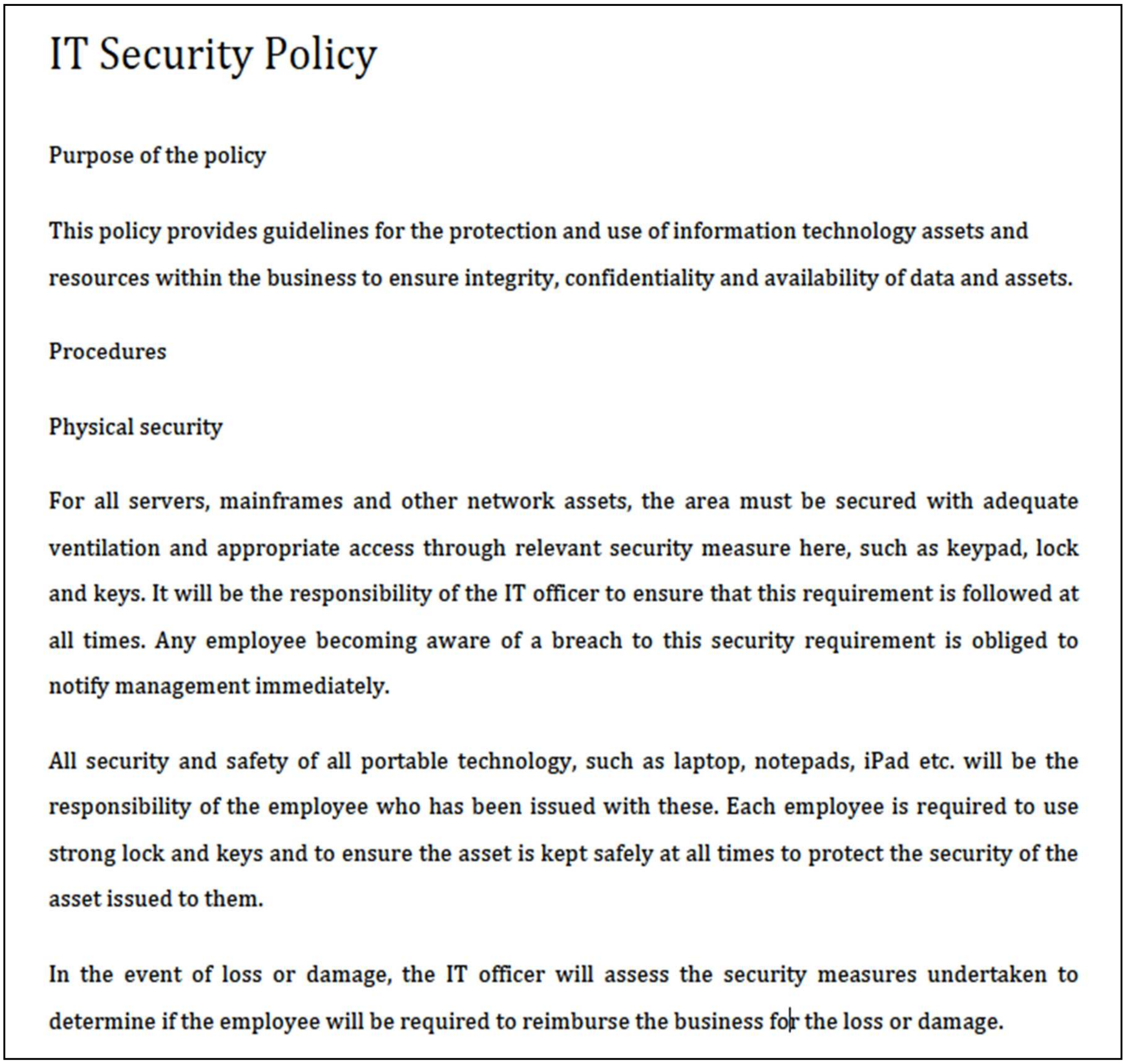
4.2 IT assets security

No equipment *should* be used except for Organization work purposes.

The loss, theft or damage to hardware equipment *shall* be immediately reported to the relevant department.

For laptops in particular: lock the laptop with appropriate **steel cables** or docking station locks, where possible; never leave the laptop in poorly protected places (*i.e.* hotel rooms, cars, *etc.*); if travelling by plane, the laptop *shall* be carried on board as hand luggage.

Figure 1. IT policy. A direct excerpt from the policy on access security and IT assets security that illustrated what the SME leader put in place to control access to information and IT assets.



IT Security Policy

Purpose of the policy

This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets.

Procedures

Physical security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through relevant security measure here, such as keypad, lock and keys. It will be the responsibility of the IT officer to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify management immediately.

All security and safety of all portable technology, such as laptop, notepads, iPad etc. will be the responsibility of the employee who has been issued with these. Each employee is required to use strong lock and keys and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, the IT officer will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

Figure 2. Information security policy. An excerpt from IT security policy of SME firm that indicated the physical security measures in place to protect IT assets.

Theme 3: Strong Password Policy

Bélanger et al. (2017) posited that password protection is one of the most commonly used security control techniques in information security. The fundamental techniques in using password protection were the creation of strong password and frequent password changes for enhanced security (Bélanger et al., 2017). Ference and

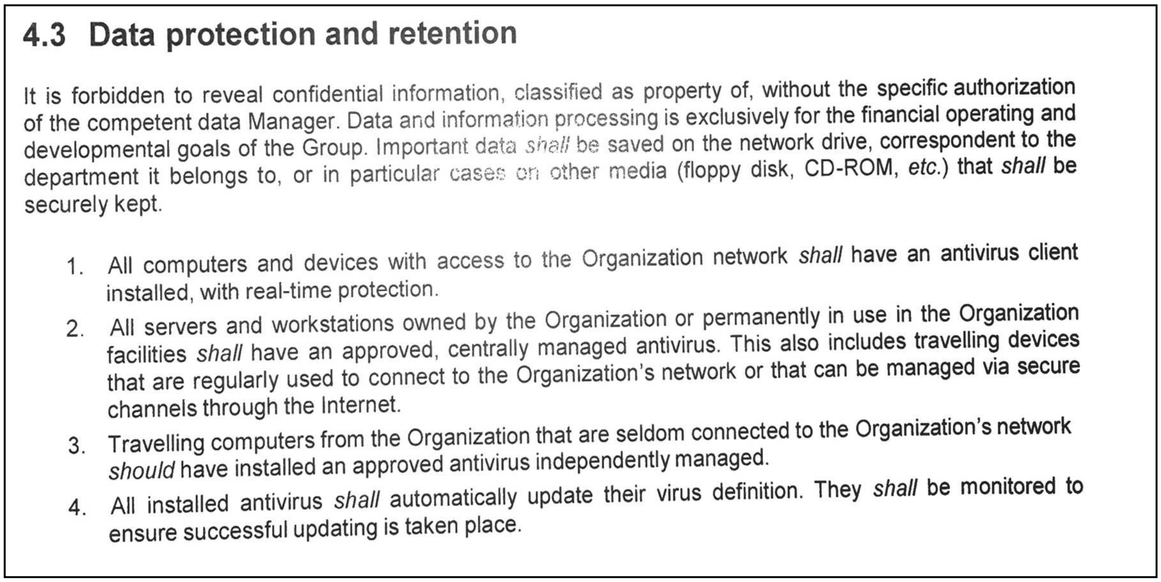
Graf (2016) posited the use of passwords for access control and advised that users should use long passwords or phrases, 16 to 20 characters in length, that are changed periodically instead of using complex passwords, which are easily forgotten. Khera (2017) explained the importance of password security and noted that reduced security of inbuilt passwords in medical devices made it easy for hackers to circumvent their login protection. Weber (2015) advised users to avoid the security hazard from sticking password on computer monitors or laptop keyboards.

The theme of strong password policy emerged from Interview Questions 1 and 6. Participants C3 and E5 stated that use of passwords was an important strategy for minimizing the effects of information security threats on business performance. In response to Interview Question 1, Participant E5 stated, “We also ensure that password staff use to log onto the laptop at least uphold or recognize the maximum password strength by way of characters.” Responding to Interview Question 6, Participant C3 stated, “Also part of the system is a password for access restriction. People don’t have access to data.” The participants’ responses were aligned with Bélanger et al.’s (2017) statement that password is a common strategy that organizations use to minimize threats to information security. The IT policy (see Figure 1) indicated that SME leaders implemented password access control system to reduce threats to information security.

Theme 4: Antivirus Protection and Software Update

Antivirus software is one of the most important and widely used as the last line of defense against a variety of information security threats (Al-Saleh, AbuHjeela, & Al-Sharif, 2015). Antivirus software is a program or set of programs designed to prevent, search for, detect, and remove software viruses and other malicious software such as Trojan horses, worms, adware, and malware. Many antivirus programs include an anti-spyware program designed to prevent and detect unwanted spyware program installations and remove those programs if installed (Ference & Graf, 2016). An important information security strategy that organizations should consider was the use of effective antivirus software on servers and individual workstation to protect data on them (Brown, 2015). Budzak (2016) noted that e-mail was a tremendous threat to information security. Security technologies, such as antivirus software alone is not sufficient to manage the security challenges and protect information (Gangwar & Date, 2016).

The theme antivirus protection and software update emerged from Interview Questions 1 and 6. Participants A1, B2, and E5 stated that antivirus protection and software update was a useful strategy for minimizing the effects of information security threats on business performance. The participants’ responses and data protection policy (see Figure 3) indicated that SME leaders implemented antivirus protection to minimize threats to information security.



4.3 Data protection and retention

It is forbidden to reveal confidential information, classified as property of, without the specific authorization of the competent data Manager. Data and information processing is exclusively for the financial operating and developmental goals of the Group. Important data *shall* be saved on the network drive, correspondent to the department it belongs to, or in particular cases on other media (floppy disk, CD-ROM, *etc.*) that *shall* be securely kept.

1. All computers and devices with access to the Organization network *shall* have an antivirus client installed, with real-time protection.
2. All servers and workstations owned by the Organization or permanently in use in the Organization facilities *shall* have an approved, centrally managed antivirus. This also includes travelling devices that are regularly used to connect to the Organization's network or that can be managed via secure channels through the Internet.
3. Travelling computers from the Organization that are seldom connected to the Organization's network *should* have installed an approved antivirus independently managed.
4. All installed antivirus *shall* automatically update their virus definition. They *shall* be monitored to ensure successful updating is taken place.

Figure 3. Data protection policy. An excerpt from the data protection and retention policy of SME firm that showed installation of antivirus clients to protect organization network.

In response to Interview Question 1, Participant A1 stated,

> What we did was to avoid physical attack or Internet attack by putting the firewall in place and what do we do to make sure that this firewall can stand the test of time is the continuous upgrade (Hardware Level), constant firmware update, and continuous software update.

In response to Interview Question 1, Participant B2 stated, “You ensure that your systems that have direct connection to the Internet have virus patches up to the latest level, ensure that they are updated, and you are current with the trends in what’s going on.” Responding to Interview Question 1, E5 stated, “With Apple product, you don’t need to install antivirus measures and some programs like that, but in our Windows, we do install antivirus soft wares” and remarked that most information security attacks come from social engineering. Participants’ responses aligned with Gyunka and Christiana’s

(2017) statement that social engineering attacks were the top most threat against information security within the cyberspace in recent years.

In response to Interview Question 6, Participant B2 stated, “We ensure that you have a good virus monitoring and virus scan system to ensure that you don’t have virus in your system.” Participant E5 stated,

> I have in place amongst others include the antivirus software that we use basically to support the implementation of the strategies because if we do not have such an antivirus software program in place, the information security infrastructure of the firm would still be exposed to that threat.

The participants’ responses to the interview questions and company documents aligned with Al-Saleh et al.’s (2015) and Brown’s (2015) statement that antivirus protection and software upgrade are useful strategy for minimizing threats to information security.

Theme 5: Information Security Policy

Information security policy is a formal document that states how a company plans to protect its physical and IT assets, which organizational leaders use to influence and manage the behavior and activities of their employers (Allassani, 2014). Organization leaders use security policies to specify access rights in using systems and deploy security controls to ensure consistency and accountability (Gangwar & Date, 2016). The information security policies outline the *do’s* and *don’ts* of the use of computer systems (Allassani, 2014). Ifinedo (2014) noted that organizations establish and implement information systems security policy to influence their employees' behaviors toward efficient use of information system assets and resources.

Safa et al. (2016) posited that proper information security policies have significant effects on the formation of organizational culture toward information security attitudes and behaviors within the organizations. Y. Chen, Ramamurthy, and Wen (2015) posited that security education, training, and awareness (SETA) programs have significant influence on employee's knowledge on organizational security policy. Department for Business, Innovation & Skills (2015) reported that 60% of small organizations had documented information security policies.

