2020

Tailored Information Security Strategies for Financial Services Companies in Nigeria

Kayode Alawonde
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Kayode Olasunkanmi Alawonde

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. Donald Carpenter, Committee Chairperson, Information Technology Faculty
Dr. Steven Case, Committee Member, Information Technology Faculty
Dr. Jodine Burchell, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Tailored Information Security Strategies for Financial Services Companies in Nigeria

by

Kayode Olasunkanmi Alawonde

MSc Higher Education, 2014

MSc Information Systems Management, 2008

MSc Personnel Psychology, 2005

BSc Computer Engineering, 1994

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2020

Abstract

Some financial institutions in Nigeria have not deployed strategies that mitigate cyber exploitation risks in the financial services industry. Financial institution leaders are concerned because cyber exploitation contributed to the reduction in the adult banking population to a low 38%. Grounded in the integrated systems theory of information security management, the purpose of this multiple case study was to explore strategies some financial institution leaders in Nigeria use to prevent cyber exploitations. The participants included 6 chief information security officers of 6 financial institutions. Data were collected from semistructured interviews and company and public documents. A thematic analysis identified themes to include the need to align information security plans of actions with corporate strategies, ensuring there are information security policies, processes, and procedures to guide disciplined efforts for information risk mitigation. A comprehensive risk management process can be used to determine information security strategies to ensure all risk areas are covered. This study may contribute to positive social change when a much more significant percentage of the Nigerian public use financial services because institutions adopt strategies to protect confidentiality, integrity, and availability of information.

Tailored Information Security Strategies for Financial Services Companies in Nigeria

by

Kayode Olasunkanmi Alawonde

M.Sc Higher Education, 2014

M.Sc Information Systems Management, 2008

M.Sc Personnel Psychology, 2005

B.Sc Computer Engineering, 1994

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

April 2020

Dedication

I dedicate this work to my wife Adeola and children Olasubomi and Oladiwura for their support, encouragement, and understanding while I was going through this process. I also dedicate the work to my parents Mr. Mohammed Ayoola and Mrs. Mobonike Adigun-Alawonde, without whom I will not have assayed to pursue a doctoral degree.

Acknowledgments

I appreciate Dr. Mike McGivern, Dr. Donald Carpenter, Dr. Steven Case, Dr. Jodine Burchell, for their support and guidance throughout the process of this work. The dissertation would not have been possible without them. I would also like to thank the participants who offered their time and knowledge in support of the study.

My appreciation also goes to Mr. Taiwo Otiti, Mrs. Ronke Bammeke, Dr. Ebun Ekunwe for being such great mentors to me over time and on this work. I also appreciate my colleagues Stephen Olateru, Cletus Okolie, Grace Eyong, Liza Gwomson, and Zainab Mungonu for helping me on this journey.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

The finance sector uses information technology (IT) solutions extensively. The technology in use by financial institutions comes in different forms, with individual characteristics and consequently varying risk elements. Financial breaches have far-reaching implications whenever they occur. Breaches range from loss of business, reputational damage, financial losses due to an actual loss in the course of the breach or fines, and payment of compensation whenever a breach occurs. The purpose of this study was to explore strategies some financial institutions use to prevent cyber exploitations that jeopardize the confidentiality, availability, and integrity of information assets. These strategies may be used by similar financial services institutions that lack strategies to avoid losses and other consequences of cybercrime.

Background of the Problem

The Nigerian finance sector has evolved significantly in the adoption of technology in service delivery. This evolution is in response to the demands of customers who generally have become sophisticated, wanting services always, and in specific ways, which technology facilitates (Tarhini, Mgbemena, Trab, & Masa'deh, 2015). Internet banking, automatic teller machines, mobile banking, fintech services, and other technology-driven service outlets are now commonplace. However, the use of those technologies in finance operations comes with attendant risks (Hinchliffe, 2017). The institutions can lose money, and they can lose customers and market share if the outcome of a technology risk exploitation is not well managed (Chakkaravarthy, Sangeetha, Venkata Rathnam, Srinithi, & Vaidehi, 2018). It is also common to see exploited

institutions fined by regulatory authorities, and in some cases, entire businesses can close. It is, therefore, important for financial institutions to take the issue of preventing cyber exploitation seriously.

Several finance sector companies in Nigeria have begun to take steps to mitigate the risks that come out of the use of technology for offering services; nevertheless, some do not have corporate strategies that indicate they view the issue of preventing cyber exploitation as serious. Therefore, I investigated strategies that have helped players in the sector prevent cyber exploitation, which other institutions can adopt to prevent cybercrime in the adoption of technological tools to provide financial services.

Problem Statement

Financial institutions continue to be the target of cybercriminals, leading to a loss of confidentiality, availability, and integrity of information (Chakkaravarthy et al., 2018). Cybercrime incidences, which include those affecting financial institutions in Nigeria, has been on the increase since 2014 (Hinchliffe, 2017). Nigeria ranked third in the list of the top 10 sources of cybercrime in the world (Ibrahim, 2016). The general IT problem is that financial institutions suffer data breaches due to cyber exploitation because of increased adoption of technology for delivering services. The specific IT problem is that some chief information security officers (CISO) lack strategies to prevent cyber exploitation that jeopardizes confidentiality, availability, and integrity of information in financial institutions in Nigeria.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies that CISOs deploy to prevent cyber exploitation that jeopardizes the confidentiality, availability, and integrity of information within financial institutions in Lagos, Lagos State and Abuja, Federal Capital Territory, Nigeria. The population for this study was CISOs of six Nigerian companies within the financial services sector who have implemented strategies that mitigate cyber risks. The implication for social change includes reducing the unbanked population in Nigeria through the possible increase in confidence in the use of available technology to deliver and access financial services.

Nature of the Study

The nature of the study was explorative to identify strategies that CISOs have used to achieve the security of information in financial institutions. I looked at financial institutions that have either the ISO 27001 or Payments Cards Industry (PCI-DSS) certification. Qualitative studies are explorative and useful when there is a need to track unique events or issues when investigating complex phenomena (Runfola, Perna, Baraldi, & Gregori, 2017). Thus, I used the qualitative method to examine strategies to prevent cyber exploitations.

In contrast, the quantitative method typically involves testing theories and using statistical data to confirm a hypothesis (Guo, 2014). The quantitative method was not chosen because a theory was not tested, and statistical data were not used in the study. Mixed methods were also not suitable because the mixed method requires combining

quantitative and qualitative methods (McKim, 2017). The method chosen for the study was only the qualitative method.

The qualitative study involved using multiple cases at different site locations. Case studies are typically useful when there is a need to focus on the selected representation of objects, situations, or phenomena for exploration and research to gain specific insights or knowledge (Elman, Gerring, & Mahoney, 2016). The focus of this study was on exploring strategies in use by CISOs in six financial sector institutions in Nigeria. The case study design was most appropriate for the study in comparison to other designs. I did not choose the ethnographical design. Ethnographical designs focus on investigating social groups, culture, or customs by being embedded in a group (Fayard & Van Maanen, 2015). Additionally, the phenomenological design is useful for exploring the lived experience of a given phenomenon (Willis, Sullivan-Bolyai, Knafl, & Cohen, 2016), but this was not the focus of the current study. Finally, studies that connect events from people, based on some form of experiences and captures stories around a phenomenon, use the narrative design (McAlpine, 2016); however, the study did not connect events or narrate experiences.

Research Question

What strategies do CISOs adopt to prevent cyber exploitations that jeopardize information confidentiality, availability, and integrity of Nigeria's financial institutions?

Interview Questions

1. What are the risks that are of concern as a player in the financial services sector in Nigeria in the use of IT tools for operations? Please briefly describe the existent

information security management process in the company. Is there an information security policy in place? Is there an internal control process that monitors for compliance? When policy violations occur, how are arising contingencies addressed?

2. In what ways have financial organizations experienced cyber exploitations? What was the nature of the most common exploitations experienced? Which of the exploitations are prevalent, and why?

3. Has there been a time the company experienced information security exploitations? Which of integrity, confidentiality, or availability of information did it affect? If the previous is true, was there an incident management system in place? What were the lessons learned? What was done differently after the incident?

4. How do you decide what to do in your role to support the IT strategy and, ultimately, the corporate strategy of the organization where you work? Are there policies, regulations that affect what you do in your role? Please state specific strategies that you must deploy (if any) to ensure confidentiality, availability, and integrity of information because of your industry.

5. What have you done to ensure that the confidentiality of information is preserved? What have you done to ensure information is not illegally modified? What have you done to be sure legal users are not denied access to information when they need them? Which specific risks did you have in mind while carrying out the activities above?

6. Are there steps you take in securing your operations while hiring staff at any level and for different roles? What skill levels do you look at for hiring purposes? How necessary is, background checks to your business?
7. How do you ensure you discover weaknesses in your IT systems before hackers exploit the weaknesses? Do you do conduct vulnerability assessments/penetration tests? If you do, has there been a time you had to deploy new strategies for information security after the assessments? What were they
8. In what ways have regulatory certifications helped you to prevent cyber exploitations that could have violated confidentiality, availability, and integrity of information. Which of the regulatory certifications do you possess as an organization?
9. What is the existing management process that supports your efforts to prevent cyber exploitation of information assets? Please describe your board's role in your information security management process.
10. Please explain the measures you have in place to prevent cyber exploitation of your information assets because of your staff leaving, which in some cases may be to join your competitors. To what extent are those processes documented?

Conceptual Framework

Hong, Chi, Chao, and Tang (2003) proposed a theory that I used as a conceptual basis to explore strategies that CISOs could use to provide tailored information security strategies to prevent cyber exploitation of financial institutions in Nigeria. The theory is the integrated systems theory (IST) for information security management, which includes

five individual theories: contingency theory, risk management theory, security theory, control, and audit theory, and management system theory (Hong et al., 2003). IST indicates that each of these theories is individually inadequate when used without the other theories to address the issues that pertain to achieving confidentiality, availability, and integrity of information. The IST is predicated on managing eventualities and combines all the theories in such a way as to meet the information security objective of a company by developing an information security strategy suited for the organization. The arising security architecture provides for mitigation of information security issues contingent on the fast-paced environment within which businesses operate.

The IST for information security management affirms that adequate information security needs to be a function of information security policy, risk management, information auditing, contingency management, and internal control (Ismail, Sitnikova, & Slay, 2014). The internal control is dependent on several factors: access control, system development and maintenance control, personnel security control, physical security control, systems and network security control, and business continuity management. The theory also affirms that the management of information security risks to achieve continuity of business requires a consideration of the internal and external environment of the organization while using the IST (Baskerville, Stage, & DeGross, 2000)

The IST sets up a possible conceptual framework for comprehensive investigations of issues that affect the security of information, confidentiality, availability, and integrity of information (Ismail et al., 2014). Thus, the theory provided a

basis to explore information security strategies for financial sector companies in Nigeria. The theory assumes that individual theories cannot provide a holistic approach to treat issues of information security management, but the combination of various theories that make up the IST would. IST is appropriate given the need to explore multiple strategies that CISOs use to keep finance companies safe from cyber exploitations in Nigeria. The theory helped to provide explanations that indicate the appropriateness of a plan compared with another in practice.

Operational Definitions

Availability: Availability refers to the quality of information assets that ensures that they are available whenever users require them for use (Tchernykh, Schwiegelsohn, Talbi, & Babenko, 2016).

Confidentiality: Confidentiality is the attribute that describes the state where access to information is only available to authorized persons, individuals, or systems (Saunders, 2016).

Cybercrime: Cybercrime covers crimes that use computers, computer networks, and IT tools to advance (Prayudi, Ashari, & Priyambodo, 2015)

Financial services/business: Financial services/businesses are financial services provided by the finance industry, which encompasses a broad range of companies that manage money, including banks, insurance, credit card companies, consumer finance companies, stock brokerages, investment fund companies, and the like (Homeland Security, 2017).

Information security risks: Information security risks are exposure to the danger of a breach of confidentiality, integrity, and availability of information (Joshi & Singh, 2017).

Integrity: Integrity is the ability to trust an information or information system (Vigil, Buchmann, Cabarcas, Weinert, & Wiesmaier, 2015).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are reasonable generalizations taken to be true without empirical proofs (Grant, 2014). Assumptions made in research enable an understanding of the context of the study and facilitate a comprehensive understanding of outcomes (Wolgemuth, Hicks, & Agosto, 2017). I made three fundamental assumptions. The first assumption is that participants to be used for the study, based on defined criteria, were knowledgeable enough on the subject matter to respond to interviews that helped to understand the phenomenon under study. The second assumption is that the participants would speak truthfully to all aspects of interview questions to give proper perspective to the subject under investigation. The third assumption is that the research would lead to executable, vendor-agnostic strategies, which could provide a guide for implementation irrespective of the vendor leaning of the organization.

Limitations

Limitations are characteristics that impact on the generalizability of the outcome of research as a result of decisions made on the research methodology or design (Busse, Kach, & Wagner, 2017). Limitations are potential weaknesses of the study. Damages can

arise due to unfair generalization when limitations in research are not considered relative to outcomes (Cowls & Schroeder, 2015). A limitation of this qualitative multiple case study is that the findings may not be generalized for all financial institutions in Nigeria because the location of the study sites is in the southwestern zone and federal capital territory. Another potential limitation of this research is that the population size for data collection per organization is small. CISOs are typically one per organization, and the study had to depend on the extent of their willingness to share information for the study even after sharing nondisclosure agreements (NDA). The possible limited desire of CISOs is a limitation because financial institutions are most often than not reluctant to share information around their cybersecurity strategies (and incidences), as many still believe an obscurity is a form of security.

Delimitations

Delimitations capture controllable elements of an investigation or research. Delimitations are choices made to define the scope or boundaries of the research (Thomas, Silverman, & Nelson, 2015). One delimitation for this study is that locations involved only a few cities in Nigeria. The places for the research will be Lagos, Lagos State, and Abuja, Federal Capital Territory, Nigeria. Another delimitation of the study is that it is limited to companies within the financial institution sector that have either the ISO 27001 or PCI-DSS certification.

Significance of the Study

Contribution to Information Technology Practice

The significance of the study is that it may help to identify the direction of efforts within IT of cybersecurity to prevent cyber exploitations. It may also provide CISOs with strategies they can adopt to avoid cyber exploitations that may undermine confidentiality, availability, and integrity of information within the financial sector in Nigeria. Results may also increase the body of knowledge currently available on the subject and extend the applicability and discourse of the IST theory of information security management.

Implications for Social Change

The study may help contribute to social change through improved financial inclusion by encouraging increased use of digital finance. Financial inclusion has the potential to provide financial support opportunities to the previously excluded citizens who are unbanked due to information security concerns of saving money in financial institutions in Nigeria. Improved confidence in the finance sector may increase the banked population from the current level. In Nigeria, 38.3% of the adult population is currently banked (Central Bank of Nigeria, 2018). The assurance of possible safe use of finance through technology can provide opportunities to access funding for businesses, which may lead to economic development and other associated benefits of the improved banked population (Ngwu, 2014). Digital finance stimulates growth, which in turn leads to improved gross domestic product (GDP) in developing economies (Ozili, 2018).

A Review of the Professional and Academic Literature

Overview

A literature review is a systematic search of accredited literature on a topic that provides foundations for a study (Hart, 2002). A review of literature helps to identify prior scholarship on the subject, establish gaps in a study, and give credence to people who have previously researched the topic. The literature review also positions every previous work in the context of the current study, especially the contribution or relevance to the present study (McEvoy & Machi, 2012). Additionally, literature reviews help to identify quickly aspects of the study that have been studied to prevent duplication of efforts and directs concentration on areas that require investigations for extending knowledge on the topic (Durach, Kembro, & Wieland, 2017). Literature reviews also provide a valid basis to answer the research question of a study.

To find sources for this literature review, topics used for searching related to technological development, technological adoption in finance in Nigeria, risks, and management of risks associated with IT adoption, theories of information security management, and strategic views and directions for information security risk management. The databases used for the search include Academic Search Complete, Sage Journals, ScienceDirect, IEEE Xplore Digital Library, and Google Scholar. In this literature review, over 86% of the sources have been peer-reviewed, and about 90% of the sources have publication dates within the last 5 years.

The next section discusses the application to the applied IT problem. It contains a synthesis of the literature that relates to the information security management and

financial services industry in Nigeria. The section also includes the changing IT landscape within Nigerian finance that necessitates a strategy for information security management. Then I present a review to support IST, the conceptual framework chosen for the study. The following section presents different other theories, which also relates to the topic of study and identifies reasons why the IST is more suited for the study. Then I explain some relevant information security management concepts and practices, especially as it relates to the conceptual model. The literature review then presents research similar to this one and explains the differences.

Application to the Applied Information Technology Problem

The purpose of this qualitative multiple case study was to explore strategies that CISOs deploy to prevent cyber exploitation that jeopardizes the confidentiality, availability, and integrity of information within financial institutions in Lagos, Lagos State and Abuja, Federal Capital Territory, Nigeria. The financial services sector includes retail, point of sale services, SWIFT services, and electronic stockbroking services, all of which are the result of technological advances (Macaulay, 2017). The Internet of things and other evolving technical concepts are shifting the technological paradigm (Weber & Studer, 2016). However, technological advances do come with risks (Sullivan & Kamensky, 2017) from the nature of data generated, manipulated, and processed to deliver desired services (Arabo, 2015). The risks also come through the access points, the processing points, trading partners, service providers, and the people and processes involved in the data use process to support new and evolving business models

(Leuprecht, Skillicorn, & Tait, 2016). Risks from technological adoption arise from the targeting of adopted technology by adversaries as well (Kenney, 2015).

Companies in the financial sector are vulnerable to information security risks such as exploits of operating systems, database systems, applications, and hardware deployed to deliver financial services (Scarfò, 2018). The exploits may lead to loss of sensitive trade secrets, corruption of data through viruses, or exposure of confidential information (Qiu, Gai, Thuraisingham, Tao, & Zhao, 2018). The exploits may eventually lead to financial losses to the company, such as loss of shareholder value (Modi Wiles, & Mishra, 2015; More, Jadhav, & Nalawade, 2015). In some instances, the IT tools deployed directly prevent the delivery of predetermined value to customers and institutions in the financial sector through denial of service attacks (Sicari, Rizzardi, Miorandi, & Coen-Porisini, 2018). The information security risks exist because the organization depends on the IT tools to serve its customers (Qiu et al., 2018).

One of the reasons that organizations are vulnerable to risks is because the financial sector is a heavy user of data. The generation of data occurs at different points within the financial industry (Bholat, 2015). The data vary in complexity, variety, and generated from disparate systems (Günther, Rezazade Mehrizi, Huysman, & Feldberg, 2017). The data range from customer data, transactional data, policies, and other data that support the operations of a financial institution. Systems in financial institutions aggregate a significant amount of data (Neal & Ilsever, 2016). Data aggregation occurs, for example, in enterprise resource planning systems and business intelligence systems (Gambetta, García-Benau, & Zorio-Grima, 2016; Neal & Ilsever, 2016). The aggregated

data conveys information about customers and their financial habits (Srivastava & Gopalkrishnan, 2015). Cybercriminals who hack companies' systems and networks can obtain aggregated or consolidated data, which they can use to damage a company's reputation or cause other harm (Ali, Khan, & Vasilakos, 2015). The variety of data, multiplicity of endpoints, and the gravity of a compromise are the driving issues for the need to have a strategy for securing systems in financial institutions (Spanos & Angelis, 2016). A significant number of financial institutions have, therefore, incorporated protective mechanisms for their operations, leading to investments in computer security technologies.

Although some companies incorporate computer security, they are not generally strategic or thorough in their deployments (Burdon & Coles-Kemp, 2019). Computer security investments are still limited to firewall-specific expenditures (Gambetta et al., 2016). For example, several institutions have deployed majorly technical countermeasures to achieve information security, even though they know they need other measures as well (Soomro, Shah, & Ahmed, 2016). Further, security research has focused on the technical aspects of information security (Siponen & Oinas-Kukkonen, 2007). Current efforts in research and literature maintain that acceptable information security strategy must be holistic, covering critical elements of people, process, and technology or technical components of IT (Sohrabi Safa, Von Solms, & Furnell, 2016).

A significant number of countries have also increased their regulation of financial institutions in the area of information security, with penalties handed down to violators of compliance requirements of information security for the sector (Rajan, Ravikumar, &

Shaer, 2017). Deposit money banks, switches, and payment card processors in Nigeria were by regulation required to be Payment Card Industry/Data Security Standards compliant (PCI-DSS) by November 30, 2014 (Omotubora & Basu, 2018). The requirement for PCI-DSS certification in deposit money banks in Nigeria led to the evolution of strategies and allocation of budget by the management of institutions to achieve the same within Nigeria's financial industry.

The global trend of increased regulation is also increasing fines due to violations (Pearson, 2014). The United States continues to enforce laws and guidelines that make it costlier for establishments not to pay attention to information security (Massacci, Ruprai, Collinson, & Williams, 2016). The general data protection regulation (GDPR) of the European Union equally requires all businesses and parties to do business within the region to fulfill all requirements and comply (Tankard, 2016). Compliance with the standard ensures that organizations pay more attention to the matter of data security.

The IT services delivery model has also changed from the conventional "I own my infrastructure" model to the adoption of managed IT services, cloud services external to the control of the organization (Phaphoom, Wang, Samuel, Helmer, & Abrahamsson, 2015). Adoption is accompanied by its risks and vulnerabilities, for example, unapproved access to client and business information, loss of access, or denial of service (Sen & Borle, 2015). Globalization and the need for interconnection of operational systems is another issue that exposes organizations to information security risks. Enterprises that want to prevent cyber exploitations understand that their security is as adequate as the strength of their connecting partners (Skopik, Settanni, & Fiedler, 2016). Security

strategies to deal with IT security risks arising from new IT tools must take all of that into account.

There must exist a comprehensive strategy for the protection of data and other technology services to ensure the appropriate level of security within the financial sector. There is an increasing trend in customers wanting services on their terms (Marjanovic & Murthy, 2016), creating a supply and demand that leads to the adoption of technology for service adoption (Kauffman, Liu, & Ma, 2015). Therefore, stakeholders expect to see more adoption of technology tools within the financial sector in Nigeria. For instance, information communication technology adoption has been connected to more consummation of technology-based bank services (Efobi, Beecroft, & Osabuohien, 2014). Thus, organizations need security strategies that are complete, in-depth, and cover all aspects of a typical financial enterprise. It must also be the best fit, tailored, and deemed appropriate for the sector (Mansfield-Devine, 2016a).

Conceptual Framework: Integrated Systems Theory for Information Security Management

The theory that underpins this study is the IST for information security management that Hong et al. (2003) proposed. The theory was a conceptual basis for exploring strategies that CISOs could use to provide tailored information security strategies to prevent cyber exploitation of financial institutions in Nigeria. The theory includes five individual theories: contingency theory, risk management theory, information security policy theory, control, and audit theory, and management system theory (Hong et al., 2003). Though there is no consistent security policy theory, one of

the fundamental theories of the IST (Hong et al., 2003), there is a general consensus that one of the key and fundamental means of achieving information security is by the establishment, operationalization, and maintenance of information security policy (Flowerday & Tuyikeze, 2016). The information policy theory of IST advocates the identification of information security requirements in an organization, drafting, and implementing policies to meet those security requirements. The policy states there must be an explicit and formal declaration of what is allowed and what is not allowed in terms of using information assets within the allowance of the information security objectives in an organization (Bélanger, Collignon, Enget, & Negangard, 2017). Information policies of an organization must also be current and relevant (Soomro et al., 2016). The information security policy must be regularly maintained and updated to be relevant for information security in the context of the organization to be protected. Information security policies address the human element of information security in organizations (Sohrabi Safa et al., 2016). The postulates of the theory will, therefore, help to achieve the security that pertains to the human element.

The risk management theory component of the IST suggests that through an analysis of the risks existing in an organization, information security threats and vulnerabilities can be identified, estimated, and assessed. The theory expects using the outcome of the risk assessment to determine information security risk control measures (Ismail et al., 2014). The objective of the risk management theory is to deploy controls that will help the organization reduce risks to an acceptable level (Hong et al., 2003). Risk management theory achieves its objectives through a comprehensive risk

assessment. It is the interplay of risk assessment and deployment of controls that help to get the information security risks in an organization to an acceptable level as required by the risk management theory. Acceptable risk level varies from organization to organization. Organizational risk appetite, the amount and type of risk that an organization is willing to take to achieve its objectives, determine acceptable risk levels. Risk appetite has been considered an essential factor in making strategic decisions in organizations (Zhang, Paraskevas, & Altinay, 2019). The inclusive risk management theory of the IST, therefore, indicates that what the acceptable risk is will be determined in the context of each organization applying the theory to its operations.

The management system theory of the IST requires organizations to have a formal and documented information security management system. The management system is to include the definition of the policy, establishment of the scope of the information security management system, management of risk, the definition of control objectives, and establishment of a statement of applicability (Hong et al., 2003). The management system theory, among other things, underscores the importance of having an integrated theory for information security management because it requires the definition of a security policy, risk assessment, risk management, and control deployment. Another constituent theory of IST, the security policy theory, defines policy, and the control and auditing theory of the IST supports the process of implementing relevant controls. Risk management precedes risk controls. The dependency on the fulfillment of the requirement of the management systems theory on other theories strengthens the need for an integrated system theory to address the issue of information security in organizations. The management system

theory must consider the business strategy and the scope of information security management system for the organization where it will be used (Andress & Leary, 2017).

The contingency theory of the IST indicates that information security management should be part of the contingency planning of organizations that cover prevention, detection, and mitigation of vulnerabilities and threats to information assets (Ismail et al., 2014). Contingency planning includes the whole set of activities that organizations deploy to ensure that business can continue when there is a disruption of service or a disaster (Carbaugh, Antonio, Lynch, & Nelsen, 2019). The activities around contingency planning in recent times come under information security responsibility (Mubarak, 2016). Information security violations can cause disruptions or disasters. Contingency theorists indicate that to proactively respond to issues that may affect the ability of organizations to continue their business, organizations need to take one or more information security management steps or actions proactively. These actions can be risk management actions, security policy actions, or system management actions. The contingency theory positions organizations to be able to respond to the situational need of organizations if there is an information security issue. The contingency theory considers possible information security problems that may arise and recommends provision for the appropriate response.

The control and auditing theory suggests that it is not enough to deploy controls that mitigate discovered threats and vulnerabilities, but controls require monitoring as well. The control and auditing theory expect that actions will be taken based on the outcome of risk analysis and assessments by deploying controls (Rahimian, Bajaj, &

Bradley, 2016). In addition to implementing controls, the control and auditing theory postulates that monitoring mechanisms must be in place (Casola et al., 2019). The control and auditing theory states that organizations should deploy auditing mechanisms to monitor the performance of controls implemented to address information security concerns in organizations. The control and auditing theory covers efforts made to detect, prevent, and correct information security breaches in organizations. One method that organizations have used for control and auditing theory is adopting information security standards that support the achievement of information security objectives of confidentiality, integrity, and availability of information assets. An example of such a standard is ISO 27001, which defined 133 controls across 11 security domains, with 39 control objectives. The compliance of an organization with the standard can be presumed to be an indication that the company has exercised due diligence to mitigate information security risks (Fazlida & Said, 2015; Tang & Liu, 2015). The intersection of the requirements of the IST and ISO 27001, especially in areas of internal controls covering physical security control, access control, systems, and network security control, personnel security control, system development, and maintenance control, and business continuity management confirms the relevance of the theory for understanding strategies to prevent cyber exploitations.

The objective of IST is to manage information security eventualities in line with the constituent contingency theory, which arises in the use of technology and combines all the theories in such a way as to meet the information security objectives of a company by developing an information security strategy suited for the organization. The arising

security architecture sets up a framework for the mitigation of information security issues that consider the fast-paced environment within which businesses operate in contemporary days.

Analysis of Supporting Theories

Socio-technical theory. Another relevant theory of information security management is the socio-technical systems (STS) theory. The theory was initially formed by Eric Trist and Fred Emery (Leung & Wang, 2015; Szabla, Pasmore, Barnes, & Gipson, 2017). The theory has previously been used in organizations to explain complex systems in organizations. It explains that organization systems are a combination of social and technical systems (Stanton & Harvey, 2016). It indicates that organizations need to pay attention to the social and technical elements of organizations to achieve effectiveness (Read, Salmon, & Lenné, 2016). The social aspect deals with humans, while the technical aspect relates to technology (Leung & Wang, 2015).

The application of the STS to information security management is that an organization needs to consider not just technical aspects when looking at security strategies for implementation in their efforts to achieve information security. The IST also supports the expectations of the STS theory when we consider the contingency theory, the risk management theory, and the security policy theory. The reason IST agrees with the tenets of STS is that in crafting security policies, doing risk assessments and providing for contingent security issues that may arise, the technology, environment, and people available in the related institution will be considered to craft appropriate security strategies (Carayon et al., 2015).

The IST is more suited for the study because it provides a detailed and definite approach to information security management in organizations. IST ensures complete coverage of all information risk areas. The STS merely indicates elements to be covered and does not state or indicate the depth or details of the areas to be covered. Li, Trutnevyte, and Strachan (2015) noted the difficulty of operationalizing the STS, which is a significant drawback for its application. The problem in operationalizing relates to the lack of a method for implementation, which the IST provides. The STS also does not cover the issue of monitoring for effectiveness, which IST does through the control and audit policy. STS may be used on an ad hoc basis or in combination with any other theory. The STS would, therefore, be inadequate to explore the study Tailored information security strategies for financial institutions in Nigeria.

