2022

Leadership Strategies to Reduce Cyberattacks During a Merger

Denise Durham
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Denise Durham

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. Marilyn Simon, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Olivia Herriford, Committee Member, Doctor of Business Administration Faculty

Dr. Judith Blando, University Reviewer, Doctor of Business Administration Faculty

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

Walden University
2022

Abstract

Leadership Strategies to Reduce Cyberattacks During a Merger

by

Denise Durham

MS, New Jersey Institute of Technology, 2000

BS, York College, 1995

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

October 2022

Abstract

The difficulty that leaders in the wine industry have in rapidly responding to cyber threats to secure sensitive information and intellectual property while undertaking a merger can have a direct economic cost and disrupt the merger. Grounded in Habermas's systems theory, the purpose of this single case study was to examine strategies used to mitigate the risk from cyberattacks during a merger. The participants were five business leaders in a wine company in Northern California. Data were collected using semistructured interviews, company documentation, and publicly available documents. Through thematic analysis, four themes were identified: protection of data integrity, formal and informal communication/feedback methods, training, and establishing cybersecurity frameworks to increase security. A key recommendation is for business leaders to fully understand where data reside and who is managing data to ensure that cybersecurity control measures are working. Implications for positive social change include the potential for business leaders to build prevention strategies that can lower the risk of a data breach during a merger to provide better safeguards to protect the privacy of customers' information and preserve companies' sensitive information and intellectual property. These change initiatives can positively impact customer satisfaction and help promote job growth within the community.

Leadership Strategies to Reduce Cyberattacks During a Merger

by

Denise Durham

MS, New Jersey Institute of Technology, 2000

BS, York College, 1995

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

October 2022

Dedication

I want to dedicate my doctoral research study to my grandfather, Quinton Martin, who has been gone for quite some time but continues to be in my thoughts and prayers. To Quinton Martin, who saw something special within me at a very young age that I, myself, failed to realize until I reached adulthood. To my husband, Christopher James Perdue, who has the patience of a saint, provided continual words of encouragement, and most importantly gave me "eye kisses" to make me laugh and keep my spirits up. To my mother-in-law, Patricia Perdue, who has always been willing to get me to and from the airport no matter what time of day or night to keep me on my work and school schedule. To my parents, James and Editha Durham, who always encouraged me to get my education and to pursue my dreams. To my chair, Dr. Marilyn Simon, who has been my rock throughout my doctoral journey. To my SCM, Dr. Olivia Herriford, thank you for helping me develop my doctoral voice and keeping a watchful eye on my research study. And lastly, to all my other teachers/professors, friends, employees, and colleagues who continually rooted for me to succeed. I want to thank you all for being a part of my lifeline, especially when I needed it the most.

Acknowledgments

I have read quite a few acknowledgments from my school colleagues, and though most acknowledgements are not meant to be extensive, all have meaning and contain their truth about how they want to say “thank you” to those individuals who have impacted their lives, especially during their doctoral journey. While I do want to recognize and acknowledge my family, friends, teachers/professors, employees, and colleagues for their words of encouragement and convincing me to stick with my doctoral journey when I had doubts and second guessed myself, I also want to acknowledge that I believe that now I have a better understanding as to why a small percentage of the world’s population has a doctoral degree. A doctoral journey is a long, difficult, and often lonely road to travel. Pursuing a doctoral degree has the potential to impact a person’s mental and physical well-being. Even with strong support, it is often hard to explain the emotional turmoil that an individual experiences while going through the doctoral process. I recall many times when I was asked by both friend and foe, “Why are you putting yourself through a doctoral program?” My reply to this question is simply because “I can,” therefore “I am.” I believe that to succeed through a doctoral journey requires confidence, grit, and tenacity. These qualities help individuals who embark on this journey to remain focused, unwavering, and dedicated to the tasks at hand.

Therefore, not only do I want to say, “thank you,” but also I want to apologize to those individuals who crossed my path when I was not being the best “me” due to lack of sleep and poor dietary habits while going through my doctoral journey. I hope that I am deserving of a second chance to show those individuals and the world a level of kindness

that I know that I am capable of. I want to thank you all for your patience and understanding.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Mergers and acquisitions (M&As) within the wine industry have increased. In 2021, U.S. business leaders invested $1 trillion in M&A transactions (Trentmann, 2021). Hackers have become progressively more sophisticated in gathering data about the financial status and future business strategies for companies (U.S. Securities and Exchange Commission [SEC], 2017). M&As have also made the information technology (IT) environment increasingly complex, with over half of unaccounted-for devices found after completing the integration of a new acquisition (Siwicki, 2017; Vincent & Trussel, 2019). There is a need for business leaders to rapidly respond to cyberthreats to secure sensitive information and intellectual property. Due to continual changes in technology, some wine companies have struggled to maintain sound IT infrastructures and avoid the risk of cyberattacks.

Background of the Problem

There is a lack of empirical research that identifies the vulnerabilities of IT infrastructures during a business merger or acquisition, specifically within the wine industry. Little is known about established processes or procedures that serve as guides for business leaders to develop a framework to successfully evaluate the risk associated with cyberattacks during a business merger or acquisition. One of the most common mistakes that business leaders entering a M&A make is not having a comprehensive understanding of the inherent risk of cyberattacks.

Fritz and Kaefer (2017) highlighted the critical importance of establishing security controls and formulating policies to reduce the risk of a cyberattack. Bauer et al.

(2017) suggested that complacency has caused business leaders to not address outdated IT infrastructures during a merger or acquisition. This complacency has provided opportunities for hackers to infiltrate wine company information systems and disrupt operations. Leaders and employees share thousands of documents between networks during a merger or acquisition. Unfortunately, some business leaders lack the insight to check and verify the security of the documents being shared. This issue may cause a business to lose revenue and customers (Watad et al., 2018).

Problem Statement

For M&As to be successful in advancing a business's competitive advantage, comprehensive security control measures must be enacted to reduce the risk of cyberattacks (Schmidt et al., 2020). In 2017, the costs involved in M&As were estimated at $4.7 trillion, and more than one third of businesses involved in those M&As contended with IT failures caused by security breaches and cyberattacks (Bashan & Armon, 2019; Triche & Walden, 2018). The general problem is that industry leaders enter a merger without the appropriate strategies to manage the risk of cyberattacks. The specific business problem is that some wine industry leaders lack cybersecurity strategies to manage the risk of data breach from cyberattacks during a merger.

Purpose Statement

The purpose of this qualitative single case study was to explore strategies that leaders in the wine industry used to mitigate the risk from cyberattacks during a merger. The targeted population was business leaders at a wine company located in California who successfully protected their company's data during a business merger. The

implications for positive social change include the reduction of loss of company revenue, which directly impacts jobs and services, therefore having a positive economic effect on local communities.

Nature of the Study

The three research methods used by scholarly researchers are quantitative, qualitative, and mixed methods (Saunders, 2020). I selected the qualitative method for my research study as the appropriate method to address issues related to strategies for cybersecurity. Qualitative researchers collect data to understand real-life situations that are dependent on the human experience (Tracy, 2019). Quantitative researchers seek to examine relationships among variables using numerical data to generalize from a sample using mathematical techniques and/or statistical models to relate to the phenomena (Johnson & Christensen, 2020). Mixed methods researchers use both qualitative and quantitative methodology, which could lead them to conflicting analyses (Halcomb, 2018). Quantitative and mixed methods research were not appropriate for this study, as both methods depend on analyzing numerical data and hypothesis testing to examine relationships between measured variables associated with the phenomenon, and this was not in accord with the intent of this study.

There are a variety of research designs available for a qualitative research study. The three designs that I considered were ethnographic, phenomenological, and case study. According to Cardoso et al. (2017), ethnography is the study of organizational culture and provides insight into the beliefs and assumptions of individuals within a given culture. An ethnographic design involves extensive training and time in the field to

interpret participants' experiences (Johnston et al., 2017; Preece et al., 2019). I did not focus on culture or on participant experiences; therefore, an ethnographic design was not appropriate for this study. I also considered the phenomenological design. The purpose of using a phenomenological design is to understand specific human social and psychological phenomena experienced by participants (Qutoshi, 2018).

The purpose of this study was to explore strategies and not to focus on the meaning of experience; therefore, the phenomenological design was not appropriate for this study. In a case study design, the focus is on a general situation in a real-life setting (Yin, 2018). When conducting a case study, the researcher is in control the parameters of the study (Zainal, 2017). Case study design is appropriate to explore the behaviors and events in research that result in certain conditions (Ponelis, 2015; Ridder, 2020). Using the single-case study design may provide a deeper understanding of the strategies necessary to combat cyberattacks. Single-case studies are ideal for revelatory cases where an observer may have access to a phenomenon that was previously inaccessible (Ponelis, 2015; Ridder, 2020). A single qualitative case study was appropriate for exploring the strategies used by business leaders in the wine industry to manage the risk of data breach from a cyberattack during a merger.

Research Question

What strategies do business leaders in the wine industry use to manage the risk of data breach from a cyberattack during a merger?

Interview Questions

1. What strategies did you use to protect each company's data from cyberattack during a business merger?
2. How did you integrate strategies to safeguard the company's data from cyberattack into your organizational policies to improve compliance during a business merger?
3. How did you communicate the strategies you enacted during the merger to the companies involved in the merger?
4. How did the strategies you put in place protect each company's data during the integration phase of the merger?
5. How did you determine the efficacy of the strategies you put in place to protect each company's data from a cyberattack?
6. What other factors were necessary to reduce the risk of cyberattack during a merger within your organization?
7. What additional information can you provide regarding strategies you used to manage the risk of data breach from a cyberattack during a merger?

Conceptual Framework

The conceptual framework for this study was Habermas's (1989) systems theory. Habermas's systems theory combines aspects of social science and systems thinking. Systems are designed based on degree of complexity and randomness. Systems theory involves consideration of all system inputs, outputs, feedback loops, and processes

(Shafritz et al., 2015). At the core of systems theory, there is a required level of communication and control.

Both subtle and dramatic changes in cybersecurity can amplify the long-term effect of an IT infrastructure. Business leaders, government leaders, and scholars believe that cyberattacks are increasing because of inadequate cybersecurity policies and procedures (Luo, 2016). Systems theory is a useful framework to improve cybersecurity compliance to ensure better data security to prevent a cyberattack during a merger. Cybersecurity needs a holistic approach and strategy to understand and address nontechnical and technical risks contributing to cybersecurity (Burita, 2019). Wine industry leaders should identify strategies for better data protections. IT systems are multifaceted; therefore, wine industry leaders should establish enhanced decision making and cybersecurity controls to reduce the vulnerabilities between the systems of merging companies (Hawkins, 2017). The absence of adequate protection enables cybercriminals to breach IT system networks during a business merger or acquisition. This conceptual framework is applicable because systems theory can guide business leaders' actions to understand the interdependence of complex systems and interactions to improve the efficiency of IT systems during a merger and reduce the risk of cyberattack.

Operational Definitions

Cyberattack: An attempt by an individual, group, or organization to damage, alter, disrupt, or attack computer networks, infrastructures, or systems for competitive advantage or for political, religious, or financial gains (Fen et al., 2020).

Cybercrime: Cybercrime involves the use of a computer as an instrument to commit illegal activity such as fraud, cyber ransom, or phishing (Latto, 2020).

Cybersecurity: Cybersecurity refers to the controls, strategies, or measures used to protect a computer system against unauthorized or criminal use of electronic data (Berkman et al., 2018).

Data breach: A data breach is an incident that consists of unauthorized access to sensitive or confidential data that compromises an organization's computer network (Shabani & Borry, 2018).

Mergers and acquisitions (M&As): Mergers and acquisitions refer to the consolidation of two or more companies to transfer or combine assets or equity interests. M&As are one approach used by business leaders to strengthen their organization's competitive advantage (González-Torres et al., 2020)

Phishing: Phishing refers to the fraudulent practice of sending emails to email users to elicit confidential information such as customers' personal information, financial status, or intellectual property (Wu et al., 2016).

Private cloud: A private cloud is a data center that is not available for public use to store electronic information (Tissir et al., 2020).

Assumptions, Limitations, and Delimitations

Some vital components of scholarly research are the assumptions, limitations, and delimitations of a study (Uprichard & Dawney, 2019). To improve the credibility of a study, a researcher must establish, define, and delineate the assumptions, limitations, and delimitations relevant to their study (Theofanidis & Fountouki, 2019).

Assumptions

Assumptions are defined as the presumed facts that the researcher considers true and relevant to a study without formal verification (Collins & Stockton, 2018). There were three assumptions for this research study. The first assumption was that the interview questions developed were comprehensive enough to maintain participant engagement during the interview process. The second assumption was that the business leaders who participated in this research study would provide honest and open responses to the interview questions. The third assumption was that participants would have a clear understanding of effective strategies used to reduce cyberattacks during a merger. I believe that all three assumptions were realized. Because I assured confidentiality and noted that participation was strictly voluntary, the participants were pleased to take part in the study. The participants remained engaged throughout the interview process. They provided responses that were regarded as open, honest, and insightful, and they had a clear understanding of effective strategies to reduce cyberattacks during a merger. For informational purposes, some of the participants also provided guidance to help locate and allow me access to relevant company documentation stored on the partnering company's portal.

Limitations

Limitations of a research study refer to issues or weaknesses not within the control of a researcher (Brusse et al., 2016). When conducting research, limitations could derive from bias introduced to a study by the participants during the interview process (Theofenidis & Fountonki, 2019). The first limitation was that the participants might

provide insufficient data based on their limited knowledge about cybersecurity. The second limitation was that advancements in cybersecurity are continuous, which may also limit the knowledge of the participants. Some participants during the interview process affirmed that advancements in cybersecurity are continuous and that new technology in cybersecurity should be considered when companies venture into a merger or business acquisition.

Delimitations

Research delimitations help researchers define the scope or boundary of their study prior to conducting research (Marshall & Rossman, 2016). The delimitations of a research study are the factors and variables included in the investigation (Park & Park, 2016). In addition, delimitations are the boundaries that the researcher sets in terms of study duration, population size, and type of participants (DiscoverPhDs, 2020). I selected participants who were business leaders in the wine industry with experience defining strategies to migrate cyberattacks during mergers or business acquisitions.

Significance of the Study

Business leaders face many challenges due to globalization. To remain competitive, some wine industry leaders have chosen to expand their business through M&As. The purpose of this study was to explore effective business practices that may contribute to the leaders of an organization's capability to improve cybersecurity control strategies during a merger.

Contribution to Business Practice

The results of this study may be of value to businesses whose leaders seek to maintain productivity and increase the ability to compete in the wine industry. The results of the study could contribute to effective business practices by identifying strategies to mitigate data breaches during a business merger. If wine industry leaders use the findings to avoid cyberattacks, these leaders may avert a potential threat to a successful merger.

Implications for Social Change

The results of this study may contribute to positive social change by providing economic stability to organizations that partake in a merger or acquisition. The implications for positive change include providing better safeguards to protect the privacy of customers' information. Businesses' ability to better educate their employees and customers could lead to less data breaches and improved data security. In addition, merged businesses can pass along cost savings to consumers and offer better quality of products and services (Chron, 2020). Customers' access to better products and services could improve their overall quality of life. Pursuing M&As involves both advantages and disadvantages. The advantage of a business going through a merger is that it could improve the confidentiality and privacy of customer information by increasing security awareness through effective employee training. A potential disadvantage of a merger is that a business merger going public may result in exposure to cyberattack, which can put customers' information at risk of being comprised. Because there is a possibility of a comprise, it is important to establish cybersecurity controls and strategies to minimize the risk of cyberattack (Cook, 2015).

Review of the Professional and Academic Literature

The purpose of the study was to explore effective strategies used in the wine industry regarding cybersecurity when two companies are involved in a merger or business acquisition. I synthesized information from various sources related to current literature, knowledge, and discussions on the theory, concepts, and recommendations for future studies. The conceptual frameworks guiding this study were Habermas's systems theory, adaptive systems theory, and the theory of structuration.

This literature review includes analysis of peer-reviewed articles, dissertations, and books on M&As. My search included studies pertaining to the conceptual frameworks. In reviewing the literature, I sought to compare and contrast related scholarly, professional, and government studies related to cybersecurity. The primary databases used were the Walden University Library, Google Scholar, EBSCO eBooks, Academic Search Complete, ACM Digital Library, Business Source Complete, IEEE Xplore Digital Library, ProQuest Central, and SAGE Premier. Among sources used for the literature review, 80% were published from 2018 through 2022, and 70% were scholarly peer-reviewed articles.

Systems Theory

The purpose of this qualitative single case study was to explore the strategies of business leaders in the wine industry used to mitigate the risk from cyberattacks during a merger. Cybercriminals' methods to launch attacks against businesses have become progressively sophisticated and complex (Connelly & Wall, 2019). The performance of a business is dependent on economic, ecological, and social challenges to maintain

competitive advantage at domestic and global levels (Ibarra et al., 2019). Globalization affects the complexity of a company, demanding a systematic approach to succeed and prosper (Vermeulen, 2015). Evaluating the conceptual framework of systems theory is important to understand the complexity of computer systems that can affect a business merger or acquisition and to guide business leaders to institute applicable strategies to combat cyberthreats.

Habermas (1989) characterized systems theory as the study of interrelationships rather than individual modules. Habermas contended that systems operate through purposive actions that are self-regulating and self-correcting. Kuusisto and Kuusisto (2013) described Habermas's theory as involving systems that cannot be analyzed because of complexity and cannot be analyzed statistically because of the inability to depict randomness in behavior. Systems that can be categorized as depicting organized complexity can be demonstrated by a hierarchy of levels. Each level in a hierarchy is more intricate than the level directly below it and has emergent properties, which only exist at higher levels and are irrelevant at lower levels (Salim, 2014).

Habermas posited that systemic differentiation and integration help to determine risk (Habermas, 1987). If systems become decoupled, these systems can only provide integration and coordination within boundaries and often fail to support broader integration (Yun et al., 2019). This decoupling leads to a situation in which system integration prevails over the broader integrative efforts used by business leaders (Habermas, 1987).

Bambauer (2013) described the existing approaches to cybersecurity as significantly flawed; however, scholars, governments, and computer scientists agree that inadequate security is an emerging threat and preventative action is required. Inadequate security could lead to unintended consequences (i.e., cyberattack) for an organization (Young et al., 2021). Cybersecurity technologies are insufficient to achieve secure operations without strategies, procedures, ongoing risk assessments, and review of secure network protocols to achieve efficient and secure information delivery (Kopel et al., 2019). Volkova and Cherny (2018) suggested that the systems theory approach provides a solid foundation for cybersecurity.

Applying systems theory to business leaders' cybersecurity strategies captures the influences under which firms operate in an unpredictable, dynamically changing, cyber-dependent market. Exploring successful strategies that business leaders have implemented to protect their businesses from cyberattacks during a business merger or acquisition may contribute to best practices, increase consumer confidence, and result in greater economic prosperity. Using a clear framework could provide elements to identify and prioritize actions for reducing cybersecurity risk and can help business leaders align policy and technological methodologies to manage those risks (National Institute of Standards and Technology [NIST], 2015). Bambauer (2013) explained that computer and network security problems exist because cybersecurity is undertheorized and lacks a framework to guide change.

Von Solms and Marnwick (2019) examined cybersecurity frameworks from a system view and suggested that interdependences between critical infrastructures are

becoming increasingly apparent and that understanding how to manage critical infrastructures is an emerging issue for businesses. Global interconnections have caused systems to converge, meaning an isolated attack on one vital infrastructure system can result in a cascading effect on other critical infrastructures and affect business operations (Volkova & Cherny, 2018). Exploring effective business leaders' strategies aligns with the systems theory conceptual framework.

Some business leaders underestimate the possibility of large, unexpected changes in their network systems. Though some business leaders try their best to keep organizational data secure, cybercriminals find ways to intercept computer systems, creating vulnerabilities within a network's infrastructure. Business decisions made by business leaders can be complicated due to the inherent complexity of network systems. Businesses need clear strategies and guidelines for employees to follow to protect those network systems. As sudden and drastic changes are likely to occur, business leaders should be ready to adopt new strategies and guidelines as necessary (Park et al., 2018).

An organization is a classic example of a nonlinear system in which minor events have the potential to set off grave consequences or chain reactions and major changes may have little or no effect on the system (Wilkinson & Klaes, 2017). Instead of pinpointing causes of organizational problems, a company is better served by looking for organizational patterns that lead to certain types of behavior within the organization. An organization whose leaders encourage this type of management is a *fractal organization,* which is an organization whose leaders trust natural phenomena to establish order within the organization (Wilkinson & Klaes, 2017).

Business owners build models of organizational practice and policy with the hope that this will yield better information on how to improve the organization's business functions (Gonen & Sawant, 2020). Business leaders can use systems theory to provide a framework to improve strategies, policies, and procedures needed to reduce the risk of cyberattack with a merger or acquisition. Applying the concept of systems theory may provide ways for business leaders to institute effective cybersecurity control measures and contribute to inhibiting cyberattacks during a business merger or acquisition.