The theme information security policy emerged from Interview Questions 1 through 4. Participants B2, C3, and E5 stated that implementing an information security policy was essential in minimizing information security threats on their business performance. In response to Interview Question 1, Participant A1 said, "We make sure we have a code of conduct for the use of the Internet and social media to ensure that we don't get in malicious content into our systems." C3 stated, "We have a security trading policy in place, and if you go against that security policy, the staff will be shown the way out" while E5 stated, "In our policy statement we don't allow our staff to keep their system open, probably for maybe just five minutes." The participants' responses aligned with Safa et al.'s (2016) and Gangwar and Date's (2016) assertions that organization leaders establish information security policies to minimize threats to information security and improve information security efficiencies within their organizations.

In response to Interview Question 2, Participant B2 stated, “You choose according to the threats that are prevalent, which are evolving and you are shifting your policy to ensure that you are protected.” Responding to Interview Question 3, Participant C3 stated the top management’s commitment to security policy, “The board has to give approval to the security trading policy before the company can go ahead so that any staff that falters will have to face the penalty.” In response to Interview Question 4, Participant C3 stated, “All of us have been made to sign the security policy.” The participants’ responses aligned with Department for Business, Innovation & Skills’ (2015) report that organization ensure formal documentation of their information security policies. The IT and security policies (see Figures 1 and 2) and data protection policy (see Figure 3) indicated that SME leaders implement policies to minimize the effects of information security threats on business performance.

Theme 6: Security Education, Training and Awareness

An organization’s overall security program depends on creation of awareness about information security issues through proper education and training modules (S. Mishra, Caputo, Leone, Kohun, & Draus, 2014). S. Mishra et al. (2014) posited that information security awareness is the backbone for effective information systems security programs. Safa et al. (2015) posited that information security awareness is a key factor in information security assurance. Employees were willing to obey security controls if they are aware of the rationale and significance of the controls and the motives governing organizational actions (S. Mishra et al., 2014). Corporate leaders organize regular training programs on information security to supplement the effectiveness of security policies and procedures (Allassani, 2014).

Sollars (2016) stated that business leaders should train and enable staff to bring out the best security practices to the heart of everything they do in the workplace. Firm owners should ensure that employees receive regular security awareness training to minimize data breaches (Ference & Graf, 2016). Department for Business, Innovation & Skills (2015) reported that small businesses that provided ongoing security awareness training to their staff increased from 54% in 2014 to 63% in 2015. Y. Chen et al. (2015) demonstrated that SETA programs have significant influence on employee’s awareness of organizational security policy and impact on security culture.

The theme security education, training, and awareness emerged from Interview Questions 1, 3, 4, 5, 6, and 7. All the research participants acknowledged the use of employee awareness, training, and education to minimize information security threats on their business performance. In response to Interview Question 1, E6 stated that “One of the key strategies we use in our firm to minimize the effects of information threats on our business performance is primarily through education.” B2 stressed the need for organizational leaders to ensure that “people that work with you understand this policy and apply it.” Responding to Interview Question 1, D4 pointed out that “education, that is, taking care of the people angle to things,” was second to technology in their strategy for minimizing information security threats on their business performance. The participants’ responses supported S. Mishra et al.’s (2014), Y. Chen et al.’s (2015), and Safa et al.’s (2015) statements that employee awareness of information security was a key strategy for minimizing the effects of information security threats on business performance.

In response to Interview Question 3, B2 stated, “First of all is information, people that are working with you must be aware what is happening. When they are aware, they are in a better position to conform to whatever policy that is put in place.” Responding to Interview Question 2, C3 noted that “staff education is very key” and “there is this information security staff training” for different departmental units. Buttressing the importance of staff awareness in strategy implementation, Participant E5 affirmed, “We also invite subject matter experts to help our organization to talk to staff about how best to implement strategies.” The participant’s responses aligned with Gyunka and Christiana’s (2017) report that security awareness and training of users was crucial in ensuring good cybersecurity work behaviors and minimizing information security threats on firms.

In response to Interview Question 4, B2 indicated that sharing information through security education, training, and awareness “you teach people, train people, people awareness,” organizational leaders could reduce the challenge of individuals’ inertia during implementation of strategies, which could reduce the consequences of information security threats on business performance. Responding to Interview Question 5, Participant A1 explained the importance of creating security awareness, “when you plan, you make sure that the stakeholders are well informed,” in managing the challenges faced in implementing the strategies to minimize the effects of information security threats. Participant C3 and E5 echoed A1. C3 stated, “Part of the thing we did was to educate the staff,” while E5 stated,

> What we usually do is to invite a subject matter expert, people who have had a good experience in information system to come to have some sensitization session with my staff on letting them know of best practices in information security and how best to minimize threats that could hamper the business performance in our firm.

In response to Interview Question 6, E5 confirmed the use of e-mailing system to create security awareness, “I usually send occasional e-mail reminders to my staff warning them if you never negotiated for any e-mail, initiated an e-mail you don’t respond to an e-mail a strange e-mail that comes to you.” Responding to Interview Question 7, E5 stated, “I think the most efficient strategy is education” which echoed S. Mishra et al. (2014), which indicated that security awareness through education and training was imperative in implementing effective security strategy. The participants’ responses were aligned with Y. Chen et al.’s (2015) and B. E. Kim’s (2014) assertion that SETA programs have significant influence on peoples’ attitude and positive impact on organizational security culture.

Theme 7: Network Security Monitoring and Audit

Department for Business, Innovation & Skills (2015) reported that 61% of organizations utilize internal audit to identify and assure information security threats. Laybats and Tredinnick (2016) noted that firms use audit logs to maintain integrity of information systems. Organizations should consider investing in network security control and monitoring of access to data (Gangwar & Date, 2016).

The theme network security monitoring and audit emerged from Interview Questions 1, 2, 3, 6, and 7. Participants A1, B2, and C3 stated that network security monitoring and audit was useful strategy for minimizing the effects of information security on their business performance. In response to Interview Question 1, Participant A1 stated, “Today, everyone that is on that network, everything you are doing is being logged somewhere.” Responding to Interview Question 1, Participant B2 noted that “So that anybody that is on the network is known, and there is a monitoring to know where you are going through the company server, the sites you are accessing, and what you are doing on those sites.” Participant C3 stated, “There is this Internet access control, which the IT department monitor.” The participants’ responses agree with Gangwar and Date’s (2016) advice to invest in security control and monitoring of access to data.

In response to Interview Question 2, Participant A1 stated, “So whatever that is going out of the network if being logged here. They are analyzing it; we are analyzing it.” Responding to Interview Question 3, Participant C3 said, “Part of what we do is we have customized operating systems and applications that we can monitor and know who is doing what at every point in time.” In response to Interview Question 6, Participant A1 stated “I am seeing all packets that are coming in and are going out, and they are all categorized” while B2 noted, “We monitor incoming traffic and content and ensure that those things are not allowed in the systems.” Participant B2 further explained, “There is monitoring to know where you are going through the company server, the sites you are accessing, and what you are doing on those sites." Participant A1 allowed me to observe the processing of the Solarwind monitoring system used in monitoring inflow and outflow of packets on the network.

In response to Interview Question 2, Participant A1 stated, "We bring in an expert, there is this company that is responsible for Cisco secure information security, they come and check." Responding to Interview Question 3, Participant A1 noted that security audit was the first step in the process of implementing the strategies to minimize the effects of information security on their business performance. The theme extends the body of knowledge on network security monitoring and audit as a strategy for reducing the effects of information security threats on business performance.

Theme 8: Intrusion Detection

Intrusion detection system (IDS) is a security tool that captures and monitors the network traffic and or system logs and scans the system/network for suspicious activities (P. Mishra, Pilli, Varadharajan, & Tupakula, 2017). Organizations use intrusion detection and protection systems to actively block traffic to and from malicious address (Brown, 2015). IDS act as the main way of filtering and defense in control systems (Cazorla, Alcaraz, & Lopez, 2015). P. Mishra et al. (2017) posited that researchers had used several intrusion detection techniques to detect intrusions in cloud computing environment scientists. Brown (2015) noted that an informed and knowledgeable user was the primary defense against intrusion.

Researchers have proposed the use of IDS as a defensive approach in the field of cloud security (P. Mishra et al., 2017). IDS is one of the tools available to organizations to protect their critical infrastructures from threats through preparedness and protection mechanisms (Cazorla et al., 2015). Li, Meng, Kwok, and Horace (2017) noted that IDS had been implemented in many networks to defend against a variety of attacks. AlEroud and Alsmadi (2017) introduced a novel intrusion detection approach to identify and mitigate denial of service (DoS) attacks on software-defined networks (SDNs). Li et al. designed a supervised intrusion sensitivity-based trust management model which was efficient and sensitive in detecting insider attacks from malicious peers.

The theme intrusion detection emerged from Interview Questions 1, 6, and 7. Participants A1, B2, and D4 stated that intrusion detection was a useful strategy for minimizing the effects of information security on their business performance. In response to Interview Question 1, Participant A1 said,

> The first layer log will pick it and log it for us, or we have an alert like in the SolarWinds, we can have an alarm that will tell us that you have an intruder, and so when we see that and quickly go in to have a restoration.

Responding to Interview Question 6, Participant B2 stated: “You can have a hardware system that detects and cuts off those systems upfront.” In response to Interview Question 7, D4 said, “At the end of the day, we know who has done what and in the process, if anything inappropriate has been done or there is a break in, we’ll also to be able to identify it.” The participants’ responses to the interview questions aligned with Cazorla et al.’s (2015), Li et al.’s (2017), and P. Mishra et al.’s (2017) reports on the use of IDS to minimize the effects of information security threats on business performance.

In this study, the participants viewed intrusion detection as a strategy for reducing the effects of information security threats on business performance.

Theme 9: Data Backup

Data backup and recovery is a critical issue in cloud computing systems (Chuang & Wang, 2017). Organizations backup data to fulfill ethical obligation to their clients, affirm professionalism, minimize financial losses, and ensure business sustainability (Allen, 2016). Except for company network with automatic backup system, ideally, users should back up every computer every day (Weber, 2015). The two primary considerations in data backup were the infrastructure and the data (Allen, 2016). Allen (2016) posited that computer is the most significant aspect of data backup. Weber (2015) noted that Apple Corporation MacBook laptops have sophisticated but easy hourly data backup which use proprietary Time Machine application and a simple recovery process if the need arises.

Chuang and Wang (2017) demonstrated a better way to backup data and recovery scheme which enhanced the performance and efficiency of data backup and recovery at reduced computation overhead in cloud computing systems. Weber (2015) advised organizations to use high-capacity external drives, thumb drives, and third-party services for daily backup of data. Some relatively inexpensive cloud-based services include Dropbox, Google Drive, and SugarSync (Weber, 2015).

The theme data backup emerged for Interview Questions 1, 4, and 6. Participants A1, B2, C3, and E5 stated that data backup was a useful strategy for minimizing the consequences of information security on their business performance. Responding to

Interview Question 1, Participant A1 said, “We have been able to put some things in place that we call backup application and data backup at the data center” while Participant E5 noted, “The data that we have in our system is usually backed up” in an external hard drive. In response to Interview Question 4, Participant B2 explained that organizations should “have a good backup system and fall back system” to minimize “the consequences of such threats when they happen.” Responding to Interview Question 6, Participant C3 stated, “We have data recovery sites whereby para venture anything happens to the data of the company or people who have access to the information, you can recover back from the attack.” The participants’ responses to the interview questions aligned with Chuang and Wang’s (2017) and Weber’s (2015) statements that organizations backup data to minimize the consequences of possible attack on their business. The theme extends the body of knowledge on data backup as a strategy for reducing the effects of information security threats on business performance.

Theme 10: People Management

A new challenge for organizations is managing peoples’ information security behavior. Budzak (2016) noted that users’ behavior is a threat to information security. Human beings are inherent source of information security incidents (Da Veiga & Martins, 2015; Gangwar & Date, 2016). Organizational leaders should focus their information security strategies toward finding ways to motivate employees to improve protection of corporate information assets (Boss et al., 2015). Organizational leaders should not understate the importance of human factors in the domain of information security because users, intentionally or through negligence, pose significant threat to information security (Safa et al., 2015). Sollars (2016) noted that organizations should enlist and motivate staff to not only follow the rules but should also re-orientate staff from being the weakest link to becoming the first line of defense in information security.

Information security experts should consider the human information security behavior and technology aspects of information security to guarantee a secure environment (Safa et al., 2015). According to Safa et al. (2015), users intentionally delay complying with the mandatory password change because they considered such change an unnecessary interruption. Bélanger et al. (2017) noted that employees fail to perform the security behaviors their organization put in place to protect information assets. Safa et al. pointed out that users understand the severe consequences of password breach but do not change their attitudes and resistance behavior toward implementing the information security policy.

Safa et al. (2015) demonstrated that information security awareness has a significant effect on users' information security attitude toward a positive behavior. SETA programs and awareness of security monitoring had significant influence on security culture (Y. Chen et al., 2015). Bélanger et al. (2017) highlighted the importance of information security awareness in influencing security change behaviors amongst employees. Boss et al. (2015) demonstrated that organizations need not only establish information security policy but should also present employees with strong arguments for adhering to behavioral security policies. Gyunka and Christiana (2017) showed that vulnerabilities from human factors were prime target for hackers through social engineering attacks. Gyunka and Christiana highlighted some of the damaging human factors to include (a) ignorance or illiteracy to the core security practices, (b) carelessness, and (c) sabotage by disgruntled employees.

