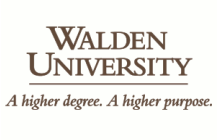



2018

# Managerial Strategies Small Businesses Use to Prevent Cybercrime

Doreen Lynn Maahs
*Walden University*

# Walden University

College of Management and Technology

This is to certify that the doctoral study by

Doreen Maahs

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. Patsy Kasen, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Janet Booker, Committee Member, Doctor of Business Administration Faculty

Dr. Neil Mathur, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Managerial Strategies Small Businesses Use to Prevent Cybercrime

by

Doreen Lynn Maahs

MS, Kaplan University, 2014

BS, Lakeland College, 1997

BS, Lakeland College, 1989

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

August 2018

Abstract

Estimated worldwide losses due to cybercrime are approximately $375-575 billion annually, affecting governments, business organizations, economies, and society. With globalization on the rise, even small businesses conduct transactions worldwide through the use of information technology (IT), leaving these small businesses vulnerable to the intrusion of their networks. The purpose of this multiple case study was to explore the managerial strategies of small manufacturing business owners to protect their financial assets, data, and intellectual property from cybercrime. The conceptual framework was systems thinking and action theory. Participants included 4 small manufacturing business owners in the midwestern region of the United States. Data were collected via face-to-face interviews with owners, company documentation, and observations. Member checking was used to help ensure data reliability and validity. Four themes emerged from the data analysis: organizational policies, IT structure, managerial strategies, and assessment and action. Through effective IT security and protocols, proactive managerial strategies, and continuous evaluation of the organization's system, the small business owner can sustain the business and protect it against potential cyberattacks on the organization's network. The findings of the study have implications for positive social change by informing managers regarding (a) the elimination or reduction of cybercrimes, (b) the protection of customers' information, and (c) the prevention of future breaches by implementing effective managerial strategies to protect individuals in society.

# Managerial Strategies Small Businesses Use to Prevent Cybercrime

by

Doreen Lynn Maahs

MS, Kaplan University, 2014

BS, Lakeland College, 1997

BS, Lakeland College, 1989

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

August 2018

# Dedication

To my husband, Carl, you have supported me through this long journey to reach my goal of completion of my doctoral degree. You have endured my stress through the endless process, providing me with the encouragement and support I needed to make it possible to complete my study. Your endless love made it possible for me to reach my goal to finish my doctoral study, and once again obtain the degree needed to become a professor to fulfill my aspirations of allowing me to share the knowledge I have gained through this experience.

# Acknowledgments

I am thankful for the support and encouragement of family members and friends who believed in me. I especially would like to acknowledge my cousin, Debbie, who supported me through this challenging journey and unfortunately passed away from cancer recently. May God bless her and keep her. I know she is the angel that has shined upon me as I completed this doctoral study.

Dr. Patsy Kasen, my Walden University chair, continued to support me and her dedication to my success through this journey made it possible for my accomplishment. I sincerely, thank her and will never forget the positive relationship and the kindred spirit between us. She provided me with the encouragement, drive, and fortitude I needed to complete my doctoral study. I can never thank her enough and hope to remain steadfast friends and colleagues.

Dr. Cheryl McMahan, my Walden University second committee member, provided me with corrective and valuable feedback to succeed in this doctoral journey. I value every review to help me to reach my goal and wish her the best. Dr. Janet Booker, my Walden University second committee member who replaces Dr. McMahan after she retired. I value your reviews at the end of my journey. Dr. Neil Mathur, my Walden University Research Reviewer, enabled me to transform my doctoral study into a substantial piece of work. Through his commitment to thoroughly reviewing my study, he assisted in transforming my doctoral study into a polished piece of work.

Table of Contents

List of Tables

List of Figures

# Section 1: Foundation of the Study

Many businesses that experience cyberattacks also experience the loss of financial assets, tarnished reputations, and reduction of revenue as a result (Romanosky, 2016). Managers must budget resources to implement strategies in an effort to prevent breaches and strengthen the protection of the business's network (Srinidhi, Yan, & Tayi, 2015). All organizations, worldwide, currently experience 122 or more cyberattacks per week (Aiken, Mc Mahon, Haughton, O'Neill, & O'Carroll, 2016). Protection of the financial data, assets, intellectual property, and personnel information remains critical for all organizations, given that no one is immune to cybercrime (Aiken et al., 2016). Resources for protection include the time and cost allocated for employee training programs.