Complex Adaptive Systems Theory

Like Habermas's systems theory, complex adaptive systems theory is derived from the natural sciences. Srinivasan and Mukherjee (2018) described complex adaptive systems theory as involving interacting agents that coevolve and adapt logically over a period. Complex adaptive systems theory evolves around constant change in reasonable linearity (Malik & Pretorius, 2018). A complex adaptive system is a macroscopic gathering of microstructures shaped to alter a setting (Van Brussel et al., 2016). Conversely, Akgun et al. (2014) argued that complex adaptive systems theory is a framework for explaining the emergence of system-level order arising from the interactions of a system's interdependent agents. Christo et al. (2016) identified complex adaptive systems theory as an effort to understand complex emergent behavior by reviewing exchanges between inhomogeneous parts at a micro level. Ghazzawi et al. (2016) outlined emergent behaviors and nonlinear processes as tenets of complex adaptive systems. Afzaal and Zafar (2016) noted that complex adaptive systems involve agents of dynamic networks continuously responding to other agents. Fidan and Balci

(2017) proposed that in complex adaptive systems, optimal performance occurs only when the actors work as a network of dependent components. Marjanovic and Cecez-Kecmanovic (2017) surmised that complex adaptive systems act as one unit and trade information in an open network.

Structuration Theory

In contrast to Habermas's systems theory and complex adaptive systems theory, structuration theory involves the formation and imitation of social systems. Nsiah (2022) explained that structuration theory is neither macro- nor micro-focused. Structuration theorists found structure associated with the imitation of social systems by posting structure as resources and rules (Sergeeva et al., 2017). Nasution et al. (2017) studied cybersecurity using structuration theory to investigate how security policies are formed in business to prevent data breaches. The results of the study informed the development of a theoretical model to formulate and implement comprehensive security policies.

Context of Mergers and Acquisitions

The goal of this case study was to reveal strategies that business leaders use to maintain business and maintain cybersecurity in the wine industry during a merger. The wine industry is gradually employing the merger process to deal with technological changes, increases in competition, and government regulation (DeHaas et al., 2017). Every merger is unique with respect to key factors such as business processes, location, size, and resources (Angwin & Meadows, 2015). When wine businesses merge, there is an integration process that normally engages both people and processes (DeHaas et al., 2017). Mergers often fail because organizations struggle to execute a merger effectively

(Friedman et al., , 2016). A potential merger failure is partly due to the considerable number of variables involved (Angwin, 2012). Therefore, it is important for business leaders to require strategies to address those expected variables.

A failed merger carries extraordinary risk for customers, consumers, employees, shareholders, and business partners (Eaton & Kilby, 2015; Osarenkhoe & Hyder, 2015). Garzella and Fiorentino (2014) asserted that there is a risk of diminished value that threatens the expected value creation that was the basis for a merger. The profitability of a winery can impact the success or failure of a merger.

Business leaders constantly modify and restructure processes that contribute to their overall operation to maintain or improve productivity as desired (Naus etal., 2018). Some business leaders still rely on manual processes to complete functions while others have enhanced their capabilities with the adoption of current technologies, each with varying degrees of success (LaPointe, 2017).

Theories Supporting Cybersecurity

Cybersecurity potentially impedes technological and scientific advances in information security by reinforcing the predominantly technical view of cybersecurity (von Solms & von Solms, 2018). For example, a spectrum of technical solutions supports cybersecurity. However, these solutions alone do not solve the problem; there are numerous examples that demonstrate challenges related to the organizational, economic, social, and political issues inextricably tied to cybersecurity efforts (Deibert, 2012). According to the Department of Homeland Security (2020), cybersecurity refers to the activity or process, ability or capability, or state whereby information and

communications systems and the information contained therein are protected from or defended against damage, unauthorized use or modification, or exploitation. This definition does not expound on how cybersecurity is used to reduce the risk of malicious attacks on software, computers, and networks, including the tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, and enable encrypted communications.

Monat and Gannon (2018) noted that a dynamic structure can be defined by components and configuration that consist of several interacting elements involving processing inputs and producing outputs, interconnections between different functioning parts of the system, and structured relationships (Monat & Gannon, 2018). In a modern system, each level of information is related to a level of correspondent security risk. Each level must be well defined, including a proper measure to control risks to data security (Doherty & Tajuddin, 2018).

A systemic method is a process used to manage data security; the process is based on understanding how a system's processes can effectively be structured to secure all components of the system (Doherty & Tajuddin, 2018). A system consists of integrated objects, either logical or physical, qualities that describe the objects, the objects' relationship with other objects, and the system's control environment (Gutierrez-Martinez et al., 2015). Classic security and safety problems, such as ensuring the reliability of hardware and protection from natural phenomena, modern systems are so complexed and interconnected that security threats from malicious adversaries must be carefully considered and reviewed (Alves & Morris, 2018). Cybersecurity issues are becoming

more prevalent, and cyberbreaches and malicious threats are increasingly critical and challenging (Kesan & Hayes, 2017). Onwubiko (2017) suggested that businesses can implement a protective process by introducing data security solutions to improve data security awareness while reducing cybersecurity threats.

The holistic system approach can be applied when analyzing and implementing cybersecurity strategies. By understanding the root of a breach, business leaders can support and tighten the disintegrated parts of the target system to prevent future data breaches (King et al., 2018). A shared functionality formed the process used to identify the different system functions may occur at multiple levels of the system (Rothrock et al., 2018). Chalvatzis et al. (2019) described systems that consist of diverse components to help business leaders monitor their environment by collecting information about environmental deviations.

Business leaders need to analyze and process this information to formulate solutions to their cybersecurity needs (Bagschik et al., 2017). An open system is a process used to respond and adjust to environmental changes through the input of information. These adjustments can sometimes affect organizational processes (Rothrock et al., 2018). These adjustments may reduce, increase, or support environmental change deviations (Marti, 2015). The organization can analyze information in the throughput to tailor its process to fit its goals (Rothrock et al., 2018). When wine businesses adapt to cybersecurity changes, their actions and messages represent the output, and these outputs form the process used to measure effectiveness (Hof, 2018).

When technological improvements resulting from developed security techniques become outdated, practitioners create new systems (Schabacker et al., 2019). In the past, security techniques were mainly composed of electro-mechanical components and were less complicated than today's intensive systems (Joo & Hovav, 2016). Marti (2015) found that throughput feedback creates new changes in a system. If the messages and actions are not sufficient, the process repeats until it finds a proper solution. If a winery is unable to adopt a cybersecurity strategy variation, then it will ultimately cease to exist. Jenab and Moslehpour (2016) noted that systems theory could be useful in understanding the feedback derived from cyberbreaches and creating consistent cybersecurity strategies based on information from the throughput stage. When investigating a breach in a system, it is necessary to understand the relationships between the elements of the environment and the system, as well as the impact's effect on the environment, in formulating the estimated effect of the impact on the system (Naudet et al, 2016).

Computer Threats and Cybercrimes

Researchers at the U.S. Department of Homeland Security reported that cybercriminals can hack a computer network without activating malware (Nakashima, 2015), which allows them to upload malware to the victim’s machine. Cybercriminals can use malware to copy information remotely to customize attacks for each victim (Horvath & Lovasz, 2018). Cybercriminals distribute viruses through unsolicited emails, using cheap and easily distributed programs to take control of a computer remotely when those emails are opened by the recipients. Cybercriminals use viruses to obtain data and intellectual property illegally and then demand cyber ransoms from organizations for

their return or accessibility. In 2020, there were over 4,000 daily cyberattacks on organizations, which included privacy violations, phishing crimes, and data breaches (Romanosky, 2016; Sobers, 2021).

Cybersecurity Strategies

Some business leaders in the wine industry use effective cybersecurity strategies to ensure business infrastructure assets and intellectual property remain secure. (Van de Weijer & Leukfeldt, 2017). Cybersecurity threats in the wine industry can be detrimental and computer hackers can exploit and attack the integrity of a company and release confidential information (Narayanan et al., 2018). Cybersecurity decisions require insight into current security threats and the ability to forecast potential vulnerabilities (National Institute of Standards and Technology, 2020). Some business leaders lack the proper processes to control the evolving cybersecurity risks (Njenga & Jordaan, 2016). In addition, business leaders may lack the resources to respond to cybersecurity threats, which can potentially threaten the survival of the business; therefore, they should adopt risk management strategies and methodologies (Avogundade et al., 2020). Cybersecurity models aid business leaders by identifying security threats and system vulnerabilities, thereby enabling business leaders to quantify the risks in economic terms (Duench, 2020).

One of the biggest issues facing business leaders is their ability to defend the organization from potential cyberattacks (Georgiadon et al., 2020). Badhwar (2021) conducted a qualitative multiple case study to explore the technology that leaders use to minimize security breaches and increase business performance. Four components that can

further reduce security breaches and improve business performance are (a) an organizational culture promoting security awareness, (b) consistent organizational security policies and procedures, (c) implementation of security awareness education and training to mitigate insider threats, and (d) organizational commitment to adopt new technologies and innovative processes (Badhwar, 2021). When leaders of organizations increase their use of mobile devices and cloud services, criminals that use handheld devices could commit cybercrimes against those leaders (Besliu, 2017). It is important that leaders of those organizations address those security issues. Researchers, leaders of federal organizations, and leaders of commercial companies are working together to identify the primary factors that contribute to a secure business environment (Federal Communications Commission, 2017).

Prevention of attacks on computers and networks is a high priority in businesses; specifically, during a business merger or acquisition (Boteanu & Fernandez, 2013). Human-related incidents have caused many security threats and constantly evolving developments in technology make it difficult to keep up with new threats (Ahirwar et al., 2011). Security solutions and provided possible resources to assist businesses in staying current on security measures (Preiser et al., 2018). Traditional techniques are not enough to protect data and security should start with the education of business leaders (Adauto & Guerrini, 2018). Four factors that affect the security of networks in organizations are security policy documentation, access control, employee awareness, and top-level management support (MacDougall, 2019).

Security awareness and malware identification are critical components in preventing cyberattacks and cybercrimes (Jalali & Kaiser, 2018). Malware, viruses, and spyware are prevalent on computers and infiltrate the operating systems that support tablets and mobile devices (Jalali & Kaiser, 2018). Likewise, malware is one of the most serious threats associated with cybersecurity (Yadev, 2019). Yadev, (2019) reported trojans as the most deployed malware by phishers, which account for 77% of all malware attacks (Shen et al., 2018). Trojans occur when phishers install malware to steal credentials or link the host system to a network of private computers that may have malware installed. Malware and malicious software have been increasing in numbers and are becoming more sophisticated, are difficult to detect, and are almost impossible to stop (Jagular et al., 2018).

Malware is often a mechanism for cybercriminal activities because malware characteristics usually elude most forensics experts' detection and analysis methods (Zhou & Yu, 2018). An infected application could potentially impact thousands of devices (Zhou & Yu, 2018). To combat malware exposure, computer, tablet, and mobile users must become more knowledgeable about protecting their devices, invoke limited-permission grants by not allowing the applications to access sensitive user information, and prevent exposure to cybercriminal activities (Piplai et al., 2020). Business leaders must find security-critical computer bugs, more commonly known as software errors or flaws in a computer program or system, before hackers and cyberterrorists exploit the breached systems (Piplai et al., 2020). Systems administrators should keep cybersecurity as a top priority while implementing opportunities created by mobile and cloud

computing (Okafor, 2021). Making cybersecurity a top priority is important since the proliferation of mobile devices connecting business networks has expanded the number of potential targets for cyberattacks (Okafor, 2021).

Cloud computing is a less expensive option for organizational leaders to enhance cybersecurity controls. Organizations with limited IT resources have cloud computing as the primary resource to combat cyberattacks (Sunyaev, 2020). Cloud computing is one of the newest digital security strategies in computing used by some businesses (Kumar et al., 2018). Cloud computing is used directly and indirectly by businesses. Shulur et. al (2020) noted that there is no longer a need for company leaders to invest solely in physical computer networking technology (i.e., hardware and software). Instead, cloud computing serves as an alternative for businesses to plan, store, and maintain company information (Krishna et al., 2016). Chou (2015) also cautioned that developers must know how to work with specific software to run business operations on a cloud infrastructure effectively. Business leaders must be well-informed and make an increased effort to ensure document control during a business merger or acquisition. Asija and Nallusamy (2016) noted that cloud computing offers flexibility to organizational leaders in maintaining cybersecurity control. Tabrizchi and Rafsanjani (2020) concurred that a variety of cloud-based technologies such as web services, virtualization, and grid computing are effective applications.

Business leaders must assess information security risk using a qualitative and quantitative approach as part of the risk management strategies to explore any potential vulnerabilities affected by employee use of a computer network (Sunyaev, 2020). A

quantitative security risk assessment is needed to identify, assess, and implement security controls (Sun,2020). Carrying out a qualitative risk assessment allows an organization to view all applications holistically from an attacker's perspective

A private cloud purposely restricts network access to lower the risk of cyberattack and allows an organization to maintain the same workflow and security procedures (Sun, 2020). The advantage of a private cloud versus a public cloud is greater control and resilience for business users to sustain a harmonious level of authority and privacy (Jain & Kumar, 2014). However, some disadvantages for organizations whose leaders choose to adapt a private cloud are cost and limited scalability compared to public cloud applications (Bacis et al., 2017).

Significant computation assets must be in place to facilitate the cloud environment and provide a foundation to support business operations (Olokunde, Sanjay & Adewumi, 2017). IaaS supports flexible and scalable computer infrastructure. but users must secure their IT systems to minimize risk. Platform as a Service (PaaS) gives the freedom of managing applications without the complexity of maintaining the infrastructure. PaaS provides a platform for executing applications and allow IT leaders to develop and run software to deliver significant levels of service (Krishna et al., 2016). IT leaders manage the cloud base for performance devices help protect computer networks from cyberattacks and unauthorized access. They do this by trying to anticipate and defend against cyberthreats and responding to security breaches when they happen. IT leaders play a key role in protecting an organization's valuable data (Wulf et al., 2021). PaaS enables self-service capabilities that can enable IT leaders to build and manage

applications quickly without having to build development tools or worry about the underlying infrastructure. As businesses modernize, platforms need upgrading. Bayramusta and Nasir (2016) noted that IT leaders regulate the servers and operating systems to control their application design. PaaS application security involves two programming layers such as security of the PaaS stage and security of client applications conveyed on a PaaS stage. Okafor (2021) surveyed the effect of IT infrastructure development and vulnerabilities to cloud applications through numerous client browsers and transportable devices. IT leaders can have workers build a cybersecurity model, regardless of whether they consider these IaaS or PaaS issues. The effects of technological and environmental components on IaaS and PaaS selection are a requirement for cybersecurity (Wulf et al., 2021).

Cybersecurity Models

Strategic measures take place in collaboration with the IT leadership team within an organization to provide the necessary preventive protection of their intellectual data and customer information (Herrmann & Pridohl, 2020). Running security checks and conducting a system backup daily is important. Safety objectives to protect a company's intellectual data and other potential information of value include creating a failsafe security system to protect all vital data (Vigano et al., 2020). Some organizational leaders minimize involvement, especially in aiding IT staff to engage managerial strategies to prevent breaches, fraud, and other types of cybercrime (Allodi & Massacci, 2017). New attitudes are necessary among leadership to understand system administrators' need to foster comprehensive cybersecurity control measures (Arief & Adzmi, 2015).

Some business leaders' perceptions toward cybercrime and Internet security remain a major concern to combating cybercrime. To compete on a global level, business leaders use cyberspace for business transactions (Jordan, 2020). The use of cyberspace increases an organization's level of vulnerability to significant loss of data due to cybersecurity breaches. Robust cybersecurity requires the implementation of adequate controls to protect intellectual property and customer information (Jordan, 2020). Gibson (2019) noted cybersecurity is a challenge to all types of businesses, regardless of size. Cybercrime also continues to be an issue within the United States. Loopholes within the U.S. legal system makes it difficult in some cases to prosecute hackers for cybercrimes (Abdelrahman & Nimrat, 2018). Kumari (2019) developed a threat model as a defense mechanism business leaders use to avoid exploitation by hackers. Prakash and Singaravel (2015) proposed a three-phase anonymization method to protect data from cyberattack to preserve companies' confidential information.

Business leaders should evaluate the financial costs associated with cybersecurity. the financial costs associated with managing cybersecurity have a direct link to the cost of companies building trust with the customer base and upholding a competitive edge in the marketplace (Sarre et al., 2018). Not all U.S. businesses victimized by security breaches report those breaches (Konradt et al., 2016). McMahon et al. (2016) contended there is a need for further advancement of new security control software to deal with cybersecurity.

Computer hackers exploit security issues in IT systems. Exploitation can propagate across systems in the infrastructure and that a quantitative estimation of the

risk posed by these vulnerabilities is a critical step toward a more efficient allocation of resources and a more secure overall environment (Jordan, 2020). Security information is often difficult to analyze for actionable information. Opitz (2018) proposed new data-extraction algorithms and models for big data in recent research advancements. For example, Khorshidi et al. proposed a technique for aggregating qualitative data features with the aim of fostering the risk management activities of complex systems whose data sources may be incomplete or not enough for the analysis. Susto et al. (2016) proposed a method for aggregating multiple data sources to build models of the data to statistically link security alarm data in IT infrastructures to security events and risk. Kumari (2019) identified the limitations of security monitoring technologies that limit the accessibility to risk modeling. Risk assessment procedures consisting of standards and best practices often fall short in providing quantitative instruments for risk estimation. For example, the National Institute of Standards and Technology's *Information Security Handbook* was used to suggest the use of risk matrices to estimate qualitatively the risk associated with an event (Bowen et al., 2006). The risk matrices may cause risk mis-categorization and risk mis-prioritization. Aven and Cox (2016) determined that IT professionals should be aware of the vulnerabilities within a system and how these vulnerabilities impact the daily workflow.

Bossler and Berenblum (2019) noted that proposing a risk estimation model that explicitly quantifies the likelihood of attack by leveraging data available to any organization will deploy common perimeter defenses and perform periodic vulnerability assessments. In addition, organizations that invest in policy monitoring are in a better

position to increase the effectiveness of their cybersecurity policies. Also, expansion of employees' knowledge base of cybersecurity will lead to the systematic collection of data and rigorous evaluation of computer surveillance to reduce the risk of cyberattack.

Management of Cybersecurity

Cybercrime occurs when hackers gain access to a computer system to modify or destroy data without the owner's permission (Aiken et al., 2016). The techniques hackers use to gain illegal access to computer systems include botnets, worms, and viruses (Asghari et al., 2015). Some business leaders have developed a capable workforce to address the demands for effective cybersecurity through continuous education (Park et al., 2016). Continuous education involves learning cutting-edge information security technology to help business leaders ease the problems affiliated with information security (Cabaj et al., 2018). Maintaining knowledgeable and skillful IT employees as well as providing continuous education in cybersecurity meets the demand of maintaining the integrity of a computer infrastructure (DeSouza & Valverde, 2016). Extensive knowledge allows business leaders to understand and implement cybersecurity control measures (Burley et al., 2014). Samtani et al. (2017) noted that global leaders should collaborate on the definition of cybersecurity to create global policies and procedures to combat cybercrime.

Ahmad et al. (2014) noted organizational leaders are in a preventive mind-set regarding information security measures. Leaders may expose organizations to unnecessary security risks to ensure continued access to services for users (Yetgin et al., 2015). Hussein et al. (2014) examined security issues in small businesses and discovered

that although most small business leaders have systems and procedures in place to address threats, some of the systems and procedures are ineffective. Hussein et al. (2014) also discussed information threats that occur from within an organization by authorized users and the processes executed. Few security resources defend against information leakage and encryption of data is a critical measure that needs implementing (Hussein et al., 2014). Business leaders should use effective security measures in combination with a staircase concept with a strong foundation (Papanikolaou et al., 2013). Schwartz (2015) mentioned that when an organization is running optimally, the positive momentum leads to a productive and successful network security team. Cultural aspects impact decisions about security threats and the resources that control those threats (Ifinedo, 2014). Mohammed et al. (2013) indicated even though many organizations take the proper steps to protect information, there are still areas that business leaders can overlook and that are not up to current standards, which leaves them vulnerable to attacks during the transition stage of a business merger or acquisition.

Cybersecurity can play a critical role in mitigating the risk of a cyberattack on an organization's confidential information. Parsons et al. (2014) noted effective cybersecurity controls used by companies can defend against unauthorized access and disruption of business. Spyridopoulos et al. (2014) contended there is a problem with the use of traditional approaches to correctly manage computer systems. The flow of information is continuous; therefore, restricted information can lead to issues within an infrastructure or intellectual property (George et al., 2014; von Solms & van Niekerk, 2013). Business leaders should realize that knowledge sharing is the best course of action

to protect the integrity, accessibility, and confidentiality of information during a business merger or acquisition (Marques et al., 2015; Leal et al., 2016). Though knowledge sharing of cybersecurity controls is ideal, company leaders should invest in obtaining a better understanding of employees' behavior and willingness to uphold security expectations (Akhavan et al., 2016).