Laybats and Tredinnick (2016) posited that people's problem and their messy, unpredictable, organic nature is a threat to information security because individuals intentionally behave in ways that they shouldn't. People's behaviors include: (a) use simple or predictable passwords, (b) use same passwords on multiple systems, (c) write down the passwords, (d) share login details with colleagues, (e) leave systems logged-in, (f) take files home on memory sticks, and (g) use same e-mail for personal and business purposes. Posey et al. (2013) advised organizational leaders to recognize the important role of corporate insiders rather than relying on technology to protect the organizations' information resources. All participants recognized the important role of employers and did not solely rely on technology to protect their information resources.

The theme people management emerged for Interview Questions 3, 4, 5, and 7. Participants A1, B2, C3, and D4 stated that people management is a useful strategy for minimizing the effects of information security on their business performance. In response to Interview Question 3, Participant D4 discussed the need to "progressively change or update human management to address gap identified, weaknesses noted, in the course of implementation." Responding to Interview Question 4, Participant A1 pointed out the need for human management due to, "the resistance that I get from the direct users" while B2 stated, "We have the challenge of inertia, people don't want to do anything, people do not want to change." In response to Interview Question 4, Participant C3 noted that staff management is the second challenge "because some of them just feel that there is nothing bad" while D4 said, "the other challenge also, is with people, and I think that turned out to be the biggest problem." The participants' responses to the interview questions aligned with Budzak's (2016) statement that people's behavior was a significant threat to information security.

In response to Interview Question 5, Participant B2 noted that "People post challenges, machines don't have feelings. Human beings have feelings; machine don't have feelings" and "People that operate these machines must be motivated." Responding to Interview Question 7, Participant B2 explained the human being was the most efficient strategy because "It is the people that work on the systems, which operate on the data." The participants aligned with Gyunka and Christiana' (2017) statement that health cybersecurity work behavior was essential to information security as firewalls and anti-malware. In this study, participants viewed peoples' management as a strategy for minimizing information security threats on business performance.

Findings Related to GST

The foundation of GST is the evolution of organisms or systems and the interdependence of systems with one another and their components (Von Bertalanffy, 1972). In GST, systems of factors work together to achieve organizational goal (Toscano & Toscano, 2016). All the participants agreed information security was a critical component and threats to information security could affect their business sustainability. Researchers and scholars used GST as lens to understand the wholeness of organization systems (Ceric, 2015; Yawson, 2013). Mangal (2013) utilized GST to demonstrate that websites with cohesive integration of system components provide more enjoyable experience than websites with dysfunctional elements. Coole and Brooks (2014) posited that a system was prone to decay leading to security failures when all components of the system were not efficaciously functioning or performing as a unified whole. Participants demonstrated that inability to establish good information security culture could be due to non-alignment of SETA, security policy, and people management.

Da Veiga and Martins (2015) posited that information security training and awareness is a significant factor in positively influencing information security culture within an organization. Chandrashekhar, Gupta, and Shivaraj (2015) noted the information security awareness was an essential element for successful implementation of information security plan. As applied in this study, all participants confirmed that information security education, training, and awareness was key to minimizing information security threats on business performance. Da Veiga and Martins indicated that human aspect, technology, and process control were integral parts of information security program. From the lens of GST, the interdependence of human aspect, technology, and process control was critical to minimizing the effects of information security threats on business performance. In this study, participants confirmed the integration of human dimension, technology, and process controls to achieve effective information security.

Parsons et al. (2015) posited that a significant positive relationship exist between information security decision making and organizational information security culture. Parsons et al. asserted that improving the security culture of an organization would mitigate the risk to the organization’s information systems and data. Y. Chen et al. (2015)

indicated that SETA programs have significant influence on information security culture. Tsohou, Karyda, and Kokolakis (2015) expressed the need to align security awareness programs with factors affecting internalization of communicated security-related information and making security-related decisions. In this study, the participants confirmed that information security education, training, and awareness could positively influence employees' behaviors to comply with information security policies, which would minimize the effects of information security threats on business performance.

Chandrashekhar et al. (2015) posited that organizations should implement information security strategy to reduce the risk of information security breaches. Safa et al. (2015) indicated that technology and users' behavior were important factors to consider to guarantee a secure environment for information. Ifinedo (2014) stated that organization utilize multi-perspective approaches to protect their information system assets and resources. Researchers have found out that organizations that do not align individual and other organizational issues with technology-based solutions might fail in their information security (Ifinedo, 2014). In this study, all participates implemented various information security strategies to minimize the consequences of information security threats on business sustainability. From the lens of GST, the implementation of several information security strategies may result in efficient information security culture within an organization.

Findings Related to Transformational Leadership Theory

Burns' (1978) transformational leadership theory described how leaders could inspire followers to change expectations, perceptions, and motivations to work toward common goals. The primary constructs underlying the transformational leadership theory are (a) idealized attributes, (b) idealized behaviors, (c) intellectual stimulation, (d) inspirational motivation, and (e) individualized consideration. Dinh et al. (2014) indicated that leaders determine the fate of their organizations through their decisions, strategies, and influence on others. T. Carter (2013) stated that transformational leaders inspire positive change in followers while Meuser et al. (2016) posited that transformational leaders influence their followers. Effelsberg et al. (2014) showed that a positive relationship exists between transformational leadership and employee's willingness to engage in a behavior while Sosik et al. (2014) stated that transformational leadership characteristics have an idealized influence on subordinates. Participants responses to the interview questions confirmed the transformational leadership theory that leaders inspire followers' willingness to positive change.

Ifinedo (2014) confirmed that organizational leaders influence employees' behavior to achieve desired information security through establishment of information security policy which contains the rules, guidelines, and requirements on information security assets and resources. Safa et al. (2015) posited that attitude, perceived behavioral control, and subjective norms influenced users' intention to comply with information security policies. Da Veiga and Martins (2015) posited that organizational leaders could achieve desired information security through assessment, monitoring, and influencing an information security culture. Tsohou et al. (2015) explained that corporate leaders used information security awareness to positively influences users' intentions to comply with information security policy. Deschamps, Rinfret, Lagacé, La Capitale, and Privé (2016) indicated that transformational leaders utilized inspirational engagement tactics to connect emotionally with employees, and demonstrated that transformational leaders could and did influence their followers' behavior. As applied in this study, participants confirmed transformational leadership theory that leaders could influence their followers' actions.

Martin (2016) illustrated the high correlation between transformational leadership and effective organizations. Da Veiga and Martins (2015) opined that organizational leaders influenced employees through implementation of various information security controls (education, training, and awareness) and processes (risk assessments) to change the information security culture. Tsohou et al. (2015) indicated that organizational leaders influenced users' security behavior when they understood the way users perceive risks and make security-related decisions. Deschamps et al. (2016) posited that transformational leaders entrust employees with autonomy to do their work and influence them to increase confidence in their work.

In this study, participants integrated various information security strategies to minimize the effects of information security threats on their business performance. The participants confirmed utilizing leadership skills to influence and motivate employees to adopt positive information security culture. The participants' answers to the interview questions supported the fundamental propositions of GST and primary constructs underlying transformational leadership theory, which were the conceptual framework for this study.

Applications to Professional Practice

The identification of strategies SME leaders use to minimize the effect of information security threats on business performance was essential in securing a firm's information system assets and resources for robust business sustainability. The findings from this study were about GST and transformational leadership theory and showed that SME leaders need a system of effective strategies and leadership skills to minimize the effects of information security threats on business performance. Study findings might assist SME leaders to gain a better understanding of the strategies to reduce the consequences of information security threats on business performance. The high rates of business failure and economic loss from security incident in SMEs and the resulting effect on global economy have been an increasing concern for organizational leaders (Bojanc & Jerman-Blazic, 2013; P. Jones et al., 2014). IBM and Ponemon Institute (2016) estimated the average total organizational cost of data security breaches in the United States in 2016 was $7.01 million.

All the participants' responses to Interview Question 1 indicated the utilization of a system of strategies to minimize the effects of information security threats on their business performance. The study findings were about GST and showed that SME leaders used a system of effective strategies involving human aspect, technology, and process control to minimize threats to information security (Da Veiga & Martins, 2015; Ifinedo, 2014). The study findings were also about transformational leadership theory and indicated that SME leaders used transformational leadership skills to influence employees' positive behaviors to desired security culture, which minimized threats to information security (Deschamps et al., 2016; Safa et al., 2015). Organizational leaders could gain significant knowledge from this study, which was conducive for maximizing sustainable business growth (Lawal et al., 2014; Oluga et al., 2014; Valli et al., 2014). SME leaders should use systems of strategies to minimize the effects of information security threats on business performance.

Eighty percent of the participants’ responses to Interview Question 7 indicated the most effective strategies for reducing the effects of information security threats depend on common threats and available resources. Da Veiga and Martins (2015) stated human aspect, technology, and process control were critical components of information security culture. Safa et al. (2016) posited that organizational leaders established information security policies as integral part of the corporate culture, which positively influenced employees’ information security attitudes and behaviors within the organizations. Y. Chen et al. (2015) advised corporate leaders to implement SETA programs to affect employee’s awareness on organizational security policy. All the participants have established information security policies and implemented SETA programs to enhance their corporate security culture.

Alegre et al. (2013) and Carraher and Van Auken (2013) indicated lack of leadership skills might set back SME development and overall business performance. Parsons et al. (2015) stated a significant positive relationship exists between information security decision-making and organization information security culture. Webb, Maynard, et al. (2014) posited that SME leaders faced challenges of coping with the rapidly evolving information security threats. Chae et al. (2014) showed no significant relationship exists between IT capability and firm financial performance. Information security incidents might result in multiple negative impacts, including loss of company reputation and customer confidence, litigations, loss of productivity, and direct financial loss (Tondel et al., 2014). All participant responses to the interview questions acknowledged their organization’s exposure to evolving information security threats.

Implications for Social Change

Servaes and Hoyng (2017) pointed out that ICT are techno-centric development tools for social change. Steinbart, Raschke, Gal, and Dilla (2016) explained how organizations are faced with ever-increasing number of security incidents. Securing computer systems and protecting sensitive and confidential data were critical to business success (Teh, Ahmed, & D'Arcy, 2015). This study’s findings could contribute to positive social change through SME leaders identifying strategies for minimizing the effects of information security threats on business performance and use profits from business to provide social amenities to the community.

Department for Business, Innovation & Skills (2015) reported an increase in small businesses that experienced security breaches and the negative effects on the firm’s turnover, productivity, and profitability. The adoption of these strategies could affect social change by influencing SME leaders to improve their business performance and sustainability. Security breaches decreased the share prices of both direct and similar companies (Hinz, Nofer, Schiereck, & Trillig, 2015). The findings of this study could assist business leaders to adopt strategies that could impact on organizational market value, which could allow individuals to drive economic value from ownership of stock to support their families and communities.

The findings from this study might be of importance to community leaders because the business improvement could result in increased flow of funds to the local community, which community leaders would utilize to build schools, health centers, and libraries for Port Harcourt city residents. The global communities could also gain from the available information on strategies to minimize the effects of information security on business performance, which could inspire positive social change in attitude toward information security. Findings might contribute to the body of knowledge regarding information security. Researchers and scholars could utilize the study findings to explore a greater understanding of strategies that organizational leaders could use to minimize the effects of information security threats on their business performance. With improved business performance, organizations would engage in corporate social responsibility (CSR) initiates and provide social amenities and utilities, such as electricity, road, borehole water, recreation centers, and sponsorship of local festivals. The people and society would benefit from these CSR projects.

Recommendations for Action

SMEs constitute about 97% of companies in Nigeria (Agwu, 2014) while small businesses constitute 99.9% of all businesses in United States (Armstrong, 2013). Uluyol and Akci (2014) pointed out that SMEs experience problems about incapability of managing technological issues. Seventy-four percentage of small businesses suffered at least one security breach in 2014 (PWC, 2015). Karyda and Mitrou (2016) identified external threats as the primary threat to information security, noting that Home Depot Inc. paid about $19 million in 2014 to compensate its customers. Based on the findings from this study, I recommend that SME leaders do the following:

- Take a meticulous and systematic approach to data security that effectively integrates all components, such as technology, people, processes, and systems.
- Establish rules, guidelines, or controls in place to enhance information security culture.
- Develop a combination of strategies that focus on minimizing their organization- specific information security threats to improve business performance.
- Employ information security management system to mitigate security incidents. PWC (2015) noted information system security management is a critical activity organizations use to mitigate security incidents.
- Increase the installation of security controls on company-owned devices. Department for Culture, Media, & Sport (2016) reported most organizations did not place security controls on company-owned devices.

The findings of this study are important to business leaders, researchers, and scholars in understanding and managing information security threats to business performance. I will disseminate the results of this study at training opportunities, conferences, and literature publications, which might stimulate organizational learning and stakeholders' interest.