Distributed cognition theory. Distributed cognition theory (DCT) is another theory used previously to explore topics in information security management. The theory was useful in studying human and computer interactions. Hutchins crafted DCT (Jones, 2010). DCT advocates the consideration of cognition as a distributed phenomenon. The theory postulates that to understand a system, all aspects of the cognitive systems are essential. The study of a cognitive system should not just include individuals, but also social networks and the related environment (McNeese & Hall, 2017). DCT is concerned about functional relationships and interactions of people, resources, and materials wherever they occur in systems.

The direct application of the theory to information security is that information security management ought not to be from a traditional and individualistic perspective.

Information security should be addressed instead of a distributed, organizational broad threat identification and awareness across people and technological areas (Banks, Stanton, Burnett, & Hermawati, 2018). The theory mandates a networked view of information (D'Angelo & Rampone, 2018). It also encourages consideration for how people interact with technology as they use information across distributed interconnected systems without compromising confidentiality, integrity, and availability of information assets.

The network view of information lines up with the intention of IST because the information is shared and distributed in a computing environment. It makes sense that in the process of deploying strategies for information security management, all these areas of the cognitive system, in this case, an organization, needs to be well considered for appropriate security. The principle of distributed cognition theory captures the fundamentals of STS in information security management with an extension of consideration for interactions and environments that link people with technology (Leung & Wang, 2015). The DCT contrasts with the IST because while the IST advocates for holistic coverage from a process point of view, the DCT, just as the STS, looks at information security from a subject or object's point of view (Li et al., 2015). The process view using multiple theories ensures all subjects or elements (people and technology) are covered, and it gives the approach (the how, and models to use) which makes the IST a better framework to use.

Activity theory. The activity theory (AT) is another relevant theory for the topic of discourse. The AT was crafted between the 1920s and 1930s by a group of

psychologists, notably Vygotsky and Leont'ev (Jørgensen, 2017). The AT is a descriptive theory that considers entire work activity shared by others (teams, organization) as against individual actors or users (subjects) to achieve a purpose (object) (Carvalho et al., 2015). It looks at the environment, history of the subjects, and considers the use of artifacts (tools, instruments, Karanasios, Allen, & Finnegan, 2015). The AT looks at mediating or involving activity used to achieve an object (objective).

A particular activity is a goal-oriented interaction of a subject with an object using tools. The unit of analysis by AT is an activity system with all the described elements (White, Burger, & Yearworth, 2016). The AT describes the interrelationship between activities, actions, motives, and objectives and environments in the context of operations. The AT provides a deeper understanding of systems and its components than what the DCT or the STS offers. The AT considers the historical and state of objects and context that it provides. The AT offers a more enhanced model to explore information security management.

The AT applied to information security management is employed to look at the context of the use of information systems as against individual user behavior to explain non-compliance to security requirements and breaches to information systems (Jingguo, Gupta, & Rao, 2015). The theory considers the need to provide protection looking at the whole lifecycle and acceptable norms and rules at activity level rather than at individual components (Leukfeldt & Yar, 2016). The AT does this by considering the various elements of the system and the interactions. Razak, Jalil, Krauss, and Ahmad (2018) supports the critical position that AT considers multiple aspects of systems and

relationships. The AT assumes the existence of rules to guide interactions of components involved in an activity. The regulations that AT requires are similar to elements of the security policy theory of the IST. The AT nonetheless does not indicate what would be the nature of the rules but assumes the rule will evolve from the existing culture imposed by the interactions in the system. The IST expects that standards will guide these rules through the requirement of the management system theory of the IST. The IST suggests a formal mechanism or standard way to capture the behavior of the actors in a system, to define policies or rules through the risk management theory component of the IST. The AT does not capture such formal means to regulate the application of rules. The IST, therefore, is more suited for the study than the AT.

Analysis of Contrasting Theories

Deterrence theory. The study could have used the deterrence theory (DT) as a comparative framework. The theory evolved from the work of Hobbes, Beccaria, and Bentham (Onwudiwe, Odo, & Onyeozili, 2007). Historically, DT has been used to deploy safety countermeasures that extend to securing infrastructure. DT has three elements, which are severity, certainty, and celerity (Bates, Darvell, & Watson, 2017). Classical DT states that penalties must be perceived to be severe, swift, and sure to prevent or to deter crime (Lee, 2017). DT assumes the rational behavior of subjects involved in an interaction. DT has been used to avert inappropriate behaviors in the use of IT, such as computer misuse and violations of security policies (Xu, Xu, & Li, 2016). Classical DT would only be useful to the extent of addressing people's aspect of information security management. The usefulness of the theory is in contrast to IST that assumes rational and

irrational behavior when one considers the impact of the theories that make up IST, especially the contingency theory (Hong et al., 2003). In the context of the study, the theory assumes rational behavior in the utilization of information assets to desist from violation of confidentiality, availability, and integrity of information assets.

The deterrence theory focuses on the subjects or objects involved in a process that uses technological tools and, therefore, limited in coverage. The IST, on the other hand, focuses on processes, subjects as well as the technology involved, which makes it more suited for consideration concerning the study. IST provides a comprehensive framework for addressing information security matters. IST also caters for contingency issues of security where opportunities for violations are not intentional and could jeopardize integrity, availability, and confidentiality (Ismail et al., 2014). IST recommends that protection should be through a combination of frameworks. IST advocates that security issues cannot be adequately addressed alone by any of its constituent or any other individual theory but rather by a combination for holistic and effective resolution.

DT prides itself on human psychology and compliance to prevent information security violations; IST provides a method to envisage worst-case scenarios by providing for inappropriate behaviors even when irrational behaviors occur (Onwudiwe et al., 2007). DT thrives on the availability of compliance standards or policies that subjects must comply with to achieve information security or face severe penalties. That characteristic of the DT is fulfilled by the information security policy theory, a constituent of the IST. There is a need for a thorough understanding of expected standards for deterrence theory to support information security (Lee, 2017). IST, on the

other hand, has a couple of theories that take care of nonunderstanding of regulations and standards, e.g., risk management theory, contingency theory. The implication is that IST would do better where the deterrence theory fails. The risk management theory embedded within the IST ensures that all risk areas, which include a lack of understanding of compliance expectations, are taken care of in the design of information security remedies or strategies. It thus shows that IST potentially provides a better basis to deliver encompassing and inclusive plans for information security management. DT has its strong point for consideration as an applicable theory in the fact that people cause a significant amount of information security breaches within the organizations. An assumption that information security incidents will not occur if people understand that there is a specific, definite, swift, and quick punishment for behaviors not consistent with information security.

Securitization theory. Another applicable theory of information security management for the study is the securitization theory. The securitization theory evolved from the work of the Copenhagen school, which consists of Buzan, Woever, p de Wilde, and others (Balzacq, Léonard, & Ruzicka, 2016). The proponents suggested that security is not a function of what constitutes a risk (objective view) or what is perceived to be a risk (subjective view). They indicated that security should be a function of what is said to be a risk (Gearon, 2017). They suggested that a securitizing speech or risk attribution would drive towards survival and defense from a risk scenario (Harrison, Ahn, & Adolphs, 2015). It, therefore, follows that by securitizing an issue, it becomes an information security matter and, therefore, the issue of supreme importance for resolution

(Gearon, 2017). The tenets of securitization policy contrast IST because IST looks at risk from all possible angles.

The theory has found application in cybercrime prevention by labeling events as dangerous and thereby leading to proactive preventative efforts. The securitization theory supports the idea of risk management like IST. The securitizing speech where risks are attributed is substantially similar to what goes on in using the risk management theory of the IST. The securitization theory, compared with the IST, seems inadequate and insufficient to look into the topic of the study. The securitization theory seems inappropriate because the theory is limited and lacks the depth to discover the universe of risks when looking at the secure use of information systems. The securitization theory leaves out some risk elements. Securitization speech attributes risks when organizations use securitization theory (Gearon, 2017). The IST utilizes a formal risk management process that identifies all risks and subsequently provides for management of the same. The securitization theory takes as risks what a select set of people considered as a risk. It implies that the securitization theory will not be able to provide comprehensive protection for information systems.

The securitization theory is conceived with a referent object in view, just like some other earlier-discussed theories are also object or subject-based, to the extent that labels of insecurity are affected by subject or elements of the system involved (Balzacq, 2015). The IST defines required security goals across all aspects of a function, which includes processes. The IST sets standards that mitigate risks and describes processes that cover subjects or objects that may not yet be in an ecosystem such that even where an

issue, process or objects in a system is not a risk presently but becomes one, there is a provision for handling (Ismail et al., 2014).

The IST of information security management assumes that there are peculiar threats to specific areas of the business environment, described as contingencies (Ismail et al., 2014). The IST assumes that not a single theory can address all threats. It affirms the position of Dimase, Collier, Heffner, and Linkov (2015) that for holistic information security management, it is vital to define security goals based on the contingencies in the environment. IST seeks to fulfill these goals through its fundamental theories. IST makes provision for comprehensive coverage of necessary elements, which are processes, people, and technology, to address the risks arising in a business environment.

Information Security Management Themes and Practices

Defense in depth. An approach that is useful for holistic mitigation of information security risks is the defense in depth principle. IST for complete information security management supports the defense in depth principle. The defense in depth principle was used first by Luttwark to describe the military strategy employed by the Roman military in the 3rd and 4th Century CE. Defense in depth described the change in strategy of the Roman military from the forward defense or (preclusive defense) war plan during the first period of the Roman Empire (30 BCE-CE 284) to the defense in depth to prevent threats coming from outside from bridging the Roman territory (Fettweis, 2018). The defense in depth idea came from the consideration that the Roman border or area was a war zone; the intention was to contain incursions within the designated border areas without allowing internal infrastructure to be affected.

The defense in depth principle encourages the modular application of mitigation, where risks are first encountered (Conteh & Schmick, 2016). As applied to the topic of this study, the principle supposes that there are different aspects or elements of the security of the IT infrastructure of a financial services company. These aspects cover networks, applications, databases, endpoints, processes, and people.

The principle assumes that IT infrastructure architecture components are like portions of the physical Roman Empire. The principle recommends efforts to stop attacks on these individualistic portions instead of subscribing to a security component that will assume to cater for all areas. The principle expects each component of a system should have the capacity to stop any potential breach of security without allowing a spread just as was the intention in the move of the Roman Empire from the previous preclusive security to defense in depth. The defense in depth principle applies not only to on-premise IT infrastructure but to cloud-based systems as well (Racuciu & Eftimie, 2015).

Defense in depth: Pros and cons. The defense in depth principle is also called the castle model, where advocates indicate that security must start from the perimeter to other segments of a castle or typical house (Chierici, Fiorini, Rovere, & Vestrucci, 2016; Leuprecht et al., 2016). Security should be entire and in-depth because the weakest link will constitute an opportunity for a potential breach, especially when other defenses fail (Genge, Graur, & Haller, 2015). The defense in depth principle has become a tested and practical strategy to ensure an appropriate level of information assurance in today's highly networked environments.

The defense in depth principle admits that the security of IT infrastructure requires measures at different points of a system, such that if the protection at a point fails, other available measures can still prevent breaches (Mansfield-Devine, 2016a). Seago (2015) identified a potential pitfall in the adoption of defense in depth for information security. The trap is the tendency of inadvertently depending on other layers of protection to keep hackers out, leading to a relaxing of security of some other elements in the technology stack of any enterprise. The defense in depth theory is useful where each component of the depth of defense has been treated individually and ensured to be in place accordingly. Defense in depth assumes every layer across the path that data transverse in an organization has protection in place as appropriate (Byrne, 2006). Applying ISTto the defense in depth principle will require that risk assessment be carried out across the various elements of the IT infrastructure of a company covering networks (external and internal segments), endpoints, databases, and applications. It also require policies that ensure risk mitigation across the elements in line with the requirements of the information security policy theory of the IST. The control actions for risk mitigation will be in line with any contingencies that could arise as required by the contingency theory of the IST.

Information technology risk management. The issue of providing an appropriate solution to risks that arises because of the adoption of technology tools within the financial services sector cannot be well-handled except by conducting a robust and comprehensive risk assessment. Shameli-Sendi, Aghababaei-Barzegar, and Cheriet (2016) affirmed that for the protection and security of information assets, organizations

must adopt a risk-based approach. A risk-based approach implies that a holistic risk assessment must be part of the process of risk mitigation. Hemanidhi and Chimmanee (2017) noted that risk assessment would identify vulnerabilities and areas where controls and protections are needed.

The requirement for a comprehensive risk assessment is consistent with the expectations of the IST theory to be used in this study. The risk management theory of the IST theory noted that through risk analysis and assessments, there is the identification of the threats, and vulnerabilities of systems, this can then be used to deploy appropriate controls to ensure the security of information assets (Han, Huang, Li, & Ren, 2016). Risks analysis must be structured, deliberate, and aligned to technologies deployed (de Gusmão, e Silva, Silva, Poleto, & Costa, 2016). The issue of alignment is related to another theory of technology use, technology, organization, and environmental (TOE) theory. The TOE theory explains the adoption of technology in organizations. The theory states that technology adoption is affected by the perception of a specific technology (perceived characteristics of technological innovation). The theory advocates that Technology adoption is influenced as well by organizational (firm's characteristics) and environmental (characteristics of firm's external environment) factors (Leung, Lo, Fong, & Law, 2015; Oliveira, Thomas, & Espadanal, 2014). The TOE theory stated that these three factors affect the propensity for an organization to go the way of a particular technology. The TOE explains that the three factors that affect technology adoption influence the risks that are presented to the organization by the adoption of technology.

The deployment of strategies to deal with information security risks that result from using technology to offer financial services is the final step in a formal risk management process. The IST also affirms the same through its risk management theory (Hong et al., 2003). Several frameworks have described the IT risk management process categorized into four stages. The four stages are (a) identify risk, (b) assess risk, (c) deploy controls, and (d) monitor the effectiveness of controls (Lyon & Popov, 2016; Riza, 2017). These elements also map out to the National Institute of Standards and Technology (NIST) Risk Management framework (Meszaros & Buchalcevova, 2017). The process will identify all assets, processes, and capabilities involved in operations that have vulnerabilities that could be exploited by threat agents (Wei, Wu, & Chu, 2017). The identification would then lead to a determination of the various risk scenarios that could lead to exploitation of the confidentiality, availability, and integrity of those assets, processes, and capabilities, with a consideration of existing controls in place (Ali, Warren, & Mathiassen, 2017). The various efforts arising from what to do to bring risks to tolerable limits are strategies that organizations, through their CISOs, put in place to mitigate IT risks, which can cause cyber exploitation of confidentiality, availability, and integrity of information assets. Planning against risk exploitations is always future-looking (Purvis et al., 2016).

IT risk assessments can either be quantitative or qualitative. Quantitative risk assessments use numerical values to calculate loss indices when threat agents exploit a risk, while qualitative uses relative values such as high, low medium to gauge the extent of risks. In practice, risk assessments use both quantitative and qualitative methods (Lyon

& Popov, 2016). Models or frameworks that support quantitative or qualitative risk assessments do exist, some of them are a chain of events model, fault and tree model, and bow tie model (Akinwumi, Iwasokun, Alese, & Oluwadare, 2017).

Before the process of IT risk assessment, organizations must determine their risk appetite and risk tolerance levels. Risk appetite captures the extent of risk that is acceptable to an organization. It captures limits within which the organization can safely do business without damage to it in the context of a violation of confidentiality, availability, and integrity. Risk tolerance captures acceptable deviations from the allowed acceptable risk levels (Fraser & Simkins, 2016).

Risk assessments indicate areas within an organization where IT systems are in use and require the deployment of controls (Shameli-Sendi et al., 2016). Controls, nonetheless, need to be deployed strategically. Options available to address risks may include any of the following.

- Risk mitigation. Risk mitigation involves deployments of additional controls that could be technical, administrative, and operational or preparedness (in the case of business continuity issues) (Lyon & Popov, 2016).
- Risks can also be transferred or shared, this involves the procurement of insurance, and in recent years, situations exist where companies insure against cyber risks (Lyon & Popov, 2016).
- Risks can be accepted. Risks are accepted when the costs of mitigating the risk are much more than the value will come out from mitigation or the benefit it will deliver, or there is no budget to mitigate the risks. ISO 27001 indicated

that in this case, senior management must sign off the acceptance of the risk across all elements of it. Risk management is consistently being seen as senior management responsibility and covers part of the due diligence, due care expected of them.

- Risks avoidance. Risk avoidance involves choosing an alternative cause of action or path that would be less risky. Risk avoidance may include selecting a technology stack that is more secure or less risky (Fraser & Simkins, 2016).

The ISO 31000 captures standards that can be employed to do risk management formally while the ISO 31010 details techniques that can be applied to do actual risk assessments (Aven, 2016; Proenca, Estevens, Vieira, & Borbinha, 2017). The ISO 27005 is the ISO 27001 companion that covers issues around standards for Information security risk management. Standards approach to risk management identifies all possible risk areas and ensure the use of appropriate strategies to mitigate them. The mitigation of discovered risks in risk assessments is consistent with the requirement of the risk management theory of the IST used as a conceptual model.

Information security risk management approaches. Barni, Bartolini, and Furon (2003) identified two significant approaches to ensuring confidentiality, integrity, and availability of information. These approaches can affect the choice of strategies for preventing cyber exploitations in line with the control and audit theory of the conceptual model. These approaches are Open Security (or Security by Design) and Security by Obscurity. Calvo, Etxeberria-Agiriano, Iñigo, and González-Nalda (2016) noted that proprietary technologies promote security by obscurity. The approach chosen by the

organization will be a function of a whole lot of factors. These factors may be related to the information risk management strategy of the organization, availability of skilled personnel, and readiness to expend budget to mitigate risks, amongst others.

Open security (security by design). Open security paradigm acknowledges that a target system is open to all, including potential attackers, and therefore seeks to build security into the use of the system to mitigate risks to an acceptable level and ensure that only legal users have access to the system (Veloudis et al., 2019). The open security paradigm of information security management considers the entire lifecycle of the use of technology to access information and resources and deploy processes, technology, and acculturate people. The objective is to prevent the violation of the confidentiality, integrity, and availability of information assets (Casola, De Benedictis, Rak, & Rios, 2016; Nazir, Patel, & Patel, 2017). The open security paradigm delivers better security than security by obscurity (Rasekh, Hassanzadeh, Mulchandani, Modi, & Banks, 2016).

Security by obscurity. This paradigm of security assumes that a system has protection from violation of confidentiality, integrity, and availability, as long as the internal workings of the systems are not known to a malicious user or cybercriminal. This paradigm of securing systems covers renaming accounts, hiding access point names, renaming script names, and avoiding the use of default directories on systems. Security by obscurity paradigm does not directly deal with inherent weaknesses in systems but tries to hide the fact that a vulnerability exists from cyber exploiters (Rasekh et al., 2016). Pieters, Hadžiosmanović, and Dechesne (2015) argued that security by obscurity is not as secure as open security or security by design. The reason is that the weakness in the

system remains in unmitigated form, and all it takes for exploitation is a discovery by a potential hacker. There are also arguments that security by obscurity is useful when combined with open security (Padayachee, 2016). Open security thrives on best practices and standards (Mansfield-Devine, 2017). It, therefore, appears that an effective strategy for information security management will be inclusive of open and closed security models as deemed relevant for chosen internal control tools to be deployed in line with the Control and Auditing theory of the conceptual model.

Strategies for Information Security Management

Open systems interconnection model and technology approach to information security management. The information security market today presents products that address network, application, database, and user vulnerabilities in the use of technology to access services. One model that explains this particular approach to information security management in the utilization of IT services is the open systems interconnection (OSI) reference model. The OSI model defined seven layers that information transverse before users have access to it in system interactions or communications (Orzen, 2014). The layers are the application layer, presentation layer, session layer, transport layer, network layer, data link layer, and physical layer. The OSI layer is relevant to understanding computer system interactions and pertinent to describe the vulnerabilities that organizations would typically be exposed to as they become more dependent on IT services to serve customers.

The OSI reference model indicates that the distinct layers that data transverse from system to system, are individually implemented because they have different

characteristics to function. The consideration of the OSI model implied that there are vulnerabilities, risks, and threats at each layer of the model. Consequent upon the thoughts of the TOE, vulnerabilities that will be risks to an organization will be related to the technology adopted in that organization, which will be determined by the layers of the OSI model involved in the delivery and consummation of such services (Weyrich & Ebert, 2016).

In as much as the consummation of the technology adopted can be mapped to the OSI models in organizations, the chosen technology and consumed processes/services in an organization determines the risks to be mitigated (Aldosari, 2015; Orzen, 2014). The implication of this outcome has evolved into tools at different OSI layer to achieve information security, leading to deployments of firewalls, which protect a secure network from an unsecured, encryption which protects against sniffing at the network level, and other technology solutions (Stergiou, Leeson, & Green, 2004). Lu, Yang, Wen, Ju, and Zheng (2011), noted that the OSI reference approach has its drawbacks because solutions deployed to address the weakness at some levels may not necessarily address gaps at other layers. Information security may, therefore, not be holistic in such environments.

The fundamental pitfall of the OSI reference approach is that it does not directly address the vulnerabilities that come from processes and people that use technology in organizations (Fraser & Simkins, 2016). It only addresses the technology side. The OSI/Technology approach seems to manage security purely from a technology point of view. Another issue with this approach is that organizations that utilize the method will

have many solo systems delivering less than perfect protection from a holistic perspective. The single point systems require proper integration for effectiveness.

To have in-depth protection or strategies to be deployed that will address potential vulnerabilities at all the OSI levels and beyond, consideration is needed to address risks across people, process, and technology areas (Naseer, Shanks, Ahmad, & Maynard, 2017). The IST framework supports the holistic approach that looks at people, process, and technology for information security management.

Standards approach in information security management. Another approach to information security management is the standards approach to information security management. The approach means that an organization can take a position to identify a relevant information security standard and seek to comply with the standard to mitigate risks in its operations using IT tools. Regulation is a crucial driver of the standards approach. The fact that a company is operating in a peculiar sector that warrants specific information security certification is another primary driver for the standards approach. Other institutions adopt the standards approach for a competitive edge or economic reasons (Ramsey, 2016). Standards such as the ISO 27001, PCI-DSS are typical examples of standards that organizations strive to comply with to achieve confidence concerning information security risks (Soyemi, Soyemi & Hammed, 2015).

The ISO 27001 standard is more general and could apply to various sectors. The PCI-DSS is related to financial institutions that process payment cards (Ashish, Ds, & Milind, 2017). There are requirements for each standard for certification. These requirements cover every perceivable aspect of IT, where risks arise in the operation of

the organization. These requirements include network, physical and logical access to information, and policy crafting. The PCI-DSS standard, for example, has 12 minimum requirements that card processing companies must comply with, while the ISO 27001 has about 133 controls required for compliance certification. Institutions achieve information security management when they make efforts to achieve compliance with relevant security certifications. The information security efforts are what sums up to strategies that organizations deploy to mitigate cybercrimes that undermine confidentiality, integrity, and availability of information assets.

It is typical to see organizations adopt more than one standard in information security management efforts. There could be several intersections in the requirements of chosen standards. Federal agencies and companies trading or having connectivity with federal agencies in the US, for example, will be required to comply with the requirements of the National Institute of Standards and Technology control standard NIST 800-53. Organizations complying with NIST 800-53 within the financial services sector in the US would also be required to comply with the PCI-DSS to process card-related transactions (Hemphill & Longstreet, 2016). The same organization that wants to be competitive or trade globally and would like to communicate the availability of standard information security measures to assure investors may also implement ISO 27001 (Mesquida, & Mas, 2015).

The implementations as unique as they may seem, do not necessarily mean individual costs or efforts. The reason is that controls in one standard do map to another standard, howbeit at different levels of details depending on the focus of the standard.

Some organizations also implement security standards to mitigate information security risks without subscribing to a certification linked standard. One approach is to implement a group of identified controls seen as relevant to their industry and business at the minimum. These efforts agree to the ideas of a constituent of the IST theory used for this study, which is the control and auditing theory. The control and audit theory requires that active information security management in organizations requires the use of security control systems in conjunction with other IST theory components. The idea is also consistent with what Shulong (2014) recommended.

Organizations choosing the path of a noncertification linked standard can use summarised and abridged controls such as the Centre for Internet Security (CIS) Top 20 Critical Security Controls (previously SANs Top 20 Critical Security Controls). The controls are a set of requirements that have been carefully selected by extensive industry consultation, which started by an effort of the National Security Agency (NSA) and was concretized by the SANs Institute, research, and education organization of security professionals over time (Sansorg, 2019). The controls have transformed threat information and remediations into best in class and actionable approaches to safeguard organizations (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016).

Organizations always consider many factors before they deploy controls or strategies that mitigate cyber exploitations, especially within the financial services sector in Nigeria. The cost of the strategy is taken into consideration to prevent expending more money than the assets that are to be protected. Organizations also strategically assess risks with imperatives of business functions to deploy controls that address cyber threats.

Contingencies in information security management. The identified conceptual framework used, which is IST, through its risk management theory facilitates the identification of risk elements that can lead to cyber exploitation of confidentiality, availability, and integrity of information assets within the financial sector in Nigeria. CISOs mitigate risks through deployment of strategies that address identified or known risk elements across the various technology stack that is in use in their institutions to offer financial services. The risk management nature is consistent with the TOE framework, which entails that decisions in an organization often relate to technology in use within the organization and environment (Leung et al., 2015). Hence, the strategy deployed by CISOs will be specific as well as directly related to a known and identified risk element. Conklin and Shoemaker (2017) advocate that such a plan by organizations should be to achieve cyber resilience to ensure the protection of critical technological infrastructure in every situation.

In the exercise of the due care and the due diligence functions of the CISO, they ensure that there is no violation of information security regardless of the situation (Shackelford, 2016). There are unknown risk elements requiring remediation as well; such risks emanate from the use of technology tools and information systems. Those risks exist because they are not known to exist, thus unidentified, but portend danger to information systems and can lead to severe losses if not mitigated (Tran, Campos-Nanez, Fomin, & Wasek, 2016). Those are risks that before the day they occur, they do not have a mitigant. It is the provision for known and unknown risks that will accord financial institutions confidence that they have deployed adequate strategies to guard against

losses, which may emanate from all classes of cyber exploitations. It is worthy of note that unknown risks can come from new vulnerabilities in an IT system, which does not have mitigation; it can come from a possible exploit, which as at that moment does not have remediation. The attacks that come from unknown risks are Zero-day attacks.

Zero-day attacks. Zero-day attacks often result from zero-day weaknesses or vulnerabilities. Zero-day vulnerabilities are vulnerabilities that are unknown to those who will be willing to mitigate the vulnerability. They are undisclosed vulnerabilities that hackers can exploit (Sano, Okamoto, Winarno, Hata, & Ishida, 2016). Zero-day attacks are frequent due to increased dependence on applications by organizations. Contemporary organizations depend extensively on applications and utilize methodologies, such as agile development, to support increasing digitalization (Fagioli, 2019). Agile development capitalizes on the principle of continuous improvements to respond to new service demands by customers. Agile development facilitates software releases in useful increments to meet business requirements (Hanssen, Stålhane, & Myklebust, 2018). The extensive use of applications to meet evolving business requirements is particularly peculiar with financial institutions to stay ahead of the competition. The use of an agile framework for software development introduces flaws, which may be unknown in addition to those already documented and related to other technological infrastructures such as switches, routers, and other interconnecting devices (Kaur & Singh, 2015).

Zero-day vulnerabilities present risks to information systems because the related vulnerability is unknown, and therefore, no corresponding mitigation exists. Zero-day

attacks can persist on the average for about 310 days undetected (Singh, Joshi, & Kanellopoulos, 2019). When discovered, zero-day vulnerabilities and corresponding exploits can have a rather long average life expectancy of about 6.9 years (Ablon & Bogart, 2017). Traditional/conventional defenses are ineffective in addressing zero-day vulnerabilities. Traditional defenses are inefficient because the nature of risks and signature of attack is unknown for zero-day security issues. Zero-day attacks and vulnerabilities, therefore, require novel, unique, and innovative strategies and solutions to be adequately mitigated (Singh et al., 2019). Therefore, financial institutions must include provisions to address zero-day vulnerabilities as a strategy for information security management that will, in turn, deliver optimum value. The field of Artificial Intelligence through machine learning (ML) and deep learning (DL) has facilitated the evolution of strategies for zero-day vulnerabilities and risks. Tools that that support strategies for information security have ML and DL built into them. Examples of these tools are Intrusion Detection systems (IDs), security information, and event management systems (SIEMs).

Artificial Intelligence and Information Security Management

Artificial intelligence (AI) is the term generally used to describe the concept where computer systems take on intelligent behaviors that are common to human beings (Hernández-Orallo, 2016). It is what makes computer systems to do things without human intervention such as visual perception, speech recognition, and decision-making (Pan, 2016). DL and ML are aspects of Artificial Intelligence that has been of great use for information security management. The pioneer of ML, Arthur Samuel, defined ML as

an aspect of computing that enables computers to learn without being directly programmed. ML is used to establish baselines of acceptable behavior for deviations to be interpreted and used as a measure of preventing violations of confidentiality, availability, and integrity of information assets. ML relates to computational statistics, which focuses on prediction using computers. ML establishes baselines by focusing on previously known features learned from the data used for training.

DL evolved from progress made in ML research, and it is an ML method that characterizes data. It stimulates the human brain for analytical learning to interpret data, sound, and text. In order words, deep learning characterizes data and, therefore, able to decode the context of data such as shades of color and the intensity of sound. DL delivers extended capabilities when compared with ML (Biggio & Roli, 2018).

There are fundamental differences between ML and DL. ML uses small data sets, while DL needs large data sets for effectiveness. The performance of DL increases as the data set increases. ML systems require the extraction of acceptable data sets and features by an expert and programmed into systems. DL reduces the efforts that are necessary for such extraction by delivering advanced algorithms that facilitate automatic learning and feature set. The process of setting up intelligence for ML and DL systems can occur through supervised, unsupervised, or semi-supervised learning.