The literature supports the intent and problem statement of the current study. Cybersecurity has a limited number of extensive studies and models. As technology continues to evolve, cybersecurity will become a viable field of study due to the pressing need to secure data in all settings. The growth of cybersecurity is important for the wine industry because they are vulnerable to cyberattacks. Hackers are aware of complacency among businesses concerning cybersecurity, any weakness within their computer infrastructure can be exploited making businesses vulnerable to attack. In short, existing researchers studying cybersecurity breaches have predominantly focused on the impact of public disclosure of such incidents on the affected organizations' market valuation. Chen (2019) examined the impact of data breaches on consumers and ways at which owners of small businesses can reduce the impact of data breached. The author further indicated that business leaders should be able to provide insights on how to prevent and manage data breaches. The impact and cost associated with a single breach can be catastrophic to a winery. It is necessary to address the different factors that influence the lack cyber-defense strategies by business leaders. In this literature review, I substantiated the need for business leaders to be aware of cybersecurity threats, as well as develop preventative strategies to combat security threats and eliminate privacy concerns.

Transition

Section 1 included the problem statement, purpose statement, nature of the study, research question, interview questions, conceptual framework, operational definitions, and significance of the study. Section 2 includes a discussion on the role of the researcher, participants, research method and design, population and sampling, ethical considerations in the research, data collection, organization techniques, and data analysis. Section 3 will include a presentation of the findings, the application to professional practice, the implications for social change, recommendations for action, recommendations for further research, reflections, and a conclusion of the study.

Section 2: The Project

Section 2 includes an in-depth analysis of the method that I used to conduct this study on strategies to reduce cyberattacks during a merger. Section 2 addresses the study's purpose, the researcher's role, participants, research method and design, population and sampling, ethical research, data collection instruments, data collection technique, data organization technique, data analysis, and reliability and validity. I also include the steps I followed to ensure the validity, reliability, and confidentiality of the study outcomes.

Purpose Statement

The purpose of this qualitative single case study was to explore strategies that leaders in the wine industry used to mitigate the risk from cyberattacks during a merger. The targeted population was business leaders at a wine company located in California who successfully protected their company's data during a business merger. Implications for positive social change include the reduction of loss of company revenue, which may directly impact jobs and services, thereby having a positive economic effect on local communities.

Role of the Researcher

In qualitative research, the researcher is the instrument for data collection, analysis, and interpretation (Tomkinson, 2015). The qualitative researcher's role is to maintain strict adherence to ethical guidelines when selecting participants (Pacho, 2015). Researchers must understand that participants will see the work through their own perspective and cultural experiences (Hoover et al., 2018). As a qualitative researcher, I

was held accountable for maintaining the rigor and integrity of the study (Collins & Stockton, 2018). I did not have any personal connection to any of the participants used in this study. I became interested in IT systems during the rise of the dot-com era and received a master's degree in information systems. My qualifications provided opportunities to work with business leaders in the wine industry.

Researchers should take the necessary steps to avoid bias and ensure that their perspectives do not adversely affect the results of a research study. In accordance with the *Belmont Report* (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979), I treated all participants with respect of persons, beneficence, and justice. In addition, according to the *Belmont Report,* participants' interviews must remain confidential, and researchers must always, without exception, favor the well-being and interest of the participants over the research. During the research process, researchers are to remain honest, transparent, and objective (Hoover et al., 2018).

Researchers must maintain transparency in a credible manner (Avasthi et al., 2013). National Institutes of Health participant protection training also assists researchers with implementing the necessary informed consent process to ensure participant protection and to combat ethical challenges in the research process (Fusch et al., 2017).

Participants

Researchers need to set specific criteria to identify individuals who are relevant to their research goal (Queirós et al., 2017). Before identifying a target population, researchers should comply with a list of attributes that are essential to their field of

research (Roulston, 2018). Researchers can achieve accurate results when the experiences and characteristics of the participants align with the field of research (Lewis, 2015). Researchers often choose participants based on their professional or personal experiences related to the research topic (Peck & Mummery, 2017). The key for this research study was to focus on participants with relevant knowledge and experience with mergers in the wine industry. To be effective, researchers need to communicate and build a rapport with their participants (Aggarwal et al., 2019, Peek & Mummery, 2017)). To ensure that I received complete responses to the interview questions, I made the participants feel comfortable sharing their experiences.

The participants selected for this qualitative single case study were from my current employer. Single-case studies are ideal for revelatory cases where an observer may have access to a phenomenon that was previously inaccessible (Yin, 2018). I had no direct contact or relationship with the potential participants, who worked in different departments at different locations. I took care to negotiate at the beginning of the research process exactly what information I had access to, and I ensured that I maintained confidentiality of all information provided by the participants. The vice president of human resources acted as a liaison and provided recommendations for the initial contacts to select participants.

Arranging semistructured interviews involves several challenges. Semistructured interviews organized by researchers should include clear communication to avoid any misunderstanding between researchers and participants. Bowden and Galindo-Gonzalez (2015) noted that using phone calls or emails can be effective in selecting participants

and streamlining the interview process. These techniques can provide a level of comfort to help participants feel at ease (Peticca-Harris et al., 2016). After the Institutional Review Board (IRB) approved this research study, I used phone calls and email correspondence to build relationships with the participants.

Research Method and Design

Research Method

The flow or process of a research method helps to guide researchers to answer questions and build an in-depth understanding about a research study (Boddy, 2016). Quantitative, mixed method, and qualitative are three methods that researchers can use to explore, examine, and/or measure research (Creswell & Creswell, 2018). Quantitative researchers use statistical analysis to ensure that their results have a statistical relationship (Bernard, 2018). That was not the intent of this study.

The mixed methods approach involves both quantitative and qualitative data collection. Researchers use mixed methods to integrate data at one or more stages of the research process (Gibson, 2017). A mixed methods approach provides researchers with an in-depth understanding of a study while offsetting any weaknesses that may be inherent when using only a quantitative or a qualitative research approach (Abdalla et al., 2018). The advantage of using a mixed method approach is that it provides a framework for researchers to identify, clarify, and explore different angles of a research study (Fusch et al., 2017). Because quantitative methods were not used, the mixed methods approach was not applicable for this study.

I chose the qualitative method to explore the participants' experiences and perspectives as they related to the research study. A chosen research method should serve as a lens to make informed decisions regarding how to interpret the research data accurately (Hays et al., 2016). Researchers use select methods to clarify and define the variations and differences from previous related research studies (Creswell & Creswell, 2018). Choosing a research method that promotes a clear understanding of the scope of a study is important (Stewart, 2014). In this qualitative case study, I focused on the insights of the participants to build strategies to combat cyberthreats during a merger or business acquisition.

Research Design

Qualitative designs include phenomenological, ethnography, and case study (Yazan, 2015). In the phenomenological research design, researchers can share the events, experiences, and perceptions of their participants (Ferreria & dos Santos, 2016). Researchers can use phenomenology to obtain an in-depth understanding of the experiences of participants (Handwerker, 2018). I chose not to use the phenomenological design because I did not explore the lived experiences of the selected participants.

The ethnographic research design involves using examples of the past and present to examine cultural and social experiences and issues (Thornham & Cruz, 2018). Ethnographic researchers study the conditions of their participants rather than set the conditions for the participants (Mol et al., 2017). Researchers collect data for ethnographic studies in an informal manner to explore the cultural experiences of the participants. I did not collect data regarding cultural experiences.

Researchers may choose to use a single case study design to support the qualitative research method (Haydon et al., 2018). The case study design for this study supported an exploration of the strategies used during a merger or business acquisition to reduce the threat of cyberattack. The use of a single case study allowed me to identify the key attributes necessary to capture the details related to the business problem. Using a single case study design for this study involved exploring one organization to demonstrate how its business leaders strategized to institute cybersecurity controls to reduce the threat of cyberattack. I collected data for this single case by reviewing company archival information stored on the company's portal, interviewing participants, and retrieving publicly accessible information regarding wine industry M&As in the past 5 years.

Population and Sampling

The target population for this case study consisted of business leaders at a wine company located in California who successfully protected their company's data during a business merger. After receiving IRB approval, I was able to solicit and enroll participants. The chosen sample size for this qualitative single case study was five participants. The sample size for a qualitative study is based on the context of the study (Kasim & Al-Gahuri, 2015). For qualitative case studies, an adequate sample size is four to 10 participants (Yin, 2015). I chose the participants for this qualitative case study based on the following criteria: (a) leader in the wine industry and (b) success in protecting companies' data during a business merger. Researchers should determine what is adequate without bias to ensure the collection of rich data (Gentles et al., 2015). For

this case study, a sample size of five participants met the criteria to ensure the collection of rich data and obtain data saturation. Participant responses in a case study should result in the replication of the results and data saturation validated through member checking (James, 2018).

Researchers must choose a sampling method that supports their research study. I chose to use purposive sampling as the sampling method for this qualitative single case study. Researchers use purposive sampling to access the appropriate number of participants to obtain rich data (Robinson, 2014). I gathered data from relevant organization documents located on the company's website, archival documents located on the company's portal, the company's 3-year strategy plan, and publicly accessible wine industry M&A information.

Ethical Research

A critical aspect of a research study is the ethical protection of the participants. Walden University has strict guidelines to ensure that the research study process is ethical. To commence the research portion of the study, I obtained the permission of the Walden IRB. Walden IRB provided approval # 05-12-22-0661787 for this research study. Approval from the IRB was dependent on three principles outlined in the *Belmont Report*, which are (a) justice, (b) beneficence, and (c) respect (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). After receiving IRB permission to conduct the study, the next step in the process was to obtain permission from the company identified for this qualitative single case study.

The participants chosen for this research study received an email asking them to consent to the study, with the disclaimer that doing so was voluntary. The names of the participants and all their personal information are being protected. Adhering to ethical principles in research helps to prevent any direct injury or loss of privacy (Jeanes, 2016). Researchers need to consider and protect the well-being of participants for ethical considerations (Wessels & Visagie, 2016).

After the business leaders from the organization agreed to participate in the study, the informed consent process begun. The informed consent process consists of participants giving their written consent to participate in a research study (Forster & Borasky, 2018). I provided each participant with a formal introduction and outlined all aspects of the research study, the informed consent form, and the letter of cooperation from the organization. The participant introduction included the scope and purpose of the study, the requirements for participation, participants' right to withdraw from the study, and participants' acknowledgment that study participation was voluntary. Participants confirmed in writing that they had a clear understanding of the scope of the study and agreed to participate. Participants were able to withdraw at any time through email, phone call, or text notification. Participation in this case study was voluntary, and there were no consequences or repercussions for withdrawing.

To adhere to ethical guidelines, I did not offer the participants any incentives to participate. Guetterman (2015) noted that incentives may improve the participant response rate; however, providing incentives could lead to ethical concerns and affect the

vitality of a research study. I also maintained confidentiality throughout the case study. Researchers must protect the identities of their participants (Killawi et al., 2014).

To enhance confidentiality, I created codes using letters and numbers to protect and preserve the names and identities of the company and participants involved in the study and refrained from using any personal information that could reveal the identity of the participants. Yin (2018) noted that a coding system can maintain the privacy and anonymity of participants. I assigned codes such as P1, P2, and so forth to identify the participants in the study.

The data collected from this research study will be kept in electronic files on a security-protected USB drive that includes multiple-level authentication to maintain the security of the data. Any physical documents such as notes or journals was scanned to the USB drive. I have placed all files, including the interview protocol and summary findings, in a fire- and waterproof safe for 5 years to preserve the identities and names of the participants and the company. Five years after the completion of the research study, I will destroy the USB drive and any documents obtained from the study.

Data Collection Instruments

I was the primary data collection instrument for this qualitative single case study. Researchers in qualitative case studies should use a minimum of two data-gathering methods (Hagaman & Wutich, 2016). The data collection for this study involved conducting semistructured video conferencing interviews with five business leaders in the wine industry who were knowledgeable of the cybersecurity used during a merger or business acquisition. I also collected secondary data through firm paperwork such as

relevant strategic reports that described the strategies used to institute cybersecurity controls to combat cyberattacks during a merger. To capture the participants' responses to the interview questions, I took detailed notes during the video conferences and recorded the sessions on the computer.

Mohajan (2018) pointed out that a semistructured interview can elicit participants' viewpoints and insights about a phenomenon. I conducted semistructured interviews, as outlined in the interview protocol (see Appendix A), to collect data from participants in the wine industry. Researchers use interview protocols to improve the effectiveness of interviews and to ensure that they collect all relevant information within the specified duration (Amankwaa, 2016; Yeong et al., 2018). I asked each participant similar questions in the protocol (see Appendix A) in the same order.

Data collection is a critical element of a research study. Personal interviews should highlight human emotion and interaction (Van de Berg & Struwig, 2017). For this study, the data collection process included the interview questions (see Appendix B), the participant recruitment letter (see Appendix C), the letter of cooperation (see Appendix D), and the interview protocol (see Appendix A).

After each interview was completed, I used member checking to verify my interpretations of the participant's answers. Member checking validates the accuracy of qualitative research (Harvey, 2015). Researchers also use member checking to confirm the context and meaning of the choice of words and phrases used by participants (Kasim & Al-Gahuri, 2015; Pacho, 2015). I asked each participant to review my interpretation of the interview session for accuracy and provide feedback.

Data Collection Technique

I was the primary instrument of data collection for this study. The interview method was suitable for this case study because it offered the opportunity to uncover data that cannot be accessible using other techniques such as observations and questionnaires (Oltmann, 2016). Interviewing is not just a data collection tool, but rather an interactive means used to gain information; as such, it has its advantages and disadvantages. The advantage of using interviews includes controlling the answering order, relatively flexible interaction, and a high return rate with the presence of the interviewer (Hunter, 2017).

After obtaining IRB approval, I generated a list of participants from company's organization charts stored on the company's HR portal. I recruited the study participants using the company's Microsoft Teams directory to obtain their email and phone number information. Five participants were selected for this case study once management approval had been obtained. There were no incentives offered to the study participants to avoid any undue bias. Since face-to-face interviews are not possible, semistructured interviews were conducted using Microsoft Teams after the study's participants consented to participate as stipulated in the interview protocol (see Appendix A).

I compared and contrasted the top recording devices and chose the digital audio recorder that best captures conversations and recording interviews for collecting data; this was a similar process used by Clark and Veale (2018). I used triangulation by observing and noting participants' body language during each interview session, reviewing company documents, and recording participants responses to the interview, which was a similar process used by Oltmann (2016). To prepare for the interviews. I reviewed

protection strategy plans approved and used by other business leaders to protect their business data against cyberattacks. I used open-end, semistructured questions, which permitted me to collect data while trying to understand the dynamics of the interview as suggested by Weis and Willems (2017).

I used an interview protocol and follow-up questions for clarity, I maintained a detailed protocol to support consistency when constructing the interviews questions. Also, I retained an electronic reflective journal to categorize the patterns and themes of the study. It is imperative in qualitative data interpretation for the researcher to guarantee reliability and validity. I used member checking for data interpretation to summarize and restate the information to strengthen the accuracy, applicability, validity, and credibility of the participants' responses. The participants were given 5 business days to review their individual responses and provide feedback. I anticipated that some of the participants either would disagree or agree that the summarized information reflecting their experiences or views. I discussed any disagreements to make certain that we were in accord. Also, I reviewed historical information from archival company documents to help strengthen the validity of this case study. The benefits for reviewing historical company information include (a) the researcher having documentation to compare and contrast with the research data generated through participants' interviews (Yin, 2017) and (b) the researcher having access to information that is not available to the general public to provide better insight.

Data Organization Technique

Researchers must efficiently manage the data collected for their research study (McTate & Leffler, 2017). I reviewed and categorized all the data collected and then imported the information gathered during the research study into the NVivo software program. NVivo, is a data analysis tool designed to help researchers evaluate data to determine common themes (Phillippi & Lauderdale, 2017; Zamawe, 2015). Ballaro and Polk (2017) indicated that the right software will provide an audit trail and increase the rigor of a research study. NVivo, version 12 is an effective software tool that has an audit trail component that researchers can use to organize and analyze the data collected from literature reviews, company documentation reviews, completed consent forms, participant interviews, interview protocols, transcripts, and participants' transcript reviews (Woods et al., 2016). I uploaded each transcript into NVivo and assign letters and numbers (i.e., F12, E56, Q97) to identify the participants, which will help to establish the confidentiality of the organization and the participants in this qualitative single case study. I labeled the company documentation files obtained for this case study using a coding process of random numbers and letters (i.e., 45Yum2z, 81Dwx0a, 73Apk4b) Also, I kept track of my research notes by maintaining an electronic reflective journal. The electronic reflective journal was a useful tool for identifying themes and patterns within the data collected.

Preserving and protecting the documentation collected for a research study is important. The electronic reflective journal will remain confidential, protected, and kept on an encrypted USB drive which aligns with the recommendations by Weis and Willems

(2017). Additionally, I stored all paper and electronic copies of company-related IT policies and procedures on a USB drive and placed in a safe for 5 years from the date of the completion of the data collection process and I will destroy the documents and USB drive after 5 years have passed.

Data Analysis

Data analysis is the process of gathering, organizing, and interpreting data to obtain conclusions and reaching decisions (Guler, 2015). There are multiple ways to analyze data. A common method that qualitative researchers use to analyze data is thematic coding. Leedy and Ormrod (2015) described thematic coding as a process to translate data. The intent of the data analysis for this case study was to identify answers to the research question: What strategies do business leaders use to avoid the threat of cyberattack during a business merger or acquisition? To accurately answer the research question, I inputted the responses from the semistructured interviews into the NVivo software tool to identify patterns and themes. As a researcher, I looked for similarities and differences, relationships, repetitions, and analogies to seek patterns within data to develop themes and trends.

I explored the strategies developed by business leaders to institute cybersecurity control measures during a merger and determine through the application of thematic coding whether those experiences and practices were similar between the participants. I reviewed relevant company documentation obtained from the company's website, portal and 3-year strategy plan to identify key terms and phrases. Yang et al. (2018) emphasized placing data into distinct categories and groupings. I used NVivo 12 to develop a coding

system to group and categorize the data to determine relationships and trends. Researchers use multiple sources of data to establish a phenomenon for a single case study (Keutel et al., 2014).

The purpose of using triangulation is to correlate and extract patterns and themes. I extracted the thematic coding derived from this data analysis based on the interviews and documents analyzed. Hussein (2015) posited that data triangulation involves using two collection methods to explore and analyze a similar phenomenon. Examining the data allows for the building of themes regarding strategies to safeguard against cyberattacks during M&As. The results of the data analysis provided predictive metrics to forecast future ways to combat cyberattacks.

Reliability and Validity

Researchers must be able to demonstrate that the results of their study are reliable and valid. Barry et al. (2014) posited that reliability consists of dependability, credibility, transferability, and confirmability. Yin (2018) indicated validity involves construct validity, internal validity, and external validity. To demonstrate that the results from this single case study are factual, I showed that the data collected are reliable and valid.

Reliability

A key difference between quantitative and qualitative researchers is that qualitative researchers typically use four criteria to confirm that their study is reliable and valid: dependability, credibility, transferability, and confirmability (Moser & Korstjens, 2018). To establish reliability, researchers must document the entire research process. Madill and Sullivan (2018) suggested recording all phases of data collection and data

analysis. Creating an interview protocol and maintaining a research journal will help to achieve the dependability necessary to maintain reliability. I verified the accuracy of the participants' transcribed responses through member checking. Using data triangulation helped to reinforce the credibility of the findings.

Dependability

Dependability relies on the consistency of research data over time and the actions documented by the researcher (Forero et al., 2018). Dependability defines the study's factors of consistency and reliability (Forero et al., 2018). It is important for researchers to keep an audit trail or reflective journal to document the procedures and decisions that impacted the study (Korstjens & Moser, 2018).

The use of audit trails or reflective journal will ensure the process of the study was conducted in such a way that the results can be considered dependable. I kept records throughout the study to allow for an independent audit of the study after completion. Amin et al. (2020) provided categories of information that are useful to conduct an audit: a) raw data, including recordings, field notes, and other documents; b) data reduction and analysis products, including summaries; c) data reconstruction and synthesis product, including themes, results, conclusions, and reports; d) process notes, including notes related to methods reflexive notes; and e) instrument development information, including pilot forms and observation charts. These items were used to document the entire interview process and saved to prove dependability of the results.

Credibility

Credibility is defined as the trustworthiness and believability of the research findings (Twining et al., 2017). Credibility assures integrity and accuracy in the data (Marshall & Rossman, 2016). Understanding what makes a study credible and how it leads to trustworthiness helped me to determine which strategies were most appropriate for this qualitative study. Korstjens and Moser (2018) indicated that credibility relates to the truth value and whether the interpretation correctly reflects the participants' views.

Credibility makes sure the findings of the research align with the objectives of the research and signifies that the participants are the core agents in the research (Nelson, 2016). Accurate documentation is essential to the credibility of a qualitative research study.

I took measures to maintain credibility of my research by aligning the research questions, data collected, and conclusions with the conceptual framework of the study. I was able to recognize when data saturation occurred. I collected and analyzed data on an ongoing basis, continually comparing to see if new ideas, constructs, and themes developed or if the same notions reemerge. The data were obtained through semistructured interviews, reviewing company and public documents pertaining to mergers in the wine industryI involved the participants in member checking to ensure the accuracy of their interview responses. I used trianguation to validate the interview data with the document data until no new themes or patterns emerged to ensure that data saturation was reached.