Recommendations for Further Research

The purpose of this study was to explore the strategies SME leaders from firms supporting oil and gas sector in Port Harcourt, Nigeria use to minimize the effects of information security threats on business performance. Information security is a prevalent issue among experts and users (Safa et al., 2015). The study findings, recommendations, and conclusions might contribute to existing and future research and close gaps in business practice regarding strategies SME leaders use to minimize the effects of information security threats on business performance. Security of computer systems and protection of sensitive and confidential data are critical to business success (Teh et al., 2015). Safa et al. (2015) noted that understanding users and their perceptions could assist organizational leaders to minimize the effects of information security on business performance.

Organizational leaders and stakeholders were concerned about cyber security and demonstrated interest in minimizing information security risks (Safa et al., 2015). However, organizational leaders found it difficult to anticipate and quantify information security risks because of the rapidly changing and dynamic nature of technology and threat to information security (Safa et al., 2015). Da Veiga and Martins (2015) posited a system of effective strategies involving human aspect, technology, and process control could minimize threats to information security. Department for Culture, Media, & Sport (2016) stated that business leaders use regular software update, malware protections, and configured firewalls to minimize threats to information security on business performance.

A limitation of this study was that I used the exploratory qualitative multiple case study involving semi-structured interview. Future researchers may explore using either mixed methods, quantitative method, qualitative phenomenological design, or qualitative ethnography design. Utilizing these research methods or designs might provide an opportunity for larger sample size and cross-industry research. Researchers use mixed methods to examine and explore an issue (Archibald, 2016; Maxwell, 2016). I recommend future researchers use a quantitative correlation design to examine whether a relationship exist between information security strategies, leadership style, and business performance.

Another limitation of this study was the sample size, which was limited to five SME leaders from firms that support oil and gas sector in Port Harcourt, Nigeria. O. C. Robinson (2014) and Royset (2013) posited that using larger sample size might yield different themes. I recommend further studies with larger sample size from cross-industry sectors in various geographical locations such as Africa, America, and Europe, which could provide useful insight on strategies to minimize the effect of information security threats on business performance. The final limitation was my limited skills as a researcher in data collection. I recommend further studies might involve several experienced researchers with diverse contextual skills in conducting qualitative research.

Reflections

I utilized the qualitative multiple case study to explore the strategies SME leaders use to minimize the effects of information security threats on business performance. The doctoral research process was helpful in expanding my perspective and understanding regarding the level of detail and alignment required for doctoral level research. My doctoral study process was helpful in improving my communication, problem solving, analytical, networking, and interpersonal skills. The doctoral study was useful in enhancing my scholarly and professional knowledge on information security and common strategies organizational leaders use to minimize the effects of information security threats on business performance.

Reflecting on my experiences throughout this research process, I learned from the challenges encountered which changed my personal biases, ideas, and perceptions about this study. I utilized purposive sampling technique to select five SME leaders, from five case organizations, who had appropriate knowledge and experience about information security. Using the qualitative research method, I studied the participants in their work environment and gained in-depth understanding of the research problem.

During the semistructured interview, the participants spoke freely and expressed themselves in a manner that enabled me to understand what strategies they use to minimize the effects of information security threats on their business performance. The data that emerged from the participants' responses to the interview questions were overwhelming. The findings from this study aligned with contemporary literature on information security management system and increased my understanding of the research problem.

Conclusion

The purpose of this qualitative multiple case study was to explore the strategies SME leaders use to minimize the effects of information security threats on business performance. Data were collected from five SME leaders from five case organizations that support oil and gas sector in Port Harcourt, Nigeria. During the data analysis, 10 themes emerged which illustrated the strategies SME leaders use to minimize information security threats on business performance. The 10 themes were (a) network security, (b) physical security, (c) strong password policy, (d) antivirus protection and software update, (e) information security policy, (f) security education, training and awareness, (g) network security monitoring and audit, (h) intrusion detection, (i) data backup, and (j) people management.

The findings of this study aligned with the conceptual frameworks involving GST and transformational leadership theory and indicated that SME leaders used a system of effective strategies and leadership skills to minimize the effects of information security threats on business performance. The integral components of information security program are human aspect, technology, and process control (Da Veiga & Martins, 2015). The ability of corporate leaders to make decisions, establish strategies, and influence on other determine the fate of the organization (Dinh et al., 2014). The study findings supported previous literatures on information security strategies (Bélanger et al., 2017; Bingman, 2016; Budzak, 2016; Gangwar & Date, 2016; Ifinedo, 2014; Safa et al., 2015). SME leaders should implement a system of information security strategies working as a whole to minimize the effects of information security threats on business performance.

References

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

Abebe, M. (2014). Electronic commerce adoption, entrepreneurial orientation and small- and medium-sized enterprise (SME) performance. *Journal of Small Business and Enterprise Development*, *21*, 100-116. doi:10.1108/JSBED-10-2013-0145

Abrams, K. M., Wang, Z., Song, Y. J., & Galindo-Gonzalez, S. (2014). Data richness tradeoffs between face-to face, online audio-visual, and online text-only focus groups. *Social Science Computer Review*, *33*, 80-96. doi:10.1177/0894439313519733

Abro, M. M. Q., Khurshid, M. A., & Aamir, A. (2015). The use of mixed methods in management research. *Journal of Applied Finance & Banking*, *5*, 103-108. Retrieved from http://www.scienpress.com

Abualrob, A. A., & Kang, J. (2016). The barriers that hinder the adoption of e-commerce by small businesses: Unique hindrance in Palestine. *Information Development*, *32*, 1528-1544. doi:10.1177/0266666915609774

Adeleye, I. (2015). Accelerating corporate transformation in emerging markets: The case of First Bank. *South Asian Journal of Business and Management Cases*, *4*, 182-191. doi:10.1177/2277977915596247

Agwu, M.O. (2014). Issues, challenges and prospects of small and medium scale enterprises (SMEs) in Port Harcourt city, Nigeria. *European Journal of*

Sustainable Development, *3*(1), 101-114. doi:10.14207/ejsd.2014.v3nlp101

Ahmad, S. Z. (2014). Small and medium enterprises' internationalization and business strategy: Some evidence from firms located in an emerging market. *Journal of Asia Business Studies*, *8*, 168-186. doi:10.1108/jabs-03-2013-0012

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security*, *42*, 27-39. doi:10.1016/j.cose.2014.01.001

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

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*, 717-723. doi:10.1016/j.ijinfomgt.2015.08.001

Al-Ansari, Y., Pervan, S., & Xu, J. (2013). Innovation and business performance of SMEs: The case of Dubai. *Education, Business and Society: Contemporary Middle Eastern Issues*, *6*(3/4), 162-180. doi:10.1108/EBS-04-2013-0012

Alegre, J., Sengupta, K., & Lapiedra, R. (2013). Knowledge management and innovation performance in a high-tech SMEs industry. *International Small Business Journal*, *31*, 454-470. doi:10.1177/0266242611417472

AlEroud, A., & Alsmadi, I. (2017). Identifying cyber-attacks on software defined networks: An inference-based intrusion detection approach. *Journal of Network and Computer Applications*, *80*, 152-164. doi:10.1016/j.jnca.2016.12.024

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, *305*, 357-383. doi:10.1016/j.ins.2015.01.025

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

Allen, J. (2016). Backing up to save your practice. *American Journal of Family Law, 30*(2), 88-91. Retrieved from http://lrus.wolterskluwer.com

Alonso-Almeida, M. D. M., & Llach, J. (2013). Adoption and use of technology in small business environments. *The Service Industries Journal*, *33*, 1456-1472. doi:10.1080/02642069.2011.634904

Al-Saleh, M. I., AbuHjeela, F. M., & Al-Sharif, Z. A. (2015). Investigating the detection capabilities of antiviruses under concurrent attacks. *International Journal of Information Security*, *14*, 387–396. doi:10.1007/s10207-014-0261-x

Archibald, M. M. (2016). Investigator triangulation: A collaborative strategy with potential for mixed methods research. *Journal of Mixed Methods Research*, *10*, 228-250. doi:10.1177/1558689815570092

Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration*, *54*, 46-56. doi:10.1080/01930826.2014.893116

Armstrong, C. E. (2013). Competence or flexibility? Survival and growth implications of competitive strategy preferences among small US businesses. *Journal of Strategy* *and Management*, *6*, 377-398. doi:10.1108/jsma-06-2012-0034

Astuti, N. C., & Nasution, R. A. (2014). Technology readiness and e-commerce adoption among entrepreneurs of SMEs in Bandung city, Indonesia**.** *Gadjah Mada International Journal of Business*, *16*, 69-88. Retrieved from http://jurnal.ugm.ac.id/gamaijb

Awiagah, R., Kang, J., & Lim, J. I. (2016). Factors affecting e-commerce adoption among SMEs in Ghana. *Information Development*, *32*, 815-836. doi:10.1177/0266666915571427

Aykol, B., & Leonidou, L. C. (2014). Researching the green practices of smaller service firms: A theoretical, methodological, and empirical assessment. *Journal of Small Business Management*, *53*, 192-209. doi:10.1111/jsbm.12118

Bahl, S., & Wali, O. P. (2014). Perceived significance of information security governance to predict the information security service quality in software service industry: An empirical analysis. *Information Management & Computer Security*, *22*, 2-23. doi:10.1108/IMCS-01-2013-0002

Baines, J. T., Taylor, C. N., & Vanclay, F. (2013). Social impact assessment and ethical research principles: Ethical professional practice in impact assessment Part II. *Impact Assessment and Project Appraisal*, *31*, 254-260. doi:10.1080/14615517.2013.850306

Bala Subrahmanya, M. H. (2015). Innovation and growth of engineering SMEs in Bangalore: Why do only some innovate and only some grow faster? *Journal of Engineering and Technology Management*, *36*, 24-40.

doi:10.1016/j.jengtecman.2015.05.001

Balasubramanian, S., Jagannathan, V., & Natarajan, T. (2014). Information systems success in the context of Internet banking: Scale development. *Journal of Internet Banking and Commerce*, *19*(3), 1-15. Retrieved from http://www.arraydev.com/commerce/jibc/

Beattie, V. (2014). Accounting narratives and the narrative turn in accounting research: Issues, theory, methodology, methods and a research framework. *British Accounting Review*, *46*, 111-134. doi:10.1016/j.bar.2014.05.00

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*. Advanced Online Publication. doi:10.1016/j.im.2017.01.003

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

Berbary, L. A. (2014). Too good at fitting in: Methodological consequences and ethical adjustments. *International Journal of Qualitative Studies in Education*, *27*, 1205-1225. doi:10.1080/09518398.2013.820856

Bin-Abbas, H., & Bakry, S. H. (2014). Assessment of IT governance in organizations: A simple integrated approach. *Computers in Human Behavior*, *32*, 261-267. doi:10.1016/j.chb.2013.12.019

Bingman, K. L. (2016). C4ISR via dark webs: An alternative concept for protecting critical information in contested cyberspace environments. *Air & Space Power*

Journal, *30*(4), 69-77. Retrieved from http://www.au.af.mil/au/afri/aspj/

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*, 1802-1811. doi:10.1177/1049732316654870

Blackburn, G. (2014). Elements of successful change: The service Tasmania experience to public sector reform. *Australian Journal of Public Administration*, *73*, 103-114. doi:10.1111/1467-8500.12054

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal*, *19*, 426-432. doi:10.1108/qmr-06-2016-0053

Bojanc, R., & Jerman-Blazic, B. (2013). A quantitative model for information security risk management. *Engineering Management Journal*, *25*, 25-37. doi:10.1080/10429247.2013.11431972

Borrego, M., Foster, M. J., & Froyd, J. E. (2014). Systematic literature reviews in engineering education and other developing interdisciplinary fields. *Journal of Engineering Education*, *103*, 45-76. doi:10.1002/jee.20038

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*, 837-864. Retrieved from http://www.misq.org/

Bowden, C., & Galindo-Gonzalez, S. (2015). Interviewing when you’re not face-to-face: The use of email interviews in a phenomenological study. *International Journal of Doctoral Studies*, *10*, 79-92. Retrieved from http://ijds.org

Bradshaw, A., Cragg, P., & Pulakanam, V. (2013). Do IS consultants enhance IS competences in SMEs? *Electronic Journal of Information Systems Evaluation*, *16*, 13-24. Retrieved from http://www.ejise.com/main.html

Bredart, 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*, 15. doi:10.1186/1477-7525-12-15

Bronkhorst, B., Steijn, B., & Vermeeren, B. (2015). Transformational leadership, goal setting, and work motivation: The case of a Dutch municipality. *Review of Public Personnel Administration*, *35*, 124-145. doi:10.1177/0734371X13515486

Brown, T. (2015). A primer on data security. *CPA Journal, 85*(5), 58-62. Retrieved from www.nysscpa.org/news/publications/the-cpa-journal/issue

Budzak, D. (2016). Information security–The people issue. *Business Information Review*, *33*, 85-89. doi:10.1177/0266382116650792

Burns, J. (1978). *Leadership*. New York, NY: Harper & Row.