Supervised learning involves the use of representative data while training the algorithm to be used (Peikari, Salama, Nofech-Mozes, & Martel, 2018). Thus, data is tagged with an indication of response when it occurs. Unsupervised learning requires systems to identify patterns and classify them, and then make deductions from such learned data when

specific patterns or occurs. Unsupervised learning does not use representative data. It does not also involve pre-labeling data for responses when encountered. Semi-supervised learning combines the characteristics of supervised and unsupervised learning. It uses labeled and unlabeled data (da Silva, Coletta, Hruschka, & Hruschka Jr., 2016).

ML can analyze threats and respond to cyber-attacks and security incidents. ML can respond to cyber-attacks by storing up a baseline for normal system behavior and able to intelligently determine whenever there is a deviation and provide protection. ML and DL are particularly useful in information security management because they deliver capabilities that address limitations imposed by conventional tools (due to aging and noncurrent attack signatures) typically deployed for the protection of information assets. They can process large volumes of information and determine when an exploit is about to take place and ensure information security (Diro & Chilamkurti, 2018). The ability to process large amounts of data is what makes machine learning potent in remediating zero-day vulnerabilities. Liu et al. (2018) acknowledged that the efficacy of the use of machine learning in cybersecurity but noted that the use of machine learning to prevent cyber exploitation does come with its issues or challenges. The problems that come with the use of ML and DL for cybersecurity thus confirms that a secure technology-based service environment is not possible. Information security strategy, therefore, is an ongoing journey.

Experiments have shown that it is possible to poison ML/DL algorithms to achieve wrongful behavior in its response to potential exploits by hackers (Liu et al., 2018). The poisoning can be done by deliberately introducing malicious data during the

training process or baseline setting process of ML/DL systems. The system is thus falsely trained to believe attack signatures are normal behavior baselines. Attack scenarios can continue leading to suppression of alerts or success of an exploit, depending on which system is involved. In some other instances, ML/DL systems can be evaded by spoofing learned and acceptable signature and adapting exploits to be like acceptable patterns to perpetrate attacks (Biggio & Roli, 2018; Chah, 2019). Strict control over the process of setting baseline data for ML/DL systems is a real way to protect tools using DL/ML principles. The need for process control underscores the need for integration of technology, process, and people to achieve a holistic information security strategy using ML/DL techniques. Data sanitization and obfuscation (Security by Obscurity) of ML/DL tools also help to improve the secure use of ML/DL systems (Biggio & Roli, 2018). An effective information security management strategy would need to incorporate tools that utilize the principle of ML/DL but with the arising risks adequately identified and mitigated.

Google and Amazon are among the many technology giants that currently use machine learning in the area of information security management (Diro & Chilamkurti, 2018; Hatcher & Yu, 2018). Google currently uses ML to analyze threats against mobile endpoints running the Android operating system. Amazon utilizes machine learning to achieve data classification in its S3 cloud storage services offerings. Many of the security technology offering companies have moved from signature-based systems to machine learning, and deep learning supported systems. The need to provide proactive protection for zero-day attacks has been a significant driver in the move from signature-based

systems to machine learning and deep learning systems because of their capabilities to address previously unknown risk elements. Deep learning and Machine learning have also been instrumental in doing repetitive information security tasks, e.g., interrupting ransomware, notifying of an imminent threat.

The contingency theory of the IST of the conceptual model requires strategies to prevent, detect, and react to cyber exploitations are put in place. The use of AI tools through ML and DL technologies is a way to fulfill the requirement of the contingency theory for strategies that prevent, detect, and react to cyber exploitations. The contingency theory stirs action of security policy, risk management, system management, or internal control and audit, which ultimately may require the deployment of innovative tools that utilize AI.

Incident Management and Information Security Management

CISOs usually deploy strategies targeted at preventing cyber exploitation of information assets through the preservation of confidentiality, availability, and integrity of information. Nonetheless, the state of total security to avoid cyber exploitation does not exist (Conklin & Shoemaker, 2017). In the face of best efforts to ensure information security, breaches do occur primarily through exploits of vulnerabilities or weaknesses in information systems by persistent attacks by hackers (Kumar, Raj, & Jelciana, 2018; Settanni et al., 2017). It is, therefore, essential for CISOs to have a robust incident management plan in addition to other strategies that are available for preventing cyber exploitation of information assets. Incident management is the process of responding to information security failures or breaches. Incident management helps to minimize losses

due to a violation of confidentiality, integrity, and availability of information assets (Ab Rahman & Choo, 2015). Incident management is one of the pivotal elements of ISO 27001. A vital component of incident management is the communication of incidences promptly, which facilitates quick responses to incidences.

One of the critical values of incident management is that it helps to identify failures or weaknesses in existing strategies that allowed incidences, and so provides a basis for information security strategy improvements. Information security incident management also set the platform for information sharing amongst related entities that help firms to stay safe from cyber exploitations. Notwithstanding the benefit of incident response teams, research shows that there is a significant disconnect between incident response teams and security management teams in organizations (Ahmad, Maynard, & Shanks, 2015). It appears in many organizations most of the lessons learned do not translate to actual improvements in security management because of that disconnect. Effective management of information security contingencies as required by the conceptual model, need to include a robust incident management system. Lessons learned from a formal incident management framework also supports the risk management requirements of the risk management theory of the conceptual model for the prevention of information security exploitations or incidences.

Internal Controls and Information Security Management

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission framework which is one of the well-accepted frameworks for internal control defines internal control as a process, effected by an entity’s board of directors,

management and other personnel, designed to provide “reasonable assurance” regarding the achievement of objectives in effectiveness and efficiency of operations (Rae, Sands, & Subramaniam, 2017). In this case, effectiveness and efficiency in information security management operations. Internal control is, therefore, a necessary component of the strategy for organizations to prevent cyber exploitation of information assets. The COSO framework provides a means for top-level executives to perform their due diligence role in the area of preventing cyber exploitation of information assets (Lanz, 2017). The COSO framework aligns risk management to the strategic objective of the organization (Karanja, 2017)

The Control and Auditing theory of the IST used for this study suggest that organizations should have an internal control structure that will support their information security management efforts (Hong et al., 2003). The management theory, another constituent theory of IST, requires standard approaches to Information security management. The adoption of standards ensures valid and proven controls are in place that look to address information security issues in organizations. Internal controls serve as a means to ascertain that mitigation for information security risks are in place, and ensures controls are effective. Adequate internal controls proactively identify potential exploitations and prevent incidences. Companies with robust internal controls operate their processes with greater efficiencies (Cheng, Goh, & Kim, 2018). Internal controls function to minimize risks, protect assets, ensure accuracy of records, promote operational efficiency, and encourage adherence to policies, rules, regulations, and laws.

In an “effective” internal control system, according to Rae et al. (2017), the following five components work to support the achievement of an entity’s mission, strategies, and related business objectives.

- Control Environment. The control environment promotes integrity and ethical values. The control environment sets the tone of an organization, influencing the conscience of its employees. It is the base for all other components of internal control, providing discipline and structure
- Risk Assessment. Cover the company-wide objectives that evaluate the risks in the entire company from various perspectives and decides on control measures
- Control Activities. These are the actions established through policies and procedures that help ensure the implementation of management’s directives to mitigate risks to achieve objectives. The selection and development of control activities include the segregation of duties. This measure works to ensure that strategies deployed to prevent cyber exploitation of information are operational and practical.
- Information and communication. The objective of this objective is the effective communication of control measures, e.g., policies.
- Monitoring. Continuous controls monitoring (CCM) is a set of technologies to reduce business losses through constant monitoring and reducing the cost of audits through continuous auditing of the controls in financial and other transactional applications.

The management system theory component of the conceptual model requires that every organization define security policies and the scope of information security management systems to preserve confidentiality, availability, and integrity of information assets. Internal control systems are the management systems that ensure the effectiveness of these efforts (Lanz, 2017).

Security Policies & Internal Controls in Information Security Management

Internal control and audit mechanisms support information security management in organizations (Bozkus Kahyaoglu & Caliyurt, 2018). There is, however, a need for well-defined information security policies for the internal control function to work effectively (Flowerday & Tuyikeze, 2016). The standards approach of information security, where an organization adopts a standard like the ISO 27001 standards easily facilitate the crafting of policies that support the effective functioning of internal controls. Policies capture at the corporate level decisions of executive management on how to handle information assets to ensure they are safe (Stafford, Deitz, & Li, 2018). Policies determine what is acceptable and what controls need to be in place and delineate the work of the internal control function to ensure compliance (Niemimaa & Niemimaa, 2017). There is an intersection between the security policy theory and the internal control and auditing theory of IST, in that both work together to achieve an effective information security management system. Internal control monitors to establish compliance with documented policies. Policies address existing information security risks in enterprises (Flowerday & Tuyikeze, 2016).

The security policies in organizations are influenced by the applications, culture, and technology in place, which is consistent with the TOE framework (Leung et al., 2015). These policies will change as technology or culture changes, but what will ensure the changes are in line with changing culture and technology is an effective internal control monitoring. Internal control ensures that the controls deployed are adequate to address current risks (Bozkus Kahyaoglu & Caliyurt, 2018). Internal control also does significant work in ensuring compliance with policies that keep organizations secure by making sure employees are aware of existing policies. One of the key objectives of the internal control function is the communication of policies and compliance with policies. Sohrabi Safa et al. (2016) notes that communication of policies facilitates policy compliance. Policy communications occur through information security awareness campaigns, and it is a critical part of fulfilling the people's requirement of ensuring information security (Bauer, Bernroider, & Chudzikowski, 2017).

The internal control function in organizations, therefore, deliver proactive protection to prevent cyber exploitations to information assets. The audit function works after the fact to extract value from incidents for remediation and future prevention through deployment of controls. Steinbart, Raschke, Gal, and Dilla (2018), in their investigation on the contribution of the control functions to adequate security within enterprises, confirmed that collaboration of the internal control and audit function with the information security functions has a positive influence in achieving effective prevention of cyber exploitations. Practical strategies to prevent cyber exploitation within the financial services sector no doubt must include the reliable deployment of internal

control mechanisms, which are only possible where well-documented policies exist. Hong et al. (2003) affirm that security and internal control actions are usually efforts towards achieving contingent management of information security risks that can come from the use of the risk management theory of IST, the conceptual model used for the study.

Relationship of this Study to Previous Research

This study investigated strategies that CISOs have used to prevent cyber exploitations of information assets within Nigeria's finance sector institutions. Similar studies have looked at what end-users and audit committee members of financial institutions should do to prevent cyber exploitations within the sector. The previous researches used the case study design to assess the current situation and presented a feasible strategy that CISOs can adopt. Gana, Abdulhamid, and Ojeniyi (2019) examined the risks that are associated with accessing services within the financial sector through technology and possible ways to address associated risks. The collection of data was through interviews with 16 respondents. The significant findings were that it is essential that end-users are aware of the risks of cyber-crime and that there is a need to ensure adequate protection of end-user devices to achieve information security in transactions. The study recommended a strategy, financial institutions to step up user awareness to prevent cyber exploitations.

There was a recommendation for users to ensure they do more by paying attention to the protection of computer systems and access devices they utilize to access financial services. The recommendation will help to achieve improved security in preventing cyber

exploitations of confidentiality, availability, and integrity. The study also recommended focusing on securing platforms that provide financial services, which this study will focus on somewhat.

The study in Ojeka, Ben-Caleb, and Ekpe (2017) looked at the audit committee's effectiveness in combating cybersecurity in the Nigerian banking sector. The study explored strategies that board committees deploy to prevent cyber exploitations within the financial services sector (Ojeka et al., 2017). The study used surveys to collect data from 13 institutions but correlated with secondary data collected from all the 21 banks listed on the Nigerian stock exchange. The study noted that the board committee has a due care responsibility to ensure institutions comply with applicable laws and standards that will guarantee security (Ojeka et al., 2017).

Ojeka et al. (2017) found out that as it stands presently, most audit committees are not able to provide the necessary support to ensure cybersecurity in financial institutions as required by their due care role majorly because of lack of technical know-how. The study recommends the deployment of strategies to empower board members with knowledge to be able to strengthen organizations to win the battle against cyber exploitations that undermine confidentiality, availability, and integrity of information. The study, therefore, noted that a strategy for preventing cyber exploitations within the financial sector is the education of critical stakeholders. Markelj and Zgaga (2016) equally supported the conclusion on the need for user education to ensure information security. The recommended strategy is similar to the position of Gana et al. (2019).

There seems to be a convergence of intentions in preventing cyber exploitation of

information assets, in that most organizations tend to deploy measures with a mindset of avoiding malicious intents. Organizations also direct efforts for deterrence and countering any attack that may eventually occur (Kreutz et al., 2016). The view of Soomro et al. (2016) is that while some companies recognize the need to have a comprehensive information strategy, costs are always a significant factor for consideration (Srinidhi, Yan, & Tayi, 2015). Smaller organizations still have challenges implementing comprehensive or holistic strategies when compared to more prominent companies. Larger companies with bigger budgets are, therefore, able to deploy more holistic strategies, while smaller companies may not.

Several factors can influence the disposition of players within the financial sector to the issue of securing data or information assets. The risk appetite and potential problems that may arise (e.g., financial or reputational damage) if there is a breach are potent drivers (Sen & Borle, 2015). The legal implications or ramifications are another profound influencer for security services within the financial sector. The absence of relevant laws or commensurate punishments to deter cybercriminals may influence how financial institutions make provisions to prevent attacks. The availability of robust legal frameworks to dissuade cybercriminals may make institutions in the financial industry have a false sense of security, which may influence their attitude to deploy strategies to mitigate information security risks (Eboibi, 2017).

Transition and Summary

The previous section discussed the IST theory, the conceptual model used for the study. The section enumerated the reasons for choosing IST relative to other discussed

theories. The section also discussed some information security management concepts and themes. These themes cover several existing practices and approaches to information security management in institutions in responding to identified cyber exploitation risks and possibilities. The section further discussed how AI affects information security management, especially dealing with zero-day risks. The section also discussed how to manage incidents if, after best efforts, cyber exploitations still occur. The next section covers the procedure for the research and writing of the report.

Section 2: The Project

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies that CISOs deploy to prevent cyber exploitation that jeopardizes the confidentiality, availability, and integrity of information within financial institutions in Lagos, Lagos State and Abuja, Federal Capital Territory, Nigeria. The population for this study was CISOs of six companies within the financial services sector of Nigeria who have implemented strategies that mitigate cyber risks. The implication for social change includes reducing the unbanked population in Nigeria through increasing confidence in the use of available technology to deliver and access financial services.

Role of the Researcher

The role of the researcher in qualitative research includes data gathering, data analysis, and interpretation of collected data to answer the research question (Palinkas et al., 2015). As the researcher, I identified the financial institutions for investigation, made contacts with gatekeepers, and obtained letters of cooperation from the institutions for the study. Data came from developing interview questions, scheduling, and conducting interviews with the participants who met the eligibility criteria for the study. I once managed the information security unit for a bank in one of the locations of the study, which enabled the use of the right language in communicating while conducting interviews for data collection. It also facilitated the interpretation of statements made in the context of the study appropriately.

As part of my role as the researcher, I used interview protocols (see Appendix) to prevent bias and to ensure consistency in questions the participants responded to. Relevant and useful data can only be obtained objectively without bias when interviewees give personal views in response to similar questions asked each participant (van de Wiel, 2017). Interview protocols helped to ensure that participants respond to identical interview questions. The use of interview protocol also kept the interview process focused on the objective of the study and facilitated the use of the time available for the interview process.

Interviews allow for the use of open-ended questions that supports the exploration of a phenomenon (Mitchell, 2015), which is why they were used to understand the personal experiences of CISOs in terms of strategies they use to prevent cyber exploitation within the financial sector in Nigeria. However, data collected to study cases take various forms (Gentles, Charles, Ploeg, & McKibbon, 2015). Aside from interviews, data can also come from archival records, policies, company records, applicable routine or statutory information security reports, and publicly available information, which help to validate data gathered during other exclusive sources. The sources of additional data in this study were company records, policies, archival records, relevant information security reports, and publicly available information. The other data sources provided a means to confirm the details noted in the course of interviews.

Additionally, member checking is a method of affirming recorded ideas in interviews to help validate interview data (Birt, Scott, Cavers, Campbell, & Walter, 2016). Member checking made sure that the data reflected the actual responses by sharing

summaries of interpretation of responses with interviewees. Member checking also provided an opportunity for participants to validate the intent of their responses and make corrections where necessary.

Furthermore, bracketing was useful to minimize bias. Bracketing is a technique in research where the researcher suspends his or her beliefs, assumptions, prejudices, or previous experiences to study or describe a phenomenon (Gearing, 2004). The interview process did not involve discussion of any previous personal view or opinion about the phenomenon under investigation with the participants.

Finally, as the researcher, I used ethical standards by following the Belmont Report protocol that covers research involving human subjects. Procedures were also in line with the requirements of the institution review board (IRB). Researchers involving human subjects require oversights of the IRB (Stang, 2015), and the Belmont Report advocates the adoption of three core principles: respect of persons, beneficence, and justice (U.S. Department of Health & Human Services, 2010). These principles were applied by ensuring participants give informed consent to research, understand the risks and benefits, and participate willingly in the research. These guidelines ensure that there is no violation of the rights of human subjects in the research by preventing unjustifiable exploitation by researchers. Thus, the principles of the Belmont Report guided the interview process.

Participants

Participants for the study were CISOs drawn from the companies in the Nigerian financial sector identified for this case study because the objective was to seek strategies

that CISOs use to mitigate cyber exploitations. The financial sector consists of insurance companies, microfinance banks/institutions, stock brokerage firms, and deposit money banks (Central Bank of Nigeria, 2015). Participants were CISO role holders; CISOs have overall responsibility for crafting and implementing strategies that financial institutions deploy to mitigate cybercrimes (Erastus, 2017; Karanja & Rosso, 2017). The companies in this study have strategies to prevent cyber exploitations because they have either the ISO 27001 or PCI-DSS certification. Any ISO 27001 or PCI-DSS certified company has shown efforts for mitigating cyber exploitations that violate confidentiality, integrity, and availability of information.

The financial institutions of the participating CISOs have evidence of having implemented strategies for mitigating cybercrimes, which is the possession of an information security certification relevant to the financial sector. Examples of such are PCI-DSS or the ISO 27001 certification that shows efforts for IT risk management. ISO 27001 certification affirms the deployment of specific IT controls that provide security across an organization in particular areas (Fazlida & Said, 2015). The PCI-DSS accreditation implies that an organization has taken steps to meet requirements of information protection for safe processing of cards related transactions (Hemphill & Longstreet, 2016). The CISO of any company in the Nigerian financial services sector that have any of these certifications was a qualified participant. These CISOs know what strategies help to prevent cybercriminals from carrying out cyber exploitations that violate confidentiality, integrity, and availability of information assets.

Relevant executive-level officers (CIOs, executive directors) of the institutions studied provided information on organizational protocols/approvals required to gain access to the participants (CISOs). Knowing the officer to contact for approvals in the participating organizations facilitated quick support for the study (see Dempsey, Dowling, Larkin, & Murphy, 2016). The executive-level officers enabled contact with gatekeepers. Gatekeepers grant formal approvals for access to subjects of research in organizations (Kay, 2019). I contacted the executive-level officers or CIOs by leveraging existing relationships in the targeted institutions.

Gatekeepers or designated representatives notified participants of permissions to participate in the study. Gatekeepers give participants confidence and assurance to share information in a study (Høyland, Hollund, & Olsen, 2015). Gatekeepers also facilitate the smooth running of the research process (McFadyen & Rankin, 2016). The gatekeepers or their designated support for the research of the institutions facilitated access to the participant's e-mail and phone details. Participants were contacted initially by email before calling them after the organization approved the study. The letter of the participants' consent to participate in the study was also was sent by email. I provided the participants details of the study in the email sent to them to establish a working relationship. The email was followed by a phone call to finalize the timing for interviews. The participants got assurance of the anonymity of the outcome of the research. The assurance encouraged their willingness to participate in the study.

Research Method and Design

Research Method

I used a qualitative exploratory methodology for this study. Qualitative studies are explorative or investigative in approach (Hammarberg, Kirkman, & de Lacey, 2016). Qualitative studies help to understand phenomena (Runfola et al., 2017) and enhance the understanding of issues and the context of issues and processes from the perspective of a participant in research (Fusch & Ness, 2015). This method is appropriate because, through the method, participants were able to share in context their understanding of the security strategies they use to prevent cyber exploitations in the chosen financial institutions in Nigeria. The objective was to identify and understand possible strategies that CISOs use to secure information assets in financial institutions to prevent cyber exploitations that can violate the confidentiality, availability, and integrity of information in Nigeria's financial institutions.

The quantitative research method was not the choice for the study. Quantitative methods support the testing of theories (Green et al., 2015). Quantitative methods also utilize finite or real measures of variables in an investigation (Everett, Neu, Rahaman, & Maharaj, 2015). Further, quantitative studies fundamentally assume that there is a world that exists independently of human influences (Florczak, 2014). Because I did not test any theory or use finite or numerical measures, I did not choose the quantitative method for the study. Additionally, the perception of humans through interviews was the basis of answering the research question.

I also did not use a mixed methods methodology. A mixed-method study requires a combination of quantitative and qualitative methods (Doyle, Brady, & Byrne, 2016). Mixed methods involve investigations using finite measures or statistical data as well as human perceptions and context to arrive at conclusions (Griensven, Moore, & Hall, 2014). Mixed methods are also useful where combining methods will provide more value than using a single method by providing a deeper understanding of the phenomenon from the perspectives of two methods (McKim, 2017). However, I used context and data from human subjects and perceptions without any finite measure. This study was accomplished by strictly using the perspectives of a qualitative method because of the need to capture the human context of the organizations, which only a qualitative study will provide.

Research Design

I used a case study design for this study. Case studies are useful for providing answers to *how* and *why* questions in a qualitative study of a select small group, event, or person in real-life settings (Yin, 2014). The design is also useful when the context of a phenomenon is essential to its understanding, the boundaries between phenomenon and context of the phenomenon are not clear, especially when they go together for a proper understanding of the phenomenon or when the researcher has minimal control over events (Amerson, 2011; Yazan, 2015). Case studies are particularly useful for the exploration and study of the unique but complex phenomenon which finite terms cannot conceptualize (Yin, 2014).

The case study design was the appropriate choice because case studies allow the particular context of targeted institutions to come into consideration in a study. The

design was also appropriate because there was no control over events to be studied, as case studies involve representative samples to understand the phenomenon where the researcher cannot control events around cases of the study (Yin, 1981). I specifically chose a multiple case study because multiple case studies are generally more convincing and provide confidence for the representativeness of ideas. A multiple case study is also useful when there is a need for a deeper understanding of the phenomenon (Yin, 2017). I used this design to explore the situation of how CISOs in the context of some financial institutions in Lagos, Lagos State, and Abuja, Federal Capital Territory, Nigeria, prevent breaches of information security. I investigated *how* and *why* the CISOs use specific strategies to prevent cyber exploitation of confidentiality, integrity, and availability of information assets in five chosen institutions within the financial sector in Lagos and Abuja, Nigeria. The process of interviewing six CISOs of financial institutions in Nigeria helped deepened the study. Interviewing the six CISOs also provided a basis to identify the repetitiveness of data that improves the validity of the outcomes of the study.

I did not use an ethnographic design for the study. In ethnographical studies, researchers are embedded within the target population to understand people and their culture (Mannay & Morgan, 2015). However, the study did not involve embedding the researcher in any organization for this study. It was also not ideal because the study did not look at cultural inclinations, and ethnographies facilitate the study of the culture of a population (Baskerville & Myers, 2015). Additionally, a primary data collection method for ethnographical studies is participant observations over a long period in the location of the study (Hammersley, 2017), but I did not use participant observation over a long

period in the location of the study. Case studies also utilize observations as a data collection method but over a short period when compared with ethnographical studies.

The phenomenological design was also not chosen as the design. Phenomenological designs deal with the exploration of the lived experiences presented by targeted study participants (Willis et al., 2016). Phenomenological studies capture the perception of the population of study as it concerns a phenomenon (van Manen, 2017). This study, however, was not about describing a lived event experience or phenomenon or the personal perception of CISOs about the phenomenon under study. Further, the study relates to how CISOs function in their organizations within the financial sector to prevent cyber exploitation of information assets. Hence, context is important, which a phenomenological design does not consider. The phenomenological design focuses on the individual participant without any relation to the environment, social norms, or traditions (Peeler, Fulbrook, Edward, & Kinnear, 2019).

Finally, the design of this study was not a narrative. Narrative studies connect events from people based on some form of experiences and capture stories around a phenomenon (McAlpine, 2016). The narrative design also involves investigating individuals or persons who are related by some elements of the phenomenon under study to connect events chronologically (Clandinin, Cave, & Berendonk, 2017). Narrative designs are useful in circumstances when there is a need to tell a specific or unique story about a place or individuals, which requires people who are connected to the story to tell it directly. However, the study did not involve uniquely linked individuals to a story, and the study was not about connecting events or narrating experiences. The study was about

the strategies of CISOs in separate entities that do not work directly together for mitigating cyber exploitations.

Further to the design chosen for the study, data saturation helped ensure the validity of the outcomes of the study. Data saturation occurs when the data collected have a high volume of information, and no new information or themes come from further data collection (Aldiabat & Le Navenec, 2018; Malterud, Siersma, & Guassora, 2016). The more data collected for the study, the more information was available for conclusions, ensuring the validity of outcomes. The study achieved data saturation by ensuring interview questions and secondary data covered every foreseeable theme identified in the literature review.

Population and Sampling

The population for this research was six CISOs representing six companies from the financial sector in Lagos and Abuja, Nigeria. In Nigeria, financial institutions have one CISO per organization that oversees cybersecurity initiatives (Balogun, 2018). CISOs have the overall responsibility for information security matters and work to prevent cyber exploitations of information assets (Karanja, 2017). A CISO has a certain level of technical and business competence, with the ability to design strategies that help organizations prevent cyber exploitations (Reece & Stahl, 2015). CISOs also work with business leaders to support them professionally and to ensure information security (Hooper & McKissack, 2016). Thus, the participants were able to provide data for the study.

Data collection was by the census sampling method. Census sampling is applicable when data are to be collected from every member of a population to be studied (Alexander, 2015). In a census, population size is equal to the available sample size (Singh & Masuku, 2014). I investigated strategies in use by CISOs from six institutions within the financial sector in Nigeria. The census sampling method was appropriate for this study because each of the target organizations has one CISO role holder, and each provided data for their respective organization. Census sampling has the advantages of providing accurate and complete data for analysis in a study. Census sampling can, however, be costly since data needs to be collected from all samples of the population, especially where the sample size is large. Census sampling also requires skilled human resources to ensure the collection of useful data for analysis (Martínez-Mesa, González-Chica, Duquia, Bonamigo, & Bastos, 2016).

Data saturation occurs when no new theme, code, or idea comes up from the data in a study (Aldiabat & Le Navenec, 2018). Data saturation is needed to ensure the validity of the outcomes of the study (Fusch & Ness, 2015). Data saturation happens at the point the data collected have a high volume of information, and no new information will come up from the collection of new data (Malterud et al., 2016). The study achieved data saturation by ensuring interview questions and secondary data collected cover extensively every foreseeable theme identified in the literature review.

The population that met the eligibility criteria provided data for the study. Ensuring requisite eligibility criteria for a study increases the generalisability and validity of the findings by making sure data come from the right sources (Green et al., 2007). The

eligibility criteria were (a) the participants must be a CISO, and (b) the financial institution of the participant must have been certified to the ISO 27001 and or the PCI-DSS standards. The identified criteria were such as to identify factors that foster a focus on the population identified for the study and to establish that there is proof of actual strategy for the prevention of cyber exploitation. Data collection was by face to face interviews based on the availability of participants. Interviews were conducted at the participants' office meeting room in line with the required protocol in place in the organization. It is better to do interviews away from distractions to achieve its purpose (Slade & Sergent, 2019).

Ethical Research

Ethical issues in this research were handled consistently with the expectations of the IRB. The registration of participants for participation in the research was by meeting the requirements set under the participants' section. Contacts with the participants were through a formal e-mail. The letter of consent was attached to the mail to the CISOs of the companies. The e-mail followed after the organizations confirmed their willingness to participate in the study. Informed consent ensures the preservation of the rights of participants in line with the Belmont protocol and confirms their willing participation in the study (Hammer, 2016). The participants completed and returned the letter of consent before participating in the study. The return of the completed letter of consent before participating demonstrated the preservation of the rights of participants. The letter of consent sent in also showed their willing participation in the study. The approval of the

IRB was sought before data collection to ensure that ethical protection for participants is adequate. Adequate ethical protection of participants led to IRB approval.

Participants had the opportunity to withdraw from the research by placing a telephone call or by formal notifications through a written letter or e-mail. Participants did not get any monetary incentive for participating. Participating companies will get details of the outcomes of the study with the hope that they will benefit from the research. The participating institutions knew they would get the research outcome through the formal letter written to them to elicit their participation in the study.

It is a good practice to preserve the identity of participants to safeguard them in line with ethical requirements (Saunders, Kitzinger, & Kitzinger, 2015). Participants and their results are therefore not named directly, but identified by aliases were necessary for the dissertation. This practice ensures the confidentiality of opinions and information of the companies. The storage of the data collected for the research will be for five years in line with Walden University requirements in a google drive within a folder set up for the research. Security of the folder is through google authentication and encryption protocols. Personal safe keeps physical documents. Access to the google drive will be at the provision of authentication credentials required for authentication to access the contents. Destruction of research data will occur securely after five years.