Transferability

Transferability refers to the results of the study being transferable and applied to other industries or physical settings. (Madill & Sullivan, 2018) Researchers achieve transferability when the results of their research are reproducible and researchers establish confirmability through member checking (Palinkas et al., 2015). Patino and Ferreira (2018) supported the possibility of transferability based on the knowledge that investigators offer sufficient data for other investigators to transfer findings. By thoroughly describing the research context and the assumptions that were central to the research I enhanced the possibility of transferability. The person who wishes to transfer the results to a different context is responsible for deciding how sensible the transfer is. Having a comprehensive audit trail or reflective journal should also help other researchers decide transferable research findings and the possibility of applying the findings for future research

I ensured that future researchers would have accurate study descriptions through meticulous documentation of the research process by maintaining a reflective journal and adhering to the interview protocol. I transferred the findings to another context to ensure that the dependability and credibility of the findings of this research study were met. I mitigated personal biases and presented reliable and valid outcomes to increase the probability of the transferability of the findings.

Confirmability

Confirmability refers to the extent to which reviewers can verify the interpretation of the research study findings from a particular viewpoint (Morar et al., 2016).

Confirmability is defined as the extent to which other researchers can verify the meaning of the research findings (Patino & Ferreira, 2018). Confirmability is also related to how the data are presented (Bengtsson, 2016). The outcome a reflection of the participants' responses, therefore, it is important for the researcher to use triangulation to contrast and compare findings obtained from analyzing interviews and reviewing documents from the organizations. I assured confirmability by making certain the data was analyzed in a precise and consistent manner with enough detail to assure credibility.

Validity

Researchers can ensure the validity of their qualitative research study through the process of data verification and validation, and they can achieve data validation and verification through member checking. I used member checking as noted in prior subsections. Member checking enhances the credibility and trustworthiness of a research study (Nowell et al., 2017). Using multiple data resources will increase the validity of this research study.

Renz et al. (2018) noted that using triangulation can strengthen the transferability and validity of a research study. Researchers use triangulation to test validity through the convergence of various data sources (Renz et al, 2018). I used the purposeful sampling method to select five business leaders and examined their cybersecurity control strategies to prevent cyberattacks during mergers and business acquisitions. I went through a review process and analyzed the data until I achieved data saturation.

Transition and Summary

In Section 2, I provided a review of the purpose of this research study and identified the research method and design. This section also included information on the data collection instrument and the data collection technique to ensure the reliability and validity of the study. In Section 3, I will provide an overview of the qualitative case study. Based on the data analysis, I will make recommendations on strategies to use to institute effective cybersecurity measures to combat cyberattacks during mergers and business acquisitions. Also, in Section 3, I will provide reflections on the research process and recommendations for future research.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The objective of this single case study was to investigate strategies that wine industry organizations' leaders employ to safeguard against cyberattack during a merger or business acquisition. I collected data from semistructured interviews with five IT professionals, managers, and administrators from a partnering organization in California with experience with managing and overseeing IT security systems. Using Habermas's (1989) systems theory as the study's conceptual framework, I explored the strategies that these leaders employed within the selected organization, including their past work experiences, to obtain information on the success of these strategies and recommendations for improvement. The participants highlighted multiple strategies that included protection of data integrity, formal and informal communication/feedback methods, training, and elimination of redundant or obsolete software and/or hardware systems.

The strategies to improve the process during M&As by the participants included the necessity for business leaders and IT personnel to have a full understanding of where all the data reside and determine who is managing the data and whether the data are being used correctly to maintain the merging companies' cybersecurity controls. Other strategies included annual training in IT policies; planned communication via email, in-person meetings, and virtual meetings; and the administration of redundant checks of software and hardware systems during the merging or business acquisition process. Section 3 comprises the presentation of findings, application of results to professional

practice, implications for social change, recommendations for action and further research, reflections, and a conclusion.

Presentation of the Findings

This qualitative single case study was conducted to answer the research question: What strategies do business leaders in the wine industry use to manage the risk of data breach from a cyberattack during a merger? Of the five individuals who were invited to participate in the study, all agreed to do so. The interviews lasted 20–30 minutes. The interviews were recorded using multiple devices. Microsoft Teams was used for virtually conducting the interviews. In addition, I used a digital recording device, specifically, an Olympus VN-541PC, as a backup. I also reviewed publicly available documents on the practices of merging wine companies within the past 5 years. To ensure each participant's confidentiality, I identified the participants as P1, P2, P3, P4, and P5. Thematic analysis was employed, and the data collected were analyzed until data saturation was attained with no new themes emerging. The thematic analysis of transcripts included descriptive codes and NVivo codes.

Following data collection, I used Yin's (2018) five-step process of qualitative data analysis. The steps were compiling, disassembling, reassembling, interpreting, and concluding. This began with the transcription information being collected into Microsoft Word through manual coding and analysis of the data to determine the key themes. These data were then transferred into the NVivo software for qualitative analysis to provide computer-aided coding, interpretation, and development of the relevant themes.

I manually evaluated the themes generated and confirmed the findings using NVivo software. The evaluation generated four themes: (a) protection strategies to ensure data integrity, (b) communication/feedback, (c) IT training to establish increased awareness, and (d) cybersecurity frameworks to increase security between merging companies. Each of these themes validated the primary themes inherent in the study's reviewed literature and linked to the conceptual framework. Table 1 contains an outline of the four themes generated by the data analysis.

Table 1

Coding of Participants' Responses Related to Themes

Theme	Participants [a]	Responses [b]
Protection strategies to ensure data integrity	5	15
Encouraged the use of communication/feedback	4	8
Encouraged IT training to increase awareness	4	5
Cybersecurity frameworks to increase security between merging companies	3	7
Total	16	35

[a] Number of IT leaders who contributed responses linked to the themes. [b] Number of interview questions for which participant responses related to the themes.

Theme 1: Protection Strategies to Ensure Data Integrity

The participants reported that the partner organization and past organizations where they were employed used protection strategies to ensure data integrity. The relevant subthemes under protection strategies include elimination of obsolete data, understanding the impact of the merger, methodology used to merge companies, and validation of data integrity. Table 2 highlights the subthemes under protection strategies to ensure data integrity.

Table 2

Coding of Participants' Responses Related to Subthemes

Subtheme	Participants [a]	Responses [b]
Elimination of obsolete data	3	8
Understanding the impact of the merger	4	10
Methodology used to merge companies	4	27
Validation of data integrity	4	13
Total	15	58

[a] Number of IT leaders who contributed responses linked to the themes. [b] Number of interview questions for which participant responses related to the themes

Elimination of Obsolete Data

Outdated knowledge and routines can seriously hinder data transfer between merging companies (Wang et al., 2017; Yildiz & Fey, 2010). Eliminating obsolete data is essential to maintaining data integrity. P2 stated, "we eliminated devices that weren't properly managed by the company." P4 affirmed that the key is "to look at anything that is out-of-date, things that might not align with your current company." By eliminating obsolete data, the merging companies could increase their cybersecurity control measures. P1 explained that "if the data has a wide footprint, then you have to either minimize that footprint or create plans so that you can shut down all those systems cleanly". Failure to identify and to clean up obsolete data could lead to data breach.

Understanding the Impact of the Merger

There is a variety of reasons why company leaders would elect to venture into a merger or business acquisition. Often, company leaders decide to expand through M&As to gain control of resources and technology (Kapil & Dhingra, 2021). The importance of the roles played by business leaders of the merging companies are in terms of the

commitment to the process of M&As. M&As have been found to be essential to achieve compliance and generate synergistic gains (Vasilaki & O'Regan, 2008). P2 mentioned that it is important to make sure that everything is well documented throughout the merger so that the data transfer is done appropriately to ensure compliance. P1 suggested that "appropriate access, appropriate security is [a] very important aspect of determining user access". It is prudent that users are not granted more access to company data than necessary for end users to continue to function in their current job capacities. P4 cautioned that if end users are given "too much security," this "can lead to a downfall that prohibits productivity"; therefore, allowing too much accessibility to end users could become a liability to merging companies. P5 affirmed that the lack of productivity could "affect the livelihood of everybody" across merging companies.

Methodology Used to Merge Companies

Based on the participants' responses and review of documents, organizations must establish strategies to ensure data integrity. P2 suggested that it is essential to "bring people and data and information and processes together" when merging companies. It is best to take "a very holistic approach". P5 cautioned that there is "not a cookie cutter methodology" to ensure a successful merger or business acquisition. Cybersecurity needs a holistic approach and strategies to understand and address the risks associated with M&As (Burita, 2019). P5 stated that "not one company does the same thing as the other, everybody protects their data differently." P4 corroborated that "identifying critical data points, things like servers, that house databases are critical for cybersecurity". Using a methodology that includes guidelines and interventions to encourage effective leadership

during a merger or business acquisition is a critical factor. M&A events have the potential to create trauma and stress resulting in negative outcomes across merging companies (Ivancevich, Schweiger, & Power, 2002). P1 cautioned that mergers can be hard and costly; therefore, authentication of data and appropriate user access is essential.

The findings supported the conceptual framework, which suggested that systems theory can guide business leaders' actions to understand the interdependence of complex systems and interactions to improve the efficiency of IT systems during a merger and reduce the risk of cyberattack. Hawkins (2017) posited that it is important for company leaders to understand the complexities of their computer infrastructure and the types of cyberthreats that their IT systems could experience. Business leaders should have plans and strategies in place in preparation for a data breach at any given time to minimize the damage and limit the impact to the business (Hawkins, 2017).

Validation of Data Integrity

Kayser et al. (2019) suggested the importance of having solid policies and procedures related to cybercrime protection and the necessity of working with standards that can be applied in the cyberspace environment. Validation of data integrity and addressing any changes in policies and procedures are helpful to expose any issues that could increase the risk of cyberattack (Aldawood & Skinner, 2019). P2 suggested "doing a side-by-side comparison during a merger or business acquisition to make sure that processes aren't going to fail". P4 and P5 stated that conducting checks and balances is vital when investigating whether any differences exist between merging companies. P1 cautioned that if "data that is being accessed is hanging out there, and get into some

wrong hands, it can comprise your data". Smith (1989) also contended that "operator error and user carelessness are the greatest threats" (p. 5) due to the complexity of data management systems leaking key data to unauthorized entities. Establishing and sustaining a secure data environment may create a climate of trust and safety for the end user (Barosy, 2019). A comprehensive framework can enable the development, institutionalization, assessment, and improvement of cybersecurity controls to develop a comprehensive security strategy (Kakucha & Buya, 2018). P3 stated that the partnering organization's security strategy is to have an incident management policy in place to assess and validate data integrity.

Theme 1 Findings Related to the Literature

The participants' responses highlight the significance of the essence of protection of data integrity, which coincides with the literature. Most organizations experience data breaches and security interference because of the limited funding extended toward IT development and control. Poor funding has resulted in inferior protection strategies or understanding between merging companies (Mierzwa & Scott, 2017). Organizational personnel have limited understanding of cybersecurity because of their lack of cybersecurity expertise, resulting in failure to align their goals with good cybersecurity practices (Jagalur et al., 2018). Motivated cybercriminals rely on these limitations to identify their potential targets (Lee & Choi, 2021). Knowledge of strategic protection plans helps in projecting the criticality of cybersecurity in terms of policy (Efthymiopoulos, 2019; Jallow et al., 2017). When employees between merging companies understand cybersecurity strategic plans, they also appreciate the importance

of enhanced methods for the organization's cybersecurity operations, resulting in a comprehensive cybersecurity control strategy. Osuma et al. (2021) also suggested that an organization's information protection strategic plan has the potential to evade information risk associated with people, technologies, and processes.

Theme 1 Findings Related to the Conceptual Framework

Habermas's theory indicates that systems operate through purposive actions that are self-regulating and self-correcting (Habermas, 1993). Business leaders must evaluate their computer infrastructures, depicting their level of organized complexity. Habermas posited that systemic differentiation and integration help to determine risk (Habermas, 1987). If systems become fragmented or compromised, these systems will often fail to support broader integration (Yun et al., 2019). Therefore, pursuing protection strategies across merging organizations to enhance their protection mechanisms against data breaches and hackers must be prioritized through the training of staff on the necessary technical and organizational measures on security to increase their protection knowledge (Samuel & Odor, 2018). Such cybersecurity protection knowledge will empower employees to understand and maintain comprehensive data security controls during the implementation of a merger or business acquisition. The reviewed company documentation confirmed the assertion for the necessity to institute protection strategies to maintain comprehensive cybersecurity control measures.

Theme 2: Encouraged to Use Communication/Feedback

Communication and feedback constitute a strategy used to provide transparency and clarity across merging companies. Lott and Abendroth (2019) highlighted that

communication challenges emanate when employees use different languages, gestures, behaviors, and symbols while communicating. People with diverse backgrounds are likely to misinterpret/misunderstand communication among them (Midgley et al., 2017). Table 3 contains the number of references to the theme of the use of communication and feedback to maintain alignment across organizations.

Table 3

References to the Use of Communication and Feedback

	Participant		Documents	
Major theme	Count	References	Count	References
Use of communication and feedback	5	42	5	34

The participants recognized the importance of using communication as a strategy for managing a merger or business acquisition. P5 reported that the partner organization used emails and in-person meetings as primary means to provide updates pertaining to the merger and solicited feedback on merger activities and events. Similarly, P3 and P5 reported that planned announcements to provide updates helped to minimize employees feeling threatened by the activities associated with the merger.

P4 reported that they wanted to provide transparency as much as possible to avoid users becoming “bad actors.” A “bad actor” was defined by P4 as an individual who purposely hid or omitted data in the attempt to gain job security or to prevent job loss because of the merger. To avoid this situation, the participant also indicated that they had departmental meetings and would share opinions and provide feedback regarding the merger or business acquisition. P5 indicated that they solicited information through face-to-face meetings, email, virtual meetings, town halls, and unit meetings. The participants

also reported that they believed that maintaining open communication and addressing any emerging issues as they occurred were key factors in executing a merger or business acquisition. The company documents also emphasized the need for open and continuous communication.

Theme 2 Findings Related to the Literature

Based on the participants' responses of this study and the reviewed literature, effective communication is critical to obtain the support of employees across merging companies. Ahmad and Rahman (2019) highlighted that the most appropriate prevention strategy to increase employee awareness is to establish two-way communication. The communication, however, should be friendly and respectful, and the communicating parties should be willing to prevent escalation (Ahmad & Rahman, 2019). Cletus et al. (2018) also inferred that training can facilitate positive communication between groups. This is indicative of the importance of communication and feedback.

Croucher et al. (2015) noted that communication breakdowns can come from employees experiencing language barriers and having varied philosophical perspectives and/or approaches to different cultural norms, expectations, or cultural biases. Organizational leaders who limit communication with their employees can hamper creativity and innovation and may miss critical information when diagnosing an issue (Vardaman et al., 2020). The participants recommended that business leaders within the wine industry who venture into a merger or business acquisition be sure to create two-way communications between their administration and impacted employees to show value among all team members.

Theme 2 Findings Related to the Conceptual Framework

Habermas' theory supports the theme of communication and feedback to employees/end users. Habermas' theory related to communicative action is used as the basis for establishing democracy (Habermas, 1987). Communication can be used to establish understanding and revise or renew knowledge (Habermas, 1987). It is critical to obtain alignment and maintain effective methods of communication during a merger or business acquisition. Providing effective channels of communication is key to increase employee awareness. Gaining consensus through shared opinions and providing feedback can help business leaders to address any issues as they arise to reduce the risk of data breach during a merger or business acquisition. The reviewed company documentation highlighted the importance of effective communication to ensure clear and concise messaging during a merger or business acquisition.

Theme 3: Encouraged Information Technology Training to Increase Awareness

Failure to provide training is risking losing company business and incurring the additional costs for replacing employees (Di Fabio, 2017). IT training is deemed to be a direct approach for promoting and addressing cybersecurity associated issues and risks. (Maj, 2015; Patrick & Kumar, 2012). IT training is among the most effective means to reduce associated conflict (Cletus et al., 2018). Participants 2, 3,4 and 5, reported IT training as a strategy employed within their organization. Table 4 references the theme of IT training to enhance awareness.

Table 4

References to Information Technology Training to Increase Awareness

	Participants		Documents	
Major theme	Count	References	Count	References
IT training to increase awareness	5	58	6	81

The participants' responses are in tandem with the reviewed literature of the study. Training programs that focus on positive communication and collaboration between groups is the most effective technique for reducing conflicts (Cletus et al., 2018). Such training involves teaching individuals to increase their awareness of issues related to cyberattacks and to understand to how to efficiently work to mitigate risk to the organization (Cletus et al., 2018). Awareness training is designed to empower employees to make decisions on an individual basis to lower the risk of exposing the organization computing network systems to negative internal/external influences. Cybercrimes and different approaches to mitigate them through a culture of prevention and security awareness is very useful. Cybercriminals can use malware such as viruses, worms, Trojan horses, and spyware to access credentials or manipulate the entire system sessions (Leukfeldt et al., 2017). Although there are many tools to detect and prevent cyberattack, one of the most common ways that cybercriminals use to infiltrate and cause significant harms to businesses and organization computers involves employees, therefore, building and implementing security strategies such as IT training positively can impact the prevention of cybercrimes. Security education and awareness training effectively reduce users' susceptibility to phishing attempts (Tschakert & Ngamsuriyaroj, 2019).

Organizations must develop adequate training programs by providing security awareness training courses that can comprehensively influence attitudes to information security management and improve cybersecurity awareness (Zwilling et al., 2020). A review of company policies indicates that the partnering organizations needed to create an educational environment to improve the company's security posture and increases employees' awareness related to cybersecurity.

Theme 3 Findings Related to the Literature

Having solid policies and procedures related to cybersecurity is critical between merging organizations (Kayser et al, 2019). Policies and procedures play a huge role in the security awareness education by demonstrating the ability of the organization to provide training to employees through a general session on security awareness focusing on commitment to ethical business behavior (Aldawood & Skinner, 2019).

Theme 3 Findings Related to the Conceptual Framework

Organizations must have appropriate laws and policies to fight cybercrime (Schreck, 2017). All the participants agreed that their organizations put in place several policies to prevent cyberattacks. The theme of using policies to prevent cybercrimes is supported by the Habermas framework (1989) which addressed protective measures to improve guardianship. Strong policies implemented by organizations contribute to prevention of being cyberattacked. Cybercriminals use the vulnerabilities of their victims to perpetrate their crimes (Vakhitova et al., 2016). Cybersecurity policies that are well implemented are useful to reduce those vulnerabilities and prevent cyberattacks. Reyns et al. (2016b) used Habermas Theory to address the importance of identifying the risk

factors. The reviewed company documentation affirmed the necessity to identify those risk factors. It is important for organizations to have a clear assessment of the risk factors associated with a merger or business acquisition to understand the impact of the newly formed organization's valuation and understand the needs and concerns of their consumer base. Business leaders must evaluate their data security controls, privacy compliance obligations and data ethics for any ambiguity within their computer networks across merging companies. Policies are created based on these risk factors that organizations face daily therefore it is important for all the participants within organizations to use those policies to minimize data breaches.

P5 suggested that regular audits for cybersecurity controls are implemented. Conducting penetration tests to ensure that the environment security is intact is necessary to ensure an organizations' compliance level are not at risk. It is crucial to make sure that computer infrastructure is compliant with cybersecurity controls that take preventive measures to minimize security flaws and avoid attacks.

Threat assessment comprises of the outcomes of risk-taking, including perceptions of vulnerability, severity, and the consequences of risky behavior (Chen et al., 2017). This opinion is consistent with the approach of cybersecurity culture in which end users/employees should be involved and part of the protection of all security aspects related to their organizations. Protecting an organization from being cyberattacked is the same as physically safeguarding an organization's property, which should be viewed as a normal way to operate any organization.

Theme 4: Cybersecurity Frameworks to Increase Security Between Merging Companies

P2 reported that cyberattacks "affect security measures and controls because they take advantage of vulnerabilities." P5 also affirmed that organizations should work towards relying on numerous cybersecurity policies to prevent cybercrimes. P3 noted,

> The use of many templates to create policies using different frameworks such as the National Institute of Standards and Technology (NIST CSF 2.0), Control Objective for Information and Related Technologies (Cobit by ISACA), and International Organization for Standardization 27001 (ISO 27001) can be used to combat cyberattacks.

Both P4 and P5 have adopted emergency policies in case of cyberattacks. P1 affirmed that the partnering organization follows a protocol that ensures that continuous monitoring occurs during a merger or business acquisition. P3 also noted that they perform "a vulnerability scans every six months to ensure no vulnerability are present in their system." The commitment to following protocols to assess business risk level should be routine (Aldawood & Skinner, 2019). Table 5 illustrates the number of references to the theme that references the use of cybersecurity frameworks to increase security between merging companies.

Table 5

References to Cybersecurity Frameworks to Increase Security

Major theme	Participant Count	Participant References	Documents Count	Documents References
Cybersecurity frameworks to increase security	3	23	4	32

Theme 4 Findings Related to the Literature

The participants' views related to the necessity of instituting cybersecurity frameworks aligns with the literature. Von Solms and Marnwick (2019) examined cybersecurity frameworks from a system view and suggested that interdependences between critical infrastructures are becoming increasingly apparent and that understanding how to manage critical infrastructures is an emerging issue for businesses. Global interconnections have caused systems to converge, resulting in isolated attacks on vital infrastructure systems that has cascading effects on other critical infrastructures and affect overall business operations (Volkova & Cherny, 2018).