Burton, J. (2015). Small states and cyber security: The case of New Zealand. *Political Science*, *65*, 216-238. doi:10.1177/0032318713508491

Cai, S., Chen, X., & Bose, I. (2013). Exploring the role of IT for environmental sustainability in China: An empirical analysis. *International Journal of Production Economics*, *146*, 491-500. doi:10.1016/j.ijpe.2013.01.030

Caine, V., Estefan, A., & Clandinin, D. J. (2013). A return to methodological commitment: Reflections on narrative inquiry. *Scandinavian Journal of*

Educational Research, *57*, 574-586. doi:10.1080/00313831.2013.798833

Cao, Q., Thompson, M. A., & Triche, J. (2013). Investigating the role of business processes and knowledge management systems on performance: A multi-case study approach. *International Journal of Production Research*, *51*, 5565-5575. doi:10.1080/00207543.2013.789145

Carcary, M., Doherty, E., & Conway, G. (2014). The adoption of cloud computing by Irish SMEs – An exploratory study. *Electronic Journal of Information Systems Evaluation*, *17*, 3-14. Retrieved from http://www.ejise.com

Carraher, S., & Van Auken, H. (2013). The use of financial statements for decision making by small firms. *Journal of Small Business & Entrepreneurship*, *26*, 323-336. doi:10.1080/08276331.2013.803676

Carter, T. (2013). Global leadership. *Journal of Management Policy and Practice*, *14*, 69-74. Retrieved from http://www.na-businesspress.com/jmppopen.html

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, *41*, 545-547. doi:10.1188/14.ONF.545-547

Caruth, G. D. (2013). Demystifying mixed methods research design: A review of the literature. *Mevlana International Journal of Education*, *3*, 112-122. doi:10.13054/mije.13.35.3.2

Cazorla, L., Alcaraz, C., & Lopez, J. (2015). A three-stage analysis of IDS for critical infrastructures. *Computers & Security*, *55*, 235-250. doi:10.1016/j.cose.2015.07.00

Ceric, A. (2015). Bringing together evaluation and management of ICT value: A systems theory approach. *The Electronic Journal of Information Systems Evaluation*, *18*, 19-35. Retrieved from http://www.ejise.com/main.html

Chae, H. C., Koh, C. E., & Prybutok, V. R. (2014). Information technology capability and firm performance: Contradictory findings and their possible causes. *MIS Quarterly*, *38*, 305-326. Retrieved from htpp://www.misq.org/

Chairoel, L., Widyarto, S., & Pujani, V. (2015). ICT adoption in affecting organizational performance among Indonesian SMEs. *The International Technology Management Review*, *5*, 82-93. doi:10.2991/itmr.2015.5.2.3

Chan, Z. C., Fung, Y. L., & Chien, W. T. (2013). Bracketing in phenomenology: Only undertaken in the data collection and analysis process? *The Qualitative Report*, *18*(30), 1-9. Retrieved from http://nsuworks.nova.edu/tqr/

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/

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4), 49-87. doi:10.1080/07421222.2014.1001257

Chen, K., Lei, H., Li, G., Huang, W., & Mu, L. (2014). Cash incentives improve participation rate in a face-to-face survey: An intervention study. *Journal of Clinical Epidemiology*, *68*, 228-233. doi:10.1016/j.jclinepi.2014.08.002

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. doi:10.1080/08874417.2015.11645767

Cheng, C. C., Yang, C. L., & Sheu, C. (2014). The link between eco-innovation and business performance: A Taiwanese industry context. *Journal of Cleaner Production*, *64*, 81-90. doi:10.1180/EBS-04-2013-0012

Chiumento, A., Khan, M. N., Rahman, A., & Frith, L. (2016). Managing ethical challenges to mental health research in post conflict settings. *Developing World Bioethics*, *16*, 15-28. doi:10.1111/dewb.12076

Chuang, P-J., and Wang, C-H. (2017). An efficient group-based backup and recovery scheme in cloud computing systems. *Journal of Information Science & Engineering, 33*, 183-198. Retrieved from http://jise.iis.sinica.edu.tw/

Cibangu, S. K., & Hepworth, M. (2016). The uses of phenomenology and phenomenography: A critical review. *Library & Information Science Research*, *38*, 148-160. doi:10.1016/j.lisr.2016.05.001

Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: Does size matter? *Journal of Advanced Nursing*, *7*0, 473-475. doi:10.1111/jan.12163

Coffie, R. M. (2013). *The impact of social venture capital and social entrepreneurship on poverty reduction* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3556987)

Collins, K. M., Onwuegbuzie, A. J., Johnson, R. B., & Frels, R. K. (2013). Practice note:

Using debriefing interviews to promote authenticity and transparency in mixed research. *International Journal of Multiple Research Approaches*, *7*, 271-284. doi:10.5172/mra.2013.7.2.271

Colombo, M. G., Croce, A., & Grilli, L. (2013). ICT services and small businesses' productivity gains: An analysis of the adoption of broadband Internet technology. *Information Economics and Policy*, *25*, 171-189. doi:10.1016/j.infoecopol.2012.11.001

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

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). Thousand Oaks, CA: Sage.

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher*, *21*(5), 19-27. doi:10.7748/nr.21.5.19.e1240

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. C*omputers & Security*, *32*, 90-101. doi:10.1016/j.cose.2012.09.010

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

Cunliffe, A. L., & Karunanayake, G. (2013). Working within hyphen-spaces in ethnographic research: Implications for research identities and practice.

Organizational Research Methods, *16*, 364-392. doi:10.1177/1094428113489353

Cuthbert, C. A., & Moules, N. (2014). The application of qualitative research findings to oncology nursing practice. *Oncology Nursing Forum*, *41*, 683-685. doi:10.1188/14.ONF.683-685

Dasgupta, M. (2015). Exploring the relevance of case study research. *Vision: The Journal of Business Perspective*, *19*, 147-160. doi:10.1177/0972262915575661

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162-176. doi:10.1016/j.cose.2014.12.006

Deakin, H., & Wakefield, K. (2014). SKYPE interviewing: Reflections of two PhD researchers. *Qualitative Research*, *14*, 603-616. doi:10.1177/1468794113488126

Debreceny, R. S. (2013). Research on IT governance, risk, and value: Challenges and opportunities. *The Journal of Information Systems*, *27*(1), 129-135. doi:10.2308/isys-10339

de Gusmão, A. P. H., e Silva, L. C., Silva, M. M., Poleto, T., & Costa, A. P. C. S. (2016). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management*, *36*, 25-34. doi:10.1016/j.ijinfomgt.2015.09.003

De Massis, A., & Kotlar, J. (2014). The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy*, *5*, 15-29. doi:10.1016/j.jfbs.2014.01.007

Department for Business, Innovation & Skills. (2015). *Information security breaches* *survey 2015: Technical report*. London, United Kingdom. Retrieved from https://www.gov.uk/government/publications/information-security-breaches-survey-2015

Department for Culture, Media, & Sport. (2016). Cyber security breaches survey 2016. Retrieved from https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016

Deschamps, C., Rinfret, N., Lagacé, M. C., La Capitale, C., & Privé, C. (2016). Transformational leadership and change: How leaders influence their followers' motivation through organizational justice. *Journal of Healthcare Management*, *61*(3), 194-213. Retrieved from https://ache.org/pubs/jhm/jhm_index.cfm

Devos, J., & Van de Ginste, K. (2015). Towards a theoretical foundation of IT governance: The COBIT 5 case. *The Electronic Journal of Information Systems Evaluation*, *18*, 95-103. Retrieved from http://www.ejise.com/main.html

Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse Researcher*, *20*(5), 28-32. doi:10.7748/nr2013.05.20.5.28.e327

Dinh, J. E., Lord, R. G., Gardner, W. L., Meuser, J. D., Liden, R. C., & Hu, J. (2014). Leadership theory and research in the new millennium: Current theoretical trends and changing perspectives. *The Leadership Quarterly*, *25*, 36-62. doi:10.1016/j.leaqua.2013.11.005

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*, 92-100. doi:10.4236/jis.2013.42011

Drew, H. (2014). Overcoming barriers: Qualitative interviews with German Elites. *Electronic Journal of Business Research Methods*, *12*, 77-86. Retrieved from http://www.ejbrm.com

Edwards-Jones, A. (2014). Qualitative data analysis with NVIVO. *Journal of Education for Teaching: International Research and Pedagogy*, *40*, 193-195. doi:10.1080/02607476.2013.866724

Effelsberg, D., Solga, M., & Gurt, J. (2014). Transformational leadership and follower's unethical behavior for the benefit of the company: A two-study investigation. *Journal of Business Ethics*, *120*, 81-93. doi:10.1007/s10551-013-1644-z

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open*, *4*(1). doi:10.1177/2158244014522633

Emmel, N. (2015). Themes, variables, and the limits to calculating sample size in qualitative research: A response to Fugard and Potts. *International Journal of Social Research Methodology*, *18*, 685-686. doi:10.1080/13645579.2015.1005457

Fan, X. (2013). "The test is reliable"; "The test is valid": Language use, unconscious assumptions, and education research practice. *The Asia-Pacific Education Researcher*, *22*, 217-218. doi:10.1007/s40299-012-0036-y

Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance*, *28*, 243-248. doi:10.1016/S2212-5671(15)01106-5

Ference, S. B., & Graf, N. (2016). Controlling your data. *Journal of Accountancy, 222*(2), 18-20. Retrieved from http://www.journalofaccountancy.com/

Ferguson, C., Green, P., Vaswani, R., & Wu, G.-H. (2013). Determinants of effective information technology governance. *International Journal of Auditing*, *17*, 75-99. doi:10.1111/j.1099-1123.2012.00458

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

Fjellström, D., & Guttormsen, D. S. A. (2016). A critical exploration of "access" in qualitative international business field research: Towards a concept of socio-cultural and multidimensional research practice. *Qualitative Research in Organizations and Management: An International Journal*, *11*, 110-126. doi:10.1108/qrom-05-2014-1225

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

Ford, J., & Harding, N. (2015). Followers in leadership theory: Fiction, fantasy and illusion. *Leadership*. Advance online publication. doi:10.1177/1742715015621372

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development*, *91*, 184-194. doi:10.1002/j.1556-6676.2013.00085.x

Fu, H.-P., & Chang, T.-S. (2016). An analysis of the factors affecting the adoption of cloud consumer relationship management in the machinery industry in Taiwan. *Information Development*, *32*, 1741-1756. doi:10.1177/ 0266666915623318

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*, 1408-1416. Retrieved from http://nsuworks.nova.edu/tqr/

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*, 117. doi:10.1186/1471-2288-13-117

Gangwar, H., & Date, H. (2016). Critical factors of cloud computing adoption in organizations: An empirical study. *Global Business Review*, *17*, 886-904. doi:10.1177/0972150916645692

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Developing a cloud-computing adoption framework. *Global Business Review*, *16*, 632-651. doi:10.1177/0972150915581108

Garrison, D. R., &Vaughan, N. D. (2013). Institutional change and leadership associated with blended learning innovation: Two case studies. *The Internet and Higher Education*, *18*, 24-28. doi:10.1016/j.iheduc.2012.09.001

Gbandi, E. C., & Amissah, G. (2014). Financing options for small and medium enterprises (SMEs) in Nigeria. *European Scientific Journal*, *10*, 327-340. Retrieved from http://eujournal.org

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*, *20*, 1772-1779. Retrieved from http://nsuworks.nova.edu/tqr/

Gibson, S., Benson, O., & Brand, S. (2013). Talking about suicide: Confidentiality and anonymity in qualitative research. *Nursing Ethics*, *20*, 18-29. doi:10.1177/0969733012452684

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

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research notes on the Gioia methodology. *Organizational Research Methods*, *16*, 15-31. doi:10.1177/1094428112452151

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

Green, J. (2015). Staying ahead of cyber-attacks. *Network Security*, (2), 13-16. doi:10.1016/s1353-4858(15)30007-6

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, *37*, 337-355. Retrieved from http://www.misq.org/

Grigoroudis, E., Tsitsirisi, E., & Zopounidis, C. (2013). Linking customer satisfaction, employee appraisal, business performance: An evaluation methodology in the banking sector. *Annals of Operations Research*, *205*, 5-27. doi:10.1007/s10479-

012-1206-2

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care Chaplaincy*, *20*, 109-122. doi:10.1080/08854726.2014.925660

Guetterman, T. C. (2015). Descriptions of sampling practices within five approaches to qualitative research in education and the health sciences. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, *16*(2), 1-23. Retrieved from http://www.qualitative-research.net/

Guo, C., Porschitz, E. T., & Alves, J. (2013). Exploring career agency during self-initiated repatriation: A study of Chinese sea turtles. *Career Development International*, *18*, 34-55. doi:10.1108/1362043131130

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242-251. doi:10.1016/j.cose.2012.10.003

Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management*, *33*, 861-874. doi:10.1016/j.ijinfomgt.2013.07.001

Gyunka, B. A., & Christiana, A. O. (2017). Analysis of human factors in cyber security: A case study of anonymous attack on Hbgary. *Computing & Information Systems, 21*(2), 10-18. Retrieved from http://cis.uws.ac.uk/