Data Collection

Instruments

I was the main instrument of data collection. Yazan (2015) recommended that for case study investigations, data should come from at least two of six sources. These

sources could be two of the following: interviews, information from archival records, direct observations, participant observations, artifacts, & or documents (Yazan, 2015; Yin, 2013). Interviews were the source of primary data. Archival data, artifacts, internal documents, and other publicly available information were the source of secondary data. Primary data collection occurred using the interview protocol in the Appendix. I used semi-structured interviews. Interviews allow open-ended questions to understand a phenomenon by focusing on the research question (Peters & Halcomb, 2015). Semi-structured interview formats allow interviewers to ask follow-up questions related to the research question to understand better the phenomenon under study (Mitchell, 2015).

In qualitative research, the researcher must be aware of factors that can influence the research (Barnham, 2015). As the main instrument of data collection, I was mindful of factors that could hinder objective data gathering in order to prevent them. The use of the interview protocol ensures the same questions were asked and thereby ensure reliability and validity. Interview protocols generally aid getting valid answers in qualitative research by asking similar questions in an appropriate context (Heydon & Powell, 2016). The use of the bracketing technique minimized bias. Bracketing technique ensures the researcher suspends his or her beliefs, assumptions, biases or previous experiences to study or describe a phenomenon (Gearing, 2004)

The ideas and views expressed in the course of interviews will be validated with the interviewees through the member checking concept to ensure there is no misrepresentation and that it resonates with their experiences. Member checking is a

mechanism for achieving validity, and it involves sharing a summary of the interview data with respondents to be sure it resonates with their experiences (Birt et al., 2016)

Organizational documents for each of the companies investigated and several documents related to information security management within financial services were the source of secondary data. I was the data collection instrument for secondary data collected. The documents were organizational policies, materials, or archival records, directly from the companies, and other public sources (e.g., websites and regulatory bodies). Secondary data provides a means to validate data collected from the primary sources (Dunn, Arslanian-Engoren, DeKoekkoek, Jadack, & Scott, 2015). The secondary data support triangulation with the primary data.

Data Collection Technique

Primary data for the study came from interviews that I conducted with the CISOs of participating financial organizations. The primary data collected is in addition to other relevant secondary data that were collected, as shown in Figure 1.

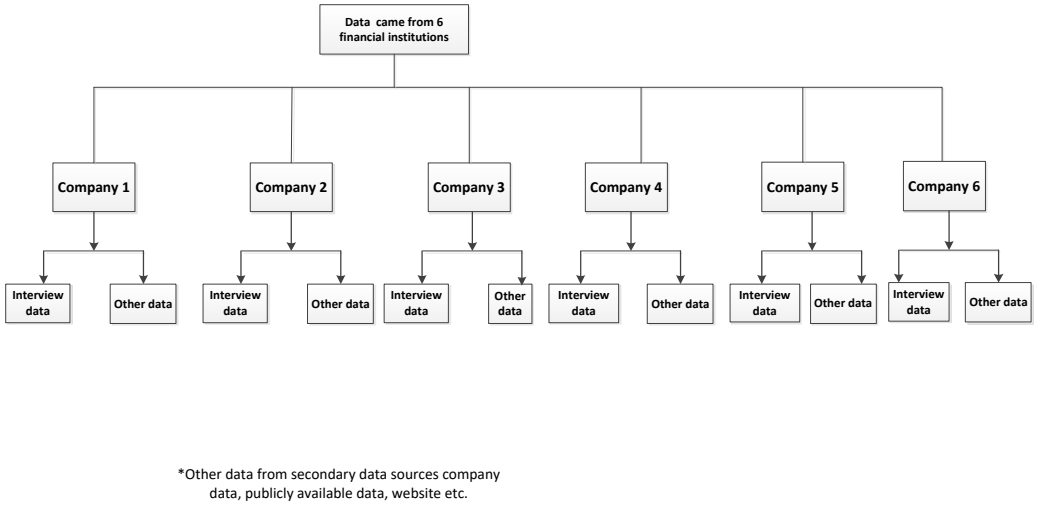

Figure 1. Data collection.

Interviews provide opportunities for open-ended questions that give detail understanding in investigations (Nelson & Cohn, 2015). Interviews have the advantages of being a natural and socially acceptable means of collecting data (Morrison & Stomski, 2015). Interviews additionally help to gain insight quickly and understand the context of data while providing the opportunity for the data collector to observe and listen (Rosenthal, 2016). The use of interviews as a data collection technique helped to have a detailed understanding of how CISOs deal with the issue of cyber exploitations that jeopardize confidentiality, availability, and integrity of information in financial institutions in Nigeria. The use of interviews supported relaxed data gathering because of its social acceptance. It also helped to understand the context of the study because interviews allow observations and listening.

Interviews, however, have the disadvantages of being time-consuming and may require significant efforts and costs to transcribe for data analysis and necessary follow-ups. Different people may also transcribe interviews in different ways leading to errors in the interpretation of collected data (Owen, 2014). Interviews can also evoke personal feelings, which would need to be handled carefully (Pickard, Roster, & Chen, 2016). Transcription of interview recordings was done in such a way as not to misrepresent interview data. Attempts were made not to invoke negative emotions during the interview sessions.

An interview protocol (Appendix) guided the interviews. Interview protocols helped guide the scope for interviews and ensured consistency of the interview process (Winchester, Salji, & Kasivisvanathan, 2017). The interview was semistructured, with

open-ended questions, to explore ideas more profoundly as deemed fit. Semistructured interviews bring subjective and individual views and perspectives of interviewees to the data collection process (McIntosh & Morse, 2015).

A record of the interviews occurred using a recording device after the participants granted permission to use a recorder. I contacted the interviewees after the initial interviews to confirm that what the interviewees expressed during interviews was captured correctly through the member checking process. Interviews recorded were transcribed and summarized clearly and concisely to reflect critical points. The summarised points were forwarded to the interviewees for them to confirm that the captured details reflect their views during the interview. In the course of the member checking, the wrong information recorded from an interview was corrected and updated. Member checking as a technique ensures that ideas and perspectives shared by interviewees are captured correctly by interviewers (Madill & Sullivan, 2018). Member checking also helps to ensure rigor, reliability, and validity of the research process (Simpson & Quigley, 2016).

Additional data were collected, as shown in Figure 1, by reviewing participating companies' archival and operational documents. Requests were made for the identified documents during the interview sessions through the CISO. As part of the data analysis activities, the review of company documents took place. Additional data also came from publicly available documents, such as company websites and other regulatory websites. A review of the companies' websites occurred before and after the interview sessions. Additional sources of data increase validity and reliability in research (Yin, 2013). The

participant's interview for the study took place after IRB's approval with number 11-01-19-0434615.

Data Organization Techniques

Electronic folders stored data for each company identified for the study to prevent a mixup. Interview audio files and the transcribed version, as well as soft copies of secondary data, were kept in folders for each organization under a parent data folder, as depicted in Figure 2.

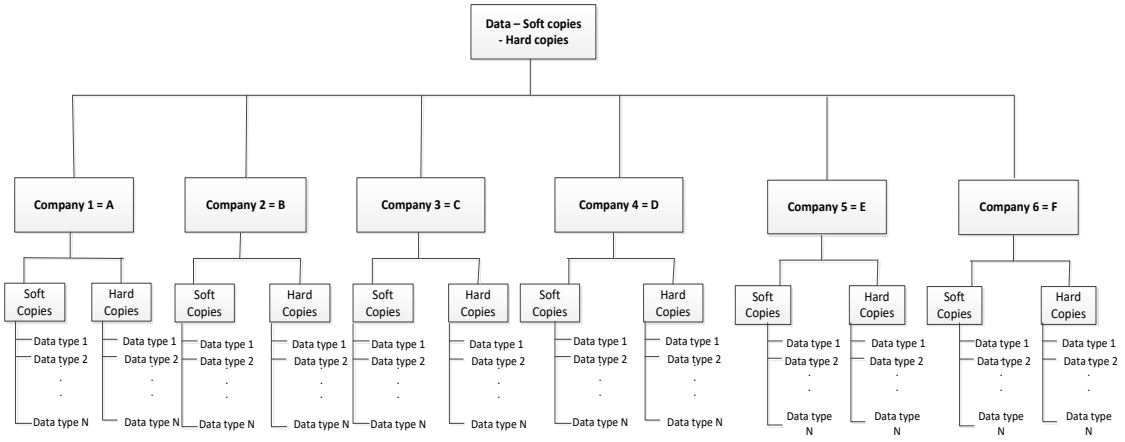

Figure 2. Data organization.

A self-descriptive name identified each data in folders indicating the type of data with the name of the company added. Hard copy documents and records that cannot be in electronic copies by scanning were arranged individually per organization; dividers separated unique types of hard copy data within files. A research log also supported data organization. Research logs provide evidence of rigor, structure, and validity in qualitative research (Fluk, 2015). The log consists of different sections; A section of the research log kept track of the file name of the interview recording of each participant against their company. This section of the log will also have a mapping for each company

in the study. A pseudonym was used for each company and participant to achieve anonymity. Pseudonymization allows a representation of data in a form that is not traceable to actual persons, places, or organizations without altering the essence of the data (Shabani & Borry, 2017). Pseudonymization reduces risks to individuals or organizations related to research data (Suomalainen & Julku, 2016). The research log captured for each company, additional documents obtained for secondary data collection.

To keep track of emerging understandings or themes in the course of investigations, another section of the research log documented emerging trends, themes, or patterns with an indication of which of the interviews have the themes or patterns. Thematic meanings are fundamental to qualitative data organization (Morse, Lowery, & Steury, 2014). Themes assign meaningful essence to texts (Crowe, Inder, & Porter, 2015). The collation of identified themes was followed by mapping to emerging strategies. Emerging strategies that are in use in financial institutions to prevent cybercrime were noted from identified themes and documented iteratively in serial or increasing numbers. This section of the log noted unique contexts to arising discoveries.

Subsequent occurrences of themes that map out to strategies accounted for amplification of the need to pay attention to that strategy. In doing this rich text analysis, I noted similarities in transcripted interview responses between organizations studied. Similar trends arising from analysis helps to quickly identify themes in qualitative samples (Bengtsson, 2016). An online repository will store electronic data for five years.

Data Analysis Technique

Qualitative data analysis covers the processes involved in organizing data, scanning the data collected for identifiable themes through coding, and assigning meaning to the data (Plamondon, Bottorff, & Cole, 2015). Data analysis used coding and thematic analysis. Coding reduced the data collected into identifiable themes. The use of coding allowed classification of data into meaningful essence or themes used to determine the relevance of collected data to the subject of study. Data identification and analysis were the basis for identifying themes. The analysis so described is thematic analysis (Nowell, Norris, White, & Moules, 2017). Data triangulation was employed to deepen the understanding of themes that came up around the phenomenon of the study.

Data triangulation permits the use of at least two data collection methods to explore a phenomenon (Kern, 2016). Triangulation also minimized all types of bias and helped to explain the phenomenon better from multiple data sources with the observed convergence or otherwise of ideas.

Initial data were organized into folders by collating data from each organization being studied into individual folders, as shown in Figure 1.

The transcription of nontextual data, such as audio files, took place into text. The data conversion was necessary because initial data were interview recordings. A transcribing service transcribed interview transcripts to text. Subsequently, The use of coding identified patterns of interest and labeled in increasing numbers, as depicted in Figure 3, across the transcribed data for each organization. To determine if there exists an intersection of ideas and concepts in the data collected from various organizations, I

performed further analysis of the data collected.

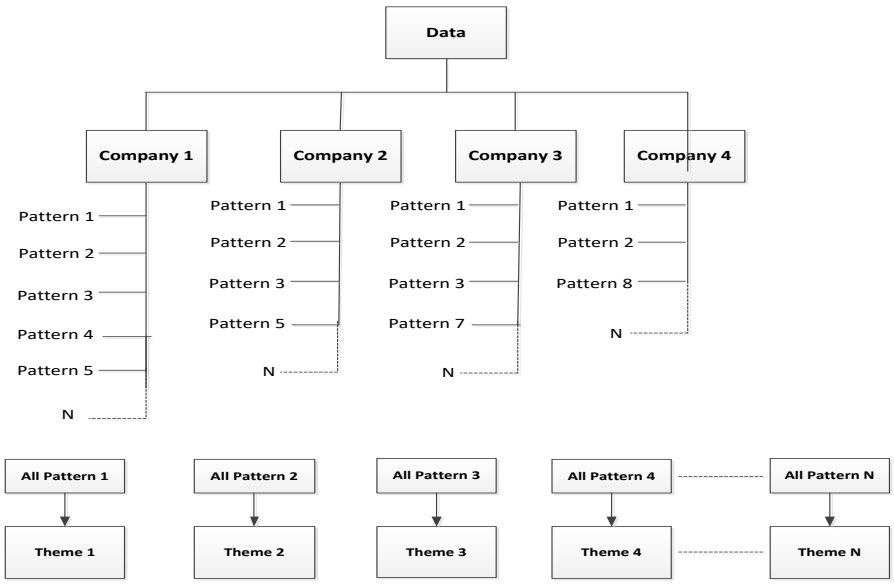

Figure 3. Data analysis, 1.

The data collected were then reviewed in the light of secondary data that were collected from individual organizations to see if they can be validated. The secondary data came from documents, reports, annual reports, and other company documents. I used NVivo software to code the data collected after identifying themes and resonating ideas. The use of the software facilitated automatic parsing of data elements and identification of data sources that have codes that are under consideration, which helped for easy collation and comprehensive aggregation. The identified patterns were useful to identify themes of resonating ideas around the subject area, which point to strategies that CISOs use to mitigate cybercrimes in financial institutions. Similar patterns across organizations were collated as a theme, as shown in Figure 3.

Consequent to the identification of the themes, the classification of aggregated themes in the context of the identified elements in the conceptual framework occurred as valid concepts of security management strategies. The components of the conceptual model used for validation are internal control and audit, risk management, management (or governance), contingency, and security theory. The mapping of evolving aggregated themes to identified concepts in the conceptual framework helped to quickly identify where elements from data sources sit in the mix. The ability to see a reasonable amount of theme mapping to identified elements under the conceptual framework validates the efforts of the organizations delivering strategies in line with the framework. The identified themes were then isolated and noted as a strategy that CISOs in financial institutions use for preventing cybercrimes in financial institutions in Nigeria, as depicted in Figure 4.

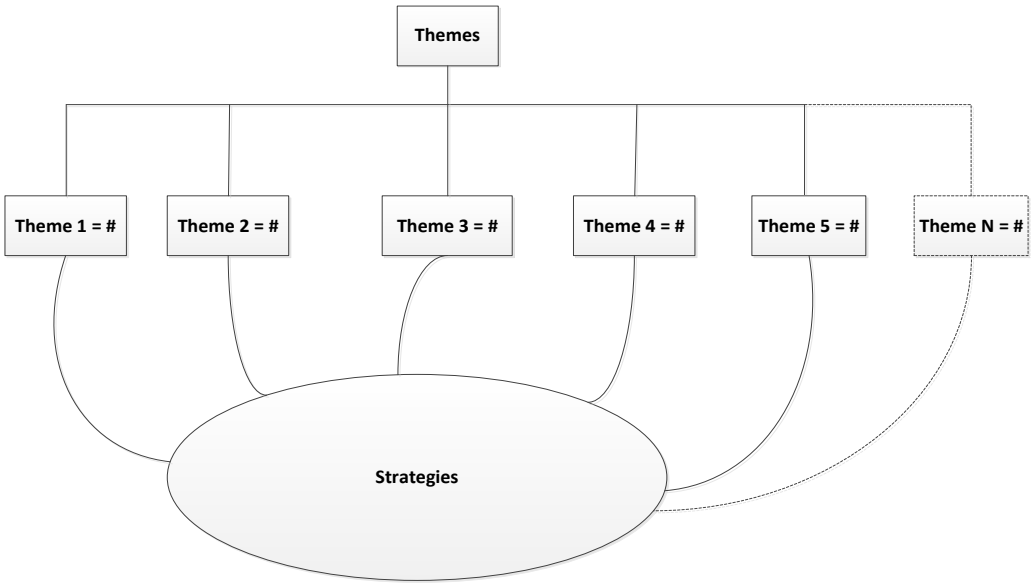

Figure 4. Data analysis, 2.

Reliability and Validity

Qualitative research ensures reliability and validity when credibility, transferability, dependability, and confirmability are established (Morse, 2015). Transferability, dependability, and confirmability came from similar principles, such as member checking and triangulation (Yazan, 2015).

Reliability

Reliability is the quality of being trustworthy always. It describes the quality that a study will produce consistent results all the time (Spiers, Morse, Olson, Mayan, & Barrett, 2018). The consistency of the results of a study ensures the dependency on the outcome of the research always. Reliability and dependability ensure the repeatability of research by other researchers with similar results. The context of the research was described in detail to ensure that the same results will be obtained under similar conditions by other researchers. Persistent engagement, persistent observation, triangulation, and member checking are methods used to achieve dependability on the outcomes of research (Korstjens & Moser, 2017a).

Dependability

Dependability indicates that the outcome or conclusions of research will always be the same under the same conditions. Dependability defines repeatability of outcomes. I documented the specific contexts of the participating companies clearly, identifying the conditions that are similar to ensure dependability. The proper capture of contexts in research prevents wrong conclusions, which could make study outcomes not dependable (Korstjens & Moser, 2017b). Member checking, triangulation, detail transcription, and

coding are some of the practices used to achieving dependability in research (Gunavan, 2015). Detail transcription ensures that results from research are from the data analyzed and thereby improve dependability (Castleberry & Nolen, 2018). Member checking helped confirm that the opinions expressed by participants were correct as recorded. It also provided an opportunity for corrections of wrongly captured opinions and views where any exist. The validation of the opinions shared during interviews by participants to the interviewer after transcription will prevent the use of wrong data that is not in line with interview responses for the study. The use of member checking after detailed transcription ensured the dependability of the results of the investigation.

Validity

Validity in qualitative research describes the quality of being able to trust or believe the outcome of the study (Teusner, 2016). It is essential to prove validity in qualitative research because of the subjective nature of interpretations that go with qualitative research. The validity of qualitative research comes from data adequacy and appropriateness for the subject of the study (Spiers et al., 2018). Participants are essential or key to establish if the outcome of research makes sense and reflects the current position on the subject matter. Member checking and triangulation are techniques used to establish the trustworthiness of information to support the believability of outcomes of the study. Triangulation provided credibility and hence, the believability of findings of the research. Member checking ensured that the views expressed during interviews were correct as recorded to ensure outcomes of the research is trustworthy, according to Cypress (2017).

Credibility

The credibility of a qualitative study establishes that the outcome of the research is believable from the view of the objects of research, the participants (Birt et al., 2016). The transcripts of the interviews were summarized and sent to the participants for review and confirmation to achieve credibility. Member checking helped to validate that the summarized details of interviews agree with the views the interviewees shared earlier. Respondent validation is one of the means to achieve credibility in qualitative research (Connelly, 2016). Lack of confirmation or review of the views captured for the participants in a study may make other researchers struggle to believe the outcome of the research (Iivari, 2018).

Confirmability

Confirmability establishes the extent to which results of the research can be corroborated by others, even though each researcher brings individual uniqueness to the study. Steps for checking results were documented and made available to establish confirmability for reliability and validity. The study achieved confirmability of outcomes through triangulation. Fusch and Ness (2015) described the use of data triangulation for confirmability. When data sources address the same research question, they are useful for achieving confirmability (Lawlor, Tilling, & Davey Smith, 2017). The use of the interview protocols eliminated bias and ensure consistency in the interviews of participants from the different companies participating in the study. The use of bracketing techniques eliminated personal bias during the interview process. Bracketing technique

ensured the suspension of personal opinions in the course of the study to avoid bias in line with Gearing (2004).

Transferability

Transferability captures the extent to which research findings can be generalized or used in other contexts, other than that set for research (Moon, Brewer, Januchowski-Hartley, Adams, & Blackman, 2016). Enumeration of the contexts of the findings of the research defines the level of transferability (Leung, 2015). Limitations, delimitations, and assumptions were well documented such that CISOs who will use the outcomes of the research could make accurate judgments about the transferability of the research outcomes. Several people who did not participate in the study also reviewed the results of the study. The reviewers have similar characteristics to the participants. The objective was to see if the findings resonate with their experiences. The disposition of non-participating individuals has helped to confirm the transferability of the findings. Outcomes of studies are judged for transferability if findings resonate with participants with similar characteristics in a study but do not participate in the study (Kamravamanesh, Kohan, Rezavand, & Farajzadegan, 2018).

Transition and Summary

The previous section was a description of the methodology used to accomplish the research process. I used the qualitative method because of its suitability for the study. The methodology chosen allowed for the use of semi-structured interviews and historical records. The method helped to discover strategies that CISOs deploy to prevent cyber exploitation in financial institutions in Nigeria. The subsequent section will show the

findings of the study. The next part also details out the application of the study to the field of IT and the implications for social change. Then follow potential areas for future exploration around the topic of the research with recommendations.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

The purpose of this qualitative multiple case study was to explore strategies that CISOs deploy to prevent cyber exploitation that jeopardizes the confidentiality, availability, and integrity of information within financial institutions in Lagos, Lagos State and Abuja, Federal Capital Territory, Nigeria. Despite the growing spate of information security issues, some financial institutions do not have strategies to combat information security issues. I sought to identify the directions CISOs are looking at as they provide information security. The intent was to derive best practice strategies that financial institutions without current cyber strategies can adopt for their operations.

Presentation of Findings

The overarching research question was, "What strategies do CISOs adopt to prevent cyber exploitations that jeopardize confidentiality, availability, and integrity of information in Nigeria's financial institutions?" As a result of interviews with six participants and a review of 12 company and public documents, several definite and specific themes emerged. The themes include (a) policies, processes, and procedures strategies; (b) people strategies; (c) corporate strategy-related plans of actions; and (d) technology strategies. Under these themes are several subthemes that had emerged in the review of the literature.

Theme 1: Policies, Processes, and Procedures Strategies

A major theme that arose from the data analysis relates to policies, processes, and procedures. This theme indicates that, for appropriate information security, the official or

approved way of doing things must be codified and communicated. Policies, processes, and procedures are approved practices of processing information, acceptable behaviors in the workplace that prevent cyber exploitation of information confidentiality, integrity, and availability (Flowerday & Tuyikeze, 2016). Table 1 contains the subthemes under this theme.

Table 1

Policy, Process, and Procedure Strategies

	Participants		Company Documents		Public Documents	
Subtheme	Count	References	Count	References	Count	References
Risk Management Processes	6	27	6	33	5	63
Information Security Policies	6	32	6	67	6	28
Internal Controls, Monitoring & Incident Management Processes	6	40	6	31	5	39
Other Processes	6	42	6	58	6	40

The themes related to policies and procedures cover the communicated formalities when it comes to the use of information and IT tools and services. Organizations use policies, processes, and procedures extensively to ensure the ongoing security of information assets (Stafford et al., 2018). This theme also addresses issues around the form in which IT infrastructure must exist in order to prevent exploits as they are used to process information. This theme underscores the importance of policies in the achievement of information objectives of organizations. Policies help to define principles that guide actions or procedures in the various stages of handling information assets or relating to information assets in its lifecycle. All six participants indicated that, as a

strategy, they have several policies, processes, and procedures in place to prevent cyber exploitations in the life cycle of handling and processing information.

Risk management processes. Information security risk management is the process of determining an organization's information security risks, identifying an organization's risk tolerance level, and deploying controls to ensuring information security risks are at acceptable levels (Akinrolabu, Nurse, Martin, & New, 2019). The risk management process starts by first doing extensive asset enumeration, which ensures identification and definition of the nature of all assets that need protection across all areas (e.g., people, hardware, and software). Risk profiles are also established (Hemanidhi & Chimmanee, 2017). Asset enumeration will help to determine the type and level of protection needed to prevent exploitations that undermine confidentiality, integrity, and availability of information assets.

All six participants stated that they have risk management processes in place that give directions on the deployment of efforts required for mitigating information security risks. Participant A said, "We do quarterly reports to the board risk management committee as well. Our Risk management committee quarterly looks at outcomes of risk assessments and ensure that mitigations are in place to deal with risk levels below acceptable thresholds." Participant B communicated that "Our risk management process starts by identifying internal and external risk elements." Participant C noted that his role as a CISO "involves identifying risks daily. Close monitoring of all our IT infrastructure of our environment, and that also includes identifying the right tools to deploy." Participant D's words were, "What do I think is a risk that can manifest. What can I

mitigate? What can I accept? You also look at, what do I have now?" The literature also indicated that proper risk identification makes adequate mitigations possible (Tubío Figueira, López Bravo, & Rivas López, 2019).

The six participants also stated that the use of a risk management process in determining what to do to prevent cyber exploitations is an indication of a structured or strategic approach to dealing with any arising information security issues. Participant A said his role "…cuts across several areas. It starts with what we call our information security strategy and planning." Participant B noted that as a CISO, he needs "to ensure that the bank's assets, that is information assets are secured using various techniques and methodologies." The use of techniques and methodologies indicates organization and strategy.

In addition to participants' responses, the six company documents, and the publicly available documents advocated that financial institutions in Nigeria should adopt a risk-based approach to determining strategies to mitigate information security risks. All six participants also affirmed that after doing the initial risk management to deploy strategies to mitigate information security risks, they set up processes that regularly check if deployed controls are keeping risks at acceptable levels. Tools aid in checking if there are weaknesses in controls, and typically, twice a year, they call in external consultants to check for vulnerabilities on systems as well. Three of the documents reviewed confirmed that for companies studied within the banking sector of financial services, it is a regulatory requirement; for other financial institutions, it is best practice for them to ensure that they always stay safe.

The findings agree with the principles of IST, the conceptual model that effective information security management requires sound risk management (Hong et al., 2003). All the participants indicated that they do risk management as a basis to know what strategy they need to deploy to prevent cyber exploitations. The risk management processes of the organizations studied also included contingency management, risk management, and internal controls, which are components of the conceptual model. The theory expects that the outcome of the risk assessment will determine security risk control measures (Ismail et al., 2014).

The risk management process discussed in the review of the literature earlier also aligns with the findings. The risk management process identifies risks and ensures control of identified risks to an acceptable level. The process also ensures that where risks crystalize, there are contingency provisions to address them through available controls or incident management processes (Ab Rahman & Choo, 2015). The companies indicated they have incident management processes that ensure proper management of risks that crystalizes. The organizations utilize risk management processes to determine what to do to mitigate information security risks.

Information security policies. Information security policies are sets of rules that guide the behavior of users of IT to ensure the ongoing security of information in organizations (Paananen, Lapke, & Siponen, 2020). They form the basis of defining what is acceptable and what is not acceptable (Niemimaa & Niemimaa, 2017) as well as other strategic elements of remediating information security risks. The information security policy determines the extent of the various elements that need to be deployed by

organizations to prevent cyber exploitation. The policy gives the direction of what technology and processes need to be in place to ensure ongoing information security of information assets (Niemimaa & Niemimaa, 2017). This subtheme defines the fact that for organizations to be secure, the strategy must include the definition of appropriate policies that will handle every foreseeable risk. Additionally, the policies are not isolated; it has to be done or crafted in the context of business imperatives of the organization (Stafford et al., 2018). Policies are only useful to the extent that it takes into account identified risks during the risk assessment process that forms parts of the risk management process.

All six participants stated that they have information security policies that set the direction for efforts for information security risk management. Participant A said, “before a profile of a new staff member is created on the network, he or she must have passed through our short induction process by reading our Information security policy.” Participant B implied the existence of policies when he said “All those experiences that we have gathered enabled us to put policies, measures in place.” Participant E indicated that “We ensure that not only that the people are aware of our strategies, they are aware of our policies, they are aware of the procedures, they know their role” indicating the existence of policies.” Participant F indicated that “Yes, we have an information security policy in place that guides information security behavior.” The company documents examined also confirm that this was the practice, and the publicly available documents affirmed that information security policies must be in place as a sign for a company to demonstrate seriousness in information security management.

The IST of information security management expresses that security policies are essential for information security management (Hong et al., 2003). Organizations create policies in strategizing for information risk management, which consider the peculiarities of the organization and especially the technology in use in the organization. This pattern of behavior is consistent with literature indicated that policies exist to ensure the safe use of technologies to avert loss of confidentiality, integrity, and availability (Leung et al., 2015). Other literature also noted that for adequate internal controls, policies that describe acceptable use of technology tools must be in place. Literature also identified that policies help to know where there are violations during the process of monitoring information security. The policies ensure that technologies are deployed in such ways as not to lead to losses to the organization through cyber exploitations. The findings of the study showed that organizations deployed policies in line with the expectation of the conceptual model and documented literature.

Internal controls, monitoring, and incident management processes. This subtheme captures processes and operational procedures that check that operation is in line with approved policies, rules, and regulations. Internal controls ensure the implementation of necessary controls policy, procedures, and technologies in the right ways to mitigate risks during risk identification and analysis in the course of the overall risk management process (Rae et al., 2017). Internal control mechanisms also ensure that there is compliance with organizations' approved way of doing things in order to control information security incidences. Monitoring helps to achieve the objectives of internal control.

This subtheme also includes processes that give directions on handling incidences if they occur in order to reduce the impact on the organization and to prevent future occurrences of the incidence (Ab Rahman & Choo, 2015). The incidence management processes ensure the use of lessons learned from information security incidences in the process of generating strategies to prevent cyber exploitations of confidentiality integrity and availability of information assets. These processes can also imply sharing information with external groups or regulatory institutions that the organizations are obliged to make such reports to. Participant B, who was in an organization within the banking sector of the financial services sector in Nigeria, said, "We make a report of incidences to regulators and the antifraud advisory group set up when there is an incidence, to especially help others to learn from our experience . . . some are major, some are minor." This fraud-monitoring group evaluates the nature of incidence and advises other participating institutions of the incidence, so it does not affect additional victims. Having an incident management process by organizations with external feedbacks could be a strategy for preventing cyber incidences. Previous research also suggested having a process that reports incidences to external stakeholders as well as advocates automation of the process (Wagner, Mahbub, Palomar, & Abdallah, 2019).