Theme 4 Findings Related to the Conceptual Framework

Exploring effective business leaders' strategies connects with the systems theory conceptual framework. The study employed the Habermas theory to explore the strategies that leaders in the wine industry uses to minimize the risk of data breach during a merger or business acquisition. Drawing on Habermas's theories gives a theoretical grounding which ensures the methodology's sensitivity to critical issues such as data breaches are being addressed (Klein & Huynh, 2004). The underlying principle inherent in the theory is that all employees are personally responsible for the security of the information and

systems that they use. The reviewed company training documentation emphasized the importance of employees taking ownership to secure company data. P5 added that

> I think that both sides should make some sort of announcement of what the merging organization is going to look like or just a rundown (of) the details of the activities of the merger. I think having open communication is necessary on both ends, I know that some information is proprietary and cannot be communicated" but still essential to gain alignment by the end users.

P2 also reported that use of effective communication will help the end user to "start learning what their functions are and help to find any potential points of failure in their processes and security related to them".

Applications to Professional Practice

The specific problem this study was that some business leaders within the wine industry lack cybersecurity strategies to manage the risk of data breach from cyberattacks during a merger. Data breaches have significantly increased over time and continue to cost organizations billions of US dollars each year regarding sensitive financial information or/and intellectual property losses (Hawkins, 2017). However, as organizations recognize the importance of cybersecurity controls, security awareness continues to increase amongst employees. Effective strategies will equip end users with adequate knowledge and tools to help them detect and prevent cyberattacks that could jeopardize the merger.

The lack of training programs can be very risky and costly for organizations when cyberattacks are not detected. Based on the finding of this study, maintaining a strong

network infrastructure is not enough to protect merging organizations from being cyberattacked because cybercriminals target end users to gain quick access to the organization network infrastructure and cause harm. Seeking to maintain compliance to strategic policies regarding cybersecurity is very useful in the prevention of cyberattacks and allows a better respect of the security procedures needed to minimize data breaches and cyberattacks.

The implementation of cybersecurity strategies within the organization is an efficient measure to respond on time to cyberattacks that face the organization on the daily bases and avoid disruption of service. The development of a cybersecurity culture within the organization is a positive way to make end users aware of the security risks and threats they face every day and make them part of the prevention of cyberattacks. The training of end-users frequently contributes to the prevention of cyberattacks within the organization in the long run and increases their knowledge in that regard. When all these measures are implemented efficiently across the merging organizations, it becomes difficult for cyberattackers to gain access to organizations' network infrastructure and commit a cybercrime. Moreover, the mentioned elements contribute to ensure in the long run the safety of the organization in terms of cyberattacks and allow the organization to minimize costs in terms of business losses and ensure business continuity.

The study findings may enhance IT understanding of best learning and security practices relative to cybersecurity. Application of the findings may improve the approach that IT professionals use to deal with threats and risks linked to cybercrimes. Information security officers may be motivated by the study's findings to improve the way they

handle cybersecurity threats, develop consistent cybersecurity policies, and enhance the training of end users/employees in the prevention of cyberattacks. Participants of this study reported a significant reduction of cyberattacks within their organizations since they received frequent security awareness training on cybercrimes and observed security policies and guidelines implemented by their organizations in that regard. Therefore, the findings from this study can contribute to an organization's awareness and implementation of effective security awareness strategies they can use to prevent cybercrimes in the long run and avoid business disruption in case of cyberattacks.

Implications for Social Change

The application of these findings may have broader social effects and can contribute to creating strategies to increase cybersecurity to prevent data breach during a merger or business acquisition. The protection of data integrity should not be solely reliant on the performance of computer networks but the involvement of all the employees/end users that rely and uses the merging companies' resources for business purposes. A successful cyberattack can lead to the devaluation of the newly formed organization in terms of financial, customer, and intellectual property losses. Merging companies should involve their employees in the prevention of cyberattacks through establishing effective channels of communication and offering cybersecurity training on a frequent basis.

The implication for positive social change includes the potential for business leaders to build prevention strategies that can lead to lowering the risk of data breach during a merger to provide better safeguards to protect the privacy of customers'

information and preserve companies' sensitive information and intellectual property. These change initiatives have the potential to positively impact customer satisfaction and help promote economic job growth within the community.

Recommendations for Action

The results from this research study are relevant to business leaders because it provides practical ways to set up strategies and practices to minimize the risk of data breach during a merger and data acquisition. Based on the results of this study, below are recommendations for actions to implement the successful strategies used by the participants to maintain data integrity between merging companies.

Recommendation 1: Data Integrity Protection

Business leaders should identify all areas where data resides within the computer infrastructures across merging companies and place robust cybersecurity control measures in place. The key items that business leaders should consider are outdated data and data that might not align with the merging companies' business model. Limit access in the computer infrastructure where sensitive information resides. Also, leaders need to establish new policies to ensure end users have increased awareness of any new guidelines requiring reliable and robust protection technologies that are implemented because of the merger or business acquisition.

Recommendation 2: Use of Communication/Feedback

Business leaders interested in embarking on a merger must determine effective communication channels and feedback loops to institute clarity and transparency during the merger or business acquisition process. Business leaders should provide formal or

informal methods of communication to engage employees about ways to maintain data integrity. Business leaders should incentivize employees to protect data and report any potential data breaches.

Recommendation 3: Information Technology Training to Increase Awareness

Establishing IT training and education for employees is an important defense mechanism to increase awareness of cybersecurity threats and maintaining data integrity. Targeted cybersecurity awareness education can address any weaknesses of the merging companies' computer infrastructure and widens the scope of surveillance to limit the potential of data breach. It is recommended that business leaders maintain yearly or bi-yearly training programs for the company's staff because cybersecurity awareness is a methodical way to educate end users about cybercrime and the vulnerability of cyberthreats to computer systems.

Recommendation 4: Cybersecurity Frameworks to Increase Security

Business leaders should consider adopting cybersecurity control measures that incorporates a holistic approach. Azmi, Tibben and Win (2018) recommend that organization use a cyberstrategy to promote action necessary to increase security. The promoted actions within a cybersecurity framework can be classified into "two main categories, the first category promotes collaborative action as an outward strategy, while in contrast, the second type advocates increasing the cybercapacity of the organization an inward strategy" (Azmi, Tibben, & Win, 2018, p.21). An outward strategy endorses positive interdependence, which emphasizes collaborative action and promotes cooperation among the entities involved in a merger or business acquisition.

Cybersecurity should be viewed as a shared responsibility given the challenges associated with the interdependencies of cyberspace. Business leader may want to consider the use of cybersecurity frameworks such as the National Institute of Standards and Technology (NIST) which offers a mechanism to increase security during a merger or business acquisition. Instituting technical controls that include processes and products such as encryption techniques, antivirus software and firewalls can also minimize the risk of data breach between merging companies. The benefit of including cybersecurity frameworks during a merger or business acquisition includes methods to identify cyberthreats that exploit access controls, business continuity, and backup capabilities. Business leaders should also consider continually evaluating their transaction process and identify opportunities to update policies and procedures to protect sensitive information and the merging companies' computer networks.

Recommendations for Further Research

I conducted a qualitative single case study to explore the strategies within the wine industry to improve the process of mergers and business acquisitions. The study's findings could be beneficial to (a) business leaders who are struggling to identify protection strategies to protect data integrity between merging companies, (b) business leaders that are experiencing challenges with communication with their employees involved in a merger or business acquisition, (c) business leaders challenged with identifying the frameworks to support cybersecurity control measures, and (d) business organizations' leaders in the wine industry lacking the necessary training programs to increase awareness of cybercrime.

Through the experience gained in completing this study, I recommend that future research be conducted using different research methodologies to investigate the different strategies used for cybersecurity and their effectiveness in wine industry organizations. The protection of the information/data within an organization is not solely the role of the business leader but the involvement of all the stakeholders who use the organization's resources for business purposes. Moreover, a successful cyberattack may be very costly to an organization in terms of financial, material, data, or/and intellectual property losses. For this reason, organizations should involve their employees in the prevention of cyberattacks by offering frequent cybersecurity awareness training programs viewed as one of the more efficient approaches for prevention of cybercrimes. A study involving a larger sample size could provide a more comprehensive and holistic comparison and improve the application of the findings in practice.

It is important that employees become aware of the real threats they face daily and the impacts to the business when exposed to cyberthreats. The study could contribute to increased employees' awareness and vigilance to detect and prevent against cyberattacks, which could transform their habits into a culture where data integrity is preserved, and the risk of data breach is minimized.

Reflections

Pursuing my advanced degree has allowed me to acquire critical academic skills and experiences. Specifically, I have learned to prioritize, balance, and undertake responsibilities through completing this project, including family, school, and work. I have learned to develop an attitude of resilience, dedication, and determination to

complete my studies. The learning process has equipped me with the skills necessary for creative thinking, synthesis of information, and scholarly writing. I have learned to be committed to attaining my goal: completing the program at a personal level.

I have also learned the ability to remain objective despite the temptation to pursue personal biases when collecting and analyzing data and drawing conclusions based on gathered evidence. Finally, the entire doctoral journey has been challenging and demanded engaging in rigorous academic work, commitment, and an immense support system. Regardless, I found the whole journey enlightening and thought-provoking.

Conclusion

Implementing strategies business leaders within the wine industry can use to manage the risk of data breach from a cyberattack during a merger is not a straightforward approach. The cybersecurity controls necessary to secure computer environments are ever-changing. It is important for business leaders to display diligence to securely implement prevention strategy measures to minimize the risk of data breach. Specifically, business leaders within the wine industry must be committed to cybersecurity and create a collaborative work environment that focuses on transparency and clarity when companies are venturing into a merger or business acquisition. The threat of cyberattack can be minimized with the advent of comprehensive IT training for the organizations' employee base along with the implementation of prevention policies and procedures that provide a roadmap of the computer frameworks needed to maintain data integrity during a merger or business acquisition.

References

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulations as a methodological alternative. *Administração: Ensino e Pesquisa, 19*(1), 66–98. https://doi.org/10.13058/raep.2018.v19n1.578

Abdelrahman, A. A., Nimrat, A., & Chafika, B. (2018). Combating cyber victimisation: Cybercrime preventing. *Cybercrimology*, 325–339. https://doi.org/10.1007/978-3-319-97181-0_16

Abdulla, M. F., & Ravikumar, C. P. (2004). A self-checking signature scheme for checking backdoor security attacks in Internet. *Journal of High Speed Networks, 13*, 309–317.

Abro, M. M. Q., Khurshid, M. A., & Aamir, A. (2015). The use of mixed methods in management research. *Journal of Applied Finance & Banking, 5*(2), 1–8.

Adauto, L. S., & Guerrini, F. M. (2018). Self-organized innovation networks from the perspective of complex systems. *Journal of Organizational Change Management*, *31*(5), 962–983. https://doi.org/10.1108/JOCM-10-2016-0210

Afzaal, H., & Zafar, N. (2016). Formal analysis of subnet-based failure recovery algorithm in wireless sensor and actor and network. *Complex Adaptive Systems Modeling*, *4*(1), 1–27. https://doi.org/10.1186/s40294-016-0037-4

Ahirwar, D., Ahirwar, M. K., Shukla, P. K., & Richharia, P. (2011). An analytical survey on network security enhancement services. *International Journal of Computer*

Science and Information Security, 9, 259–262. https://www.cscjournals.org/journals/IJCSS/description.php

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

Ahmad, S., & Rahman, F. U. (2019). Effect of workplace diversity on employees. *Pakistan Journal of Distance & Online Learning*, *5*(2), 85–100. https://files.eric.ed.gov/fulltext/EJ1266670.pdf

Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2016). A consideration of the social impact of cybercrime: Examples from hacking, piracy, and child abuse material online. *Contemporary Social Science, 11*, 373–391. https://doi.org/10.1080/21582041.2015.1117648

Akgun, A. E., Keskin, H., & Byrne, J. C. (2014). Complex adaptive systems theory and firm product innovativeness. *Journal of Engineering and Technology Management*, *31*, 21–42. https://doi.org/10.1016/j.jengtecman.2013.09.003

Akhavan, P., Ebrahim, N. A., Fetrati, M. A., & Pezeshkan, A. (2016). Major trends in knowledge management research: A bibliometric study. *Scientometrics, 107*, 1249–1264. https://doi.org/10.1007/s11192-016-1938-x

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

Aleem, A., Wakefield, A., & Button, M., (2013). Addressing the weakest link: Implementing converged security. *Security Journal, 26*, 236–248. https://doi.org/10.1057/sj.2013.14

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

Allodi, L., & Massacci, F. (2017). Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis, 37*, 1606–1627. https://doi.org/10.1111/risa.12864

Almudarra, F., & Qureshi, B. (2015). Issues in adopting agile development principles for mobile cloud computing applications. *Procedia Computer Science, 52*, 1133–1140. https://doi.org/10.1016/j.procs.2015.05.131

Almutairi, A. F., Gardner, G. E., & McCarthy, A. (2014). Practical guidance for the use of pattern-matching technique in case-study research: A case presentation. *Nursing & Health Sciences, 16*, 239–244. https://doi.org/10.1111/nhs.12096

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do it security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*, 893–916. https://doi.org/10.25300/misq/2017/41.3.10

Ao, W., Song, Y., & Wen, C. (2016). Adaptive cyber-physical system attack detection and reconstruction with application to power systems. *IET Control Theory & Applications, 10*(12), 1458–1468. https://doi.org/10.1049/iet-cta.2015.147

Armencheva, L., & Smolenov, S. (2015). From real cyber conflict through wishful cyber security to (un)likely cyber peace. *Revista Fortelor Terestre, 20*(3), 259-266. https://www.armyacademy.ro/reviste/rev3_2015/ARMENCHEVA.pdf

Asghari, H., van Eeten, M. J., & Bauer, J. M. (2015). Economics of fighting botnets: Lessons from a decade of mitigation. *IEEE Security & Privacy, 13*(5), 16–23. https://doi.org/10.1109/MSP.2015.110

Asija, R., & Nallusamy, R. (2016). Healthcare SaaS based on a data model with built in security and privacy. *International Journal of Cloud Applications and Computing, 6*(3), 1–14. https://doi.org/10.4018/ijcac.2016070101

Astakhova, L. V. (2014). The concept of the information security culture. *Scientific and Technical Information Processing, 41*, 22–28. https://doi.org/10.3103/S0147688214010067

Avasthi, A., Ghosh, A., Sarkar, S., & Grover, S. (2013). Ethics in medical research: General principles with special reference to psychiatry research. *Indian Journal of Psychiatry, 55*, 86–91. https://doi.org/10.4103/0019-5545.105525

Aven, T., & Cox, L. A. (2016). National and global risk studies: How can the field of risk analysis contribute? *Risk Analysis, 36*, 186–190. https://doi.org/10.1111/risa.12584

Avgerinos, T., Cha, S. K., Rebert, A., Schwartz, E. J., Woo, M., & Brumley, D. (2014). Automatic exploit generation. *Communications of the ACM*, *57*(2), 74–84. https://doi.org/10.1145/2560217.2560219

Avogundade, O., Abioye, T.E., & Sanjay, M. (2020). An ontological approach to threats pattern collection and classification: A preliminary study to security management. *Inderscience online*. https://doi.org/10.1504/IJESDF2020.108320

Azmi, R., Tibben, W.J. & Win, K.T (2018). Review of cybersecurity frameworks: Context and shared concepts. *Journal of Cyber Policy, 3*(2), 258-283. Retrieved from https://ro.uow.edu.au/cgi/viewcontent.cgi?article=2961&context=eispapers1

Bacis, E., Vimercati, S. D., Foresti, S., Paraboschi, S., Rosa, M., & Samarati, P. (2017). Distributed shuffle index in the cloud: Implementation and evaluation. *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing*, pp. 1–6. https://doi.org/10.1109/cscloud.2017.25

Badhwar, R. (2021). Introduction to cloud monitoring security controls. *The CISO's Next Frontier*, 289-296.

Baldwin, D. A. (1997). The concept of security. *Review of International Studies, 23*, 5–26. https://journals.cambridge.org/

Ballaro, J. M., & Polk, L. (2017). Developing an organization for future growth using succession planning. *Organization Development Journal, 35*(4), 41–42. https://www.isodc.org/page-1730212

Bambauer, D. E. (2013). Ghost in the network. *University of Pennsylvania Law Review*, *162,* 1011–1091.

Barker, I. (2015). *Multi-purpose backdoor Trojan threatens Windows systems*. https://betanews.com/2015/03/24/multi-purpose-backdoor-trojanthreatens-windows-systems/

Barratt, M. J., Ferris, J. A., & Lenton, S. (2014). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods, 27*, 119. https://doi.org/10.1177/1525822X14

Barry, A. E., Chaney, B., Piazza-Gardner, A. K., & Chavarria, E. A. (2014). Validity and reliability reporting practices in the field of health education and behavior: A review of seven journals. *Health Education & Behavior, 41*, 12–18. https://doi.org/10.1177/1090198113483139

Barosy, W. (2019). Successful operational cybersecurity strategies for small businesses. Walden University. https://scholarworks.waldenu.edu/dissertations/6969/

Bauer, S., Bernroider, E. W. N., & 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*, 145-169. https://doi.org/10.1016/j.cose.2017.04.009

Bayramusta, M., & Nasir, V. A. (2016). A fad or future of IT? A comprehensive literature review on the cloud computing research. *International Journal of Information Management, 36*, 635–644. https://doi.org/10.1016/j.ijinfomgt.2016.04.006

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

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

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

Benoot, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked sample on sexual adjustment to a cancer trajectory. *BMC Medical Research, 16*, 21. https://doi.org/10:1186/s12874-016-0114-6

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy, 37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Bernard, R. H. (2018). *Research methods in anthropology* (6th ed.). Lanham, MD: Rowman & Littlefield.

Bernik, I. (2014). Cybercrime: The cost of investments into protection. *Varstvoslovje: Journal of Criminal Justice & Security, 16*, 105–116. https://www.fvv.um.si/rV/arhiv-E.html#arhiv/2014-2-E

Besliu, D. (2017). Cyber terrorism – A growing threat in the field of cybersecurity. *International Journal of Information Security and Cybercrime, 6*, 35–39. https://doi.org/10.19107/ijisc.2017.02.05

Bevan, N., Carter, J., & Harker, S. (2015). What have we learnt about usability since 1998? *Human-Computer Interaction: Design and Evaluation,* 143–151. https://doi.org/10.1007/978-3-319-20901-2_13

Biros, M. (2018). Capacity, vulnerability, and informed consent for research. *The Journal of Law, Medicine, & Ethics, 46*, 72-78. https://doi.org/10.1177117073105187660 21

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

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

Bossler, A.M., & Berenblum, T. (2019). Introduction: New direction in cybercrime research. *Journal of Crime & Justice, 42*(5), https://doi.org/10.1080/0735648x.2019.1692426

Boteanu, D., & Fernandez, J. M. (2013). A comprehensive study of queue management as a DoS counter-measure. *International Journal of Information Security, 12*, 347–382. https://doi.org/10.1007/s10207-013-0197-6

Bowden, C., & Galindo-Gonzalez, S. (2015). Interviewing when you're not face-to-face: The use of email interviews in a phenomenological study. *International Journal of Doctoral Studies, 10*, 79–92. https://doi.org/10.28945/2014

Bowen, P., Hash, J., & Wilson, M. (2006). *Information security handbook: A guide for managers.* Gaithersburg, MD: National Institute of Standards and Technology.

Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Network Security*, *2016*(9), 5-9. https://doi.org/10.1016/S1353-4858(16)30086-1

Brusse, C., Kach, A. P., & Wagner, S. M. (2016). 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. https://doi.org/10.1177/1094428116641191

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, *75*, 24-35. https://doi.org/10.1016/j.cose.2018.01.015

Canongia, C., & Mandarino, R. (2014). Cybersecurity: The new challenge of the information society. In *Crisis management: Concepts, methodologies, tools and applications* (pp. 60–80). https://doi.org/10.4018/978-1-4666-4707-7.ch003

Cardoso, C.L., Gontijo, L.A. & Ono, M.M. (2017). Affective memory: An ethnographic approach to design. *Strategic Design Research Journal, 10*(1), 79-88. https://doi.org/10.4013/sdrj.2017.101.09

Chaudhry, P. E., Chaudhry, S., & Reese R., (2012). Developing a model for enterprise information systems security. *Economics, Management, and Financial Markets, 7*, 587–599. https://addletonacademicpublishers.com/economics-management-and-financial-markets

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., & Soulsby, H., (2016). A review of cybersecurity risk assessment methods for SCADA systems. *Computers & Security, 56*, 1–27. https://www.journals.elsevier.com/computers-and-security

Choi, K.S. (2021). The driving force behind cybercrime: Cyber resilience and cybercriminology. *Journal of Contemporary Criminal Justice, 37*(3), 308-310. https://doi.org/10.10.1177/1043986221001631

Chou, D. C. (2015). Cloud security: A value creation model. *Computer Standards & Interfaces, 38*, 72–77. https://doi.org/10.1016/j.csi.2014.10.00

Christen, M., Gordijn, B., & Loi, M. (2020). The ethics of cybersecurity. *The International Library of Ethics, Law, & Technology*. https://doi.org/10.007/978-3-030-29053-5-8

Christo, C., Dewald, V. N., & Emmanuel, R. (2016). Disaster resilience and complex adaptive systems theory: Finding common grounds for risk reduction. *Disaster Prevention and Management, 25*, 196–211. https://doi.org/10.1108/DPM-07-2015-0153

Cioca, L., & Ivascu, L. (2014). IT technology implications analysis on the occupational risk: Cloud security architecture. *Procedia Technology, 16*, 1548–1559. https://doi.org/10.1016/j.protcy.2014.10.177

Cisco. (2014) *Annual security report*. https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: Does size matter? *Journal of Advanced Nursing, 70*, 473–475. https://doi.org/10.1111/jan.12163

Cletus, H. E., Mahmood, N. A., Umar, A., & Ibrahim, A. D. (2018). Prospects and challenges of workplace diversity in modern-day organizations: A critical review.