Halverson, L. R., Graham, C. R., Spring, K. J., Drysdale, J. S., & Henrie, C. R. (2014). A thematic analysis of the most highly cited scholarship in the first decade of blended learning research. *The Internet and Higher Education*, *20*, 20-34.

doi:10.1016/j.iheduc.2013.09.004

Hamann, R., Smith, J., Tashman, P., & Marshall, R. S. (2017). Why do SMEs go green? An analysis of wine firms in South Africa. *Business & Society*, *56*, 23-56. doi:10.1177/0007650315575106

Hao, S., & Song, M. (2016). Technology-driven strategy and firm performance: Are strategic capabilities missing links? *Journal of Business Research*, *69*, 751-759. doi:10.1016/j.jbusres.2015.07.043

Harrison, J. S., Banks, G. C., Pollack, J. M., O'Boyle, E. H., & Short, J. (2017). Publication bias in strategic management research. *Journal of Management*, 43, 400-425. doi:10.1177/0149206314535438

Harvey, L. (2015). Beyond member checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education*, *38*, 23-38. doi:10.1080/1743727X.2014.914487

Hayes, B., Bonner, A., & Douglas, C. (2013). An introduction to mixed methods research for nephrology nurses. *Renal Society of Australasia Journal*, *9*, 8-14. Retrieved from http://www.renalsociety.org/RSAJ/index_nl.html

Heale, R., & Forbes, D. (2013). Understanding triangulation in research. *Evidence-Based Nursing*, *16*, 98-98. doi:10.1136/eb-2013-101494

Henry, C., & Foss, L. (2015). Case sensitive? A review of the literature on the use of case method in entrepreneurship research. *International Journal of Entrepreneurial Behavior & Research*, *21*, 389-409. doi:10.1108/ijebr-03-2014-0054

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

Heroux, S., & Fortin, A. (2013). Exploring information technology governance and control of web site content: A comparative case study. *Journal of Managing and Governance*, *17*, 673-721. doi:10.1007/s10997-011-9200-7

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

Holm, H., Sommestad, T., Ekstedt, M., & Honeth, N. (2014). Indicators of expert judgment and their significance: An empirical investigation in the area of cyber security. *Expert Systems*, *31*, 299-318. doi:10.1111/exsy.12039

Holt, M., & Powell, S. (2015). Health and well-being in small and medium-sized enterprises (SMEs). What public health support do SMEs really need? *Perspectives in Public Health*, *135*, 49-55. doi:10.1177/1757913914521157

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

Iacob, N. M. (2015). Data security for e-learning platforms. *Knowledge Horizons - Economics*, *7*(1), 85-87. Retrieved from http://www.orizonturi.ucdc.ro/

Iacob, N. M., & Defta, C. L. (2015). HTTP protocol security for e-learning platforms.

Knowledge Horizons - Economics, *7*(3), 144-146. Retrieved from http://www.orizonturi.ucdc.ro/

IBM & Ponemon Institute. (2016). 2016 cost of data breach study: Global study. Retrieved from http://www-03.ibm.com/security/data-breach/

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*, 69-79. doi:10.1016/j.im.2013.10.001

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

International Organization for Standardization/International Electrotechnical Commission 27000. (2014). *Terms and Definitions*. *ISO/IEC 27000:2014 (en) Information technology - Security techniques - Information security management systems - Overview and vocabulary*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

Jarvelainen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, *33*, 583-590. doi:10.1016/j.ijinfomgt.2013.03.001

Johnson, R. A., & Bibbo, J. (2014). Relocation decisions and constructing the meaning of home: A phenomenological study of the transition into a nursing home. *Journal of Aging Studies*, *30*, 56-63. doi:10.1016/j.jaging.2014.03.005

Jones, J. M., & Sherr, M. E. (2014). The role of relationships in connecting social work research and evidence-based practice. *Journal of Evidence-based Social Work*, *11*, 139-147. doi:10.1080/15433714.2013.845028

Jones, P., Simmons, G., Packham, G., Beynon-Davies, P., & Pickernell, D. (2014). An exploration of the attitudes and strategic responses of sole- proprietor micro-enterprises in adopting information and communication technology. *International Small Business Journal*, *32*, 285-306. doi:10.1177/0266242612461802

Karyda, M., & Mitrou, L. (2016, September). Data breach notification: Issues and challenges for security management. Proceedings of the tenth Mediterranean Conference on Information Systems(MCIS), Paphos, Cyprus. Retrieved from http://aisel.aisnet.org/mcis2016/60

Ketokivi, M., & Choi, T. (2014). Renaissance of case research as a scientific method. *Journal of Operations Management*, *32*, 232-240. doi:10.1016/j.jom.2014.03.004

Khera, M. (2017). Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications. *Journal of Diabetes Science and Technology*, *11*, 202-212. doi:10.1177/1932296816677576

Killam, L. A., & Heerschap, C. (2013). Challenges to student learning in the clinical setting: A qualitative descriptive study. *Nurse Education Today*, *33*, 684-691. doi:10.1016/j.nedt.2012.10.008

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*, 9. 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, S., & Yoon, G. (2015). An innovation-driven culture in local government do senior manager's transformational leadership and the climate for creativity matter? *Public Personnel Management*, *44*, 147-168. doi:10.1177/0091026014568896

Kirkwood, A., & Price, L. (2013). Examining some assumptions and limitations of research on the effects of emerging technologies for teaching and learning in higher education. *British Journal of Educational Technology*, *44*, 536-543. doi:10.1111/bjet.12049

Kongnso, F. (2015). *Best practices to minimize data security breaches for increased business performance* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3739769)

Kornbluh, M. (2015). Combatting challenges to establishing trustworthiness in qualitative research. *Qualitative Research in Psychology*, *12*, 397-414. doi:10.1080/14780887.2015.1021941

Lamb, D. (2013a). Promoting the case for using a research journal to document and reflect on the research experience. *The Electronic Journal of Business Research Methods*, *11*, 84-92. Retrieved from http://www.ejbrm.com

Lamb, D. (2013b). Research in the first person: Reflection on the research experience using a research journal. *Market & Social Research*, *21*(2), 32-39. Retrieved from http://www.amsrs.com.au/

Landers, R. N., & Behrend, T. S. (2015). An inconvenient truth: Arbitrary distinctions between organizational, mechanical Turk, and other convenience samples. *Industrial and Organizational Psychology*, *8*, 142-164. doi:10.1017/iop.2015.13

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/

Lantos, J. D., & Spertus, J. A. (2014). The concept of risk in comparative-effectiveness research. *New England Journal of Medicine*, *371*, 2129-2130. doi:10.1056/NEJMhle1413301

Lawal, A. A., Ajonbadi, H. A., & Otokiti, B. O. (2014). Strategic importance of the Nigerian small and medium enterprises (SMEs): Myth or reality. *American Journal of Business*, *Economics and Management*, *2*, 94-104. Retrieved from http://www.openscienceonline.com/journal/ajbem

Laybats, C., & Tredinnick, L. (2016). Information Security. *Business Information Review*, *33*, 76-80. doi:10.1177/026638211665306

Leedy, P. D., & Ormrod, J. E. (2013). *Practical research: Planning and design* (10th ed.). Upper Saddle River, NJ: Pearson.

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*, 324-324. doi:10.4103/2249-4863.161306

Li, W., Meng, W., Kwok, L. F., & Horace, H. S. (2017). Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. *Journal of Network and Computer Applications*, *77*, 135-145. doi:10.1016/j.jnca.2016.09.014

Lihong, Z., & Miguel, B. N. (2013). Doing qualitative research in Chinese contexts: Lessons learned from conducting interviews in a Chinese healthcare environment. *Library Hi Tech*, *31*, 419-434. doi:10.1108/LHT-11-2012-0104

Lin, H. F. (2014). Understanding the determinants of electronic supply chain management system adoption: Using the technology–organization–environment framework. *Technological Forecasting and Social Change*, *86*, 80-92. doi:10.1016/j.techfore.2013.09.001

Lindley, J., Sharma, D., & Potts, R. (2014). Anticipatory ethnography: Design fiction as an input to design ethnography. *Ethnographic Praxis in Industry Conference Proceedings*, 237-253. doi:10.1111/1559-8918.01030

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

Loh, J. (2013). Inquiry into issues of trustworthiness and quality in narrative studies: A perspective. *The Qualitative Report*, *18*(33), 1-18. Retrieved from http://nsuworks.nova.edu/tqr/

Lopez-Dicastillo, O., & Belintxon, M. (2014). The challenges of participant observations of cultural encounters within an ethnographic study. *Procedia - Social and Behavioral Sciences*, *132*, 522-526. doi:10.1016/j.sbspro.2014.04.347

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, *9*, 3-31. doi:10.1504/ijcis.2013.051608

Lunde, A., Heggen, K., & Strand, R. (2013). Knowledge and power: Exploring unproductive interplay between quantitative and qualitative researchers. *Journal of Mixed Methods Research*, *7*, 197-210. doi:10.1177/1558689812471087

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 http://www.ijbcnet.com/

Maree, J. E., Parker, S., Kaplan, L., & Oosthuizen, J. (2016). The information needs of South African parents of children with cancer. *Journal of Pediatric Oncology Nursing*, *33*, 9-17. doi:10.1177/1043454214563757

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

Martin, J. (2016). Perceptions of transformational leadership in academic libraries. *Journal of Library Administration*, *56*, 266-284. doi:10.1080/01930826.2015.1105069

Maxwell, J. A. (2016). Expanding the history and range of mixed methods research. *Journal of Mixed Methods Research*, *10*, 12-27. doi:10.1177/1558689815571132

Mazzarol, T. (2015). SMEs engagement with e-commerce, e-business and e-marketing. *Small Enterprise Research*, *22*, 79-90. doi:10.1080/13215906.2015.1018400

McCreight, T., & Leece, D. (2016). Physical security and IT convergence: Managing the cyber-related risks. *Journal of Business Continuity & Emergency Planning*, *10*(1), 18-30. Retrieved from https://www.henrystewartpublications.com/jbcep

Mealer, M., & Jones, J. (2014). Methodological and ethical issues related to qualitative telephone interviews on sensitive topics. *Nurse Researcher*, *21*(4), 32-37. doi:10.7748/nr2014.03.21.4.32.e1229

Mejias, R. J., & Balthazard, P. A. (2014). A model of information security awareness for assessing information security risk for emerging technologies. *Journal of Information Privacy and Security*, *10*, 160-185. doi:10.1080/15536548.2014.974407

Mesquida, A. L., & Mas, A. (2015). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 security extension. *Computers & Security*, *48*, 19-34. doi:10.1016/j.cose.2014.09.003

Meuser, J. D., Gardner, W. L., Dinh, J. E., Hu, J., Liden, R. C., & Lord, R. G. (2016). A network analysis of leadership theory: The infancy of integration. *Journal of*

Management, *42*, 1374-1403. doi:10.1177/0149206316647099

Mishra, P., Pilli, E. S., Varadharajan, V., & Tupakula, U. (2017). Review - Intrusion detection techniques in cloud environment: A survey. *Journal of Network and Computer Applications*, *77*, 18-47. doi:10.1016/j.jnca.2016.10.015

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

Mohlameane, M., & Ruxwana, N. (2014). The awareness of cloud computing: A case study of South Africa SMEs. *International Journal of Trade, Economics, and Finance*, *5*, 1-7. doi:10.7763/IJTEF.2014.V5.332

Montesdioca, G. P. Z., & Macada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, *48*, 267-280. doi:10.1016/j.cose.2014.10.015

Morse, J. M. (2015). Data were saturated . . .. *Qualitative Health Research*, *25*, 587-588. doi:10.1177/1049732315576699

Morse, A. L., & McEvoy, C. D. (2014). Qualitative research in sport management: Case study as a methodological approach. *The Qualitative Report*, *19*(31), 1-13. Retrieved from http://nsuworks.nova.edu/tqr/

Moss, J. M., Gibson, D. M., & Dollarhide, C. T. (2014). Professional identity development: A grounded theory of transformational tasks of counselors. *Journal* *of Counseling and Development*, *92*, 3-12. doi:10.1002/j.1556-6676.2014.00124.x

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

Narteh, B. (2013). SME bank selection and patronage behaviour in the Ghanaian banking industry. *Management Research Review*, *36*, 1061-1080. doi:10.1108/MRR-06-2012-0147

National Institutes of Health (NIH). (2015). *Protecting human participants (online training course)*. Retrieved from http://phrp.nihtraining.com/

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*, 123-134. doi:10.1016/j.im.2014.10.009

Nelson, G., & Evans, S. D. (2014). Critical community psychology and qualitative research: A conversation. *Qualitative Inquiry*, *20*, 158-166. doi:10.1177/1077800413510873

Neumann, K. (2013). ‘Know why’ thinking as a new approach to systems thinking. *Emergence: Complexity and Organization*, *15*(3), 81-93. Retrieved from http://journal.emergentpublications.com

Newington, L., & Metcalfe, A. (2014). Factors influencing recruitment to research: Qualitative study of the experiences and perceptions of research terms. *BMC Medical Research Methodology*, *14*, 10. doi:10.1186/1471-2288-14-10