All six participants mentioned that they have internal controls, monitoring, and incident management processes in place as a means to prevent cyber exploitation that can violate confidentiality, integrity, and availability of information assets. Participant A said, "Yes, we have an internal control function that works. We are security compliant." Participant C noted that "As part of the requirements in that Security Operations Centre

[SOC] arrangement is an intelligence. The intelligence gathered through SOC monitoring is used in the incident management plan." Participant E, giving insight to availability of monitoring and incident management process, said, "Information security has its incident management and review team." Although most of the participants did general monitoring to pick potential violations of policies or procedures or cyber exploitations, Participant B indicated that apart from monitoring general users, they monitor people that are monitoring others as well. He said, "We monitor our users and administrators so that we can monitor what they do. We also monitor those who monitor the administrators." The same participant indicated that their monitoring is very granular, identifying what connections their internal computers are connecting to even where it does not indicate an attack in progress. This monitoring has evolved out of managing previous incidences that they have experienced.

The public documents and company documents also showed that internal controls, monitoring, and incident management processes are recommended processes for an effective information security management program. The IST for information security management requires that organizations must provide for contingent management of situations where exploits occur (Ismail et al., 2014); the incident management processes mentioned by the participants is a means to respond to contingencies. Additionally, the IST noted the need for internal controls, which also emerged from the analysis of responses of participants. Thus, the outcome of the study agreed with IST that for effective information security management, there must be adequate internal controls and strong contingency management efforts (Hong et al., 2003).

The literature also supported the contingency theory of the IST, along with participants' responses. Based on the review of literature, AI tools provide solutions to address information security issues, even those not already known. Defense-in-depth is another way that provides for contingencies in information security. Tools deployed as controls by participants indicate their embrace of the defense-in-depth principle and implies that the findings align with existing literature.

Other processes. Other processes cover other fixed practices in organizations that ensure the safe use of information assets. They include processes such as the use of NDAs when sensitive information is to be shared, secure destruction of hardware, ensuring no single individual can complete sensitive operations (segregation of duties), and processes that ensure patches are applied regularly to IT systems. These processes also cover *clean desk* processes; least privileged access to systems, which ensures that users get just access they need to complete the processes they oversee; document classification that ensures documents are labeled with sensitivity labels to ensure secure handling; and system hardening to reduce attack surfaces of application and computer systems by disabling nonessential services and ports. The use of server infrastructures for single applications is part of other processes that ensure information security. The other processes involve the use of role-based access for users accessing applications, and ensuring separation of test and live application environments to achieve ongoing availability of information assets, a critical element of information security.

All six participants mentioned they have all the processes earlier described as a strategy to prevent cyber exploitations in one form or the other. Participant B pointed out

that they have a process that assigns access by roles when he said, “As a teller, if all you need to do is to post. They will give you the access that will enable you to post transactions up to a maximum limit.” Participant E indicated that “There is IT change management process in place. There is the IT configuration management process in place” in their organization that prevents unauthorized changes to IT infrastructure. Participant E further indicated that they have processes in place to harden or secure endpoints that connect to their IT infrastructure. The process came up because they see their infrastructure as a national infrastructure within the financial services, and any violation can impact on national security. The efforts of organizations concerning these processes show provision for contingencies as required by the contingency theory of the IST chosen for this study. These efforts also agree with the requirements of risk management theory, a vital theory of IST. An earlier review of literature categorically indicated that technology alone could not address the problem of cyber exploitations in financial institutions. The literature reviewed indicated that processes, policies, and technology together deliver desired levels of information security (Stafford et al., 2018). Findings show that institutions use a variety of processes to stay safe from cyber exploitations. It, therefore, goes to indicate that the findings agree with existing literature and conceptual theory.

Theme 2: People-Related Strategies

People-related strategies are plans of actions related to human subjects in organizations which financial institutions deploy to prevent cyber exploitations. They are strategies that prevent social engineering attacks or attacks that appeal to the emotional

nature of human beings. The component plans considered under people-related strategies are as captured in Table 2.

Table 2

People-Related Strategies

	Participants		Company Documents		Public Documents	
Subtheme	Count	References	Count	References	Count	References
Information Security Awareness	6	28	6	21	3	15
HR Processes	6	27	6	18	6	13
Technical Training/Skills of Information Security Practitioners	3	8	2	3	5	12

It is a common belief that even where other controls are in place, people can allow evasion of controls (Ghafir et al., 2018). People-related strategies also cover efforts to train individuals on acceptable behavior to prevent cyber exploitations of confidentiality integrity and availability of information assets (Bauer et al., 2017).

People-related strategies cover equally tactics to prevent cyber exploitations by deterring staff through the integration of human resources with information security efforts. It includes the application of sanctions, information security awareness campaigns, and extend to possession of a proper skill set by technical professionals saddled with information security management tasks. People-related strategies address potentiality for human errors that lead to a breach of information security. The people-related strategies also involve efforts that companies make through human resources to forestall insider related threats, which were a significant concern to four of the participants. All six participants believed that people related strategies are essential to

achieve information security goals. The discussion of subthemes identified in Table 2 follows below.

Information security awareness and education. This subtheme relates to the efforts made to ensure staff, IT systems users, senior management, contractors, trading partners, and everyone in the ecosystem of the financial institution are aware of their roles and functions in the information security chain. It covers making relevant stakeholders aware of policies, procedures that need to be complied with, which organizations deploy to prevent cyber exploitation that can jeopardize confidentiality, integrity, and availability of information assets. Information security awareness encompasses efforts to communicate acceptable practices to ensure that users, staff, and partners are not working unconsciously to undermine confidentiality, integrity, and availability of information in organizations (Torten, Reaiche, & Boyle, 2018). It extends to knowledge of what to do when potential scenarios that can jeopardize confidentiality, integrity, and availability arise.

Five of the participants mentioned that even where technology controls to prevent cyber exploitations exists when people are not aware of their roles in the chain of information security, they can jeopardize deployed protections inadvertently. Participant A said, “For the people aspect, we come up with a security awareness program wherein every month we have a newsletter that talks about the topical issues that are involved in security.” Participant E as well noted that “We do much awareness, and while the awareness is ongoing, we also do the check and balances. People know what to do, and people know that when there are infractions, you know they are consequences to it.”

Participant F on his part said, “Yes, and awareness is key because even if you deploy securities technologies and you did not do the awareness, the people would tend to breach the security guidelines, but if they are aware of the risks of their activities, they will protect the informational technology.” Three of the participants noted that, because of the importance of this as a strategy, they consider the ecosystem they are in for information security awareness. They organize information security awareness not just for their staff, but for people who interact with their IT infrastructure at any level. One of these participants works at a financial institution that is considered part of the national infrastructure; the others work at deposit money banks. Two of the participants indicated that they conduct follow-up assessment tests after information security education in order to ascertain that each staff is aware of policies and procedures that engender information security.

The efforts of organizations to ensure that staff and trading partners are aware of policies and procedures that prevent cyber exploitations are consistent with the tenets of the conceptual model. Security policy is one of the elements that the IST indicates must be in place for an effective information security management program (Ismail et al., 2014). The efforts towards information security awareness are also in line with risk management theory, a vital theory of IST (Hong et al., 2003). Adequate training for staff on information security matters addresses the human-related risk factors (Abraham & Chengalur-Smith, 2019). It also ensures that efforts to achieve the demands of contingency theory are not futile because people learn to keep controls deployed to address contingencies in place as specified by policies. Six of the participants indicated

that they have a mechanism of conducting awareness campaigns. Mechanisms used for such information security awareness are the use of roll-up banners, use of intranet, e-mail broadcasts, and seminars. Four of the participants also noted that as a strategy, the onboarding process of new staff includes awareness of information security responsibilities.

The findings which indicate great efforts of companies at conducting information security awareness and training also agrees with literature. Hadlington, Popovac, Janicke, Yevseyeva, and Jones, (2019) affirms that in recent times there has been increasing attention to the roles human factors play in achieving cybersecurity. Diesch, Pfaff, and Krcmar, (2020) also noted that for effective management of information security risks, organizations need to combine technical and non-technical measures. Non-technical measures they note must address human factors. The outcome of the study showing increasing efforts around information security awareness to address human factors is, therefore, consistent with the literature.

Technical training/skills of information security practitioners. Three participants mentioned that for successful efforts in preventing exploitation of information within Nigeria's financial services, it is crucial to deploy mechanisms to have CISOs and practitioners that are technically knowledgeable and experienced. Four of the participants identified the need to have practitioners that have certifications such as certified information systems security professional, certified information systems auditor, certified information security manager, certified in risk, and information systems control. Participant D mentioned this as

> Practitioners can have several technical certifications. Let me start with the Ph.D. of Information Security. It is called CISSP—Certified Information System Security Professional. Coincidentally, we will be going for the same training in December. We have a Certified Information Security Manager, and we have other technical roles like Certified Ethical hacking. You need a bit of project management.

One of the participants indicated that beyond technical IT and information security knowledge, it would help if the practitioners understood the business process related to the organization they are trying to protect. Five of the participants interviewed have at least six years' experience in the role of CISO.

The fact that five of the six participants each have at least six years' experience on the job implies that they would have had training in the identified certification areas in one way or the other. The ISO 27001 certification requires some level of training for practitioners before the certification is issued. All of the participating organizations have the ISO 27001 certification. One of the participants also indicated that project management knowledge would be helpful for information security practitioners, so they need as a strategy, training on project management discipline. He attributed this to the fact that information security risk mitigation requires projects to deal with new information security risks. The public documents reviewed also corroborated this requirement. The IT standards document and the Nigerian government's Central Bank of Nigeria risk-based document mandate that CISOs must be CISSP or certified information systems auditor (Balogun, 2018). The job descriptions of the organizations studied also

expect holders of the CISO role to have those certifications. At least three of the participant companies showed evidence of investing heavily in training their information security practitioners.

The findings agree with the IST. Hiring skilled individuals to look at information security prevents errors in the configuration and implementation of information security policies and controls. Hiring skilled staff is part of risk management. It also ensures that skilled individuals are available to manage incidences if they occur. Adequate skilled staff for business contingencies provides for the contingency management of information and ensures identified risks are well managed. Risk management and contingency management are core aspects of the IST. The findings also agree with the literature. The Apex banking regulation in Nigeria mandates CISOs to have specific certifications and skills before they can take on the CISO role (Balogun, 2018). Haqaf and Koyuncu (2018) also recommend the CISSP certification as a foundational certification for anyone that will be an information security management practitioner. This position is consistent with the findings of the study that a strategy for effective management of information security risks will include having practitioners with proper and relevant technical skills. The process of having specifically recommended certifications makes the requisite skills available in information security practitioners.

Human resources processes. The six participants noted that the human resource (HR) function in their respective organizations is involved in the implementation of their information security initiatives. Participant A said, “at the induction stage, we have been able to integrate our Information security management to the HR evaluation process.”

One key area of the involvement of HR is in the area of ensuring that individuals for any job role in the organization are background checked before employment. The intention is to keep out potential hackers or people with questionable dispositions that can violate confidentiality, integrity, and availability of information from organizations. Participant C said, “We make sure that the hiring process is stringent. Of course, before hiring, there is evidence of background checks of staff.” Participant E said they do reference checks saying, “Okay. What we do with HR, we work with HR to do this. Number one, we do a reference check.” Participant F said, “You need to know the character that you are hiring. Whether they are of good character or not. That is the essence of the background check” The background check process as a strategy according to the six participants, help to deal with insider threats which were a concern to five of the participants. Two of the participants’ companies also do a check against a regulatory database before engaging new hires. They are also bound to report any staff that exited their organizations for fraudulent activities to improve the usefulness of the regulatory database.

The participants indicated that the HR function is involved in the application of sanctions whenever there is a violation of information security policies designed to prevent cyber exploitations of confidentiality, integrity, and availability. One of the participants indicated that breaches of information security policies could lead to dismissal. Another participant clarified that depending on the severity of information security violations, staff might go through disciplinary actions. The intent of the inclusion of information security violations as punishable offenses in an organization is to prevent conduct that will undermine information security. HR also sends a notification to the

information security officer whenever a staff is exiting the organization so that the relevant information security officer can remove accesses of staff to prevent misuse at their exit from the organization. The process of eliminating staff access to systems is a reverse HR process where HR communicates the role of staff during onboarding to ensure strict provision for applications and systems that staff needs for their regular work duties.

The study, through the subtheme, agrees with the tenets of IST. The process of background check ties to the process of assessing the risk profile of potential employees to an organization and tends to determine whether the hiring will undermine information security. The process of training staff also speaks to mitigating risks that can arise due to inept staff managing information security. Training is also a form of deployment of controls under the internal control theory of IST. Background checks and staff training agree to the requirement of the conceptual model IST that adequate information security requires proper risk management and internal controls. An evolving fact from previous literature reviewed expects comprehensive risk management to drive information security strategy (Ali et al., 2017). Background checks and training are risk management efforts. The findings show that the companies studied invest efforts in several HR processes, of which some are training and background checks, which are risk management efforts. The study, therefore, agrees with existing literature.

Theme 3: Corporate Strategy Related Information Security Plan of Actions

This theme describes things that organizations do to prevent cyber exploitation of confidentiality, integrity, and availability of strategic information assets. These efforts are

peculiar to organizations because of the businesses they do within the financial services and, in some circumstances, the sensitivity of the organization to national security. The nature of the business of an organization affects the technology in use and, subsequently, information security risks that require mitigation (Weyrich & Ebert, 2016). Table 3 shows the subthemes that make up this theme.

Table 3

Corporate Strategy Related Information Security Plan of Actions

	Participants		Company Documents		Public Documents	
Subtheme	Count	References	Count	References	Count	References
Management Processes	6	27	6	13	4	19
Compliance & Regulatory	6	15	6	8	5	9
Alignment to Corporate Strategy	6	13	2	2	5	12

The subtheme also addresses efforts by the executive, and board-level management to perform due care and due diligence, responsibilities expected by regulation and trading partners. These issues show the direct actions of CISOs as a result of specific corporate strategic inclinations. The efforts here cover specific policy implementations as an effort to prevent cyber exploitations and the creation of various management committees who have the oversight of the information security function. The CISOs typically bring the need for such initiatives to the executive and board level management who sanctions such initiatives as a strategy to stay secure.

Management processes. These subthemes describe the efforts of the executive leadership of institutions towards ensuring the achievement of information security

management objectives dictated by the strategic imperatives of the organization (Andress & Leary, 2017). Organizations adopt standards as a means to establish management standards for information security management (Meriah & Arfa Rabai, 2019). All six participants affirmed that they have in place the ISO 27001 standard that provides the framework for information security management within their organizations. All the available organizational documents confirm the availability of such management processes. Four of the six public documents reviewed also corroborated that organizations within financial services have such management processes that are part of their strategies for effective information security management.

The findings agree with the chosen conceptual model, which is IST. The IST for information security management advocates the existence of management processes to have a holistic information security management process. The need for robust internal control and monitoring processes are critical outcomes of the study. Internal control is one of the management processes that organizations use to ensure compliance with policies and achieve information security. Internal controls are evident in the adoption of frameworks and standards for information security management. The organizations studied have all adopted the ISO 27001 standard. The outcome of the study, therefore, agree with the expectations of IST, which requires internal control to be in place for information security management (Hong et al., 2003). Reviewed literature also indicates that the COSO framework provides a means for top-level executives to perform their due diligence role in the area of preventing cyber exploitation of information assets (Lanz, 2017). The COSO framework aligns risk management with the strategic objective of the

organization (Karanja, 2017). The COSO framework is an internal control framework. The alignment of risk management to the strategic objective of organizations studied shows that the findings of the study, which shows organizations have in place internal controls by the adoption of relevant standards and deployment of efforts for risk management, agrees with literature.

Compliance and regulatory strategy. This subtheme relates to information security initiatives that organizations embark on to achieve regulatory compliance. The need for compliance is closely related to the earlier discussed management processes subtheme. Financial institutions in Nigeria are all required by the Apex Regulatory Bank–Central Bank of Nigeria to have in place ISO 27001. All banks that process cards for payments are also to be PCI-DSS certified (Central Bank of Nigeria, 2019; Omotubora & Basu, 2018). Effective August 2019, all financial institutions in Nigeria are to comply with the NITDA's Nigeria data protection regulation (National Information Technology Development Agency, 2019). All six participants answered that they have in place efforts that demonstrate compliance with the applicable regulations to their organizations. This information security strategy could be as simple as a strategic directive of executive management mandating CISOs to get particular certifications because they are operating certain lines of financial services or because they operate within Nigeria.

All six participants are ISO 27001 certified; four mentioned they are Nigeria data protection regulation-compliant as well. Two of the participants who are within the Nigerian banking sector confirmed that they are also PCI- DSS compliant because they

process cards for payments. Compliancy implies that they deploy strategies that were mandated by the applicable regulation and standards. The PCI-DSS requires the deployment of 12 controls; this means the organizations have in place control across the 12 areas. The PCI-DSS control deployment intersects with the internal control processes discussed above, which are a core requirement of the IST. The adoption of standards such as ISO 27001 also affirms the presence of management processes that agrees with the expectation of the IST for information security management. This position is also in agreement with literature that states that organizations adopt standards to ensure mitigation of all possible risks in a comprehensive manner (Meriah & Arfa Rabai, 2019). The use of standards to mitigate information security risks also agrees to the risk management component of the IST.

Alignment to corporate strategy. This subtheme relates to specific practices or efforts in organizations that are in place to ensure an appropriate level of protection to ensure confidentiality, integrity, and availability of information assets that match or are commensurate with the strategic objective of the organization. All six participants mentioned that they have some strategies or practices that may be peculiar to them, which other organizations may not have in place except where their business strategies are similar. Participant C indicated that his organization keeps its ecosystem close to be safe, saying, “One of the benefits that we had is that we always kept our ecosystem very closed through minimal interactions on day-to-day with external firms due to the nature of our business.” The process of maintaining a closed ecosystem is one of the concepts identified in the review of literature as security by obscurity (Rasekh et al., 2016).

Participant E mentioned that they uniquely identify and configure for their environments endpoints that connect to their infrastructure because of the sensitivity of the IT platforms. She had said, “Another thing we have done is that the only system that is allowed connection to the enterprise is our company-owned system, and all the ports are locked down because we manage a national infrastructure and stakes are high.” Participant B said that they are exploring innovative strategies such as micro-segmentation within local area networks to control what endpoints connect to ensure the security of information assets because of the peculiarity of risks they face in their ecosystem. Participant B said, “To prevent attacks. It is end-to-end. I have my firewalls and implement micro-segmentation. We do Micro-segmentation, implying that these systems even though they are in the same room, they cannot talk to each other except they are expressly allowed to, this is to cut out malware, which could be an issue for our business.” Participant A mentioned that they had developed secure application deployment templates which they make available to developers because of their adoption of coding methodologies such as agile to build information security into applications. He said, “What we do, we have an application security baseline document which details minimum security measures that need to be put in place when you are developing your web apps, where you are developing mobile apps.” The organization uses agile to compete strategically within the market they play in the financial services.

Two of the company documents validated the position that organizations deploy specific strategies in line with their corporate strategy to be secure. Five of the public documents examined expects that organization should take into account their business

strategies in evolving plans of action for information security management. IST agrees with this position because the risk management theory of IST expects that information risks to being mitigated will be related to the nature of IT tools in use because of the business strategy. The risk management theory of the IST theory noted that through risk analysis and assessments, there is the identification of the threats and vulnerabilities of systems, which influences controls deployed to ensure the security of information assets (Han et al., 2016). The literature also agrees with this position. Existing literature indicates that risk analysis must be structured, deliberate, and aligned to technologies deployed (de Gusmão et al., 2016). Corporate strategy determines lines of business and, consequently, types of technology in use in organizations. The findings of the study show that organizations do risk analysis in alignment with corporate strategy. The preceding affirms that the findings agree with the literature as well.

Theme 4: Technology Strategies

The technology strategies theme describes IT tools and services used to ensure there is no violation of confidentiality, integrity, and availability of information assets. It covers technology solutions in place to achieve defense in financial services companies. The technology-related strategies affect the network, applications, databases, operating systems, endpoint, or user devices and other technology tools within the IT environment of organizations. Technology tools support the enforcement of approved policies in organizations, and they also support processes that enhance information security (Amin, Shah, Shah & Alfandi, 2016). Technology strategies provide a well the means to address

routine but manual information security tasks through automation. Table 4 details the components of the technology theme.

Table 4

Technology Strategies

	Participants		Company Documents		Public Documents	
Subtheme	Count	References	Count	References	Count	References
Other Technology Strategies (SIEM, Encryption, Doc Classification..AntiPhishingetc)	6	27	5	22	6	15
Application & Operating System Security Strategies	3	11	4	27	5	24
DataBase Security Strategies	4	7	5	12	2	7
Endpoint Security Strategies	3	8	4	18	2	3
Network Security Strategies	5	14	5	30	5	18

Other technology strategies. These are technology tools other than the network, database, and application security technologies deployed to prevent cyber exploitation that violates confidentiality, integrity, and availability of information assets. These technologies are encryption technologies that ensure confidentiality of information (Ghadirli, Nodehi, & Enayatifar, 2019) and information classification tools that label information with classification labels to ensure information users handle information appropriately to ensure security. Other technology plans of action include antiphishing tools that identify fraudulent websites to organizations and customers before they are used to exploit customers (Mao et al., 2018). The “other technologies” strategies

subtheme also covers SIEM tools that support logs aggregation and correlation with notifications or triggers for risky events.

The SIEM tool monitors policy violations and to trigger control mechanisms before they become incidences. The tools serve as mechanisms to respond to contingencies or exert control. The field of AI is one area that is influencing the nature of other technological tools being deployed by organizations to mitigate information security risks (Diro & Chilamkurti, 2018). AI has also proven to be a veritable means to extract ongoing value from SIEM solutions (Hatcher & Yu, 2018). All six participants mentioned that deployment of these other tools is essential as a strategy to prevent cyber exploitation of information assets. Participant D said, “Another thing is data loss prevention. We have a solution in place such that if you attach a memo that is confidential on your corporate email and send it to my friend, for example, in GT bank because it is confidential, administrators will be notified.” Participant E also said that “Every document is classified. Those are not the only things that we do but like I said, we ensure that we will put optimal processes in place. We are also in the process of implementing a Data Loss Prevention (DLP) solution.” Five of the company documents examined corroborated this position, while all the public documents reviewed showed that these technology tools, when deployed, strengthen information security in organizations. The utilization of the discussed IT tools needs to be part of organizational strategy.

The use of these other technologies indicated the organizations make provision for contingencies. The use of these technologies by participating organizations to address

contingencies of information security is in line with the expectation of IST according to the constituent contingency theory chosen as the conceptual model for the study. The other technologies subtheme also provides ideas about technological tools that organizations deploy to exercise control over IT systems to prevent misuse and violation of confidentiality, integrity, and availability of information assets. The process of maintaining controls to ensure the safe use of IT systems is under the internal control theory of the IST (Hong et al., 2003). It, therefore, means that the findings of the study are in congruence with the expectations of IST.

Existing literature also indicates that Google and Amazon are among the many technology giants that currently use machine learning in the area of information security management (Diro & Chilamkurti, 2018; Hatcher & Yu, 2018). Google currently uses ML to analyze threats against mobile endpoints running the Android operating system. Amazon utilizes machine learning to achieve data classification in its S3 cloud storage services offerings. The companies studied are utilizing cloud services for their operations. They are also actively involved in mobile device management and data classification. The use of cloud services indicates they are using the underlying protective technology tools for information security management as well. It, therefore, shows that the findings agree with existing practice shown in the reviewed literature.

Network security strategies. Network security strategies are efforts directed at securing the network path that information transverse as various IT systems provide financial services to customers and conduct business. The subtheme describes efforts that cover strategies such as network segregation and defining separate network security

levels, which prevents direct access to applications from the Internet. Such strategies address the creation of demilitarized zones for untrusted access and extranet networks for trusted partners (Upadhyay & Sampalli, 2020). The creation of network segments allows for the provision of an appropriate level of security to prevent cyber exploitations (Arief, Khakzad, & Pieters, 2020). Network security strategies involve the deployment of firewalls that protects secure from unsecured networks.

The network security subtheme also covers the setup of network intrusion detection systems and intrusion prevention systems that proactively identify cyber threats on networks and prevent them from becoming an incident (Koucham, Mocanu, Hiet, Thiriet, & Majorczyk, 2018). The intrusion detection systems and intrusion prevention systems use AI systems discussed in the review of literature through the use of supervised, semi-supervised or unsupervised learning mechanisms (Khalili, Sami, Khozaei, & Pouresmaeeli, 2018). Network security strategies also involve preapproving systems that have access to networks to use IT systems through the use of network admission control systems

Another critical component of network security is the SIEM, which collects and correlates logs and alerts from network components and notify of pending attacks before they become a problem (Sharafaldin, Lashkari, & Ghorbani, 2019). Five of the participants mentioned they have in-place network security solutions. The other participant merely implied they have systems in place that protects the network. Participant A said, “We have a web application firewall that protects internet-facing applications against a myriad of attacks.” Participant D said, “We are reoptimizing our

network admission control solution," indicating they have a network admission control solution in place. Participant E also said, "Even in connecting internally or externally, and beyond that, there is in place a network admission control solution in place so you know that you need to be approved before you can connect to our network." Five of the company documents and five of the public documents reviewed supported the need for organizations to have in place the items that make up network security protection in one way or the other. The use of network strategies addresses risks at the network layer in line with the expectations of IST for comprehensive risk management at all relevant areas of use of technology (Ismail et al., 2014). Efforts at the network level to manage risks is also consistent with the recommendations of reviewed literature that defense in depth principle will help manage IT risks. The defense in depth principle encourages the modular application of mitigation, where risks are first encountered (Conteh & Schmick, 2016). The defense in depth principle ensures that the security of IT infrastructure requires multiple measures at different points of a system, such that if one measure fails, other available measures can still prevent breaches (Mansfield-Devine, 2016a). In this context, the network layer can mitigate a failure at any other layer. It, therefore, implies the use of the strategy agrees with the conceptual model because of the management of risks comprehensively as required by IST. The practices of the companies studied are also consistent with the literature, which expects that detailed asset enumeration for effective risk management in the process of achieving holistic information security management.

Application and operating system security strategies. These are practices directed at securing operating systems and applications that financial services utilize to conduct their businesses. The practices here are having a secure coding method, ensuring that applications sanitize or validate inputs to prevent attacks that can lead to potential losses (Mdunyelwa, Futcher, & van Niekerk, 2019). Application security mechanisms advocate fail-safe mechanisms where the application crashes or fails for whatever reasons (Malinowski & Czarnul, 2018). It captures mandating authentication of users before using applications; it extends as well to encryption of transaction paths to achieve secure access to databases (Ajay & Umamaheswari, 2019). Application security also ensures that accesses to applications are provisioned on a needs basis and based on roles (Singh & Sittig, 2016). Strategies for application security involves having standard approaches to coding and having proper documentation in place about the applications used in organizations. Applications are at Layer 7 of the OSI model. It is, therefore, not uncommon to see the deployment of firewall solutions that protect applications as well (Hu et al., 2019). Participant B said, “We are also investing in a solution that will protect up till application level of the OSI reference model,” and thereby implied they are making investments in a firewall solution that will provide application-level protection.

Operating system security strategies address efforts that take out nonessential services from operating systems. The practice of removing services not required from operating systems reduces the attack surface that can be exploited by cybercriminals. The security strategies here ensure that patch levels of operating systems are up to date to cover discovered vulnerabilities and weaknesses (Mugarza, Amurrio, Azketa, & Jacob,

2019). Included in operating systems security is ensuring restricted access to admin passwords and ensuring only named logons. Three of the participants noted that they have specific strategies that address application and operating systems security. One of those three participants indicated that they have standards that guide programmers when developing applications to ensure organizations use secure applications. A majority of the public documents reviewed advocate safe coding practices to prevent cyber exploitations. Four of the company documents noted practices that ensure secure application development.

Database security strategies. Database security strategies cover efforts to ensure that individuals that should not access company data do not access them. The efforts also include preventing legitimate users from abusing access given to them and making sure they have just enough access to do their job functions (Veloudis et al., 2019). Organizations, to achieve security of databases, deploy database access monitoring tools to ensure they get notified whenever there are potentially dangerous accesses (Wang, 2017). Authentication is also one of the methods organizations use to ensure security, and they make compulsory the authentication of all accesses (Wang, Weng, Ma, & Yang, 2019). Information in databases can also be encrypted to prevent unauthorized access (Kelarev, Ryan, Rylands, Seberry, & Yi, 2018; Ma, Mu, & Susilo, 2018;). One vital procedure used as well to ensure the integrity of information is to deploy applications that do not permit two applications, processes, or individuals to update databases at the same time or maliciously (Wagner et al., 2017). Organizations also prevent direct modification of databases by users to ensure ongoing information security. Five of the participants said

they deploy database security tools. Participant A said, “We have the database security, database activity monitoring that monitors privileged activities on the databases.” Two company documents captured the need for database security tools; two of the public documents mentioned the need for database security tools for enhanced information security.

Endpoint security strategies. Endpoints are user access devices or systems that provide access to information (Kemper, 2019). Those systems are laptops and desktops, personal digital assistants, mobile devices, and other devices connected to the IT infrastructure of financial institutions (Tedeschi, Emmanouilidis, Mehnen, & Roy, 2019). This subtheme describes efforts that organizations deploy to ensure that the users, while accessing information, do not jeopardize confidentiality, integrity, and availability of information. The efforts here cover the installation of antivirus systems and ensuring end-user operating systems have current patches. It also includes deploying data loss prevention systems, which ensure that users adhere to classification labels on documents (Forain, de Oliveira Albuquerque, Sandoval Orozco, García Villalba, & Kim, 2017). It involves encryption of devices such that in the event devices get lost, they do not lead to sensitive information leakage. The strategies here also encompass policies that support new computing models like *bring your own device* such that while users own devices but use it to access corporate data, there is an understanding of how to treat information to achieve information security (Kemper, 2019).