Holistics – Journal of Business and Public Administration, *9*(2), 35–52. https://doi.org/10.2478/hjbpa-2018-0011

Cloherty, J., & Thomas, P. (2014). *'Trojan Horse' bug lurking in vital US computers since 2011*. https://abcnews.go.com/US/trojan-horse-bug-lurkingvital-us-computers-2011/story?id=26737476

Coccoli, M., Maresca, P., Stanganelli, L., & Guercio, A. (2015). An experience of collaboration using a PaaS for the smarter university model. *Journal of Visual Languages & Computing, 31*, 275–282. https://doi.org/10.1016/j.jvlc.2015.10.014

Collins, C. S., & Stockton, C. M. (2018). The central role of theory in qualitative research. I*nternational Journal of Qualitative Methods*, *17*(1), 1–10. https://doi.org/10.1177/1609406918797475

Command. (2015, January 7). *Cyber readiness inspection*. https://www.edwards.af.mil/news/story.asp?id=123435688

Connolly, L., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers & Security, 87. https://doi.org/10.1016/j.cose.2019.101568

Cook, M. (2015). *Securing cyber acquisitions*. https://www.dau.mil/publications/defenseATLfiles/jan-feb2015/cook.pdf

Corradini, M. L., & Cristofaro, A. (2016). Robust detection and reconstruction of state and sensor attacks for cyber-physical systems using sliding modes. *IET Control Theory & Applications, 11*(11), 1756-1766. https://doi.org/10.1049/iet-cta.2016.1313

Council PCISS. (2018, September). *PCI Data Security Standard (DSS): Requirements and security assessment procedures.* https://www.pcisecuritystandards.org/documents/pci%5fdss%5fv2.pdf

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative and mixed methods approaches* (5th ed.). Thousand Oaks, CA: Sage.

Croucher, S. M., Sommier, M., & Rahmani, D. (2015). Intercultural communication: Where we've been, where we're going, issues we face. *Communication Research and Practice*, *1*(1), 71–87. https://doi.org/10.1080/22041451.2015.1042422

Davies, A. (2015). Qualitative research in action: A Canadian primer. *Canadian Journal of Action Research, 16*(3), 79-82. https://cjar.nipissingu.ca/index.php/cjar/index

De Costa, P. I. (2014). Making ethical decisions in an ethnographic study. *TESOL Quarterly, 48*, 413–422. https://doi.org/10.1002/tesq.163

DeSouza, E., & Valverde, R. (2016). Reducing security incidents in a Canadian PHIPA regulated environment with an employee-based risk management strategy. *Journal of Theoretical and Applied Information Technology, 90*(2), 197–208. https://spectrum.library.concordia.ca/id/eprint/981740/1/22Vol90No2.pdf

Ding, D., Wang, Z., Dong, H., Liu, Y., & Ahmed, B. (2014). Performance analysis with network-enhanced complexities on fading measurements event-triggered mechanisms and cyberattacks. *Abstract and Applied Analysis*, 1–11. https://doi.org/10.1155/2014/461261

DiscoverPhDs (October 2, 2020). *Scope and delimitations-Explained and example*. https://www.discoverphds.com/blog/scope-and-delimitations

Doherty, N. F., & Tajuddin, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. Information Technology & People, 31(2), 348-367. https://doi.org/10.1177/1715163517701470

Du, Y., Zhang, R., & Li, M. (2013). Research on a security mechanism for cloud computing based on virtualization. *Telecommunication Systems, 53*, 19–24. https://doi.org/10.1007/s11235-013-9672-7

Duench, M. (2020). Cybersecurity controls as the workforce returns. *Risk Management*

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics, 20*, 701-715. https://doi.org/10.1007/s11948-014-9551-y

Eddolls, M. (2016). Making cybercrime prevention the highest priority. *Network Security, 2016*(8), 5–8. https://doi.org/10.1016/S1353-4858(16)30075-7

Edwards-Jones, A. (2014). Qualitative data analysis with NVivo. *Journal of Education for Teaching, 40*, 193–195. https://doi.org/10.1080/02607476.2013.866724

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship, 8*(1). 1-26. https://doi.org/10.1186/s13731-019-0105-z

Federal Communications Commission. (2017). *Cybersecurity planning guide*. https://transition.fcc.gov/cyber/cyberplanner.pdf

Fan, H., Ming, L. Zhao, & Li, M. (2020) Review of cyber physical system and cyberattack modeling, *2020 12th IEEE PES Asia-Pacific Power and Energy*

Engineering Conference (APPEEC), Nanjing, China, 2020, pp. 1-5, https://doi.org/10.1109/APPEEC48164.2020.9220505

Faronbi, J. O., Faronbi, G. O., Ayamolowo, S. J., & Olaogun, A. A. (2019). Caring for the seniors with chronic illness: The lived experience of caregivers of older adults. *Archives of Gerontology and Geriatrics, 82*, 8–14. https://doi.org/10.1016/j.archger.2019.01.013

Fasulo, P. (2021). *Why cybersecurity due diligence is essential in mergers & acquisitions transactions.* https://securityscorecard.com/blog/why-cybersecurity-due-diligence-is-essential-in-mergers-and-acquisitions

Feller, A., Mealli, F., & Miratrix, L. (2017). Principal score methods: Assumptions, extensions, and practical considerations. Journal of Educational and Behavioral Statistics, 42, 726–758. https://doi.org/10.3102/1076998617719726

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inacio, P. R. M. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security, 13,* 113-170. https://doi.org/10.1007/s10207-013-0208-7

Ferreira, F. A., & dos Santos, C. C. (2016). Possibilities of the phenomenological approach and of philosophical hermeneutics in type search state of art. *Philosophy of Mathematics Education Journal, 31*, 1–4. http://socialsciences.exeter.ac.uk/education/research/centres/stem/publications/

Fidan, T., & Balci, A. (2017). Managing schools as complex adaptive systems: A strategic perspective. *International Electronic Journal of Elementary Education*, 10, 11-26. https://eric.ed.gov/?id=EJ1156312

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in Pharmacy Teaching and Learning, 11*(2), 211–217. https://doi.org/10.1016/j.cptl.2018.11.014

Fletcher, D., Massis, A. D., & Nordqvist, M. (2016). Qualitative research practices and family business scholarship: A review and future research agenda. *Journal of Family Business Strategy, 7*, 8–25. https://doi.org/10.1016/j.jfbs.2015.08.001

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research, 18*(1), 120. https://doi.org/10.1186/s12913-018-2915-2

Forster, D. G., & Borasky, D. (2018). Adults lacking capacity to give consent when is it acceptable to include them in research. *Therapeutic Innovation & Regulatory Science, 52*(3), 275-279. https://doi.org/10.1177/2168479018770658

Fritz, J., & Kaefer, F. (2017). The rise of the mega-breach and what can be done about it. *Journal of Applied Security Research, 12*(3), 392-406. https://doi.org/10.1080/19361610.2017.1315700

Fusch, P. I., Fusch, G. E., & Ness, L. R. (2017). How to conduct a mini-ethnographic case study: A guide for novice researchers. *The Qualitative Report, 22*(3), 923-941. https://doi.org/10.46743/2160-3715/2017:2580

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *Qualitative Report, 20*(11), 1772–1789. https://nsuworks.nova.edu/tqr/vol20/iss11/5

George, G., Haas, M. R., & Pentland, A. (2014). Big data and management. *Academy of Management Journal, 57*, 321–326. https://doi.org/10.5465/amj.2014.4002

Georgiadon, A., Mouzakitis, S., Bounaj, K., & Askounis, D. (2020). A cyber-security culture: Framework for assessing organization readiness. *Journal of Computer Information Systems.* https://www.scimagojr.com/journalsearch.php?q=12373&tip=sid

Ghazzawi, A., Kuziemsky, C., & O'Sullivan, T. (2016). Using a complex adaptive system lens to understand family caregiving experiences navigating the stroke rehabilitation system. *BMC Health Services Research*, 16, 1-10. https://doi.org/10.1186/s12913-016-1795-6

Giacalone, M., Mammoliti, R., Massacci, F., Paci, F., Perugino, R., & Selli, C. (2014). Security triage: A report of a lean security requirements methodology for cost-effective security analysis. *Proceedings of ACM/IEE ESEM'14*, pp. 25–27.

Gibson, A. (2019). *Cybercrime prevention among small businesses in the greater Houston area: A qualitative exploratory case study*. University of Phoenix.

Gibson, C. B. (2017). Elaboration, generalization, triangulation, and interpretation: On enhancing the value of mixed-method research. *Organizational Research Methods, 20*(2), 193-223. https://doi.org/10.1177/1094428116639133

Gonen, B., & Sawant, D. (2020). Significance of agile software development and SQA powered by automation. 2020 3rd International Conference on Information and Computer Technologies (ICICT), 7–11. https://doi.org/10.1109/ICICT50521.2020.00009

González-Torres, T, Rodríguez-Sánchez, J.-L., Pelechano-Barahona, E., & García-Muiña, F.E. (2020). A systematic review of research on sustainability in mergers and acquisitions. *Sustainability*, *12*, 513. https://doi.org/10.3390/su12020513

Goodall, J. R., Lutters, W. G., & Komlodi, A., (2009). Developing expertise for network intrusion detection. *Information Technology & People, 22*(2), 92–108. https://doi.org/10.1108/09593840910962186

Gootman, S. (2016). OPM hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research, 11*, 517–525. https://doi.org/10.1080/19361610.2016.1211876

Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security, 7*(2), 49–59. https://doi.org/10.4236/jis.2016.72004

Goyal, S. (2014). Public vs private vs hybrid vs community - cloud computing: A critical review. *International Journal of Computer Network and Information Security, 6*(3), 20-29. https://doi.org/10.5815/ijcnis.2014.03.03

Green, J. (2015, February). Staying ahead of cyberattacks. *Network Security, 2*, 13–16. https://doi.org/10.1016/S1353-4858(15)30007-6

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care Chaplaincy, 20*(3), 109–122. https://doi.org/10.1080/08854726.2014.925660

Guetterman, T. C. (2015). Descriptions of sampling practices within five approaches to qualitative research in education and the health sciences. *Forum Qualitative*

Sozialforschung/Forum: Qualitative Social Research, 16(2), 1-23. https://doi.org/10.17169/fqs-16.2.2290

Guler, M. (2015). Case study: Ambitious growth target of BNP Paribas in Germany. *International Journal of Sales, Retailing & Marketing, 4*(9), 79–88. https://www.ijsrm.com/ijsrm/Current_&_Past_Issues_files/IJSRM4-9.pdf

Guynes, C. S., Wu, Y., & Windsor, J. (2011). E-commerce/network security considerations. *International Journal of Management and Information Systems, 15*(2), 1-7. https://doi.org/10.19030/ijmis.v15i2.4147

Habermas, J. (1989). *The theory of communicative action, volume 2: lifeworld and system: a critique of functionalist reason.* Beacon Press, Boston, MA.

Hagaman, A. K., & Wutich, A. (2017). How many interviews are enough to identify metathemes in multisited and cross-cultural research? Another perspective on Guest, Bunce, & Johnson's (2006) landmark study. *Field Methods, 29*(1), 23-41. https://doi.org/10.1177/1525822X16640447

Halcomb, E.J. (2018). Mixed methods research: The issues beyond combining methods. *Journal of Advanced Nursing, 75*(3), 499-501. https://doi.org/10.1111/jan.13877

Handwerker, S. M. (2018). Challenges experienced by nursing students overcoming one course failure: A phenomenological research study. *Teaching and Learning in Nursing, 13*, 168-173. https://doi.org/10.1016/j.teln.2018.03.007

Hawkins, N. (2017).. *Network Security, 3*, 12–14. https://doi.org/10.1016/S1353-4858(17)30028-4

Haydon, G., Browne, G., & Van der Riet, P. (2018). Narrative inquiry as a research methodology exploring person centred care in nursing. *Collegian, 25*(1), 125-129. https://doi.org/10.1016/j.colegn.2017.03.001

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

Herjanto, H., Gaur, S. S., Saransomrurtai, C., & Hock Quik, W. (2014). Allowing digital piracy for strategic benefits to businesses. *Journal of Information, Communication & Ethics in Society, 12*, 314. https://doi.org/10.1108/jices-12-2013-0056

Herrmann, D., & Pridohl, H. (2020). Basic concepts and models of cybersecurity. *The International Library of Ethics, Law, & Technology*. https://doi.org/10.007/978-3-030-29053-5-8

Hess, M. F., & Cottrell, J. H. (2016). Fraud risk management: A small business perspective. *Business Horizons, 59*, 13-18. https://doi.org/10.1016/j.bushor.2015.09.005

Hester, A. J. (2014). Socio-technical systems theory as a diagnostic tool for examining underutilization of wiki technology. *The Learning Organization, 21*(1), 48-68. https://doi.org/10.1108/TLO-10-2012-0065

Hof, B. E. (2018). The cybernetic "general model theory": Unifying science or epistemic change? Perspectives on Science, 26(1), 76.

Hoffmann, R., Napiorkowski, J, Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia*

Manufacturing, 44, 655-662. https://www.journals.elsevier.com/procedia-manufacturing

Holm, H. (2014). A large-scale study of the time required to compromise a computer system. *IEEE Transactions on Dependable and Secure Computing, 11,* 2–15. https://www.computer.org/csdl/journal/tq

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London, UK: Routledge.

Hoover, S. M., Strapp, C. M., Ito, A., Foster, K., & Roth, K. (2018). Teaching qualitative research interviewer skills: A developmental framework for social justice psychological research teams. *Qualitative Psychology, 5*(2), 300–318. https://doi.org/10.1037/qup0000101

Horvath, M., & Lovasz, A. (2018). Programming the vicious circle: Austen, Deleuze and viral repetition. Rhizomes: Cultural Studies in Emerging Knowledge, (33), 15. https://www.rhizomes.net/issue33/pdf/horvath.pdf

Hung, S. C., & Tu, M. F. (2014). Is small actually big? The chaos of technological change. *Research Policy, 43*, 1227–1238. https://doi.org/10.1016/j.repol.2014.03.003

Hussein, A. (2015). The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of Comparative Social Work, 4*, 1–12. https://journals.uis.no/index.php/JCSW

Hussein, O., Hamza, N., & Hefny, H., (2014). Limitations of current security measures to address information leakage attacks. *International Journal of Computer Science*

and Information Security, 12(8), 26–32. https://www.academia.edu/11700353/Limitations_of_Current_Security_Measures_to_Address_Information_Leakage_Attacks

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime, 18*, 11–30. https://doi.org/10.1080/17440572.2016.1197123

Hwarng, H. B., & Yuan, X. (2014). Interpreting supply chain dynamics: A quasi-chaos perspective. *European Journal of Operational Research, 233*, 566–579. https://doi.org/10.1016/j.ejor.2013.09.025

Ibarra, J., Jahankhani H., & Kendzierskyj, S. (2019). Cyber-physical attacks and the value of healthcare data: Facing an era of cyber extortion and organised crime. In H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, & H. Al-Khateeb (Eds). Blockchain and clinical trials. Advanced sciences and technologies for security applications. Springer, Cham. https://doi.org/10.1007/978-3-030-11289-9_5

Ifinedo, P., (2014). The effects of national culture on the assessment of information security threats and controls in financial services industry. *International Journal of Electronic Business Management, 12*(2), 75-89. https://www.inderscience.com/jhome.php?jcode=ijeb

Iivari, N. (2018). Using member checking in interpretive research practice: A hermeneutic analysis of informants' interpretation of their organizational realities.

Information Technology & People, 31(1), 111-113. https://doi.org/10.1108/ITP-07-2016- 0168

ISACA. (2017). *State of cybersecurity*. https://cybersecurity.isaca.org/state-of-cybersecurity?cid=pr_1221600&appeal=pr

Jackson, K. & Brown, R. (June 3,2020). Designing research for meaningful results in educational leadership. *Oxford Research Encyclopedia of Education*. https://oxfordre.com/education/view/10.1093/acrefore/9780190264093.001.0001/acrefore-9780190264093-e-626

Jain, A., & Kumar, R. (2014). A taxonomy of cloud computing. *International Journal of Scientific and Research Publications, 4*(7), 1-5. https://www.ijsrp.org/research-paper-0714/ijsrp-p3128.pdf

Jagalur, P. K., Levin, P. L., Brittain, K., Dubinsky, M., Landau-Jagalur, K., & Lathrop, C. (2018, November). Cybersecurity for civil society. In 2018 IEEE International Symposium on Technology and Society (ISTAS; pp. 102-107). IEEE.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Journal of Medical Internet Research, 20(5), 1-16. https://doi.org/10.2196/10059

James, L. (2018). Making cyber-security a strategic business priority. *Network Security, 8*(5), 6–8. https://doi.org/10.1016/S1353-4858(18)30042-4

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*, 973–993. https://doi.org/10.1016/j.jcss.2014.02

Johnson, R.B. & Christensen, L.B. (2020). *Educational research: Quantitative, qualitative, and mixed approaches*, 7th ed. Thousand Oaks, CA: Sage.

Jordan, A. (2020). Cybercrime prevention principles for internet service providers. *World Economic Forum: Analysis and Policy Observatory.* https://www.weforum.org/reports/cybercrime-prevention-principles-for-internet-service-providers

Kahn, C. M., & Liñares-Zegarra, J. M. (2016). Identity theft and consumer payment choice: Does security really matter? *Journal of Financial Services Research, 50*, 121–159. https://doi.org/10.1007/s10693-015-0218-x

Kakucha, W., & Buya, I. (2018). Information System Security Mechanisms in Financial Management. *Journal of Information and Technology, 2*(1), 1-16. Stratford. https://stratfordjournals.org/journals/index.php/Journal-of-Information-and Techn/article/view/115

Kasim, A., & Al-Gahuri, H. A. (2015). Overcoming challenges in qualitative inquiry within a conservative society. *Tourism Management, 50*(2015), 124–129. https://doi.org/10.1016/j.tourman.2015.01.004

Kaur, K., Pathak, A., Kaur, P., & Kaur, K. (2015). E-commerce privacy and security system. *International Journal of Engineering Research and Applications, 5*(5), 63–73.

Kayser, C. S., Ellen Mastrorilli, M., & Cadigan, R. (2019). Preventing cybercrime: A framework for understanding the role of human vulnerabilities. *Cyber Security: A Peer-Reviewed Journal, 3*(2), 159-174. Ingenta.

https://www.ingentaconnect.com/content/hsp/jcs/2019/00000003/00000002/art00007

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

Khan, S. N. (2014). Qualitative research method: Grounded theory. *International Journal of Business & Management, 9*(11), 224–233. https://doi.org/10.5539/ijbm.v9n11p224

Khorshidi, H. A., Gunawan, I., & Ibrahim, M. Y. (2016). Data-driven system reliability and failure behavior modeling using FMECA. *IEEE Transactions on Industrial Informatics, 12*, 1253–1260. https://www.ieee-ies.org/pubs/transactions-on-industrial-informatics

King, K. M., Pullmann, M. D., Lyon, A. R., Dorsey, S., & Lewis, C. C. (2019). Using implementation science to close the gap between the optimal and typical practice of quantitative methods in clinical science. *Journal of Abnormal Psychology, 128*(6), 547–562. https://doi.org/10.1037/abn0000417

Kikerpill, K. (2020). The individual's role in cybercrime prevention: Internal spheres of protection and our ability to safeguard them. *Kybernetes, 50*(4). https://doi.org/10.1108/K-06-2020-0035

Kline, T. J. B. (2017). Sample issues, methodological implications, and best practices. *Canadian Journal of Behavioural Science, 49*(2), 71-77. https://doi.org/10.1037/cbs0000054

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

Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers & Security, 58*, 39–46. https://doi.org/10.1016/j.cose.2015.12.001

Kopel, J., Hier, D., & Thomas, P. (2019). Electronic health records: Is mindfulness the solution? Baylor University Medical Center. Proceedings, 32(3), 459–461. https://doi.org/10.1080/08998280.2019.1588839

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice, 24*(1), 120-124. https://doi.org/10.1080/13814788.2017.1375092

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting Social Change, 80*, 541–555. https://doi.org/10.1016/j.techfore.2012.07.002

Kreitz, G. (2013). Flow stealing: A well-timed redirection attack. *Journal of Computer Security, 21*, 371–391. https://doi.org/10.3233/JCS-130466

Krishna, B. H., Kiran, S., Murali, G., & Reddy, R. P. (2016). Security issues in service model of cloud security environment. *Procedia Computer Science, 87*, 246–251. https://doi.org/10.1016/j.procs.2016.05.156

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Computer Science*, 125, 691-697. https://doi.org/10.1016/j.procs.2017.12.089

Kumari, M.M. (2019). Application of machine learning and deep learning in cybercrime prevention: A study. *International Journal of Trend in Research and Development*, 1-4. https://www.ijtrd.com/papers/IJTRD20407.pdf

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. *Computers & Security, 45*(2014), 58–74.