Newman, D. A., Joseph, D. L., & Feitosa, J. (2015). External validity and multiorganization samples: Levels-of-analysis implications of crowdsourcing and college student samples. *Industrial and Organizational Psychology*, *8*, 214-220. doi:10.1017/iop.2015.28

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*, 28. doi:10.1186/1472-6939-14-28

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, *18*, 34-35. doi:10.1136/eb-2015-102054

Nowduri, S. (2014). An impact of management information systems on corporate sustainability: A survey. *International Journal of Business and Management*, *9*(7), 146-154. doi:10.5539/ijbm.v9n7p146

Ody-Brasier, A., & Vermeulen, F. (2014). The price you pay: Price-setting as a response to norm violations in the market for champagne grapes. *Administrative Science Quarterly*, *59*, 109-144. doi:10.1177/0001839214523002

O'Keeffe, J. O., Buytaert, W., Mijic, A., Brozovic, N., & Sinha, R. (2015). The use of semi-structured interviews for the characterization of farmer irrigation practices. *Hydrology and Earth System Sciences Discussions*, *12*, 8221-8246. doi:10.5194/hessd-12-8221-2015

Oluga, S. O., Ahmad, A. B. H., Alnagrat, A. J. A., Oluwatosin, H. S., Sawad, M. O. A., & Mukta, N. A. B. (2014). An overview of contemporary cyberspace activities and the challenging cyberspace crimes/threats. *International Journal of Computer Science and Information Security*, *12*(3), 62-100. Retrieved from https://sites.google.com/site/ijcsis/

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*(2), 98-113. doi:10.5296/ije.v6i2.4424

Orozco, J., Tarhini, A., & Tarhini, T. (2015). A framework of IS/business alignment management practices to improve the design of IT governance architectures. *International Journal of Business and Management*, *10*(4), 1-12. doi:10.5539/ijbm.v10n4p1

Osakwe, C. N., Chovancova, M., & Agu, M. (2016). Can micro-enterprises leverage on the adoption of corporate websites to bolster their brand visibility? Examining salient adoption issues in Nigeria. *Information Development*, *32*, 904-919. doi:10.1177/0266666915573551

Osei-Assibey, E. (2013). Source of finance and small enterprise's productivity growth in Ghana. *African Journal of Economic and Management Studies*, *4*, 372-386. doi:10.1108/AJEMS-03-2012-0017

Oterkiil, C., & Ertesvag, S. K. (2014). Development of a measurement for transformational and transactional leadership in schools taking on a school-based intervention. *Educational Management Administration & Leadership*, *42*(4S), 5-27. doi:10.1177/1741143214523011

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*, 533-544. doi:10.1007/s10488-013-0528-y

Pandey, S., & Chawla, D. (2016). Using qualitative research for establishing content validity of e-lifestyle and website quality constructs. *Qualitative Market Research: An International Journal*, *19*, 339-356. doi:10.1108/qmr-05-2015-0033

Pandey, S. K., Davis, R. S., Pandey, S., & Peng, S. (2015). Transformational leadership and the use of normative public values: Can employees be inspired to serve larger public purposes? *Public Administration*, *94*, 204-222. doi:10.1111/padm.12214

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

Perez, R. G., Branch, R., & Kuofie, M. (2014). EOFISI model as a predictive tool to favor smaller gaps on the information security implementations. *Journal of IT and Economic Development*, *5*(1), 1-20. Retrieved from http://www.gsmi-ijgb.com/

Posey, C., Roberts, T., Lowry, P. B., Bennett, B., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, *37*, 1189-1210. Retrieved from http://www.misq.org

PWC. (2015). 2015 Information security breaches survey. Retrieved from http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pd

Qassimi, N. A., & Rusu, L. (2015). IT governance in a public organization in a developing country: A case study of a governmental organization. *Procedia Computer Science*, *64*, 450-456. doi:10.1016/j.procs.2015.08.541

Rahman, S. M., & Lackey, L. (2013). E-commerce systems security for small businesses. *International Journal of Network Security & Its Applications*, *5*(2), 193-210. doi:10.5121/ijnsa.2013.5215

Ramdani, B., Chevers, D., & Williams, D. A. (2013). SMEs' adoption of enterprise applications: A technology-organization-environment model. *Journal of Small Business and Enterprise Development*, *20*, 735-753. doi:10.1108/JSBED-12-2011-0035

Rebollo, O., Mellado, D., Fernandez-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, *58*, 44-57. doi:10.1016/j.infsof.2014.10.003

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. doi:10.12968/bjom.2013.21.3.215

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology*, *11*, 25-41.

doi:10.1080/14780887.2013.801543

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, *49*, 70-94. doi:10.1016/j.cose.2014.11.007

Roy, O., & Pacuit, E. (2013). Substantive assumptions in interaction: A logical perspective. *Synthese*, *190*, 891-908. doi:10.1007/s11229-012-0191-y

Royset, J. O. (2013). On sample size control average approximations for solving smooth stochastic programs. *Computational Optimization and Applications*, *55*, 265-309. doi:10.1007/s10589-012-9528-1

Runhaar, P., ten Brinke, D., Kuijpers, M., Wesselink, R., & Mulder, M. (2013). Exploring the links between interdependence, team learning, and a shared understanding among team members: The case of teachers facing an educational innovation. *Human Resource Development International*, *17*, 67-87. doi:10.1080/13678868.2013.856207

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

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70-82. doi:10.1016/j.cose.2015.10.006

Sahdev, T. S., Medudula, M. K., & Sagar, M. (2014). An analysis of barriers for the adoption of cloud computing in education sector. *Management and Labour Studies*, *39*, 249-274. doi:10.1177/0258042X15572422

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

Santos, G., Barros, S., Mendes, F., & Lopes, N. (2013). The main benefits associated with health and safety management systems certification in Portuguese small and medium enterprises post quality management system certification. *Safety Science*, *51*, 29-36. doi:10.1016/j.ssci.2012.06.014

Sarma, S. K. (2015). Qualitative research: Examining the misconceptions. *South Asian Journal of Management*, *22*(3), 176-191. Retrieved from http://www.sajm-amdisa.org

Schoenung, B., & Dikova, D. (2016). Reflections on organizational team diversity research: In search of a logical support to an assumption. *Equality, Diversity and Inclusion: An International Journal*, *35*, 221-231. doi:10.1108/edi-11-2015-0095

Scutt, C., & Hobson, J. (2013). The stories we need: Anthropology, philosophy, narrative and higher education research. *Higher Education Research & Development*, *32*, 17-29. doi:10.1080/07294360.2012.751088

Semenova, N., & Hassel, L. G. (2015). On the validity of environmental performance metrics. *Journal of Business Ethics*, *132*, 249-258. doi:10.1007/s10551-014-2323-4

Servaes, J., & Hoyng, R. (2017). The tools of social change: A critique of techno-centric development and activism. *New Media & Society*, *19*, 255-271. doi:10.1177/1461444815604419

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14-30. doi:10.1016/j.cose.2015.11.001

Silva, M. M., de Gusmão, A. P. H., Poleto, T., e Silva, L. C., & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management*, *34*, 733-740. doi:10.1016/j.ijinfomgt.2014.07.005

Simpson, A., Slutskaya, N., Hughes, J., & Simpson, R. (2014). The use of ethnography to explore meaning that refuse collectors attach to their work. *Qualitative Research in Organization and Management: An International Journal*, *9*, 183-200. doi:10.1108/QROM-01-2013-1133

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management*, *27*, 644-667. doi:10.1108/JEIM-07-2013-0052

Siu, A. H., Hung, A., Lam, A. L., & Cheng, A. (2013). Work limitations, workplace concerns, and job satisfaction of persons with chronic disease. *Work*, *45*, 107-115. doi:10.3233/WOR-121550

Small and Medium Enterprises Development Agency of Nigeria (SMEDAN). (2013). *SMEDAN and national bureau of statistics collaborative survey: Selected* *findings*. Retrieved from http://nigerianstat.gov.ng

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

Soares, S., & de Oliveira, W. F. (2016). The matrix approach to mental health care: Experiences in Florianopolis, Brazil. *Journal of Health Psychology*, *21*, 336-345. doi:10.1177/1359105316628752

Sollars, M. (2016). Risk-based security: Staff can play the defining role in securing assets. *Network Security*, (9), 9-12. doi:10.1016/s1353-4858(16)30087-3

Sosik, J. J., Chun, J., Blair, A. L., & Fitzgerald, N. A. (2014). Possible selves in the lives of transformational faith community leaders. *Psychology of Religion and Spirituality*, *5*, 283-293. doi:10.1037/a0032646

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems*, *30*(1), 71-92. doi:10.2308/isys-51257

Stewart, H., & Gapp, R. (2014). Achieving effective sustainable management: A small medium enterprise case study. *Corporate Social Responsibility and Environmental Management*, *21*, 52-64. doi:10.1002/csr.1305

Sturmberg, J. P., Martin, C. M., & Katerndahl, D. A. (2014). Systems and complexity thinking in the general practice literature: An integrative, historical narrative review. *Annals of Family Medicine*, *12*, 66-74. doi:10.1370/afm.1593

Suicimezov, N., & Georgescu, M. R. (2014). IT governance in cloud. *Procedia Economics and Finance*, *15*, 830-835. doi:10.1016/S2212-567(14)00531-0

Synnot, A., Hill, S., Summers, M., & Taylor, M. (2014). Comparing face-to-face and online qualitative research with people with multiple sclerosis. *Qualitative Health Research*, *24*, 431-438. doi:10.1177/1049732314523840

Syrek, C. J., Apostel, E., & Antoni, C. H. (2013). Stress in highly demanding IT jobs: Transformational leadership moderates the impact of time pressure on exhaustion and work-life balance. *Journal of Occupational Health Psychology*, *18*, 252-261. doi:10.1037/a0033085

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, S. J. (2015). *Exploring strategies for retaining information technology professionals: A case study* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3681815)

Tiwana, A., Konsynski, B., & Venkatraman, N. (2013). Special issue: Information technology and organizational governance: The IT governance cube. *Journal of Management Information Systems*, *30*(3), 7-12. doi:10.2753/MIS0742-1222300301

Tondel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42-57. doi:10.1016/j.cose.2014.05.003

Toscano, L., & Toscano, S. (2016). A new result concerning the solvability of a class of general systems of variational equations with nonmonotone operators: Applications to Dirichlet and Neumann nonlinear problems. *International Journal of Differential Equations*, 1-18. doi:10.1155/2016/1683759

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

Tyssen, A. K., Wald, A., & Spieth, P. (2014). The challenge of transactional and transformational leadership in projects. *International Journal of Project Management*, *32*, 365-375. doi:10.1016/j.ijproman.2013.05.010

Uluyol, O., & Akci, Y. (2014). A research on perceptions of manufacturing firms about marketing and financial problems with the method qualitative analysis: Adiyaman case. *International Journal of Business and Social Science*, *5*(4), 224-233. Retrieved from http://ijbssnet.com/

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, *15*, 398-405. doi:10.1111/nhs.12048

Valli, C., Martinus, I., & Johnstone, M. (2014). Small to medium enterprise cyber security awareness: An initial survey of Western Australian business. In *Proceedings of the International Conference on Security and Management (SAM)*

(p. 1). The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). Retrieved from http://worldcomp-proceedings.com/proc/p2014/SAM9779.pdf

Vanclay, F., Baines, J. T., & Taylor, C. N. (2013). Principles for ethical research involving humans: Ethical professional practice in impact assessment Part I. *Impact Assessment and Project Appraisal*, *31*, 243-253. doi:10.1080/14615517.2013.850307

Van Knippenberg, D., & Sitkin, S. B. (2013). A critical assessment of charismatic-transformational leadership research: Back to the drawing board? *The Academy of Management Annals*, *7*, 1-60. doi:10.1080/19416520.2013.759433

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*, 21-54. Retrieved from http://www.misq.org/

Vidalis, S., & Angelopoulou, O. (2013). Deception and maneuver warfare utilizing cloud resources. *Information Security Journal: A Global Perspective*, *22*, 151-158. doi:10.1080/19393555.2013.780273

Vohra, V. (2014). Using the multiple case study design to decipher contextual leadership behaviors in Indian organizations. *Electronic Journal of Business Research Methods*, *12*, 54-56. Retrieved from http://www.ejbrm.com

Von Bertalanffy, L. (1969). *General system theory: Foundations, development, applications.* New York, NY: George Braziller.

Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of*

Management Journal, *15*, 407-426. doi:10.2307/255139

VonSolms, R., & VanNiekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. doi:10.1016/j.cose.2013.04.004

Walden University. (2010). *Walden Institutional Review Board for Ethical Standards in Research*. Minneapolis, MN. Retrieved from http://researchcenter.waldenu.edu/Office-of-Research-Integrity-and-Compliance.htm

Wang, C. C., & Geale, S. K. (2015). The power of story: Narrative inquiry as a methodology in nursing research. *International Journal of Nursing Sciences*, *2*, 195-198. doi:10.1016/j.ijnss.2015.04.014

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*, 91-112. Retrieved from http://www.misq.org

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/

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44*, 1-15. doi:10.1016/j.cose.2014.04.005

Webb, J., Maynard, S., Ahmad, A., & Shanks, G. (2014). Information security risk management: An intelligence-driven approach. *Australasian Journal of*

Information Systems, *18*, 391-404. doi:10.3127/ajis.v18i3.1096

Weber, R. M. (2015). Oh no! All my files are gone!. *Journal of Financial Service Professionals*, *69*(6), 48-51. Retrieved from https://www.financialpro.org/

Wilding, N. (2016). Cyber resilience: How important is your reputation? How effective are your people? *Business Information Review*, *33*, 94-99. doi:10.1177/0266382116650299

Wong, W.-P., Veneziano, V., & Mahmud, I. (2016). Usability of enterprise resource planning software systems: An evaluative analysis of the use of SAP in the textile industry in Bangladesh. *Information Development*, *32*, 1027-1041. doi:10.1177/0266666915585364

Woods, M., Paulus, T., Atkins, D. P., & Macklin, R. (2016). Advancing qualitative research using qualitative data analysis software (QDAS)? Reviewing potential versus practice in published studies using ATLAS.ti and NVivo, 1994-2013. *Social Science Computer Review*, *34*, 597-617. doi:10.1177/0894439315596311

Wu, S. P.-J., Straub, D. W., & Liang, T.-P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and it managers. *MIS Quarterly*, *39*, 497-518. Retrieved from http://www.misq.org

Yammarino, F. (2013). Leadership past, present, and future. *Journal of Leadership & Organizational Studies*, *20*, 149-155. doi:10.1177/1548051812471559

Yang, C., & Ye, J. (2015). Secure and efficient fine-grained data access control scheme in cloud computing. *Journal of High Speed Networks*, *21*, 259-271.

doi:10.3233/jhs-150524

Yaokumah, W., & Brown, S. (2014). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. *Journal of Law and Governance*, *9*(2), 50-65. doi:10.15209/jbsge.v9i2.718

Yawson, R. M. (2013). Systems theory and thinking as a foundational theory in human resource development - A myth or reality? *Human Resource Development Review*, *12*, 53-85. doi:10.1177/1534484312461634

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

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*, 321-332. doi:10.1177/1356389013497081

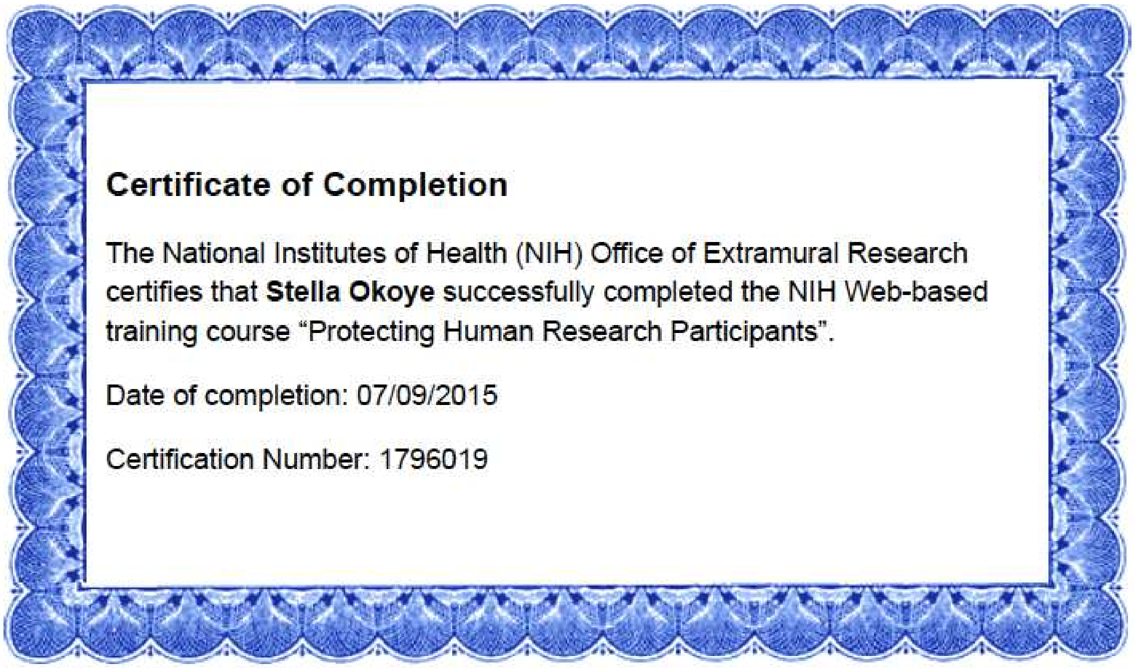
Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage.

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

Zilber, T. B. (2014). Beyond a single organization: Challenges and opportunities in doing field level ethnography. *Journal of Organizational Ethnography*, *3*, 96-113. doi:10.1108/JOE-11-2012-0043

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyber insurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems*, *30*, 123-152. doi:10.2753/mis0742-1222300104

Appendix A: NIH Certificate



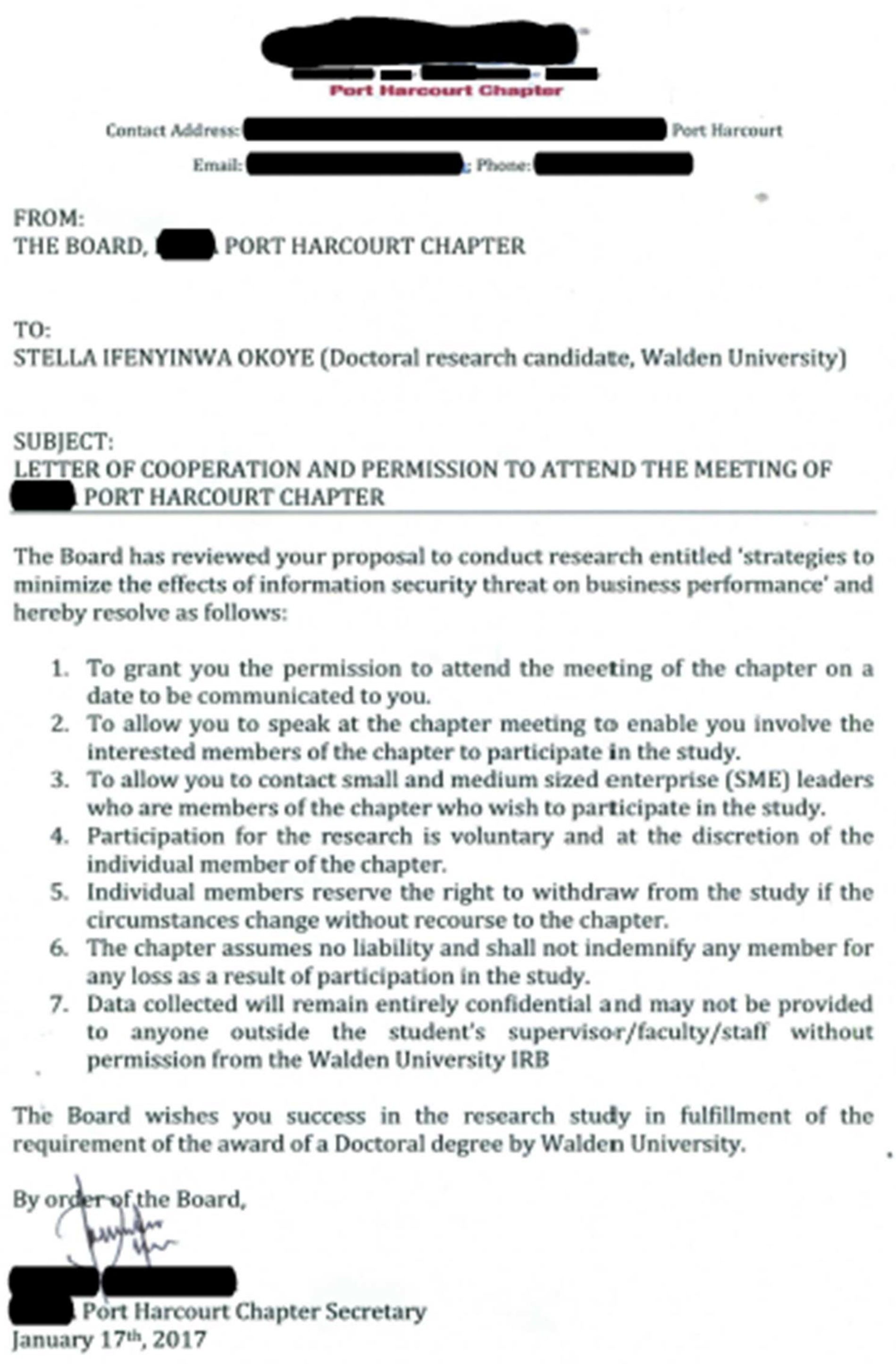
Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Stella Okoye** successfully completed the NIH Web-based training course “Protecting Human Research Participants”.

Date of completion: 07/09/2015

Certification Number: 1796019

Appendix B: Letter of Corporation



[redacted]

[redacted]

Port Harcourt Chapter

Contact Address: [redacted] Port Harcourt

Email: [redacted]; Phone: [redacted]

FROM:
THE BOARD, [redacted] PORT HARCOURT CHAPTER

TO:
STELLA IFENYINWA OKOYE (Doctoral research candidate, Walden University)

SUBJECT:
LETTER OF COOPERATION AND PERMISSION TO ATTEND THE MEETING OF [redacted] PORT HARCOURT CHAPTER

The Board has reviewed your proposal to conduct research entitled 'strategies to minimize the effects of information security threat on business performance' and hereby resolve as follows:

1. To grant you the permission to attend the meeting of the chapter on a date to be communicated to you.
2. To allow you to speak at the chapter meeting to enable you involve the interested members of the chapter to participate in the study.
3. To allow you to contact small and medium sized enterprise (SME) leaders who are members of the chapter who wish to participate in the study.
4. Participation for the research is voluntary and at the discretion of the individual member of the chapter.
5. Individual members reserve the right to withdraw from the study if the circumstances change without recourse to the chapter.
6. The chapter assumes no liability and shall not indemnify any member for any loss as a result of participation in the study.
7. Data collected will remain entirely confidential and may not be provided to anyone outside the student's supervisor/faculty/staff without permission from the Walden University IRB

The Board wishes you success in the research study in fulfillment of the requirement of the award of a Doctoral degree by Walden University.

By order of the Board,

[redacted]

[redacted] Port Harcourt Chapter Secretary
January 17th, 2017

Appendix C: Letter of Introduction

Dear SME Leader,

My name is Stella Ifeyinwa Okoye, and I am a doctoral candidate at Walden University. I am working on completing my Doctor of Business Administration (DBA) degree with specialization in Information System Management. I am conducting research study titled: *Strategies to Minimize the Effects of Information Security Threats on Business Performance*. The purpose of the study is to determine what strategies successful SME leaders use to minimize the effects of information security threats. The potential effect on business practice is helping SME leaders to gain significant knowledge, which is conducive for maximizing sustainable business growth.

I am inviting you as SME leader to participate in this study, which will take only about 45 minutes of your time. I believe your participation and knowledge on information security threats 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 strategies SME leaders use to minimize the effects of information security threats.

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 review, sign and email or scan the Consent Form to me. Also let me know of a convenient date/time and contact information for the face-to-face semistructured interview. Please contact me on [redacted] or via e-mail [redacted] with any questions or concerns.

Sincerely,
Stella I. Okoye

Appendix D: 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. Observe the participant and take notes of non-verbal queues

H. On the participant's request, paraphrase the interview questions as needed.

I. Ask follow-up probing questions

J. End interview and discuss/schedule follow-up member checking interview with participant.

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

L. End protocol.

Demographic Question

1. What is current job position (title)? ______________________
2. How many years have you served in the leadership role? _________ years
3. How many years' experience does you have in information security management? _____ years

4. What is your highest level of education? Secondary-ordinal diploma; □ Degree-higher diploma; Post graduate
5. What is your gender? Male; Female; Other
6. What is your age group? above 18-30 years; 31-40 years; 41-50 years; 51-60 years; above 60 years

Interview Questions

1. What strategies are you using to reduce the effects of information security threats on business performance?
2. How did you identify and select the strategies for reducing the effects of information security threats to your organization?
3. How did you implement the strategies for minimizing the effects of information security threats in your information security system?
4. What challenges did you encounter in implementing the strategies to reduce the consequences of information security threats?
5. How did you manage the challenges faced in implementing the strategies to minimize the effects of information security threats?
6. What systems do you have in your company to support the implementation of strategies to reduce the consequences of information security threats?
7. What strategies are most effective in reducing the effects of information security threats on business performance?
8. What strategies are less efficient in reducing the effects of information security threats on business performance?

9. What factors influence the implementation of strategies to minimize the effects of information security threats on business performance?
10. What additional information, documentation, or processes would you like to share with me that would help in this research study?