Three of the participants indicated that they have in place technology strategies that mitigate end-user information security risks. Participant A said, “We ensure that the

antivirus that we are using scans the system, removes the virus on the system." Participant D said, "Mobile device management is also in place through our bring your own device [BYOD] protection strategy." Four of the company documents reviewed confirmed this was the case. Two of the public records reviewed indicated that end-user devices need to have in place, information security strategies for related risk mitigation. The use of technology strategies and solutions for information security management is a way to provide for contingent management of information security risks. The IST has as a component contingency theory that advocates provision for contingencies in information security management. Technology strategies ultimately get setup based on approved information security policies. Technology, in effect, provide automation for information security policies. It, therefore, shows that the findings agree to the IST tenets (Hong et al., 2003). The literature reviewed also advocates the use of technology with policies and processes to achieve desired levels of information security. Available literature maintains that an acceptable information security strategy must be holistic, covering critical elements of people, process, and technology or technical components of IT (Sohrabi Safa et al., 2016). Literature does not agree with the position that technology solutions alone can deliver desired levels of information security, but that a mix of people, process, and technology-based initiatives is required (Naseer et al., Shanks, Ahmad, & Maynard, 2017).

Application to Professional Practice

Corporate Strategy Should Drive Strategies to Prevent Cyber Exploitations

Financial institutions should consider their business strategies when designing information security strategies. CISOs, while developing information security management strategies, should consider the peculiarities of the business they support and the environment in the process of recommending Information security risk mitigants. The technology landscape in organizations is influenced or driven by the nature of the business of the organization. The nature of the company determines what IT tools are in use and what data or information elements are essential to the successful operation of the organization. The position that business strategy in organizations affects the technology in use is consistent with the principles of TOE theory (Leung et al., 2015). The TOE theory explains the adoption of technology in organizations. The theory states that technology adoption is affected by the perception of the specific technology required in the organization (perceived characteristics of the technological innovation), organizational (firm's characteristics), and environmental (characteristics of the firm's external environment) factors. Organization's characteristics evolve from business nature and business strategy.

Ferreira, Frogeri, Coelho, and Piurcosky (2018) also noted business strategy determines the information of organizations, which implies that corporate strategies will influence the nature of information and information tools and methods for protection of such information. Tu, Yufei, Archer, and Connelly (2018) said that the context of organizations is essential when designing information security management strategies.

Several unique practices that came up in the study indicated that the extent of efforts and type of risk mitigating techniques is determined by what organizations prize as necessary, which is determined by their business imperatives and approach to business. An organization that sees much risk around its research department will deploy strategies to ensure that the staff of the research department does not violate confidentiality. The same organization will deploy more protection around the data or IT tools that are used by the department because any successful exploitation against the department can lead to losses that can impact the very existence of the company. Organizations that have adopted the internet as a delivery channel will have to deal with risks that brick and mortar companies will not have to consider. The risks that companies that use agile development will mitigate will be different from the ones that companies that employ more conventional and rigorous application development frameworks.

All six participants in the study indicated that they derive an information security strategy from the corporate strategy. Rothrock, Kaplan, and Van Der OORD (2018) also agreed with this position, noting that business strategy affects information security strategies. Andress and Leary (2017) also affirmed that corporate strategies affect the nature of information security strategies significantly. The participants indicated that they identify from the corporate strategy what is essential to senior management and, therefore, direct efforts accordingly to those things they note as necessary when crafting strategies to prevent cyber exploitations of information.

One of the participants noted that they configure individually endpoints that connect to their networks because a breach of security can affect national security since

they manage a national infrastructure. The process of configuring individual endpoints before allowing them to connect to their infrastructure is a form of security by obscurity because it involves renaming accounts, disabling nonessential services, hiding things from potential attackers. Security by obscurity assumes that a system has protection from violation of confidentiality, integrity, and availability, as long as the internal workings of the systems are not known to a malicious user or cybercriminal (Rasekh et al., 2016). Another participant mentioned that because they do not need to interact with many people, they keep their ecosystem close as strategy, they practice security by obscurity. One other participant indicated that because the stakes are high for them, and they are concerned with insider threats in their operations, they monitor all users and get external help to pay attention to those who watch internal users. All these are examples of plans of actions coming from corporate strategy driving information security management efforts.

The Information Security Management Role Needs to be Outside Information Technology for Effectiveness

As a strategy, organizations should look to situating the role holder for information security management outside of the IT department to achieve the effectiveness of the function. The various themes that emanated from the study showed that technology alone is not enough to prevent cyber-exploitations of confidentiality, availability, and integrity. The fact that organizations need more than technology to be secure is consistent with the view of Soomro et al. (2016). The participants in the study affirmed that they use a combination of technology, processes, and policies and procedures to achieve the desired level of information security. All except one of the

CISOs interviewed operate outside of IT. The one CISO that works within the IT department, in the study report directly to a Head of Information Technology or Chief Information Officer.

CISOs operating outside IT structure seems to be the trend with the majority of the role holders operating in the risk management group. The pattern of CISOs operating outside of IT enables them to have a holistic view of issues that goes beyond technology but covers processes and procedures to evolve strategies to prevent cyber exploitations. It also helps to have an independent role that looks at what IT does to prevent cyber exploitations. The separation of Information security management roles from IT seems appropriate because risk management, which covers information security risk management, is a top management function. Having the role with a function that has a reporting line to the board wth therefore be better. This position is consistent with the emerging regulatory framework and supported by Hooper and McKissack (2016). Inskeep (2019) suggested different CISO reporting lines based on the size of the organization, type of industry, or business strategy or imperatives of organizations. It is, however, worth mentioning that the position of Inskeep (2019) for highly regulated companies like financial institutions is that CISO should report outside of IT to the Chief Risk Officers or Chief Financial Officers, both of which are risk management roles. Feng and Wang (2019) found that Chief Financial Officers do not, as of now, influence cybersecurity risk issues in organizations, thus leaving the Chief Risk Officers as a possible reporting entity. This recommendation is consistent with the findings in the study.

Comprehensive Risk Management Drives Effective Prevention of Cyber Exploitations

Organizations need to strengthen their risk management framework to provide for every foreseeable information security risk issue. Companies should deploy mechanisms to ensure their risk management process is holistic and cover the universe of information security issues that can arise to stay safe. Information security risk management involves the process of identifying all information assets in an organization, identifying the related cyber risks, and providing risk mitigation measures to bring risk identified to an acceptable level (Akinrolabu et al., 2019). Effective risk management for information security management needs to cover all aspects of the company under consideration, her people, processes, and technology (Safa et al., 2019). Risk identification is affected by several factors such as technology products, nature of trading partners, the medium of transactions, the various people that interact with the company's IT infrastructure, and the competition (Angraini, Alias, & Okfalisa, 2019). Leaving out any information asset during asset enumeration implies the risks related to that information assets will not be identified and mitigated, which means that the asset could provide a means to exploit the company. Comprehensive risk assessment and risk mitigation protects companies from cyber exploitations. Strategies deployed in risk management can either be preventive, corrective to avert loss. The approach also can be through the deployment of policies, processes, and procedures or technological implementations (Angraini et al., 2019).

All six participants indicated that they use a structured and organized process to identify and mitigate information security risks. The risk mitigation process starts with

asset enumeration to know what to do to prevent cyber exploitations. Li et al. (2018) advocate a structured approach to risk management. The participants agreed that they do not mitigate all risks. Klingensmith and Madni (2017) indicate that it is not possible to lessen all risks. Threats that the costs of reducing outweighs loss are typically noted and documented, and top management signs off not to mitigate but to watch. This position is consistent with the requirement of ISO 27001 as well that all unmitigated risks must be signed off by top management. Management involvement in risk management decisions supports the performance of their due care and due diligence responsibilities. It is a requirement for compliance within Nigeria's financial institutions for executive management to be involved in risk management (Taiwo & Agwu, 2016).

Information Security Management Requires Advanced Technology and Information Security Operations Knowledge

Information security practitioners must ensure they have a good understanding of the technology the business they are protecting uses. They also need to have robust business and advanced information security operations knowledge. Practitioners must ensure that this knowledge is current and up to date. One key element that stood out in the course of the study is the need for practitioners to have in-depth knowledge of possible technology risk areas, and relevant mechanisms to effect protection. Three of the participants advocated specific certifications and training in order for CISO role holders and support staff to be able to effectively prevent cyber exploitations that violate confidentiality, availability, and integrity. The certifications include CISSP, certified in risk and information systems control, amongst others. The need for financial industry

knowledge was further identified as a critical requirement for the CISO role holder by one of the participants, and another identified the need for project management experience as well.

Haqaf and Koyuncu (2018) identified thirteen skills required by information security practitioners for effectiveness. Project management and risk management skills are the top two skills identified as a requirement for information security practitioners. Core information security skills form the highest percentage of the pack, while technical skills are the lowest part of the list. Haqaf and Koyuncu (2018) also noted that CISSP is the most efficient path to developing information security management skills. Evidence from the research showed that all of the institutions studied invest heavily to train their information security specialists to prevent cyber exploitations. Mansfield-Devine (2019) noted that sound knowledge is essential for practitioners to be ahead of hackers and to deploy protective strategies proactively.

To have relevant applicable strategies that protect financial institutions, they need to hire information security professionals with sound technical knowledge who also have the financial services domain knowledge. The hiring of such professionals would help the risk management process by proffering risk containments in proper measures. Mansfield-Devine (2019) noted that the availability of individuals that have requisite skills for information security roles is scarce and recommended upskilling individuals by training those that are already doing information security-related responsibilities. One effective strategy to train practitioners is to arrange a common body of knowledge (CBK) training and requesting that they write certifications after the training. The challenge to write

certification exams constrains complete coverage and revision of the entire syllabus, which will translate into actionable knowledge in practitioners for preventing cyber exploitation of confidentiality, availability, and integrity.

Information Security Awareness is a Significant Strategy for Preventing Cyber Exploitations

Information security practitioners, while deploying various strategies to mitigate information security risks, should include a robust information security awareness and training program. Organizations need to entrench within their systems frameworks to ensure that information security practices are part of the culture through regular awareness and training.

A critical element of the information security strategy of organizations is to include information security awareness. Information security awareness training has become so important because a significant number of cyber exploitations occur through the exploitation of human weaknesses through phishing and social engineering (Torten et al., 2018). The most effective way to deal with phishing and social engineering attacks is through information awareness training (Abraham & Chengalur-Smith, 2019). For information security awareness to have a positive impact on an organization, it must focus on attitude and behavior to prevent cyber exploitations (Chmura, 2017). It says that information security awareness must meet the information security needs of the organization and the learning needs of employees.

All six participants confirmed that they spend considerable time and effort to inform and train their staff, trading partners, and stakeholders of their roles and

responsibilities in keeping their information safe. They also indicated that they have several mechanisms to communicate policies, procedures, and processes that guide operations to ensure the safety of information. The participants indicated that the weakest link could be people who are not aware of safe practices in the use of information assets or who in blind trust give out information that otherwise should be secret. The participants noted that policies or processes not known can be bypassed, and information security violations can be the result. They mentioned that lack of information security awareness could also lead to circumventing technology controls, for example, sharing of passwords or writing down passwords, which can lead to exploitation of information assets. All the organizations studied indicated that they get staff to read and sign that they have read information security policies before they have access to IT systems. Two of the participants mentioned that they conduct tests to be sure that staff imbibed information security policies taught during information security awareness campaigns so that they are not weak points in the information security management chain. It is therefore pertinent to note that an effective information security strategy must include a robust information security awareness program that will be relevant and consistent. Information security awareness campaigns are used as a platform to communicate also, current threats to information security and what users are to do to prevent violations (Bauer et al., 2017). Information security awareness needs to be taken seriously as a strategy to prevent cyber exploitations.

Strategies for Information Security Must be "Defense in Depth"

CISOs, while looking for how best to secure their infrastructure, should consider the use of the defense in depth concept to ensure encompassing protection during processing of information. Information transverse many logical points in its life cycle within an organization. They are either at rest or in motion. Information processing occurs at different logical layers, such as conceptualized by the OSI model (Orzen, 2014). Different IT devices and systems process information as they transverse the OSI model. Data can be exploited at any point, hence the need to ensure that there is appropriate protection for information being processed within financial services, whether it is at rest or in motion or at any level of the logical model. The concept that ensures protection across the path that information transverse is Defense in Depth (Crossler, Bélanger, & Ormond, 2017). Defense in Depth provides that where there is a failure of any control across the path of information, there will exist other protection at another level or layer, which can stop a potential attack (Petrangeli, 2019).

Defense in Depth is typically implemented by design as graded security to prevent human errors and cyber-exploitations. The participants indicated that they deploy several technological tools and processes to preserve information confidentiality, integrity, and availability. The deployments cover endpoints, network security tools, tools that secure up till the application layer, database monitoring, and security tools, operating system tools, encryption tools, SIEM tools, antiphishing tools, and many more. Jander, Braubach, and Pokahr (2018) described the deployments of such endpoint security tools,

encryption tools, securing applications, securing protocols of access, and much more as what defense in depth is all about.

The reason for deployments of tools at different layers that information passes or using defense in depth is to ensure that if there is a failure in control at any level, there is a provision for mitigation at other levels or points. Defense in depth is useful for combating insider threats (Rubio, Alcaraz, Roman, & Lopez, 2019). Most of the participants in the study expressed concerns about insider related risks. Practical strategies for preventing cyber exploitation of confidentiality, integrity, and availability must follow the defense in depth principle by identifying risks at each layer of information processing or access. The deployed tools deliver automation as well for approved policies so that organizations can avoid manual processes with its inefficiencies.

Compliance to Regulations and Standards Supports Prevention of Cyber Exploitations

An organization should pursue compliance to an identified information security standard related to their business in Nigeria because the need to comply to information security standard was found in the study to accelerate the implementation of strategies and practices which makes information safe. When institutions are crafting information security strategies, it is essential to consider regulations requiring compliance in the applicable country (Rayev, 2017). Several financial services companies, especially the ones within the banking sector and such as have a relationship with foreign companies, are to comply with specific regulations and standards. Banks in Nigeria are required to

comply with ISO 27001 and PCI-DSS standards. The financial companies that relate to European organizations are to comply with the GDPR (Tankard, 2016). All institutions in Nigeria are also required, effective August 2019, to comply with Nigeria data protection regulation. The participants mentioned that the need to comply with standards had helped them significantly to get budgets for strategies to prevent cyber exploitation of confidentiality, integrity, and availability. Institutions, where information security is strategically important budgets, are allocated readily for information security management (Tu et al., 2018). One of the drivers of the strategic importance of information security is the need to achieve information security regulatory compliance. Three of the participants noted that the fact that they have to comply with ISO 27001 puts them on their toes to ensure employees follow processes as documented. They mentioned that it also helps them to keep an active information security awareness campaign to keep all users well informed for audits, which in turn translates to heightened information security. Policies and regulatory frameworks form the core of the syllabus of information security awareness efforts of organizations (Aldawood & Skinner, 2019).

All the participants mentioned that they have different management processes that relate to information security management. They noted that their top management takes responsibility for information security matters because of the need to comply with regulations and standards. Ionescu, Grab, and Hassani (2019) described how European organizations that complied with specific information security standards found it easy to comply with GDPR, which became mandatory in 2018. Without their previous compliance with standards such as ISO 27001, they would have had to implement actions

to demonstrate compliance with the new GDPR. All the companies needed to do, because they had previously taken a strategic decision for compliance with specific information security standards, was to establish mappings in requirements to demonstrate compliance with the new GDPR. Most of the organizations studied also mentioned their compliance with the Nigerian data protection regulation. Their compliance with the ISO 27001 is beneficial in this regard.

Compliance with information security standards helps to protect against cyber exploitations because it requires specific actions that prevent cyber exploitations. The objectives of the GDPR and Nigeria data protection regulation is to safeguard information in motion and at rest (Brunswick, 2019). It will, therefore, be helpful for organizations that may want to jumpstart their information security strategies to choose a relevant standard/or make efforts to comply with relevant regulations on information security. The study established that such a decision will deliver specific information security protection across people, process, and technology areas

Monitoring is Key to Ongoing Prevention of Cyber Exploitations

Financial institutions in Nigeria need to invest in information security monitoring solutions to stay secure. They should implement solutions that will send alerts if there are potential cyber exploitations to address any possible incident. The monitoring should proactively also check for the effectiveness of deployed controls to prevent loss due to cyber exploitations. Monitoring efforts should include the setup of security operations centers. Security operations centers enable organizations to centralize monitoring and have a focused approach to detecting potential cyber exploitations and taking action

promptly (Mansfield-Devine, 2016b). It is not enough to deploy controls; it is necessary to monitor possible violations and use the outcomes to achieve better security.

Monitoring helps organizations achieve full benefits of information security beyond the use of policies (Ahmad, Ong, Liew, & Norhashim, 2019). Tracking for the effectiveness of controls (policies, processes, and tools) deployed to prevent cyber exploitations is vital to stay secure. All of the participants mentioned that they do regular vulnerability assessments internally. They said that twice a year, they call in external vulnerability assessors to check weaknesses in their systems so they can fix before any bad actors do. They all have internal control units that check that people are adhering to safe computing practices. They conduct clean desk sweeps to ensure confidentiality; they check that HR conducts processes such as background checks as at when due to prevent cyber exploitations. They also check that staff does not misuse access rights on applications and also that password policies on information systems are correctly set. Organizations also have internal audit departments that do audits of internal control processes to be sure they are doing monitoring work properly. One of the participants noted that they have mechanisms in place that monitors people who monitor internal monitors.

Four of the participants said they have in place a SIEM tool that automates the monitoring process and triggers alerts whenever a circumstance that can lead to violation of confidentiality, integrity, and availability occurs. The other participants said they are in the process of implementing a SIEM solution because they have identified the need for the SIEM solution to be proactive about preventing cyber exploitations.

Implications for Social Change

This study may contribute to social change through improved financial inclusion by encouraging increased use of digital finance. In Nigeria, 58.4% of the adult population is financially included, of which only 38.3% is banked (Central Bank of Nigeria, 2018). A significant adult population, today in Nigeria, does not keep their money in banks due to fear of loss because of a lack of trust in the use of technology, which they need to use to access money whenever they need them. The practice of not keeping cash in banks excludes such people from financial services such as loans and other financial products. Financial inclusion has the potential to provide financial support opportunities to the previously excluded citizens who are unbanked due to information security concerns of saving money in financial institutions in Nigeria. Improved confidence in the finance sector may, therefore, increase the banked population from the current level.

This study may contribute to the assurance of possible safe use of finance through technology and may provide opportunities to access funding for previously excluded businesses, which may lead to economic development and other associated benefits of the improved banked population (Ngwu, 2014). Digital finance stimulates growth, which in turn leads to improved GDP in developing economies (Ozili, 2018).

The study may also help to keep the personal information of customers of financial institutions safe through the deployment of strategies that addresses threats to information theft, and thereby preventing harm and hurt, which may occur where unauthorized people have access to personal details of customers. The study may help

prevent issues such as identity theft, fraud, disclosure of financial habits, spendings, pension plans, which may expose customers to a myriad of dangers and risks.

The study may also lead to a greater embrace of alternative means of accessing financial services because of the assurances of safety measures in place. The implementation of information security strategies identified in the study may allow customers of financial institutions to enjoy better services in an appropriate and more flexible ways, which would otherwise not be possible except where appropriate information security is in place. Flexible and more convenient finance access will lead to improved customer services. One of the financial institutions studied is a custodian of a national economic infrastructure which can impact on national security. The study may, therefore, help to preserve national heritage and prevent the harm that can impact on national pride where there is the implementation of strategies that prevent cyber exploitations.

Recommendations for Action

CISOs in organizations should begin to document information security strategies as aligned to the organizational strategy. Enterprise risk managers should start demanding from CISOs a documented strategy for information security risk management. It appears that the practice of recording information security strategies explicitly across all lines of action is not common within financial services yet in Nigeria. Organizations only have risk management practices and supporting processes and policies, which includes plans to prevent violations of information security. One critical step that is needed now is to document information security strategies as actionable plans across all elements to the

future. Organizations need to record explicit actions required across people, process, and technology areas that will leave practitioners in no doubt as to what steps to take to prevent cyber exploitations. Documented regulatory and several organizations policies seem to be advisory, there is a need to be more direct and clearer to achieve desired levels of information security within the financial services.

Executive management of financial institutions should encourage compliance to standards related to information security in their organizations, even where it is not a mandatory requirement to comply. The demand for such compliance will help their due care and due diligence responsibility in the area of information security management. This study indicated that compliance with standards and regulations has a positive influence on efforts to prevent cyber exploitations that undermine confidentiality, integrity, and availability of information assets. Identification of a standard gives room for organizations to have the comfort of taking the right steps toward preventing cyber exploitations. Regulatory compliance requirements also aid in getting necessary budgets from management in order to achieve expected levels of information security. CISOs in organizations should identify all critical standards and regulations that impact information security that relates to their operations and make efforts to comply.

Business continuity managers within the financial services companies should work more closely with CISOs to ensure that they cater to information security contingencies in business continuity plans. One of the critical elements the study validated is that organizations need to have plans for contingencies. The conceptual model also posited through the contingency theory that organizations must be able to

respond swiftly to contingent issues that arise as a result of information security breaches. One way that organizations provide for contingencies is through correctly set out the incident management process. A robust incident management process ensures that even where violations of information security occurs, it is contained quickly and managed so that many damages do not happen. Organizations should develop incident management processes that ensure continuity of business where a breach occurs. They can only achieve this through good cooperation between the CISO and the business community manager. Organizations' incident management process should include processes to report to relevant industry bodies, the nature of incidences, and actors when they occur who will distribute such knowledge to all stakeholders to learn to reduce the impact on the industry. The sharing of incident information will afford others to gain knowledge to prevent the occurrence in their domain. The government needs to step up regulation to improve the reporting of incidences to achieve this. Government efforts should not be to reprimand or fine but to help other institutions who have not suffered similar attacks from experiencing cyber-attacks by encouraging safe sharing of incident reports at the industry level.

Human resources departments of organizations need to work with CISOs to create a curriculum that will ensure the continuous availability of the appropriate level of knowledge and expertise to perform information security-related duties. Human resources with the approval of executive management also should implement an organizational structure that will facilitate reporting of CISOs to the appropriate function outside IT, preferably risk management function or as will be determined in the context of the

organization. The human resources department, through their training plans, should identify innovative ways to achieve information security awareness to make information security knowledge simple to assimilate to achieve levels of knowledge of policies, processes to prevent cyber exploitations.

I will be presenting the findings of the study through seminars and conferences, especially ones targeted towards improving the cyber resilience of financial institutions. I will be writing a paper for presentation at academic conferences and financial services information security conferences. I will also be organizing seminars to share the findings at the local chapter of the information security associations in Nigeria, of which I am a member. The groups are the Information Systems Audit and Control Association (ISACA) and the International Information System Security Certification Consortium (ISC2)

Recommendations for Further Research

This study focused on CISOs in financial institutions in Abuja and Lagos, Nigeria. Future researchers may expand the bounds to include all states of Nigeria as a representative to improve the generalization of outcomes. It may also help to study specific sectors within the financial services and see if the findings of this study are applicable across all areas of the financial services industry in Nigeria and possibly other countries

Additionally, it may help to study the particular impact that regulation of information security practices plays in achieving information security by comparing regulated and nonregulated organizations within the sector. Banks within the financial

services company sector in Nigeria are heavily regulated. There are specific regulatory frameworks that the regulator of the banks, the Central Bank of Nigeria, expects banks to comply with to ensure security, especially with the growing adoption of technology. Information security regulation seems to have influenced the level of information security in banks. Other institutions within the financial sector have regulatory bodies, but their information security practices not regulated. Additional value may arise by studying financial companies whose information security practices are regulated and those that are not. The objective is to identify the benefits of such regulation and ensure that agencies of government regulating the various categories of financial institutions include demand in their oversight requirements for compliance to particular information security objectives.

Reflections

As an IT expert with experience in information security, the themes I saw in the study resonate with the ideas that I have encountered in a previous practice as an enterprise security lead in a bank. I had expected to discover significant gaps in maturity levels in the implementation of strategies in use in banks to prevent cyber exploitations. I am particularly impressed to note, however, that banks in financial services have stepped up their game significantly in the area of information security. The companies within the banking sector studied shows evidence they are ahead of the other nonbank institutions. Nonbanks within the financial services are the ones playing catchup.

In soliciting for participants, I was surprised at the reluctance of organizations to support work in the field of information security when it was clear the study could potentially benefit them. I had hoped that most organizations would be willing to

participate in the study because of the perceived value to the financial services sector. The reluctance persisted despite assurances that the study will not mention anything specific about the institutions in the report of the research that will point to the organizations. After the study, however, I saw the reason why some were reluctant. The organizations were reluctant because they feared they could be at risk because of some information they may share in the course of the study. This experience singularly shows that organizations within financial services are careful of the nature of the information they share in order to stay safe. They demonstrated the practice of security by obscurity identified in the review of the literature.

Additionally, in assuming that organizations will willingly participate in the study, I had expected that the use of NDAs as a means of achieving confidentiality would give required levels of comfort to the organizations. I, however, discover that even though the organizations that declined participation have NDAs they could execute, they still refuse. It thus appears to me that they may not have confidence in their processes or strategies, such as the use of NDAs to achieve confidentiality of information security. The execution of an NDA should have sufficed to ensure that I will not share details of the data I collect for the study. A lack of support for the research will not be beneficial to them as they lose the opportunity of learning from a comparative point of view with other institutions when they refuse to be part of such a comparative study. The organizations that participated have contributed to the practice of IT by agreeing to be part of the study.

Summary and Study Conclusion

Information security management is a journey, not a destination. Organizations that will be secure from cyber exploitations that violate confidentiality, integrity and availability of information assets need to have in place a program that will cover people, process, technology, and strategic areas of their business to stay secure. There must be an alignment of various strategies to prevent cyber exploitations of confidentiality, integrity, and availability with the prevalent business strategy. Adhoc efforts will not do the job. For successful information security management, the positioning of practitioners in organizations must be outside of the IT function to achieve independence and holistic coverage of all Information technology risk areas.

Information security practitioners in the financial services sector in Nigeria needs to be very knowledgeable to be ahead of cybercriminals. The starting point should be training in infrastructure security that also addresses people and process issues. CISSP training and certification can provide the necessary foundation for practitioners in Nigeria. It is essential to document information security strategies, and there is a need for organizations to be a lot more detailed in the documentation of information security risk mitigation. The documentation of information security strategies will enable adequate, enough, and appropriate deployment of controls to prevent cyber exploitations.

References

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

Ablon, L., & Bogart, A. (2017). *Zero-days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits*. Santa Monica, CA: Rand Corporation.

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers & Security, 87,* 101586. doi:10.1016/j.cose.2019.101586

Ahmad, A., Maynard, S., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management, 35*(6), 717-723. doi:10.1016/j.ijinfomgt.2015.08.001

Ahmad, Z., Ong, T., Liew, T., & Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees: An empirical analysis. *Information and Computer Security, 27*(2), 165-188. doi:10.1108/ICS-10-2017-0073

Ajay, D., & Umamaheswari, E. (2019). Packet encryption for securing real-time mobile cloud applications. *Mobile Networks and Applications, 24*(4), 1249-1254. doi:10.1007/s11036-019-01263-1

Akinrolabu, O., Nurse, J., Martin, A., & New, S. (2019). Cyber risk assessment in cloud provider environments: Current models and future needs. *Computers & Security, 87,* 101600. doi:10.1016/j.cose.2019.101600

Akinwumi, D. A., Iwasokun, G. B., Alese, B. K., & Oluwadare, S. A. (2017). A review

of game theory approach to cybersecurity risk management. *Nigerian Journal of Technology, 36*(4), 1271-1285. doi:10.4314/njt.v36i4.38

Aldawood, H., & Skinner, G. (2019). Reviewing cybersecurity social engineering training and awareness programs—pitfalls and ongoing issues. *Future Internet, 11*(3), 73. doi:10.3390/fi11030073

Aldiabat, K. M., & Le Navenec, C. (2018). Data saturation: The mysterious step in grounded theory methodology. *The Qualitative Report, 23*(1), 245-261. Retrieved from https://nsuworks.nova.edu/tqr/

Aldosari, H. (2015). A proposed security layer for the internet of things communication reference model. *Procedia Computer Science, 65*, 95-98. doi:10.1016/j.procs.2015.09.084

Alexander, N. (2015). What's more general than a whole population? *Emerging Themes in Epidemiology, 12*(1), 1-5. doi:10.1186/s12982-015-0029-4

Ali, A., Warren, D., & Mathiassen, L. (2017). Cloud-based business services innovation: A risk management model. *International Journal of Information Management, 37*(6), 639-649. doi:10.1016/j.ijinfomgt.2017.05.008

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

Amerson, R. (2011). Making a case for the case study method. *Journal of Nursing Education, 50*, 427-428. doi:10.3928.01484834-20110719-01

Amin, R., Shah, N., Shah, B., & Alfandi, O. (2016). Auto-configuration of ACL policy in case of topology change in hybrid SDN. *IEEE Access, 4*, 9437-9450. doi:10.1109/access.2016.2641482

Andress, J., & Leary, M. (2017). Develop an information security strategy. *Building A Practical Information Security Program,* 23-34. doi:10.1016/b978-0-12-802042-5.00002-0

Angraini, Alias, R., & Okfalisa. (2019). Information security policy compliance: Systematic literature review. *Procedia Computer Science, 161,* 1216-1224. doi:10.1016/j.procs.2019.11.235

Arabo, A. (2015). Cybersecurity challenges within the connected home ecosystem futures. *Procedia Computer Science, 61,* 227-232. doi:10.1016/j.procs.2015.09.201

Arief, R., Khakzad, N., & Pieters, W. (2020). Mitigating cyberattack related domino effects in process plants via ICS segmentation. *Journal Of Information Security and Applications, 51,* 102450. doi:10.1016/j.jisa.2020.102450

Ashish, U., Ds, S., & Milind, T. (2017). Analysis of payment card industry data security standard [PCI DSS] compliance by confluence of COBIT 5 framework. *International Journal of Engineering Research and Applications, 7*(1), 42-48. Retrieved from http://ijera.academia.edu/ijera

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1-13. doi:10.1016/j.ejor.2015.12.023

Balogun, K. O. (2018). *Letter to all Banks and Payment service Providers: Exposure draft of the risk-based cybersecurity framework and guidelines for deposit money banks and payment service providers*. Retrieved from https://www.cbn.gov.ng/out/2018/bsd/risk%20based%20cybersecurity%20framework%20exposure%20draft%20june.