## Background of the Problem

Trust is necessary for any business to thrive, especially in online shopping environments. The customer may experience a lack of customer service and face-to-face contact with a company's sales representatives (Banal & Zahedi, 2015). A breach of customers' confidential information could lead to the distrust of the company and its security measures of their online site (Banal & Zahedi, 2015). Estimating significant losses is difficult because many organizations do not report incidents of a breach (Herley, 2014). Many facets of cybercrime need examination including corporate espionage, compromised data, unquantified losses, and damage to the brand's reputation (Herley, 2014).

Many companies experience loss of reputation due to data breaches (Aiken et al., 2016). Managers often overlook the vulnerabilities of their network, which may result in

cybercriminals targeting the organization for theft of vital information (Aiken et al., 2016; Arora, 2016). Small businesses require budgeting resources for cybersecurity for the protection of their assets and data (Aiken et al., 2016). However, small business owners assume the scale of cyberattacks is substantially less for small businesses compared to larger businesses (Arora, 2016). However, evidence indicates that small businesses experience *more* online threats than larger businesses primarily due to the lack of investment in cybersecurity protection plans (Aiken et al., 2016). The theft of vital data could affect the survival of small businesses (Aiken et al., 2016).

Researchers have found that businesses rely on not only the protection of their network, but also the protection of its business partners, vendors, and customers (Srinidhi et al., 2015). The hacker who breaches an organization's network can steal sensitive information about the organization's partners, and potentially penetrate their partners' network (Srinidhi et al., 2015). Businesses require investment in Information Technology strategies for prevention and strategic risk management to combat intrusions and to strengthen their network (Srinidhi et al., 2015). Increased cybersecurity strategies are necessary to protect an organization's financial assets, data, and intellectual property (Arora, 2016). The organization's priority to its customers is to safeguard against unauthorized access through the implementation of adequate security measures against potential breaches (Arora, 2016). In many instances, small business owners do not realize they have experienced a breach nor the extent of their losses (Arora, 2016).

## Problem Statement

Estimated worldwide losses due to cybercrime is approximately $375-575 billion annually, affecting governments, business organizations, and the public (Waldrop, 2016). Roughly 86% of the most common cybercrime cases reported affect small-to-medium-sized enterprises (DiMase, Collier, Heffner, & Linkov, 2015). The general business problem is that the lack of cybercrime prevention in small manufacturing businesses leads to the loss of financial assets and data. The specific business problem is that some small manufacturing business owners lack managerial strategies for the protection of financial assets, data, and intellectual property against cybercrime.

## Purpose Statement

The purpose of this qualitative multiple case study was to explore the managerial strategies of small manufacturing business' owners to protect their financial assets, data, and intellectual property against cybercrime. I explored the managerial strategies implemented by four small manufacturing business owners who successfully prevented cybercrimes in the midwestern region of the United States. Cybercrime affects the businesses sector, society, and global economies. The implications of the study for social change include (a) the elimination of cybercrimes, including the theft of confidential data and assets; (b) the protection of customers' information in the business' networks; and (c) the prevention of breaches by implementing effective managerial strategies to protect individuals in society. Other businesses may use the information to improve their strategies.

## Nature of the Study

I used a qualitative methodology for this study. Qualitative researchers explore a social phenomenon, focusing on the details of the situation, subjective meanings, and motivating actions (McCusker & Gunaydin, 2015). They use a larger sample of surveys or other instruments to collect and then analyze the data (Yin, 2017). As a qualitative researcher, I explored managerial strategies for the protection of organizations' data, assets, and intellectual property.

The quantitative researcher, on the other hand, uses logic models, numeric outcomes, and statistical analysis to examine relationships and differences among variables (McCusker & Gunaydin, 2015). The quantitative researcher often analyzes data sets collected by other researchers or organizations (Yin, 2017). Whereby, the qualitative researcher may choose to explore a contemporary event, as opposed to a historical one through exploration of the practices or behaviors of the participants (McCusker & Gunaydin, 2015). Therefore, a quantitative study may not provide an understanding of the experiences and attitudes of an existing problem of a specific phenomenon (Yin, 2017).