Landwehr, C. (2015). We need a building code for building code. *Communications of the ACM, 58*(2), 24–26. https://doi.org/10.1145/2700341

Latto, N. (2020). *What is cybercrime and how can you prevent it?* https://www.avast.com/c-cybercrime

Leal, C., Marques, C. P., & Marques, C. S. (2016). Mediating effects of intellectual capital and corporate strategy on firms' sustainable value creation. In S. Moffett & B. Galbraith (Eds.), *17th European Conference on Knowledge Management* (pp. 520–526). Belfast, Northern Ireland: ACPI.

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* (11th ed.). New York, NY: Pearson.

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice, 2*(4), 23–41. https://doi.org/10.1177/1524839915580941

Li, J., Chen, N. (2019). Extended file hierarchy access control scheme with attributed based encryption in cloud computing. *IEEE on Emerging Topics Computing*.

Lim, I. K., Park, Y. G., & Lee, J. K. (2016). Design of security training system for individual users. *Wireless Personal Communications, 90*, 1105–1120. https://doi.org/10.1007/s11277-016-3380-z

Long, H. (2014). An empirical review of research methodologies and methods in creativity studies (2003–2012). *Creativity Research Journal, 26*, 427–438. https://doi.org/10.1080/10400419.2014.961781

Lott, Y., & Abendroth, A. (2019). Reasons for not working from home in an ideal worker culture: *Why women perceive more cultural barriers*, *211*(1), 1–30. *WSI Working Paper*. https://hdl.handle.net/10419/209405

Lowe, A., Norris, A. C., Farris, A. J., & Babbage, D. R. (2018). Quantifying thematic saturation in qualitative data analysis. *Field Methods, 30*(3), 191–207. https://doi.org/10.1177/1525822X17749386

MacDougall, R. (2019). Sympathetic physics: The keely motor and the laws of thermodynamics in nineteenth-century culture. Technology and Culture, 60(2), 438-466. https://doi.org/10.1353/tech.2019.0031

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. https://doi.org/10.1037/qup0000089

Madni, S. H., Latiff, M. S., Coulibaly, Y., & Abdulhamid, S. M. (2016). Resource scheduling for infrastructure as a service (IaaS) in cloud security: Challenges and

133 opportunities. *Journal of Network and Computer Applications, 68*, 173–200. https://doi.org/10.1016/j.jnca.2016.04.016

Maher, C., Hadfield, M., Hutchings, M., & De Eyto, A. (2018). Ensuring rigor in qualitative data analysis: A design research approach to coding combining NVivo with traditional material methods. *International Journal of Qualitative Methods, 17*(1), 1-12. https://doi.org/10.1177/1609406918786362

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security, 27* (2), 233-272. https://doi.org/10.1108/ICS-03-2018-0031

Malik, P., & Pretorius, L. (2018). A case study validation of the application of a generalized equation of innovation in complex adaptive systems. *South African Journal of Industrial Engineering*, *20*, 1-20. https://doi:10.7166/29-1-1780

Mansfield-Devine, S. (2016). DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare. *Network Security, 2016*(11), 7–13. https://doi.org/10.1016/S1353-4858(16)30104-0

Marjanovic, O., & Cecez-Kecmanovic, D. (2017). Exploring the tension between transparency and datafication effects of open government IS through the lens of 132 complex adaptive systems. *Journal of Strategic Information Systems*, *26*, 210- 232. https://doi.org/10.1016/j.jsis.2017.07.001

Marques, C. S., Leal, C., Marques, C. P., & Cardoso, A. R. (2015). Strategic knowledge management, innovation and performance: A qualitative study of the footwear

industry. *Journal of the Knowledge Economy*, 1–17. https://doi.org/10.1007/s13132-015-0249-4

Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage.

Martsenyuk, V., Didmanidze, I., Andrushchak , I., Kradinova, T., & Rud, K. (2020). Information security: anti-virus protection technologies. *Computer-integrated technologies: education, science, production*, (38), 79-84. https://doi.org/10.36910/6775-2524-0560-2020-38-07

Mayer, P., Gerber, N., McDermott, R., Volkamer, M., & Vogt, J. (2017). Productivity vs security: mitigating conflicting goals in organizations. *Information and Computer Security, 5*(2), 137-151. https://doi.org/10.1108/ICS-03-2017-0014

Mayoh, J., & Onwuegbuzie, A. J. (2015). Toward a conceptualization of mixed methods phenomenological research. *Journal of Mixed Methods Research, 9*, 91–107. https://doi.org/10.1177/1558689813505358

McGarry, O. (2016). Knowing 'how to go on': Structuration theory as an analytical prism in studies of intercultural engagement. *Journal of Ethnic & Migration Studies*, *42*, 2067-2085. https://doi.org/10.1080/1369183X.2016.1148593

McMahon, R., Bressler, M. S., & Bressler, L. (2016). New global cybercrime calls for high-tech cyber-cops. *Journal of Legal, Ethical and Regulatory Issues, 19*, 26–37. https://www.abacademies.org

McTate, E. A., & Leffler, J. M. (2017). Diagnosing disruptive mood dysregulation disorder: Integrating semistructured and unstructured interviews. *Clinical Child*

Psychology & Psychiatry, 22, 187-203. https://doi.org/10.1177/1359104516658190

Meissner, P., & Wulf, T. (2017). The effect of cognitive diversity on the illusion of control bias in strategic decisions: An experimental investigation. *European Management Journal*, *35*(4), 430–439. https://doi.org/10.1016/j.emj.2016.12.004

Michael, T., & Tiko, I. (2015). Politicking information technology strategy in organizations: A case study of a selected organization in South Africa. *Journal of Governance and Regulation*, *4,* 107-114. https://doi.org/10.22495/jgr_v4_i3_c1_p2

Midgley, G., Nicholson, J. D., & Brennan, R. (2017). Dealing with challenges to methodological pluralism: The paradigm problem, psychological resistance, and cultural barriers. *Industrial Marketing Management*, *62*(1), 150–159. https://doi.org/10.1016/j.indmarman.2016.08.008

Mierzwa, S., & Scott, J. (2017). Cybersecurity in nonprofit and non-governmental organizations. *Institute for Critical Infrastructure Technology*. https://www.researchgate.net/publication/314096686_Cybersecurity_in_NonProfit_and_Non-Governmental_Organization

Mohammed, A., Sulaiman, M. N., & Muhammad N. M. (2013). Analysis of network security policy—Based management. *International Journal of Computer Science and Information Security, 11*(3), 143–146.

Mol, A. M., Silva, R. S., Rocha, Á. A., & Ishitani, L. (2017). Ethnography and Phenomenology applied to game research: a systematic literature review. *Revista De Sistemas E Computação (RSC), 7*(2), 110-127. https://revistas.unifacs.br

Molenberghs, G., Kenward, M. G., Aerts, M., Verbeke, G., Tsiatis, A. A., Davidian, M., & Rizopoulos, D. (2014). On random sample size, ignorability, ancillarity, completeness, separability, and degeneracy: Sequential trials, random sample sizes, and missing data. *Statistical Methods in Medical Research, 23*, 11–41. https://doi.org/10.1177/0962280212445801

Monahan, T., & Fisher, J. A. (2014). Strategies for obtaining access to secretive or guarded organizations. *Journal of Contemporary Ethnography, 44*, 709–736. https://doi.org/10.1177/0891241614549834

Morar, P., Read, J., Arora, S., Hart, A., Warusavitarne, J., Green, J., & Faiz, O. (2016). Defining the optimal design of the inflammatory bowel disease multidisciplinary team: Results from a multicentre qualitative expert-based study. *Frontline Gastroenterology, 6*(4), 290-297. https://doi.org/10.1136/flgastro-2014-100549

Morse, A. L., & McEvoy, C. D. (2014). Qualitative research in sport management: Case study as a methodological approach. *Qualitative Report, 19*(17), 1-13. https://nsuworks.nova.edu/tqr/

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

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection, and analysis. *European Journal of General Practice,*

24(1), 9–18. https://doi.org/10.1080/13814788.2017.1375091

Nakashima, E. (2015). *U.S. establishes sanctions program to combat cyberattacks, cyberspying.* https://www.washingtonpost.com/world /nationalsecurity/us-to-establish-sanctions-program-to-combat-cyberattackscyberspying/

Narayanan, S.N., Ganesan, A., Joshi, K., Oates, T., Joshi, A., & Finn, T. (2018). Early detection of cybersecurity threats using collaborative cognition. *2018 IEEE 4th International Conference on collaboration and Internet computing (CIC)*. 354-363. https://doi.org/10.1109/CIC.2018.00054

Nasution, M. F., Dhillon, G., & Akyuwen, R. (2017). Shaping of security policy in an Indonesian bank: Interpreting institutionalization and structuration. *Kinerja*, *19*(1), 1-13. https://doi.org/10.24002/kinerja.v19i1.530

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research*. https://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

National Cybersecurity Alliance. (2020). *3 reasons hackers love your small business infographic*. https://www.staysafeonline.org

National Institute of Standards and Technology. (2020). *Cybersecurity framework*. https://www.nist.gov

Njenga, K., & Jordaan, P. (2016). We want to do it our way: The neutralization approach to managing information systems security by small businesses. *African Journal of Information Systems, 8,* 42-63. https://digitalcommons.kennesaw.edu/ajis/

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing, 18*(2), 25-34. https://doi.org/10.1136/eb-2015-102054

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16,* 1-13. https://doi.org/10.1177/1609406917733847

Nsiah, I.O (2022). Structuration theory and its relevance in research: Power structures, constituency agency and organizational change in the new patriotic party. *Academic Letters*. https://doi.org/10.20935/AL4750

Okafor, R. (2021). *Cybersecurity due to diligence in mergers and acquisitions transactions.* University of Illinois College of Law.

Okoro, E. A., & Washington, M. C. (2012). Workforce diversity and organizational communication: Analysis of human capital performance and productivity. *Journal of Diversity Management (JDM)*, *7*(1), 57–62. https://doi.org/10.19030/jdm.v7i1.6936

Olokunde, T. Sanjay, M., & Adewumi, A. (2017). Quality model for evaluating platform as a service in cloud computing. *Information and Software Technologies, 756*.

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

Osarenkhoe, A., & Hyder, A. (2015). Marriage for better or for worse? Towards an analytical framework to manage post-merger integration process. *Business*

Process Management Journal, 21(4), 857-887. https://doi.org/10.1108/BPMJ-07-2014-0070

Osho, O., & Onoja, A. D. (2015). National cyber security policy and strategy of Nigeria: A qualitative analysis. *International Journal of Cyber Criminology*, 9(1), 120.

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

Oxford University Press. (2018). *Cybersecurity*. https://www.oxforddictionaries.com/definition/english/Cybersecurity

Pacho, T. O. (2015). Exploring participants' experiences using case study. *International Journal of Humanities and Social Science, 5*(4), 44–53. https://www.ijhssnet.com/

Papanikolaou, A., Vlachos, V., Venieris, A., Ilioudis, C., Papapanagiotou, K., & Stasinopoulos, A. (2013). A framework for teaching network security in academic environments. *Information Management & Computer Security, 21*, 315–338. https://doi.org/10.1108/IMCS-11-2011-0056

Park, S., Kim, Y., & Chang, H. (2016). An empirical study on security expert ecosystem in the future IoT service environment. *Computers & Electrical Engineering, 2016*(52), 199–207. https://doi.org/10.1016/j.compeleceng.2016.04.001

Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification? Journal of Marketing Thought, 3(1), 1–7. https://doi.org/10.15577/jmt.2016.03.01.1

Park, K., Woo, S., Moon, D., & Choi, H. (2018). Secure Cyber Deception Architecture and Decoy Injection to Mitigate the Insider Threat. *Symmetry*, *10*(1), 14. https://doi.org/10.3390/sym10010014

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organizations. *Information Management & Computer Security.*1-11. http://doi.org/10.1108/IMCS-10-2013-0078

Patino, C. M., & Ferreira, J. C. (2018). Internal and external validity: can you apply research study results to your patients? *Jornal Brasileiro De Pneumologia, 44*(3), 183. https://doi.org/10.1590/S1806-37562018000000164

Paulus, T., Woods, M., Atkins, D. P., & Macklin, R. (2017). The discourse of QDAS: Reporting practices of ATLAS and NVivo users with implications for best practices. International *Journal of Social Research Methodology, 20*, 35-47. http://doi.org/10.1080/13645579.2015.1102454

Peck, B., & Mummery, J. (2017). Hermeneutic constructivism: An ontology for qualitative research. *Qualitative Health Research, 28*(3), 389–407. https://doi.org/10.1177/1049732317706931

Philbin, G., & Philbin, T. R. (2013). Finding the new high ground in cyber war: Malware as an instrument of war. *Journal of Homeland Security & Emergency Management, 10*, 1–8. https://doi.org/10.1515/jhsem-2012-0041

Phillippi, J. G., & Lauderdale, J. (2017). A guide to field notes for qualitative research: Context and conversation. *Qualitative Health Research, 28*, 381– 388. https://doi.org/10.1177/1049732317697102

Piplai, A., Mittal, M., Abdel, S., Gupta, M., Joshi, A., & Finn, T. (2020). Knowledge enrichment by fusing representations for malware threat intelligence and behavior. *IEEE International Conference on Intelligence and Security Informatics*, 1-6. https://doi.org/10.119/IS149825.2020.928050

Ponelis, S. R. (2015). Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of information systems research in small and medium enterprises. *International Journal of Doctoral Studies*, *10*, 535–550.

Prakash, M., & Singaravel, G. (2015). An approach for prevention of privacy breach and information leakage in sensitive data mining. *Computers & Electrical Engineering, 45*, 134–140. https://doi.org/10.1016/j.compeleceng.2015.01.016

Prayudi, Y., & Yusirwan, S. (2015). The recognize of malware characteristics through static and dynamic analysis approach as an effort to prevent cybercrime activities. *Journal of Theoretical & Applied Information Technology, 77,* 438–445. https://www.jatit.org

Preece, J., Sharp, H., & Rogers, Y. (2015). *Interaction design: Beyond human-computer interaction* (4th ed.). West Sussex, UK: Wiley.

Preiser, R., Biggs, R., De Vos, A., & Folke, C. (2018). Social-ecological systems as complex adaptive systems: organizing principles for advancing research methods

and approaches. Ecology and Society, (4), 46. https://doi.org/10.5751/ES-10558-230446

Quintero-Bonilla, S. & del Rey, A.M. (2020). A new proposal on the advanced persistence threat: A survey. *Applied Sciences, 10*(11), 3874, 1-22. https://doi.org/10.3390/app10113874

Rahman, M. S. (2017). The advantages and disadvantages of using qualitative and quantitative approaches and methods in language testing and assessment research: A literature review. *Journal of Education and Learning, 6*, 102–112. https://doi.org/10.5539/jel.v6n1p102

Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of things. *Ad Hoc Networks, 11*, 2661–2674. https://doi.org/10.1016/j.adhoc.2013.04.014

Reddy, K. S., Agrawal, R., & Nangia, V. K. (2013). Re-engineering, crafting, and comparing business valuation models-the advisory exemplar. *International Journal of Commerce and Management, 23*, 216–241. https://doi.org/10.1108/IJCOMA-07-0018

Renz, S. M., Carrington, J. M., & Badger, T. A. (2018). Two strategies for qualitative content analysis: An intramethod approach to triangulation. *Qualitative Health Research*, *28*(5), 824-831. https://doi.org/10.1177/1049732317753586

Robinson, O. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Research in Psychology, 11*, 25–41. https://doi.org/10.1080/14780887.2013.801543

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*, 121–135. https://doi.org/10.1093/cybsec/tyw001

Rolbiecki, A., Subramanian, R., Crenshaw, B., Albright, D. L., Perreault, M., & Mehr, D. (2017). A qualitative exploration of resilience among patients living with chronic pain. *Traumatology, 23*(1), 89. https://doi.org/10.1037/trm0000095

Ross, M. W., Iguchi, M. Y., & Panicker, S. (2018). Ethical aspects of data sharing and research participant protections. *American Psychologist, 73*(2), 138-145. https://doi.org/10.1037/amp0000240

Roulston, K. (2018). Qualitative interviewing and epistemics. *Qualitative Research,18*(3), 322-341. https://doi.org/10.1177/1468794117721738

Salim, H.M. (2014). Cyber safety: A systems thinking and systems theory approach to managing cybersecurity risks. https://web.mit.edu/smadnick/www/wp/2014-07.pdf

Samtani, S., Chinn, R., Chen, H., & Nunamaker Jr., J. F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems, 34*, 1023–1053. https://doi.org/10.1080/07421222.2017.1394049

Samuel, A. P., & Odor, H. O. (2018). Managing diversity at work: Key to organizational survival. *European Journal of Business and Management*, *10*(16), 41–46. https://www.researchgate.net/publication/326082988_Managing_Diversity_at_Work_Key_to_Organisational_Survival

Santos, J., Palumbo, F., Molsen-David, E., Willke, R. J., Binder, L., Drummond, M. Thompson, D. (2017). ISPOR code of ethics 2017 (4th Ed.). Value in Health: *The Journal of the International Society for Pharmacoeconomics and Outcomes Research, 20*(10), 1227–1242. https://doi.org/10.1016/j.jval.2017.10.018

Sarre, R., Lau, L.Y., & Lennon, Y.C.C. (2018). Responding to cybercrime: Current trends. *Police Practice and Research: An International Journal*, 6, 515-518, https://doi.org/10.1080/15614263.2018.1507888

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Participant anonymity in the internet age: From theory to practice. *Qualitative Research in Psychology, 12*, 125–137. https://doi.org/10.1080/14780887.2014.94

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7th ed.). Harlow, England: Pearson.

Saunders, M.N.K. (2020). Common and key issues in mixed methods research. https://www.academia.edu/42139643/Common_and_Key_Issues_in_Mixed_Methods_Research

Schwartz, M. (2015). *Cyberattacks target energy firms*. https://www.govinfosecurity.com/cyberattacks-target-energy-firms-a-8068

Sergeeva, A., Huysman, M., Soekijad, M., & van den Hooff, B. (2017). Through the eyes of others: How onlookers shape the use of technology at work. *MIS Quarterly*, 41, 1153-1178. https://doi.org/10.25300/misq/2017/41.4.07

Shabani, M., & Borry, P. (2018). 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. https://doi.org/10.1038/s41431-017-0045-7

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

Shakerkhan, K.O. & Abilmazhinov, E. T. (2019). Development of a method for choosing cloud computing on the platform of PaaS for servicing the state agencies. *International Journal of Modern Education and Computer Science, 9*, 14-25, https://doi.org/10.5815/ijmecs.2019.09.02

Shen, S., Huang, L., Zhou, H., Yu, S., Fan, E., & Cao, Q. (2018). Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud based IoT networks. *IEEE Internet of Things Journal*.

Shields, J., Gibson, C., & Smith, D. Y. (2013). Building and sustaining effective individual computer security practices in the workplace and in personal computing. *International Journal of Academic Research, 5*(6), 284–291. http://doi.org/10.7813/2075-4124.2013/5-6/B.48

Siddiqui, M. N. (2014). Success of an organization is a result of employees' performance. *Advances in Social Sciences Research Journal*, *1*, 179–201, 217. http://doi.org/10.14738/assrj.14.280

Singer, P. W., & Friedman, A. (2013). *Cybersecurity and cyberwar: What everyone needs to know.* New York, NY: Oxford University Press.

Singhal, N., & Bhola, P. (2017). Ethical practices in community-based research in nonsuicidal self-injury: A systematic review. *Asian Journal of Psychiatry, 30*, 127-134. https://doi.org/10.1016/j.ajp.2017.08.015

Siponen, M., Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: *An exploratory field study. Information & Management, 51*, 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siwicki, B. (2017). Companies claim mobile decision support app makes EHRs faster. https://www.healthcareitnews.com/news/companies-claim-mobile-decision-support-app-makes-ehrs-faster

Sloan, A., & Bowe, B. (2015). Experiences of computer science curriculum design: A phenomenological study. *Interchange, 46*, 121. https://doi.org/10.1007/s10780-015-9231-0

Smith, M. (1989). The people risks. *The Computer Law and Security Report, 4*(6), 2-6. https://doi.org/10.1016/0267-3649(89)90002-2

Smith, W. (2001). Chaos theory and postmodern organization. *International Journal of Organizational Theory and Behavior*, *4*, 159–286. https://www.emeraldgrouppublishing.com/journal/ijotb

Sobers, R. (2021). *134 cybersecurity statistics and trends for 2021*. https://www.varonis.com/blog/cybersecurity-statistics/

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of*

Information Management, 36, 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Sotiriadou, P., Brouwers, J., & Le, T. A. (2014). Choosing a qualitative data analysis tool: A comparison of NVivo and leximancer. *Annals of Leisure Research, 17*, 218–234. https://doi.org/10.1080/11745398.2014.902292

Srinivasan, B. N., & Mukherjee, D. (2018). Agile teams as complex adaptive systems (CAS). *International Journal of Information Technology*, 10, 367-378. https://doi.org/10.1007/s41870-018-0122-3

Stahl, B.C, Doherty, N.F. & Shaw, M. (2012). Information security policies in the UK healthcare sector: A critical evaluation. *Information Systems Journal, 22*, 77-94. https://doi.org/10.1111/j.1365-2575.2011.00378.x

Stewart, A. (2014). Case study. In J. Mills & M. Birks (Eds.), *Qualitative methodology: A practical guide* (pp. 145–159). Thousand Oaks, CA: Sage.