Balzacq, T. (2015). The 'essence' of securitization: Theory, ideal type, and a sociological science of security. *International Relations, 29*(1), 103-113. doi:10.1177/0047117814526606b

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization' revisited: theory and cases. *International Relations, 30*(4), 494-531. doi:10.1177/0047117815596590

Banks, V., Stanton, N., Burnett, G., & Hermawati, S. (2018). Distributed cognition on the road: Using EAST to explore future road transportation systems. *Applied Ergonomics, 68*, 258-266. doi:10.1016/j.apergo.2017.11.013

Barnham, C. (2015). Quantitative and qualitative research. *International Journal of Market Research, 57*, 837-854. doi:10.2501/IJMR-2015-070

Barni, M., Bartolini, F., & Furon, T. (2003). A general framework for robust watermarking security. *Signal Processing, 83*(10), 2069-2084. doi:10.1016/s0165-1684(03)00168-3

Baskerville, R., & Myers, M. (2015). Design ethnography in information systems. *Information Systems Journal, 25*(1), 23-46. doi:10.1111/isj.12055

Baskerville, R., Stage, J., & DeGross, J. (2000). *Organizational and social perspectives on information technology*. Boston, MA: Springer.

Bates, L., Darvell, M. J., & Watson, B. (2017). Young and unaffected by road policing strategies: Using deterrence theory to explain provisional drivers' (non)compliance. *Australian & New Zealand Journal of Criminology, 50*(1), 23-38. doi:10.1177/0004865815589824

Bauer, S., Bernroider, E., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68,* 145-159. doi:10.1016/j.cose.2017.04.009

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management, 54*(7), 887-901. doi:10.1016/j.im.2017.01.003

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open, 2,* 8-14. doi:10.1016/j.npls.2016.01.001

Bholat, D. (2015). Big data and central banks. *Big Data & Society, 2*(1). doi:10.1177/2053951715579469

Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition, 84,* 317-331. doi:10.1016/j.patcog.2018.07.023

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*(13), 1802-1811. doi:10.1177/1049732316654870

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cybersecurity assurance process from the

internal audit perspective. *Managerial Auditing Journal, 33*(4), 360-376. doi:10.1108/maj-02-2018-1804

Brunswick, D. (2019). Data privacy, data protection, and the importance of integration for GDPR compliance. *ISACA Journal, 1,* 14. Retrieved from https://www.isaca.org/resources/isaca-journal

Burdon, M., & Coles-Kemp, L. (2019). The significance of securing as a critical component of information security: An Australian narrative. *Computers & Security, 87,* 101601. doi:10.1016/j.cose.2019.101601

Busse, C., Kach, A., & Wagner, S. (2017). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods, 20*(4), 574–609. doi:10.1177/1094428116641191

Byrne, P. (2006). Application firewalls in a defense-in-depth design. *Network Security, 2006*(9), 9-11. doi:10.1016/s1353-4858(06)70422-6

Calvo, I., Etxeberria-Agiriano, I., Iñigo, M. A., & González-Nalda, P. (2016). Key vulnerabilities of industrial automation and control systems and recommendations to prevent cyber-attacks. *International Journal of Online Engineering, 12*(1), 9-16. doi:10.3991/ijoe.v12i1.4888

Carayon, P., Hancock, P., Leveson, N., Noy, I., Sznelwar, L., & van Hootegem, G. (2015). Advancing a sociotechnical systems approach to workplace safety – developing the conceptual framework. *Ergonomics, 58*(4), 548-564. doi:10.1080/00140139.2015.1015623

Carbaugh, E., Antonio, C., Lynch, T., & Nelsen, L. (2019). A Contingency Plan for

Catastrophic Loss of Bioassay Services. *Health Physics, 116*(1), 105-108. doi:10.1097/hp.0000000000000967

Carvalho, M., Bellotti, F., Berta, R., De Gloria, A., Sedano, C., & Hauge, J., … Rauterberg, M. (2015). An activity theory-based model for serious games analysis and conceptual design. *Computers & Education, 87,* 166-181. doi:10.1016/j.compedu.2015.03.023

Casola, V., De Benedictis, A., Rak, M., & Rios, E. (2016). Security-by-design in clouds: A security-SLA driven methodology to build secure cloud applications. *Procedia Computer Science, 97,* 53-62. doi: 10.1016/j.procs.2016.08.280

Casola, V., De Benedictis, A., Riccio, A., Rivera, D., Mallouli, W., & de Oca, E. (2019). A security monitoring system for internet of things. *Internet Of Things, 7,* 100080. doi:10.1016/j.iot.2019.100080

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning, 10*(6), 807-815. doi:10.1016/j.cptl.2018.03.019

Central Bank of Nigeria. (2015). *Regulatory and supervisory guidelines for development finance institutions in Nigeria*. Retrieved from https://www.cbn.gov.ng/

Central Bank of Nigeria. (2018). *National Financial Inclusion Strategy(Revised).* Retrieved from https://www.cbn.gov.ng/

Central Bank of Nigeria. (2019). *Nigeria Financial Services Industry IT Standards Blueprint.* Retrieved from https://www.cbn.gov.ng/

Chah, N. (2019). Down the deep rabbit hole: Untangling deep learning from machine

learning and artificial intelligence. *First Monday, 24*(2). doi:10.5210/fm.v24i2.8237

Chakkaravarthy, S., Sangeetha, D., Venkata Rathnam, M., Srinithi, K., & Vaidehi, V. (2018). Futuristic cyber-attacks. *International Journal of Knowledge Based Intelligent Engineering Systems, 22*(3), 195–204. doi:10.3233/KES-180384

Cheng, Q., Goh, B., & Kim, J. (2018). Internal control and operational efficiency. *Contemporary Accounting Research, 35*(2), 1102-1139. doi:10.1111/1911-3846.12409

Chierici, L., Fiorini, G., Rovere, S., & Vestrucci, P. (2016). The evolution of defense in depth approach: A cross-sectorial analysis. *Open Journal of Safety Science and Technology, 06*(02), 35-54. doi:10.4236/ojsst.2016.62004

Chmura, J. (2017). Forming the awareness of employees in the field of information security. *Journal of Positive Management, 8*(1), 78. Retrieved from https://www.questia.com/library/p439849/journal-of-positive-management

Clandinin, D. J., Cave, M. T., & Berendonk, C. (2017). Narrative inquiry: a relational research methodology for medical education. *Medical Education, 51*(1), 89–96. doi:10.1111/medu.13136

Conklin, W., & Shoemaker, D. (2017). Cyber-resilience: Seven steps for institutional survival. *EDPACS, 55*(2), 14-22. doi:10.1080/07366981.2017.1289026

Connelly, L. M. (2016). Understanding research. Trustworthiness in qualitative research. *MEDSURG Nursing, 25*(6), 435–436. Retrieved from http://www.medsurgnursing.net/cgi-bin/WebObjects/MSNJournal.woa

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*(23), 31-38. doi:10.19101/IJACR.2016.623006

Cowls, J., & Schroeder, R. (2015). Causation, correlation, and big data in social science research. *Policy & Internet, 7*(4), 447–472. doi:10.1002/poi3.100

Crossler, R., Bélanger, F., & Ormond, D. (2017). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. Information Systems Frontiers, 21(2), 343-357. doi:10.1007/s10796-017-9755-1

Crowe, M., Inder, M., & Porter, R. (2015). Conducting qualitative research in mental health: Thematic and content analyses. *Australian & New Zealand Journal of Psychiatry, 49*(7), 616-623. doi:10.1177/0004867415582053

Cypress, B. (2017). Rigor or Reliability and Validity in Qualitative Research. *Dimensions Of Critical Care Nursing, 36*(4), 253-263. doi:10.1097/dcc.0000000000000253

D'Angelo, G., & Rampone, S. (2018). Cognitive distributed application area networks. *security and resilience in intelligent data-centric systems and communication Networks*, 193-214. doi:10.1016/b978-0-12-811373-8.00009-4

da Silva, N., Coletta, L., Hruschka, E., & Hruschka Jr., E. (2016). Using unsupervised information to improve semi-supervised tweet sentiment classification. *Information Sciences, 355-356, 348-365*. doi:10.1016/j.ins.2016.02.002

de Gusmão, A., e Silva, L., Silva, M., Poleto, T., & Costa, A. (2016). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management, 36*(1), 25-34. doi:10.1016/j.ijinfomgt.2015.09.003

Dempsey, L., Dowling, M., Larkin, P., & Murphy, K. (2016). Sensitive Interviewing in Qualitative Research. *Research in Nursing & Health, 39*(6), 480-490. doi:10.1002/nur.21743

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security, 92,* 101747. doi:10.1016/j.cose.2020.101747

Dimase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems & Decisions, 35*(2), 291-300. doi:10.1007/s10669-015-9540-y

Diro, A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems, 82*, 761-768. doi:10.1016/j.future.2017.08.043

Doyle, L., Brady, A., & Byrne, G. (2016). An overview of mixed methods research – revisited. *Journal of Research in Nursing, 21*(8), 623-635. doi:10.1177/1744987116674257

Dunn, S., Arslanian-Engoren, C., DeKoekkoek, T., Jadack, R., & Scott, L. (2015). Secondary data analysis as an efficient and effective approach to nursing research. *Western Journal of Nursing Research, 37*(10), 1295-1307. doi:10.1177/0193945915570042

Durach, C. F., Kembro, J., & Wieland, A. (2017). *A new Paradigm For Systematic Literature Reviews in Supply Chain Management*. *Journal of Supply Chain Management, 53*(4), 67-85. Retrieved from https://onlinelibrary.wiley.com/

Eboibi, F. (2017). A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015. *Computer Law & Security Review.* doi:10.1016/j.clsr.2017.03.020

Efobi, U., Beecroft, I., & Osabuohien, E. (2014). Access to and use of bank services in Nigeria: Micro-econometric evidence. *Review of Development Finance, 4*(2), 104-114. doi:10.1016/j.rdf.2014.05.002

Elman, C., Gerring, J., & Mahoney, J. (2016). Case study research. *Sociological Methods & Research, 45*(3), 375-391. doi:10.1177/0049124116644273

Erastus, K. (2017). The role of the chief information security officer in the management of IT security. *Information and Computer Security, 25*(3), 300-329. doi:10.1108/ICS-02-2016-0013

Everett, J., Neu, D., Rahaman, A. S., & Maharaj, G. (2015). Praxis, doxa and research methods: Reconsidering critical accounting. *Critical Perspectives on Accounting, 32*, 37–44. doi:10.1016/j.cpa.2015.04.004

Fagioli, A. (2019). Zero-day recovery: the key to mitigating the ransomware threat. *Computer Fraud & Security, 2019(1*), 6-9. doi:10.1016/s1361-3723(19)30006-5

Fayard, A., & Van Maanen, J. (2015). Making culture visible: reflections on corporate ethnography. *Journal of Organizational Ethnography, 4*(1), 4-27. doi:10.1108/joe-12-2014-0040

Fazlida, M., & 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

Feng, C., & Wang, T. (2019). Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems, 32,* 59-75. doi:10.1016/j.accinf.2018.11.001

Ferreira, R., Frogeri, R., Coelho, A., & Piurcosky, F. (2018). Information security management practices: study of the influencing factors in a Brazilian Air Force institution. *Journal of Information Systems and Technology Management, 15.* doi:10.4301/s1807-1775201815005

Fettweis, C. (2018). Restraining Rome: Lessons in grand strategy from Emperor Hadrian. *Survival, 60*(4), 123-150. doi:10.1080/00396338.2018.1495438

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems, 86,* 13-23. doi:10.1016/j.dss.2016.02.012

Florczak, K. (2014). Purists need not apply. *Nursing Science Quarterly, 27*(4), 278-282. doi:10.1177/0894318414546419

Flowerday, S., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61,* 169-183. doi:10.1016/j.cose.2016.06.002

Fluk, L. (2015). Foregrounding the research log in information literacy instruction. *Journal of Academic Librarianship, 41*(4), 488-498. doi:10.1016/j.acalib.2015.06.010

Forain, I., de Oliveira Albuquerque, R., Sandoval Orozco, A., García Villalba, L., & Kim, T. (2017). Endpoint Security in Networks: An OpenMP Approach for Increasing

Malware Detection Speed. *Symmetry, 9*(9), 172. doi:10.3390/sym9090172

Fraser, J. R., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. *Business Horizons, 59,* 689-698. doi:10.1016/j.bushor.2016.06.007

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? data saturation in qualitative research. *Qualitative Report, 20*(9), 1408-1416. Retrieved from https://nsuworks.nova.edu/tqr/

Gambetta, N., García-Benau, M., & Zorio-Grima, A. (2016). Data analytics in banks' audit: The case of loan loss provisions in Uruguay. *Journal of Business Research, 69*(11), 4793-4797. doi:10.1016/j.jbusres.2016.04.032

Gana, N. M., Abdulhamid, S., & Ojeniyi, J. (2019). Security risk analysis and management in banking sector: A case study of a selected commercial bank in Nigeria. *International Journal of Information Engineering and Electronic Business, 11*(2), 35-43. doi:10.5815/ijieeb.2019.02.05

Gearing, R. (2004). Bracketing in research: A typology. *Qualitative Health Research, 14*(10), 1429-1452. doi:10.1177/1049732304270394

Gearon, L. (2017). The counter-terrorist campus: Securitization theory and university securitization -- three models. *Transformation in Higher Education, 2*(1). doi:10.4102/the.v2i0.13

Genge, B., Graur, F., & Haller, P. (2015). Experimental assessment of network design approaches for protecting industrial control systems. *International Journal of Critical Infrastructure Protection, 11,* 24-38. doi:10.1016/j.ijcip.2015.07.005

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*(11), 1772-1789. Retrieved from https://nsuworks.nova.edu/tqr/

Ghadirli, H., Nodehi, A., & Enayatifar, R. (2019). An overview of encryption algorithms in color images. *Signal Processing, 164*, 163-185. doi:10.1016/j.sigpro.2019.06.010

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., … Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing, 74*(10), 4986-5002. doi:10.1007/s11227-018-2337-2

Grant, A. (2014). Troubling 'lived experience': A post-structural critique of mental health nursing qualitative research assumptions. *Journal of Psychiatric and Mental Health Nursing, 21*(6), 544-549 doi:10.1111/jpm.12113

Green, C. A., Duan, N., Gibbons, R. D., Hoagwood, K. E., Palinkas, L. A., & Wisdom, J. P. (2015). Approaches to mixed methods dissemination and implementation research: Methods, strengths, caveats, and opportunities. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5), 508-523. doi:10.1007/s10488-014-0552-6

Green, J., Willis, K., Hughes, E., Small, R., Welch, N., Gibbs, L., & Daly, J. (2007). Generating best evidence from qualitative research: the role of data analysis. *Australian and New Zealand Journal of Public Health, 31*(6), 545-550. doi:10.1111/j.1753-6405.2007.00141.x

Griensven, H. V., Moore, A. P., & Hall, V. (2014). Mixed methods research: The best of

both worlds? *Manual Therapy, 19,* 367-371. doi:10.1016/j.math.2014.05.005

Gunavan, J. (2015). Ensuring trustworthiness in qualitative research. *Belitung Nursing Journal, 1*(1), 10-11. Retrieved from http://belitungraya.org/BRP/index.php/bnj/

Günther, W., Rezazade Mehrizi, M., Huysman, M., & Feldberg, F. (2017). Debating big data: A literature review on realizing value from big data. *The Journal of Strategic Information Systems, 26*(3), 191-209. doi:10.1016/j.jsis.2017.07.003

Guo, S. (2014). Shaping social work science: What should quantitative researchers do? *Research on Social Work Practice, 25*(3), 370-381. doi:10.1177/1049731514527517

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I., & Jones, K. (2019). Exploring the role of work identity and work locus of control in information security awareness. *Computers & Security, 81*, 41-48. doi:10.1016/j.cose.2018.10.006

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: when to use them and how to judge them. *Human Reproduction, 31*(3), 498-501. doi:10.1093/humrep/dev334.

Hammer, M. J. (2016). Informed consent in the changing landscape of research. *Oncology Nursing Forum, 43*(5), 558-560. doi:10.1188/16.ONF.558-560

Hammersley, M. (2017). What is ethnography? Can it survive? Should it? *Ethnography and Education, 13*(1), 1-17. doi:10.1080/17457823.2017.1298458.

Han, Z., Huang, S., Li, H., & Ren, N. (2016). Risk assessment of digital library information security: a case study. *Electronic Library, 34*(3), 471-487. doi:10.1108/EL-09-2014-0158

Hanssen, G., Stålhane, T., & Myklebust, T. (2018). What is agile software development? A short introduction. *Safescrum® – Agile Development of Safety-Critical Software,* 11-15. doi:10.1007/978-3-319-99334-8_2

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal Of Information Management, 43,* 165-172. doi:10.1016/j.ijinfomgt.2018.07.013

Harrison, L., Ahn, C., & Adolphs, R. (2015). Exploring the structure of human defensive responses from judgments of threat scenarios. *PLOS ONE, 10*(8), e0133682. doi:10.1371/journal.pone.0133682

Hart, C. (2002). *Doing a literature review*. London: SAGE.

Hatcher, W., & Yu, W. (2018). A survey of deep learning: platforms, applications, and emerging research trends. *IEEE Access, 6,* 24411-24432. doi:10.1109/access.2018.2830661

Hemanidhi, A., & Chimmanee, S. (2017). Military-based cyber risk assessment framework for supporting cyber warfare in Thailand. *Journal of Information & Communication Technology, 16*(2), 192-222. Retrieved from http://jict.uum.edu.my/

Hemphill, T., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society, 44,* 30-38. doi:10.1016/j.techsoc.2015.11.007

Hernández-Orallo, J. (2016). Evaluation in artificial intelligence: from task-oriented to ability-oriented measurement. *Artificial Intelligence Review, 48*(3), 397-447.

doi:10.1007/s10462-016-9505-7

Heydon, G., & Powell, A. (2016). Written-response interview protocols: an innovative approach to confidential reporting and victim interviewing in sexual assault investigations. *Policing and Society, 28*(6), 631-646. doi:10.1080/10439463.2016.1187146

Hinchliffe, A. (2017). Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime. *Computer Fraud & Security*, 2017(5), 5-9. doi:10.1016/s1361-3723(17)30040-4

Homeland Security. (2017). Financial sector. Retrieved from https://www.dhs.gov/financial-services-sector

Hong, K., Chi, Y., Chao, L., & Tang, J. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243-248. doi:10.1108/09685220310500153

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons, 59*(6), 585-591. doi:10.1016/j.bushor.2016.07.004

Høyland, S., Hollund, J., & Olsen, O. (2015). Gaining access to a research site and participants in medical and nursing research: a synthesis of accounts. *Medical Education, 49*(2), 224-232. doi:10.1111/medu.12622.

Hu, H., Han, W., Kyung, S., Wang, J., Ahn, G., Zhao, Z., & Li, H. (2019). Towards a reliable firewall for software-defined networks. *Computers & Security, 87*, 101597. doi:10.1016/j.cose.2019.101597

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic

theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice, 47*, 44-57. doi:10.1016/j.ijlcj.2016.07.002

Iivari, N. (2018). Using member checking in interpretive research practice. *Information Technology & People, 31*(1), 111-133. doi:10.1108/itp-07-2016-0168

Inskeep, T. (2019). How to properly position the CISO for success. *Security: Solutions for Enterprise Security Leaders, 56*(5), 36–37.

Ionescu, R. C., Grab, B., & Hassani, Y. (2019). Study of effects of information security management system in the context of the E.U. G*eneral Data Protection Regulation Application: Acces La Success. Calitatea, 20,* 322-328.

Ismail, S., Sitnikova, E., & Slay, J. (2014). Using integrated system theory approach to assess security for SCADA systems cybersecurity for critical infrastructures: A pilot study. 2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD). doi:10.1109/fskd.2014.6980976

Jander, K., Braubach, L., & Pokahr, A. (2018). Defense-in-depth and role authentication for microservice systems. *Procedia Computer Science, 130,* 456-463. doi:10.1016/j.procs.2018.04.047

Jingguo, W., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: analysis of attack-proneness of information systems applications. *MIS Quarterly, 39*(1), 91-A7. Retrieved from https://www.misq.org/

Jones, P. (2010). You want a piece of me? Paying your dues and getting your due in a distributed world. *AI & Society, 25*(4), 455–464. doi:10.1007/s00146-010-0271-9

Jørgensen, M. (2017). Reframing tourism distribution - Activity theory and actor-network

theory. *Tourism Management, 62, 312*-321. doi:10.1016/j.tourman.2017.05.007

Joshi, C., & Singh, U. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*, 128-137. doi:10.1016/j.jisa.2017.06.006

Kamravamanesh, M., Kohan, S., Rezavand, N., & Farajzadegan, Z. (2018). A comprehensive postpartum follow-up health care program for women with history of preeclampsia: protocol for a mixed-methods research. *Reproductive Health, 15*(1), N.PAG. doi:10.1186/s12978-018-0521-8

Karanasios, S., Allen, D., & Finnegan, P. (2015). Information Systems Journal Special Issue on: Activity Theory in Information Systems Research. *Information Systems Journal, 25*(3), 309-313. doi:10.1111/isj.12061

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security, 25*(3), 300. doi:10.1108/ICS-02-2016-0013

Karanja, E., & Rosso, M. A. (2017). The chief information security officer: An exploratory study. *Journal of International Technology and Information Management, 26*(2), 23-47. Retrieved from https://scholarworks.lib.csusb.edu/jitim/

Kauffman, R., Liu, J., & Ma, D. (2015). Innovations in financial IS and technology ecosystems: High-frequency trading in the equity market. *Technological Forecasting and Social Change, 99*, 339-354. doi:10.1016/j.techfore.2014.12.001.

Kaur, R., & Singh, M. (2015). A hybrid real-time zero-day attack detection and analysis system. *International Journal of Computer Network and Information Security, 7*(9), 19-31. doi:10.5815/ijcnis.2015.09.03

Kay, L. (2019). Guardians of research: negotiating the strata of gatekeepers in research with vulnerable participants. *PRACTICE*, 1-16. doi:10.1080/25783858.2019.1589988

Kelarev, A., Ryan, J., Rylands, L., Seberry, J., & Yi, X. (2018). Discrete algorithms and methods for security of statistical databases related to the work of Mirka Miller. *Journal Of Discrete Algorithms, 52*-53, 112-121. doi:10.1016/j.jda.2018.11.008

Kemper, G. (2019). Improving employees' cybersecurity awareness. *Computer Fraud & Security, 2019*(8), 11-14. doi:10.1016/s1361-3723(19)30085-5

Kenney, M. (2015). Cyber-terrorism in a post-Stuxnet world. *Orbis, 59*(1), 111-128. doi:10.1016/j.orbis.2014.11.009

Kern, F. (2016). The trials and tribulations of applied triangulation: Weighing different data sources. *Journal of Mixed Methods Research, 12*(2), 166-181. doi:10.1177/1558689816651032

Khalili, A., Sami, A., Khozaei, A., & Pouresmaeeli, S. (2018). SIDS: State-based intrusion detection for stage-based cyber-physical systems. *International Journal Of Critical Infrastructure Protection, 22*, 113-124. doi:10.1016/j.ijcip.2018.06.003

Klingensmith, K., & Madni, A. (2017). Architecting cyber-secure, resilient system-of-systems. *Disciplinary Convergence In Systems Engineering Research,* 157-174. doi:10.1007/978-3-319-62217-0_12

Korstjens, I., & Moser, A. (2017a). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice, 24*(1), 120-124. doi:10.1080/13814788.2017.1375092

Korstjens, I., & Moser, A. (2017b). Series: Practical guidance to qualitative research. Part 2: Context, research questions, and designs. *European Journal of General Practice, 23*(1), 274-279. doi:10.1080/13814788.2017.1375090

Koucham, O., Mocanu, S., Hiet, G., Thiriet, J., & Majorczyk, F. (2018). Efficient Mining of Temporal Safety Properties for Intrusion Detection in Industrial Control Systems. *IFAC-Papers online*, *51*(24), 1043-1050. doi:10.1016/j.ifacol.2018.09.719

Kreutz, D., Malichevskyy, O., Feitosa, E., Cunha, H., da Rosa Righi, R., & de Macedo, D. (2016). A cyber-resilient architecture for critical security services. *Journal of Network and Computer Applications, 63*, 173-189. doi:10.1016/j.jnca.2015.09.014

Kumar, P., Raj, P., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science, 125*, 691-697. doi:10.1016/j.procs.2017.12.089

Lanz, J. (2017). The chief information security officer: The new CFO of information security. CPA *Journal, 87*(6), 52-57. Retrieved from https://www.cpajournal.com/

Lawlor, D., Tilling, K., & Davey Smith, G. (2017). Triangulation in aetiological epidemiology. *International Journal of Epidemiology, dyw314*. doi:10.1093/ije/dyw314

Lee, H.-W. (2017). Taking deterrence seriously: The wide-scope deterrence theory of punishment. *Criminal Justice Ethics, 36*(1), 2–24. doi:10.1080/0731129X.2017.1298879

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280. doi:10.1080/01639625.2015.1012409

Leung, D., Lo, A., Fong, L., & Law, R. (2015). Applying the Technology-Organization-Environment framework to explore ICT initial and continued adoption: An exploratory study of an independent hotel in Hong Kong. *Tourism Recreation Research, 40*(3), 391-406. doi:10.1080/02508281.2015.1090152

Leung, K., & Wang, J. (2015). Social processes and team creativity in multicultural teams: A socio-technical framework. *Journal of Organizational Behavior, 36*(7), 1008–1025. doi:10.1002/job.2021

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care, 4*(3), 324. doi:10.4103/2249-4863.161306

Leuprecht, C., Skillicorn, D., & Tait, V. (2016). Beyond the castle model of cyber-risk and cyber-security. *Government Information Quarterly, 33*(2), 250-257. doi:10.1016/j.giq.2016.01.012

Li, F., Trutnevyte, E., & Strachan, N. (2015). A review of socio-technical energy transition (STET) models. *Technological Forecasting and Social Change, 100*, 290-305. doi:10.1016/j.techfore.2015.07.017

Li, S., Bi, F., Chen, W., Miao, X., Liu, J., & Tang, C. (2018). An improved information security risk assessment method for cyber-physical-social computing and networking. IEEE *Access, 6,* 10311-10319. doi:10.1109/access.2018.2800664

Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., & Leung, V. (2018). A survey on security threats and defensive techniques of machine learning: A data-driven view. *IEEE Access, 6*, 12103-12117. doi:10.1109/access.2018.2805680

Lu, Z., Yang, Y., Wen, X., Ju, Y., & Zheng, W. (2011). A cross-layer resource allocation scheme for ICIC in LTE-Advanced. *Journal of Network and Computer Applications, 34*(6), 1861-1868. doi:10.1016/j.jnca.2010.12.019

Lyon, B. K., & Popov, G. (2016). The art of assessing risk. *Professional Safety, 61*(3), 40-51. Retrieved from https://www.assp.org/publications/professional-safety

Ma, S., Mu, Y., & Susilo, W. (2018). A Generic Scheme of plaintext-checkable database encryption. *Information Sciences, 429*, 88-101. doi:10.1016/j.ins.2017.11.010

Macaulay, T. (2017). The anatomy of the Internet of things. *Riot Control,* 27-55. doi:10.1016/b978-0-12-419971-2.00002-9

Madill, A., & Sullivan, P. (2018). Mirrors, portraits, and member checking: Managing difficult moments of knowledge exchange in the social sciences. *Qualitative Psychology, 5*(3), 321–339. doi:10.1037/qup0000089

Malinowski, A., & Czarnul, P. (2018). Three levels of fail-safe mode in MPI I/O NVRAM distributed cache. *Procedia Computer Science, 136,* 52-61. doi:10.1016/j.procs.2018.08.237

Malterud, K., Siersma, V., & Guassora, A. (2016). Sample size in qualitative interview studies. *Qualitative Health Research, 26*(13), 1753-1760. doi:10.1177/1049732315617444

Mannay, D., & Morgan, M. (2015). Doing ethnography or applying a qualitative technique? Reflections from the 'waiting field.' *Qualitative Research, 15*(2), 166-182. doi:10.1177/1468794113517391

Mansfield-Devine, S. (2016a). The death of defense in depth. *Computer Fraud & Security, 2016*(6), 16-20. doi:10.1016/s1361-3723(15)30048-8

Mansfield-Devine, S. (2016b). Creating security operations centres that work. *Network Security, 2016*(5), 15-18. doi:10.1016/s1353-4858(16)30049-6

Mansfield-Devine, S. (2017). A process of defense – securing industrial control systems. *Network Security, 2017*(2), pp.14-19. doi:10.1016/S1353-4858(17)30018-1

Mansfield-Devine, S. (2019). Close to home: building in-house security expertise. *Computer Fraud & Security,* (9), 16-19. doi:10.1016/s1361-3723(19)30098-3

Mao, J., Bian, J., Tian, W., Zhu, S., Wei, T., Li, A., & Liang, Z. (2018). Detecting Phishing Websites via Aggregation Analysis of Page Layouts. *Procedia Computer Science, 129,* 224-230. doi:10.1016/j.procs.2018.03.053

Marjanovic, O., & Murthy, V. (2016). From product-centric to customer-centric services in a financial institution - exploring the organizational challenges of the transition

process. *Information Systems Frontiers, 18*(3), 479-497. doi:10.1007/s10796-015-9606-x

Markelj, B., & and Zgaga, S. (2016). Comprehension of cyber threats and their consequences in Slovenia. *Computer Law & Security Review, 32*(3), 513-525. doi:10.1016/j.clsr.2016.01.006

Martínez-Mesa, J., González-Chica, D., Duquia, R., Bonamigo, R., & Bastos, J. (2016). Sampling: how to select participants in my research study? *Anais Brasileiros De Dermatologia, 91*(3), 326-330. doi:10.1590/abd1806-4841.20165254

Massacci, F., Ruprai, R., Collinson, M., & Williams, J. (2016). Economic impacts of rules- versus risk-based cybersecurity regulations for critical infrastructure providers. *IEEE Security & Privacy, 14*(3), 52-60. doi:10.1109/msp.2016.48

McAlpine, L. (2016). Why might you use narrative methodology? A story about narrative. Eesti Haridusteaduste Ajakiri. *Estonian Journal of Education, 4*(1), 32-57. doi:10.12697/eha.2016.4.1.02b

McEvoy, B. T., & Machi, L. A. (2012). *The Literature Review*: Six Steps to Success. London: SAGE.