In this qualitative multiple case study, I explored business owners who have successfully prevented cybercrime and using a smaller sample size. In a quantitative study, the analysis requires a larger sample size. If I had conducted a mixed method study, qualitative data would have been needed to achieve a profound exploration of the business owners' experiences along with gathering quantifiable data, which is essential in statistical analysis.

The case study design was the appropriate form of this qualitative study due to the exploration of several aspects of small business owners and the strategies each owner employs to prevent vulnerabilities to cybercrime. I explored a real-life situation (i.e., an event) to collect data from small business organizations, along with the published literature, to provide effective managerial strategies for eliminating the threat of cybercrime.

Although qualitative researchers use other designs, such as biographical, ethnography, and phenomenology approaches. They were not appropriate for the study. The qualitative biographical researcher explores a single participant by focusing on the individual's opinion and experience (Yin, 2017).

A qualitative ethnography researcher explores the point of view and interpretation of a cultural or social group, for example, behavior, customs, and way of life (Yin, 2017). Ethnographers explore ethnicity and geographic location but can focus on the culture of a business or a business organization (i.e., Rotary Club), focusing on field research, for example, participation observations (Yin, 2017). A phenomenological researcher attempts to explore the meanings of a lived experience of several individuals with the same phenomenon and their interpretations of the world, for example, surviving cancer patients (Yin, 2017).

The rationale for using a single case study was to explore a significant theory, unusual case, a common case, revelatory case, longitudinal case, or a person or single group (Yin, 2017). I chose to do a multicase study (a) to analyze the data within each situation and across different circumstances; (b) to explore an in-depth understanding of

an entity at a particular time; and (c) to explore different small businesses owners' managerial strategies for cybercrime prevention.

## Research Question

What managerial strategies do small manufacturing business owners implement to combat cybercrimes for the protection of financial assets, data, and intellectual property?

## Interview Questions

1. What are your major concerns regarding managerial strategies to protect your systems from data breaches?
2. What are the managerial strategies you use to protect your financial assets, data, and intellectual property of possible cybertheft or breaches?
3. What internal and external managerial strategies has your organization developed and implemented to prevent theft or loss of financial assets, data, and intellectual property from cybercrime?
4. How are managerial strategies to protect your systems from data breaches engaged by employees?
5. What managerial strategies does your organization use to measure the effectiveness of the cybercrime prevention?
6. What additional information can you provide pertaining to managerial strategies to prevent breaches and cybercrime?

## Theoretical or Conceptual Framework

The concepts of general systems theory originated with the theoretical biologist, Ludwig von Bertalanffy, publishing An Outline of General System Theory in 1950 (Von

Bertalanffy, 2008). Von Bertalanffy (2008) introduced the systems theory framework illustrating the system and other systems. The system approach coordinates a mutual synergistic relationship and how it interacts with other systems through growth and change (Von Bertalanffy, 2008). Von Bertalanffy (2008) concluded that the primary objective of the biological sciences was the discovery of organizational properties applied to organisms at various levels of analysis.

Von Bertalanffy, influenced Emile Durkheim and Max Weber, both early pioneers in the field of sociology in the late 1800s and early 1900s. They applied the principles of biological organisms to human social systems (Drissel, 2012). Responding to widespread socioeconomic changes (e.g., industrialization, urbanization, capitalization, and bureaucratization), Durkheim and Weber became interested in how societies organize and maintain cohesion or group identity over time, sharing the same morals and values (Drissel, 2012).

Checkland (2012) introduced the idea of systems thinking and action theory, arguing for the existence of emergent properties, which justifies a system comprised of subsystems that support the mission of the more extensive system. Systems thinking and action theory promote a new way of exploring the world in which individual phenomena affects the whole system (Checkland, 2012). The theory ensures a view of the interrelated subsystems rather than its isolated parts (Adams, Hester, Bradley, Meyers, & Keating, 2014). The complexity of the subject of interest is explored through their relationships among the systems and subsystems (Adams et al., 2014). To adapt to change, both the system and its operational environment demand control processes that

are capable of affecting changes to the system's relationship to its environment and society (Checkland, 2012). The theory invokes improvement of explanatory power and interpretation with significant implications for systems practitioners (Adams et al., 2014). Therefore, the theory is relevant for applications for a variety of disciplines (Adams et al., 2014). For example, the system of a business organization includes many subsystems. One subsystem of a business includes cybersecurity to protect the organization's network. If a breach of the system occurs, it could affect the survival of the organization. Systems thinking and action theory correlates to the study due to the connections among business, society, economic resources, and control processes within the system's environment.