Sullivan, T. J. (2004). The viability of using various system theories to describe organizational change. *Journal of Educational Administration, 42*, 43–54. https://www.emeraldgrouppublishing.com/journal/jea

Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management, 34*, 177–184. https://doi.org/10.1016/j.ijinfomgt.2013.12.011

Sunyaev, A. (2020). *Internet computing: Principles of distributed systems and emerging Internet-based technologies*. Switzerland, AG: Springer Nature https://doi.org/10.10071/978-3-030-34957-8_1

Susto, G. A., Schirru, A., Pampuri, S., & McLoone, S. (2016). Supervised aggregative feature extraction for big data time series regression. *IEEE Transactions on Industrial Informatics, 12*, 1243–1252. https://www.ieee-ies.org/pubs/transactions-on-industrial-informatics

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

Tabrizchi, H., & Rafsanjani, M.K. (2020). A survey on security challenges in cloud computing issues, threats, & solutions. *The Journal of Super Computing, 76*, 949-9532. https://www.springer.com/journal/11227

Journal of Education and Management Engineering, 8(2), 20. https://doi.org/10.5815/ijeme.2018.02.03

Tan, C. L., Chiew, K. L., & Wong, K. (2016). PhishWHO: Phishing webpage detection via identity keywords extraction and target domain name finder. *Decision Support Systems, 2016*(88), 18-27. http://doi.org/10.1016/j.dss.2016.05.005

Theofanidis, D. & Fountouki, A. (2019). Limitations and delimitations in the research process. *Perioperative Nursing (GORNA)*, *7*(3), 155–162. https://doi.org/10.5281/zenodo.2552022

Thornham, H., & Cruz, E. G. (2018). Not just a number? NEETs, data, and data logical systems. *Information, Communication & Society, 21*(2), 306-321. https://doi.org/10.1080/1369118X.2017.1279204

Tickle, M., Mann, R., & Adebanjo, D. (2016). Deploying business excellence: Success factors for high performance. *International Journal of Quality & Reliability Management, 33*, 197–230. https://doi.org/10.1108/IJQRM-10-2013-0160

Tissir, N., El Kafhali, S., & Aboutabit, N. Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal Reliable Intellect Environ*ment (2020). https://doi.org/10.1007/s40860-020-00115-0

Tomkinson, S. (2015). Doing fieldwork on state organizations in democratic settings: Ethical issues of research in refugee decision making. *Forum: Qualitative Social Research, 16*. https://www.qualitativeresearch.net/index.php/fqs

Topham, L., Kifayat, K., Younis, Y. A., Shi, Q., & Askwith, B. (2016). Cybersecurity teaching and learning laboratories: A survey. *Information & Security: An International Journal, 35*, 51–80. https://doi.org/10.11610/isij.3503

Tracy, S. J. (2019). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact*. 2nd ed. Tempe, AZ: Wiley

Trentmann, N. (July 3, 2021). Cash-laden companies are on a mergers and acquisitions spree. https://www.wsj.com/articles/cash-laden-companies-are-on-a-mergers-and-acquisitions-spree-11625320800

Triche, J.H. & Walden, E. (2018). The use of impression management strategies to manage stock market reactions to IT failures. *Journal of the Association for Information Systems, 19*(4).

Tshakert, K.F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon, 5* (6), https://doi.org/10.1016/j.heliyon.2019.e02010

Twining, P., Heller, R. S., Nussbaum, M., & Tsai, C. (2017). Some guidance on conducting and reporting qualitative studies. *Computers & Education,* 106, A1-A9. https://doi.org/10.1016/j.compedu.2016.12.002

Uprichard, E., & Dawney, L. (2019). Data diffraction: Challenging data integration in mixed methods research. *Journal of Mixed Methods Research*, *13*(1), 19-32. https://doi.org/10.1177/1558689816674650

U.S. Department of Homeland Security. (2014). *A glossary of common cybersecurity terminology.* https://niccs.us-cert.gov/glossary#letter_c

U.S. Securities and Exchange Commission [SEC]. (2017). *The need for greater focus on the cybersecurity challenges facing small and midsize businesses*. Washington, DC. https://www.sec.gov/news/statement/

Valizadeh, S., Dadkhah, B., Mohammadi, E., & Hassankhani, H. (2014). The perception of trauma patients from social support in adjustment to lower-limb amputation: A qualitative study. *Indian Journal of Palliative Care, 20*, 229–238. https://doi.org/10.4103/0973-1075.138401

Valli, C., Martinus, I., & Johnstone, M. (2014). Small to medium enterprise cybersecurity awareness: An initial survey of Western Australian business. *In Proceedings of the International Conference on Security and Management* (SAM). https://worldcomp-proceedings.com/proc/p2014/SAM9779.pdf

Van Brussel, S., Boelens, L., & Lauwers, D. (2016). Unraveling the Flemish mobility orgware: The transition towards a sustainable mobility from an actor-network perspective. *European Planning Studies*, *24*, 1336-1356. https://doi.org/10.1080/09654313.2016.1169248

Van den Berg, A., & Struwig, M. (2017). Guidelines for Researchers Using an Adapted Consensual Qualitative Research Approach in Management Research. *Electronic Journal of Business Research Methods, 15*(2).

Van Goethem T., Chen, P., Nikiforakis, N., Desmet, L, & Joosen, W. (2014). *Large-scale security analysis of the web: Challenges and findings*. In A. Acquisti, S. W. Smith, & A.-R. Sadeghi (Eds.), Trust and trustworthy computing (pp. 110–126). New York, NY: Springer.

Van Rijnsoever, F. J. (2017). (I Can't Get No) Saturation: A simulation and guidelines for sample sizes in qualitative research. *PLoS ONE, 12*(7), e0181689. https://doi.org/10.1371/journal.pone.0181689

Vardaman, J. M., Rogers, B. L., & Marler, L. E. (2020). Retaining nurses in a changing health care environment: The role of job embeddedness and self-efficacy. *Health Care Management Review*, *45*(1), 52–59. https://doi.org/10.1097/hmr.0000000000000202

Vasilaki, A. & O'Regan, N. (2008). Enhancing post-acquisition organizational performance: The role of the top management team. *Team Performance Management, 14*(3/4), 134-145. https://doi.org/10.1108/13527590810883415

Vermeulen, W. J. (2015). Self-governance for sustainable global supply chains: Can it deliver the impacts needed? *Business Strategy and the Environment, 24*, 73–85. https://doi.org/10.1002/bse.1804

Vigano, E., Loi, M., & Yaghmaei, E. (2020). Cybersecurity of critical infrastructure. *The International Library of Ethics, Law, & Technology*. https://doi.org/10.007/978-3-030-29053-5-8

Vincent, N.E. & Trussel, J. (2019). Predicting reported cybersecurity breaches using financial measures. *Journal of Forensic and Investigative Accounting, 11*(3), 494. https://www.nacva.com/jfia

Visser, M. M., Van Biljon, J. A., & Herselman, M. (2017). Evidence-based case selection: An innovative knowledge management method to cluster public technical and vocational education and training colleges in South Africa. *South African Journal of Information Management, 19*(1), 1-13. https://doi.org/10.4102/sajim.v19i1.751

Vogel, E. (2016). Ongoing endings: Migration, love, and ethnography. *Journal of Contemporary Ethnography, 45*, 673–691. https://doi.org/10.1177/0891241616654542

Volkova, V.N., & Cherny, Y.Y. (2018). Application of systems theory laws for investigating information security problem. *Automatic Control and Computer Sciences, 52*, 1164-1170.

von Solms, R., & van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

von Solms, B. & von Solms, R. (2018). Cybersecurity and information security: What goes where? *Information and Computer Security, 26* (1), 2-9. https://doi.org/10.1108/ICS-04.2017.0025

Wang, L., Islam, T., Long, T., Singhal, A., & Jajodia, S. (2008). An attack graph-based probabilistic security metric (pp. 283–296). In *Proceedings of the 22nd IFIP WG 11.3 Working Conference on Data and Applications Security, Lecture Notes in Computer Science* (vol. 5094). Berlin, Germany: Springer.

Wang, P. & Park, S (2017). Communication in cybersecurity: A public communication model for business data breach incident handling. *Issues in Information Systems 18*(2), 136-147. https://doi.org/10.48009/2-iis-2017-137-147

Watad, M., Washah, S., & Perez, C. (2018). IT security threats and challenges for small firms: Managers' perceptions. *International Journal of the Academic Business 124 World, 12*(1), 23–30. https://jwpress.com/Journals/IJABW/BackIssues/IJABW-Spring2018.pdf#page=29

Weber, R. M., & Horn, B. D. (2017). Breaking bad security vulnerabilities. *Journal of Financial Service Professionals, 71*, 50-54. https://www.financialpro.org/pubs/journal_index.cfm

Weis, D, & Willems, H. (2017). Aggregation, validation, and generalization of qualitative data - Methodological and practical research strategies illustrated by the research process of an empirically based typology. *Integrated Psychological Behavioral Science, 51*(2):223-243. https://doi.org/10.1007/s12124-016-9372-4

Welch, D., Grossaint, K., Reid, K., & Walker, C. (2014). Strengths-based leadership development: Insights from expert coaches. *Consulting Psychology Journal: Practice & Research, 66*, 20–37. https://doi.org/10.1037/cpb0000002

Werndl, C. (2009). What are the new implications of chaos for unpredictability? *British Journal for Philosophy of Science, 60*, 195–220. https://doi.org/10.1093/bjps/axn053

Westerman, M. A. (2014). Examining arguments against quantitative research: "Case studies" illustrating the challenge of finding a sound philosophical basis of a human sciences approach to psychology. *New Ideas in Psychology, 32*, 42–58. https://doi.org/10.1016/jnewideapsych.2013.08.002

Wheatley, M. J. (2014). *The order on the other side of chaos*. San Francisco, CA: Berrett-Koehler.

Wilkenson, N., & Klaes, M. (2017). *An introduction to behavioral economics* (3rd ed.). Palgrave, UK: Macmillan.

Williams, G. P. (2014). *Chaos theory tamed*. London, UK: CRC Press.

Wilson, A. (2014). Being a practitioner: An application of Heidegger's phenomenology. *Nurse Researcher, 21*(6), 28-33. https://doi.org/10.7748/nr.21.6.28.e1251

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

Wu, L., Du, X., & Wu, J. (2016). Effective defense schemes for phishing attacks on mobile computing platforms. *IEEE Transactions on Vehicular Technologies, 65*, 6678–6691. https://doi.org/10.1109/TVT.2015.2472993

Wulf, F., Westner, M., Lindner, T., & Strahringer, S. (2021). IaaS, PaaS, or SaaS? The why of cloud computing delivery model selection-vignettes on the post-adaption of cloud computing. *Proceedings of the 54th Hawaii International Conference on System Sciences,* 6285-6294. https://doi.org/10.24251/HICSS.2021.758

Yang, Y. H. (2015). The development of logistics services in the United States. *Journal of Operations and Supply Chain Management, 8*(2), 23–35. https://doi.org/10.12660/joscmv8n2p23-35

Yang, Y., Pankow, J., Swan, H., Willett, J., Shannon, G. M., Rudes, D. S., & Knight, K. (2018). Preparing for analysis: A practical guide for a critical step for procedural rigor in large-scale multisite qualitative research studies. *Quality and Quantity, 52*(2), 815-828. https://doi.org/10.1007/s11135-017-0490-y

Yang, Z., Sun, J., Zhang, Y., & Wang, Y. (2015). Understanding SaaS adoption from the perspective of organizational users: A tripod readiness model. *Computers in Human Behavior, 45*, 254–264. https://doi.org/10.1016/j.chb.2014.12.022

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *Qualitative Report, 20*, 134–152. https://nsuworks.nova.edu/tqr

Yetgin, E., Jensen, M., & Shaft, T. (2015). Complacency and intentionality in IT use and continuance. *AIS Transactions on Human-Computer Interaction, 7*, 17–42.

Yildiz, H.E., & Fey, C.F. (2010). Compatibility and unlearning in knowledge transfer in mergers and acquisitions. *Scandinavian Journal of Management, 26*,448-456. https://doi.org/10.1016/j.scaman.2010.09.010

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

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Thousand Oaks, CA: Sage.

Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM, 57*(2), 31-35. https://doi.org/10.1145/2556938

Young, D., Lopez, J., Jr., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection, 14*, 43–57. https://doi.org/10.1016/j.ijcip.2016.04.001

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. Information & Management, 56(4), 570–601. https://doi.org/10.1016/j.im.2018.10.001

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems, 16*, 448-484.

Zamawe, F. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal, 27*(1), 13–15. https://doi.org/10.4314/mmj.v27i1.4

Zhou, W. & Yu, B. (2018). A cloud-assisted malware detention and suppression framework for wireless multimedia system in IoT based on dynamic differential game. *China Communications. 15*(2), 209-223. https://doi.org/10.1109/CC.2018.8300282

Zota, R. D., & Petre, I. A. (2014). An overview of the most important reference architectures for cloud security. *Informatica Economica, 18*(4/2014), 26–39. https://doi.org/10.12948/issn14531305/18.4.2014.03

Appendix A: Interview Protocol

Interview Protocol	
What the researcher will do	What the researcher will say (script)
Introduce the interview and set the stage	Hello (Virtual/video interview) _____. Thank you for your participation in this case study. This interview will take about 45-60 minutes. Is that still good for you? As a reminder, I am Denise Durham a doctoral student at Walden University, and I will go ahead and provide you with a copy the consent form you previously signed. As the consent form indicates, the purpose in talking with you today is to learn from your thoughts, state of mind, and experience as an electric utility manager executing renewable energy strategies. I will ask you a series of questions on this topic, and I invite you to respond with as much detail and information as appropriate. Before we begin, do you have any questions or concerns related to the consent form you signed or to the interview process in general? Thank you. At this time, with your permission I would like to turn on the audio recorder to capture our conversation. I would like to introduce Participant X_, who is conducting a semi structured interview for this case study on the _____ day of _____ in the year 2022. The current time is _____.
Watch for non-verbal cues Paraphrase as needed Ask follow-up probing questions to get more in-depth	1. What strategies did you use to protect each company's data from cyberattack during a business merger? 2. How did you integrate strategies to safeguard the company's data from cyberattack into your organizational policies to improve compliance during a business merger? 3. How did you communicate the strategies you enacted during the merger to the companies involved in the merger?

	4. How did the strategies you put in place protect each company's data during the integration phase of the merger? 5. How did you determine the efficacy of the strategies you put in place to protect each company's data from a cyberattack? 6. What other factors were necessary to reduce the risk of cyberattack during a merger within your organization? 7. What additional information can you provide regarding strategies you used to manage the risk of data breach from a cyberattack during a merger?
Wrap up interview thanking participant	This concludes our interview. I would like to thank you for participating in this interview and, as a reminder, do not hesitate to reach out to me using the contact information in your consent form if you have follow-up questions or concerns.
Schedule follow-up member-checking interview	I will transcribe our interview and provide it for your review soon, so you can confirm that it accurately reflects our conversation today. After that, I will briefly summarize my interpretations for each question and would appreciate the opportunity to revisit with you for a short follow-up video interview. What day and time works best for you for this follow-up video interview?

Follow-up Member-Checking Interview Protocol	
What the researcher will do	What the researcher will say (script)
Introduce follow-up interview and set the stage	Thank you for the opportunity to revisit with you to follow up on our previous interview. As a reminder, after our previous conversation, I reviewed the transcripts and briefly summarized my interpretations for each interview question. The purpose of this follow-up interview is to give you an opportunity to review my interpretations to determine if any information needs to be corrected, and to share any additional information or insights.
Share a copy of the succinct synthesis for each individual question Bring in probing questions related to other information the researcher may have found – note the information must be related so that the researcher is probing and adhering to the IRB approval. Walk through each question, read the interpretation, and ask: Did I miss anything? What would you like to add?	At this time, I will provide you with my interpretations for each individual question, and you will have an opportunity to review them and provide feedback one at a time. 1. Question #1 and succinct synthesis of the interpretation 2. Question #2 and succinct synthesis of the interpretation 3. Question #3 and succinct synthesis of the interpretation 4. Question #4 and succinct synthesis of the interpretation 5. Question #5 and succinct synthesis of the interpretation 6. Question #6 and succinct synthesis of the interpretation 7. Question #7 and succinct synthesis of the interpretation
Wrap up follow-up interview by thanking participant	This concludes our follow-up interview. I would like to thank you, again, for participating in this process. I will send

	you a summary of the findings electronically of the study if you are interested. Thank you for your time

Appendix B: Interview Questions

1. What strategies did you use to protect each company's data from cyberattack during a business merger?

2. How did you integrate strategies to safeguard the company's data from cyberattack into your organizational policies to improve compliance during a business merger?

3. How did you communicate the strategies you enacted during the merger to the companies involved in the merger?

4. How did the strategies you put in place protect each company's data during the integration phase of the merger?

5. How did you determine the efficacy of the strategies you put in place to protect each company's data from a cyberattack?

6. What other factors were necessary to reduce the risk of cyberattack during a merger within your organization?

7. What additional information can you provide regarding strategies you used to manage the risk of data breach from a cyberattack during a merger?

Appendix C: Participant Recruitment Letter

Dear Participant,

My name is Denise Durham; I'm a doctoral candidate at Walden University. I am conducting a doctoral study to address leadership strategies to reduce cyberattacks during a merger or business acquisition and I am soliciting your participation in this research study. You have been approached for this study because you have the required skills, knowledge, and experience in cybersecurity and your participation will be very useful in the finding of strategies that will contribute to the prevention of cybercrimes. Please feel free to reach out to me by email at denise.durham2@waldenu.edu or via my mobile phone at 623- XXX-XXXX if you need additional information in that regard. Your participation is a voluntary act for your participation in this study. Besides, you are free to accept the invitation or withdraw at any time without any penalty. I would appreciate any positive feedback in terms of your participation and thanks to you in advance for your time and consideration.

Best regards,

Denise Durham

Appendix D: Letter of Cooperation

Dear Sir/Madam,

My name is Denise Durham. I am a Doctor of Business Administration (DBA) student at Walden University, conducting a research study entitled "Leadership Strategies to Reduce Cyberattacks During a Merger". The purpose of this qualitative single case study is to investigate strategies that business leaders of the wine industry use to combat cyberattacks during a merger or business acquisition. I identified my current employer as a leading body representing the wine sector in the United States and California. I am seeking your assistance to recruit participants who meet all the following eligibility criteria to conduct 30-60 minutes interviews:

- living and working in the state of California
- have experience in a wine industry management position overseeing strategic plans for a merger or business acquisition

In addition to the interviews, I am requesting permission to review organization documents, such as strategic plans. Confidentiality is of utmost importance to me. I will not disclose any company, leader, or participant in the published study or any subsequent publications using information from this study. The company and participants will be coded to protect their identity. Participation in this research study is voluntary. You may choose not to allow recruiting of participants to take place within your company or provide access to relevant company documents at any time. Your company and its eligible participants may withdraw from the study at any time without any explanation or reason. Any data collected from the withdrawn participant will not be used in the study.

I am kindly requesting you to provide access to a list of participants who meet the eligibility criteria by providing their full name and contact information (i.e., email or telephone number). You will not be asked or be required to provide any supervision during the interviews. Eligible participants will be emailed an invitation to participate in the study along with an informed consent form to review prior to the scheduling of the interview. Providing informed consent will occur by replying to the email invitation with the words, I consent, or by signing the informed consent form prior to the start of the interview.

Because you are the official authority representing your company to grant permission and access to release company documents, I am requesting a release of documents subject to the following conditions:

1. I will use all company documents released to me exclusively for my research and I will not disclose or discuss any of the information with anyone, including friends or family. All documents will be kept confidential.

2. I will not copy, release, sell, loan, alter, or destroy any confidential information released to me, except as authorized by you as the official company representative.

3. I will not discuss confidential information released to me in any environment where other people may overhear the conversation.

4. I understand that it is not acceptable to discuss confidential information even if the company or participant's name is not used.

5. I will not make any unauthorized transmission, inquiries, modifications, or purging of confidential information.

6. I agree that my obligations under this agreement will continue in perpetuity after the completion of this study.

7. I understand that any violation of this agreement may have legal implications.

8. I will only access documents I am officially authorized to access, and I will not disclose any trade secrets, proprietary information, or any other protected intellectual property to any unauthorized individuals or entities. If the terms and conditions within this letter of cooperation and confidentiality agreement are acceptable, please print and sign your name, provide your title, and the date your signature below.

Printed name: _____

Signature: _____

Title: _____

Date: _____