McFadyen, J., & Rankin, J. (2016). The Role of Gatekeepers in Research: Learning from Reflexivity and Reflection. *GSTF Journal of Nursing and Health Care, 4*(1), 82-88. Retrieved from http://dl6.globalstf.org/index.php/jnhc

McIntosh, M., & Morse, J. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research, 2*, doi:10.1177/2333393615597674

McKim, C. (2017). The value of mixed methods research. *Journal of Mixed Methods Research, 11(*2), 202-222. doi:10.1177/1558689815607096

McNeese, M., & Hall, D. (2017). The cognitive sciences of cyber-security: A Framework for advancing socio-cyber systems. *Theory and Models for Cyber Situation Awareness,* 173-202. doi:10.1007/978-3-319-61152-5_7

Mdunyelwa, V., Futcher, L., & van Niekerk, J. (2019). An Educational Intervention for Teaching Secure Coding Practices. IFIP Advances In Information And Communication Technology, 3-15. doi:10.1007/978-3-030-23451-5_1

Meriah, I., & Arfa Rabai, L. (2019). Comparative study of ontologies based ISO 27000 series security standards. *Procedia Computer Science, 160,* 85-92. doi:10.1016/j.procs.2019.09.447

Mesquida, A., & Mas, A. (2015). Integrating IT service management requirements into the organizational management system. *Computer Standards & Interfaces, 37,* 80-91. doi:10.1016/j.csi.2014.06.005

Meszaros, J., & Buchalcevova, A. (2017). Introducing OSSF: A framework for online service cybersecurity risk management. *Computers & Security, 65,* 300-313. doi:10.1016/j.cose.2016.12.008

Mitchell, G. (2015). Use of interviews in nursing research. *Nursing Standard, 29*(43), 44-48. doi:10.7748/ns.29.43.44.e8905

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

Moon, K., Brewer, T., Januchowski-Hartley, S., Adams, V., & Blackman, D. (2016). A guideline to improve qualitative social science publishing in ecology and conservation journals. *Ecology and Society, 21*(3). doi:10.5751/es-08663-210317

More, M., Jadhav, M., & Nalawade, K. (2015). Online banking and cyber-attacks: The current scenario. *International Journal of Advanced Research in Computer Science and Software Engineering, 5*(12), 743-749. Retrieved from http://www.ijarcsse.com

Morrison, P., & Stomski, N. J. (2015). Embracing participation in mental health research: Conducting authentic interviews. *Qualitative Research Journal, 15*(1), 47-60. doi:10.1108/QRJ-05-2014-0021

Morse, J. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research, 25*(9), 1212-1222. doi:10.1177/1049732315588501

Morse, W., Lowery, D., & Steury, T. (2014). Exploring saturation of themes and spatial locations in qualitative public participation geographic information systems research. *Society & Natural Resources, 27*(5), 557-571. doi:10.1080/08941920.2014.888791

Mubarak, S. (2016). Developing a theory-based information security management framework for human service organizations. *Journal of Information, Communication, and Ethics in Society,14*(3)254-271. doi:10.1108/JICES-06-2015-0018

Mugarza, I., Amurrio, A., Azketa, E., & Jacob, E. (2019). Dynamic Software Updates to Enhance Security and Privacy in High Availability Energy Management Applications in Smart Cities. IEEE Access, 7, 42269-42279. doi:10.1109/access.2019.2905925

Naseer, H., Shanks, G., Ahmad, A., & Maynard, S. (2017). Towards an analytics-driven information security risk management: A contingent resource-based perspective. *In Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017*. Retrieved from https://aisel.aisnet.org/ecis2017_rip/17

National Information Technology Development Agency. (2019). Nigeria Data Protection Regulation. Retrieved from https://nitda.gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf

Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cybersecurity: A survey of techniques. *Computers & Security, 70,* 436-454. doi:10.1016/j.cose.2017.06.010

Neal, P., & Ilsever, J. (2016). Protecting information: Active cyber defense for the business entity: A prerequisite policy. *Academy of Strategic Management Journal, 15*(2), 15-35. Retrieved from https://www.abacademies.org/journals/academy-of-strategic-management-journal-home.html

Nelson, A., & Cohn, S. (2015). Data collection methods for evaluating museum programs and exhibitions. *Journal of Museum Education, 40*(1), 27-36.

doi:10.1080/10598650.2015.11510830

Ngwu, F. (2014). Promoting formal financial inclusion in Africa: An institutional re-examination of the policies with a case study of Nigeria. *Journal of Banking Regulation, 16*(4), 306-325. doi:10.1057/jbr.2014.13

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. European Journal of Information Systems, 26(1), 1-20. doi:10.1057/s41303-016-0025-y.

Nowell, L., Norris, J., White, D., & Moules, N. (2017). Thematic analysis. *International Journal of Qualitative Methods, 16*(1). doi:10.1177/1609406917733847

Ojeka, S., Ben-Caleb, E., & Ekpe, E. (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. International Review of Management and Marketing, 7 (2), 340-346. Retrieved from http://dergipark.org.tr/en/

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management, 51*(5), 497-510. doi:10.1016/j.im.2014.03.006

Omotubora, A., & Basu, S. (2018). Regulation for e-payment systems: Analytical approaches beyond private ordering. *Journal of African Law, 62*(02), 281-313. doi:10.1017/s0021855318000104

Onwudiwe, I., Odo, J., & Onyeozili, E. (2007). Deterrence theory. *Encyclopedia of Prisons & Correctional Facilities,* 233-237. doi:10.4135/9781412952514.n91

Orzen, S. (2014). Interaction understanding in the OSI model functionality of networks

with case studies. 2014 IEEE 9Th IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI). doi:10.1109/saci.2014.6840086

Owen, G. T. (2014). Qualitative methods in higher education policy analysis: Using interviews and document analysis. *Qualitative Report, 19*(26), 1-19. Retrieved from https://nsuworks.nova.edu/tqr

Ozili, P. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review, 18*(4), 329-340. doi:10.1016/j.bir.2017.12.003

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security, 88,* 101608. doi:10.1016/j.cose.2019.101608

Padayachee, K. (2016). An assessment of opportunity-reducing techniques in information security: An insider threat perspective. *Decision Support Systems, 92*, 47-56. doi:10.1016/j.dss.2016.09.012

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*(5), 533-544. doi:10.1007/s10488-013-0528-y

Pan, Y. (2016). Heading toward Artificial Intelligence 2.0. *Engineering*, *2*(4), 409-413. doi:10.1016/j.eng.2016.04.018

Pearson, N. (2014). A larger problem: financial and reputational risks. *Computer Fraud*

& Security, 2014(4), 11-13. doi:10.1016/s1361-3723(14)70480-4

Peeler, A., Fulbrook, P., Edward, K., & Kinnear, F. (2019). Parents' experiences of care in a paediatric emergency department: A phenomenological inquiry. *Australasian Emergency Care*. doi:10.1016/j.auec.2018.12.004

Peikari, M., Salama, S., Nofech-Mozes, S., & Martel, A. (2018). A cluster-then-label semi-supervised learning approach for pathology image classification. *Scientific Reports, 8(*1). doi:10.1038/s41598-018-24876-0

Peters, K., & Halcomb, E. (2015). Interviews in qualitative research. *Nurse Researcher, 22*(4), 6-7. doi:10.7748/nr.22.4.6.s2

Petrangeli, G. (2019). Defence in depth. *Nuclear Safety,* 115-118. doi:10.1016/b978-0-12-818326-7.00009-3

Phaphoom, N., Wang, X., Samuel, S., Helmer, S., & Abrahamsson, P. (2015). A survey study on major technical barriers affecting the decision to adopt cloud services. *Journal of Systems and Software, 103*, 167-181. doi:10.1016/j.jss.2015.02.002

Pickard, M., Roster, C., & Chen, Y. (2016). Revealing sensitive information in personal interviews: Is self-disclosure easier with humans or avatars, and under what conditions? *Computers in Human Behavior, 65*, 23-30. doi:10.1016/j.chb.2016.08.004

Pieters, W., Hadžiosmanović, D., & Dechesne, F. (2015). Security-by-Experiment: Lessons from Responsible Deployment in Cyberspace. *Science and Engineering Ethics, 22*(3), 831-850. doi:10.1007/s11948-015-9648-y

Plamondon, K., Bottorff, J., & Cole, D. (2015). Analyzing data generated through

deliberative dialogue. *Qualitative Health Research, 25*(11), 1529-1539. doi:10.1177/1049732315581603

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2015). A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia. International *Journal of Computer Network and Information Security, 7*(11), 1-8. doi:10.5815/ijcnis.2015.11.01 1

Proenca, D., Estevens, J., Vieira, R., & Borbinha, J. (2017). Risk management: A maturity model based on ISO 31000. *2017 IEEE 19th Conference on Business Informatics (CBI)*. doi:10.1109/cbi.2017.40.doi:10.1109/cbi.2017.40

Purvis, R., Henry, R. M., Tams, S., Grover, V., McGregor, J. D., & Davis, S. (2016). The impact of residual risk and resultant problems on information systems development project performance. *Project Management Journal, 47*(4), 51-67. doi:10.1177/875697281604700405

Qiu, M., Gai, K., Thuraisingham, B., Tao, L., & Zhao, H. (2018). Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. *Future Generation Computer Systems, 80*, 421-429. doi:10.1016/j.future.2016.01.006

Racuciu, C., & Eftimie, S. (2015). Security threats and risks in cloud computing. *Scientific Bulletin of Naval Academy, 18*(1).Retrieved from https://www.anmb.ro/buletinstiintific/eng/index.html

Rae, K., Sands, J., & Subramaniam, N. (2017). Associations among the five components within COSO internal control-integrated framework as the underpinning of

quality corporate governance. *Australasian Accounting Business & Finance Journal, 11*(1), 28–54. doi:10.14453/aabfj.v11i1.4

Rahimian, F., Bajaj, A., & Bradley, W. (2016). Estimation of deficiency risk and prioritization of information security controls: A data-centric approach. *International Journal Of Accounting Information Systems, 20*, 38-64. doi:10.1016/j.accinf.2016.01.004

Rajan, A., Ravikumar, R., & Shaer, M. (2017). UAE cybercrime law and cybercrimes — An analysis. *2017 International Conference on Cyber Security and Protection Of Digital Services (Cyber Security)*. doi:10.1109/cybersecpods.2017.8074858

Ramsey, D. B. (2016). Data security: Evolving legal duties and challenges for franchise systems. *Journal of Internet Law, 20*(3), 3-17. Retrieved from https://lrus.wolterskluwer.com/store/product/journal-of-internet-law/

Rasekh, A., Hassanzadeh, A., Mulchandani, S., Modi, S., & Banks, M. (2016). Smart water networks and cybersecurity. *Journal of Water Resources Planning and Management, 142*(7), 01816004. doi:10.1061/(asce)wr.1943-5452.0000646..

Rayev, A. (2017). Criminal and legal protection of information security: The experience of foreign legislation. *Journal of Advanced Research in Law And Economics, 7*(7), 1822-1827. Retrieved from https://journals.aserspublishing.eu/jarle/

Razak, N. A., Jalil, H. A., Krauss, S. E., & Ahmad, N. A. (2018). Successful implementation of information and communication technology integration in Malaysian public schools: An activity systems analysis approach. *Studies in Educational Evaluation, 58,* 17–29. doi:10.1016/j.stueduc.2018.05.003

Read, G., Salmon, P., & Lenné, M. (2016). When paradigms collide at the road-rail interface: evaluation of a sociotechnical systems theory design toolkit for cognitive work analysis. *Ergonomics*, *59*(9), 1135-1157. doi:10.1080/00140139.2015.1134816

Reece, R., & Stahl, B. (2015). The professionalization of information security: Perspectives of UK practitioners. *Computers & Security*, *48*, 182-195. doi:10.1016/j.cose.2014.10.007

Riza, I. (2017). Risk management from the information security perspective. *Junior Scientific Researcher*, *3*(2), 1-8. Retrieved from https://www.jsrpublishing.com/

Rosenthal, M. (2016). Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in Pharmacy Teaching and Learning*, *8*(4), 509-516. doi:10.1016/j.cptl.2016.03.021

Rothrock, R., Kaplan, J., & Van Der OORD, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *9*(2). Retrieved from https://sloanreview.mit.edu/

Rubio, J., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers & Security*, *87*, 101561. doi:10.1016/j.cose.2019.06.015

Runfola, A., Perna, A., Baraldi, E., & Gregori, G. (2017). The use of qualitative case studies in top business and management journals: A quantitative analysis of recent patterns. *European Management Journal*, *35*(1), 116-127. doi:10.1016/j.emj.2016.04.001

Safa, N., Maple, C., Furnell, S., Azad, M., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems, 97,* 587-597. doi:10.1016/j.future.2019.03.024

Sano, F., Okamoto, T., Winarno, I., Hata, Y., & Ishida, Y. (2016). A Cyber attack-resilient server using hybrid virtualization. *Procedia Computer Science, 96*, 1627-1636. doi:10.1016/j.procs.2016.08.210

Sansorg. (2019). *CIS Critical Security Controls*. Retrieved from https://www.sans.org/critical-security-controls

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Participant anonymity in the internet age: From theory to practice. *Qualitative Research in Psychology, 12(*2), 125-137. doi:10.1080/14780887.2014.948697

Saunders, J. (2016). Confidentiality. *Medicine*, *44*(10), 596-597. doi:10.1016/j.mpmed.2016.07.014

Scarfò, A. (2018). The cybersecurity challenges in the IoT era. *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*, 53-76. doi:10.1016/B978-0-12-811373-8.00003-3

Seago, J. (2015). Defense in depth. *Internal Auditor, 72*(5), 26-31. Retrieved from https://iaonline.theiia.org

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314-341. doi:10.1080/07421222.2015.1063315

Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., & Conroy, D., . . . Olli, P. (2017). A collaborative cyber incident management system for European interconnected critical infrastructures. *Journal of Information Security and Applications, 34,* 166-182. doi:10.1016/j.jisa.2016.05.005

Shabani, M., & Borry, P. (2017). Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European Journal of Human Genetics, 26*(2), 149-156. doi:10.1038/s41431-017-0045-7.

Shackelford, S. (2016). Business and cyber peace: We need you! *Business Horizons, 59*(5), 539-548. doi:10.1016/j.bushor.2016.03.015

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

Sharafaldin, I., Lashkari, A., & Ghorbani, A. (2019). An evaluation framework for network security visualizations. *Computers & Security, 84,* 70-92. doi:10.1016/j.cose.2019.03.005

Shulong, Y. (2014). Study on prevention and control countermeasures of information technical crimes in finance. *2014 Sixth International Conference on Measuring Technology and Mechatronics Automation*. doi:10.1109/icmtma.2014.152

Sicari, S., Rizzardi, A., Miorandi, D., & and Coen-Porisini, A. (2018). REATO: Reacting to Denial of Service attacks in the Internet of Things. *Computer Networks, 137,* 37-48. doi:10.1016/j.comnet.2018.03.020

Simpson, A., & Quigley, C. F. (2016). Member checking process with adolescent

students: Not just reading a transcript. *Qualitative Report, 21*(2), 377-392. Retrieved from https://nsuworks.nova.edu/tqr/

Singh, A., & Masuku, M. (2014). Sampling techniques & determination of sample size in applied statistics research: An overview. *International Journal of Economics, Commerce, and Management, 2*(11). Retrieved from http://ijecm.co.uk/

Singh, H., & Sittig, D. (2016). A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Applied Clinical Informatics, 07*(02), 624-632. doi:10.4338/aci-2016-04-soa-0064

Singh, U., Joshi, C., & Kanellopoulos, D. (2019). A framework for zero-day vulnerabilities detection and prioritization. *Journal of Information Security and Applications, 46,* 164-172. doi:10.1016/j.jisa.2019.03.011

Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database, 38*(1), 60. doi:10.1145/1216218.1216224

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security, 60,* 154-176. doi:10.1016/j.cose.2016.04.003

Slade, S., & Sergent, S. (2019). Interview Techniques. Retrieved from: https://www.ncbi.nlm.nih.gov/books/NBK526083

Sohrabi Safa, N., 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

Soomro, Z., Shah, M., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215-225. doi:10.1016/j.ijinfomgt.2015.11.009

Soyemi, J., Soyemi, O., & Hammed, M. (2015). Nigeria cashless culture: The open issues. *International Journal of Engineering Sciences, 4*(4), 51-56. Retrieved from https://www.researchgate.net/

Spanos, G., & and Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security, 58*, 216-229. doi:10.1016/j.cose.2015.12.006

Spiers, J., Morse, J., Olson, K., Mayan, M., & Barrett, M. (2018). Reflection/Commentary on a Past Article: "Verification Strategies for Establishing Reliability and Validity in Qualitative Research." *International Journal Of Qualitative Methods, 17*(1), 160940691878823. doi:10.1177/1609406918788237

Srinidhi, B., Yan, J., & Tayi, G. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems, 75*, 49-62. doi:10.1016/j.dss.2015.04.011 9/access.2016.2538818

Srivastava, U., & Gopalkrishnan, S. (2015). Impact of big data analytics on banking sector: Learning for Indian banks. *Procedia Computer Science, 50*, 643-652. doi:10.1016/j.procs.2015.04.098

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in

information security policy compliance. *Managerial Auditing Journal, 33*(4), 410-424. doi:10.1108/maj-07-2017-1596

Stang, J. (2015). Ethics in action: Conducting ethical research involving human subjects: A primer. *Journal of the Academy of Nutrition and Dietetics, 115*(12), 2019-2022. doi:10.1016/j.jand.2015.10.006

Stanton, N., & Harvey, C. (2016). Beyond human error taxonomies in assessment of risk in sociotechnical systems: a new paradigm with the EAST 'broken-links' approach. *Ergonomics, 60*(2), 221-233. doi:10.1080/00140139.2016.1232841

Steinbart, P., Raschke, R., Gal, G., & Dilla, W. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society, 71*, 15-29. doi:10.1016/j.aos.2018.04.005

Stergiou, T., Leeson, M., & Green, R. (2004). An alternative architectural framework to the OSI security model. *Computers & Security, 23*(2), 137-153. doi:10.1016/j.cose.2003.09.001

Sullivan, J., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *The Electricity Journal, 30*(3), 30-35. doi:10.1016/j.tej.2017.02.006

Suomalainen, J., & Julku, J. (2016). Enhancing privacy of information brokering in smart districts by adaptive pseudonymization. *IEEE Access, 4*, 914-927. doi:10.1109/access.2016.2538818

Szabla, D., Pasmore, W., Barnes, M., & Gipson, A. (2017). *The Palgrave Handbook of*

Organizational Change Thinkers. Cham: Springer International Publishing AG.

Taiwo, J., & Agwu, E. (2016). Overview of management and functional activities in Nigerian banking industry. *International Journal Of Economics, Commerce and, Management, 4*(7). Retrieved from http://ijecm.co.uk/

Tang, C., & Liu, J. (2015). Selecting a trusted cloud service provider for your SaaS program. *Computers & Security, 50,* 60-73. doi:10.1016/j.cose.2015.02.001

Tankard, C. (2016). What the GDPR means for businesses. *Network Security, 2016*(6), 5-8. doi:10.1016/s1353-4858(16)30056-3

Tarhini, A., Mgbemena, C., Trab, M., & Masa'deh, R. (2015). User adoption of online banking in Nigeria: *A Qualitative Study. Journal of Internet Banking and Commerce, 20*(132).

Tchernykh, A., Schwiegelsohn, U., Talbi, E., & Babenko, M. (2016). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science.* doi:10.1016/j.jocs.2016.11.011

Tedeschi, S., Emmanouilidis, C., Mehnen, J., & Roy, R. (2019). A Design Approach to IoT Endpoint Security for Production Machinery Monitoring. *Sensors, 19*(10), 2355. doi:10.3390/s19102355

Teusner, A. (2016). Insider research, validity issues, and the OHS professional: one person's journey. *International Journal of Social Research Methodology, 19*(1), 85–96. doi:10.1080/13645579.2015.1019263

Thomas, J. R., Silverman, S., & Nelson, J. (2015). *Research methods in physical activity*

(7th ed.). Champaign, IL: Human Kinetics.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security, 79,* 68-79. doi:0.1016/j.cose.2018.08.007

Tran, H., Campos-Nanez, E., Fomin, P., & Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *Computers & Security, 61*, 19-31. doi:10.1016/j.cose.2016.05.001

Tu, C. Z., Yufei, Y., Archer, N., & Connelly, C. E. (2018). Strategic value alignment for information security management: A critical success factor analysis. *Information and Computer Security, 26*(2), 150-170. doi:10.1108/ICS-06-2017-0042

Tubío Figueira, P., López Bravo, C., & Rivas López, J. (2019). Improving information security risk analysis by including threat-occurrence predictive models. *Computers & Security, 88,* 101609. doi:10.1016/j.cose.2019.101609

U.S. Department of Health & Human Services. (2010). *The Belmont Report*. Retrieved from https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/

Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security, 89,* 101666. doi:10.1016/j.cose.2019.101666

van de Wiel, M. J. (2017). Examining expertise using interviews and verbal protocols. *Frontline Learning Research, 5*(3), 112-140.

van Manen, M. (2017). But is it phenomenology? *Qualitative Health Research, 27*(6), 775-779. doi:10.1177/1049732317699570.

Veloudis, S., Paraskakis, I., Petsos, C., Verginadis, Y., Patiniotakis, I., Gouvas, P., & Mentzas, G. (2019). Achieving security-by-design through ontology-driven attribute-based access control in cloud environments. *Future Generation Computer Systems, 93*, 373-391. doi:10.1016/j.future.2018.08.042

Vigil, M., Buchmann, J., Cabarcas, D., Weinert, C., & Wiesmaier, A. (2015). Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: A survey. *Computers & Security, 50,* 16-32. doi:10.1016/j.cose.2014.12.004

Wagner, J., Rasin, A., Glavic, B., Heart, K., Furst, J., Bressan, L., & Grier, J. (2017). Carving database storage to detect and trace security breaches. *Digital Investigation, 22*, S127-S136. doi:10.1016/j.diin.2017.06.006

Wagner, T., Mahbub, K., Palomar, E., & Abdallah, A. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security, 87,* 101589. doi:10.1016/j.cose.2019.101589

Wang, R. (2017). Research on Data Security Technology Based on Cloud Storage. *Procedia Engineering, 174*, 1340-1355. doi:10.1016/j.proeng.2017.01.286

Wang, X., Weng, J., Ma, J., & Yang, X. (2019). Cryptanalysis of a public authentication protocol for outsourced databases with multi-user modification. *Information Sciences, 488*, 13-18. doi:10.1016/j.ins.2019.03.002

Weber, R., & Studer, E. (2016). Cybersecurity in the Internet of things: Legal aspects. *Computer Law & Security Review, 32*(5), 715-728. doi:10.1016/j.clsr.2016.07.002

Wei, Y., Wu, W., & Chu, Y. (2017). Performance evaluation of the recommendation mechanism of information security risk identification. *Neurocomputing, 279,* 48-

53. doi:10.1016/j.neucom.2017.05.106

Weyrich, M., & Ebert, C. (2016). Reference architectures for the internet of things. *IEEE Software, 33(*1), 112-116. doi:10.1109/ms.2016.20

White, L., Burger, K., & Yearworth, M. (2016). Understanding behaviour in problem structuring methods interventions with activity theory. *European Journal of Operational Research, 249*(3), 983-1004. doi:10.1016/j.ejor.2015.07.044

Willis, D., Sullivan-Bolyai, S., Knafl, K., & Cohen, M. (2016). Distinguishing features and similarities between descriptive phenomenological and qualitative description research. *Western Journal of Nursing Research, 38*(9), 1185-1204. doi:10.1177/0193945916645499

Winchester, C., Salji, M., & Kasivisvanathan, V. (2017). Gathering preliminary data. *Journal of Clinical Urology, 10*(6), 568-572. doi:10.1177/2051415817724713.

Wolgemuth, J., Hicks, T., & Agosto, V. (2017). Unpacking assumptions in research synthesis: A critical construct synthesis Approach. *Educational Researcher, 46*(3), 131-139. doi:10.3102/0013189X17703946

Xu, B., Xu, Z., & Li, D. (2016). Internet aggression in online communities: a contemporary deterrence perspective. *Information Systems Journal, 26*(6), 641–667. doi:10.1111/isj.12077

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report, 20*(2), 134-152. Retrieved from http://nsuworks.nova.edu/tqr

Yin, R. K. (1981). The case study crisis: Some answers. *Administrative Science*

Quarterly, 26(1), 58-65. doi:10.2307/2392599

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 Publications.

Yin, R. K. (2017). *Case study research and applications: Designs and methods* (6th ed.). Thousand Oaks, CA: Sage Publications.

Zhang, N., Paraskevas, A., & Altinay, L. (2019). Factors that shape a hotel company's risk appetite. *International Journal Of Hospitality Management, 77,* 217-225. doi:10.1016/j.ijhm.2018.07.001

Appendix: Study Interview Protocol & Guide

Initial Probe Questions

Thank you for the opportunity for this interview. What is the title of your current role? How long have you been on the role? Where does the role sit within your organizational structure?

Kindly describe briefly the current job responsibilities of the role. Has this role always had these responsibilities or it has evolved to be this? What were the drivers for the evolution? Are there particular prerequisites for the industry in terms of certification for anyone that takes on this role?

On a normal day what would say your activity look like?

Targeted Concept Questions

1. What are the risks that is of concern to you as a player in the financial services sector in Nigeria in your use of IT tools for operations? Please briefly describe your information security management process. Do you have an Information security policy in place? Do you have in internal control process that monitor for compliance? How do you deal with arising contingencies when policies requirements are not adhered to?
2. In what ways have organizations in your sector of the economy experienced cyber exploitations? What was the nature of the exploitations experienced? Which of the exploitations are prevalent and why?
3. Has there been a time you experienced information security exploitations? Which of integrity, confidentiality or availability of information did it

affect? If you have experienced a cyber-exploitation, did you have an incident management system in place? What were your lessons learned? What did you do differently after the incidence?

4. How do you decide what to do in your role to support the IT strategy and ultimately the corporate strategy of your organization? Are there policies, regulations that effect what you do in your role? Please state specific strategies that you must deploy (if any) to ensure confidentiality, availability and integrity of information because of your industry.
5. What have you done to ensure that confidentiality of information is preserved? What have you done to ensure information are not illegally modified? What have you done to be sure legal users are not denied access to information when they need them? Which specific risks did you have in mind while carrying out activities above?
6. Are there steps you take in securing your operations while hiring staff at any level and for different roles? What skill levels do you look at for hiring purposes? How important is, background checks to your business?
7. How do you ensure you discover weaknesses in your IT systems before hackers exploit the weaknesses? Do you do conduct vulnerability assessments? /penetration tests? If you do, has there been a time you had to deploy new strategies for information security after the assessments? what were these?

8. In what ways have regulatory certifications helped you to prevent cyber exploitations that could have violated confidentiality, availability and integrity of information. Which of the regulatory certifications do you possesses as an organization?
9. What are the existing management process that support your efforts to prevent cyber exploitation of information assets. Please describe your board's role in your information security management process.
10. Please explain measures you have in place to prevent cyber exploitation of your information assets because of your staff leaving, which in some cases may be to join your competitors. To what extent are these processes documented?

Follow up Questions

1. What are your 3 most important security projects that you are currently working on? What are the drivers for those projects?
2. How typically will you describe your current security posture, adequate? evolving? needs improvement? Please explain.
3. How do you think a CISO without a strategy will fare, 3 years from now?
4. How integrated are your Human Resources (HR) Policies and your Information security efforts

a. Are there sanctions where there are deliberate or careless failures of staff?

b. Do you have information security awareness campaigns? What role does it play in your overall information security strategy?