## Operational Definitions

*Biometric methodologies*: Biometric methodologies defined as a technology using physical attributes of individuals to reinforce security, providing strict identity control (Choi et al., 2014).

*Cyberpower*: Cyberpower defined as the potential to use cyberspace to achieve desired outcomes of intrusion into individuals' computers or servers for obtaining information, data, or intellectual property (Parker, 2014).

*Cybersecurity*: Cybersecurity defined as the specifications of security requirements to prevent unauthorized intrusions access to an individuals' computer or server (Jang-Jaccard & Nepal, 2014).

*Cyberspace*: Cyberspace defined as the domain that exists for inputting, storing, transmitting, and extracting information, utilizing the electromagnetic spectrum, including all hardware, software, and transmission media (Parker, 2014).

*Encryption*: Encryption defined as a science or cryptographic procedure to convert plaintext into ciphertext to prevent unauthorized recipients from reading the data (Henson & Taylor, 2014).

*Malware*: Malware defined as unauthorized software on an individuals' computer or server to capture keyboard, mouse, or screen output to steal login credentials (Herath et al., 2014).

*Phishing*: Phishing defined as a type of social engineering, tricking individuals to enter their credentials through a fraudulent website (Herath et al., 2014).

*Vulnerability*: Vulnerability defined as a weakness in the system's design, implementation, or operation and management violating the system's security policy (Jang-Jaccard & Nepal, 2014).

## Assumptions, Limitations, and Delimitations

### Assumptions

Assumptions of a study depend on gathering data to illustrate facts to prove and verify the information presented in the study (Brinkmann, 2016). Assumptions can consist of statements alleged to be true, but frequently only temporary in nature (Brinkman, 2016). This qualitative case study made two assumptions. First, the existence of cybercrimes is prevalent and consists of many facets of information stolen by cybercriminals. Second, the vulnerabilities of business organizations exist due to inadequate protection and managerial strategies for prevention of cyberattacks. The number of cyberattacks presented establishes patterns in managerial strategies of business leaders about the preventative measures of cybercrimes to protect financial data, assets,

and intellectual property. In a qualitative study approach, some assumption may include analysis of documentation (i.e., surveys, interviews, and literature). The importance of reflection of the findings could lead to the practical implementation of strategies to eliminate vulnerabilities for business organizations.

**Limitations**

Limitations of a study depend on matters and occurrences out of control of the researcher and sometimes may affect the results or conclusions of the study (Taguchi, 2018). The limitations of a qualitative case study reflect the method and analysis of the data (Taguchi, 2018). To promote validity and reliability, the researcher must understand the shortcomings, conditions, and influences the researcher cannot control (Taguchi, 2018). Many organizations do not share their confidential information of cybercrime losses for various reasons, primarily due to shareholders' interests. Full disclosure of the information provided by the participant's responses of the interviews questions must undergo a thorough examination to remove inference and bias. The likelihood of bias could present itself due to data from small manufacturing companies with fewer employees, rather than a selection of participants from small, medium, and a high number of employees. Due to the definition of a small manufacturing company by the Small Business Association (i.e., 1-500 employees), examining a sample size with only a few employees would not provide an accurate representation of the data collected. A final limitation is small business owners might not have the extensive knowledge and expertise to make informed responses to breaches and cybersecurity practices.

### Delimitations

Delimitations include characteristics arising from limitations in the scope of the study imposed by the researcher (i.e., defining boundaries), including exclusionary and inclusionary decisions created in the development stage of the study (Taguchi, 2018). In a qualitative study, the delimitations focus on the recognition of exclusions to the study (Robinson, 2014). Delimitations of a qualitative case study include (a) sensitivity of the information, (b) interviewing setting, (c) sample size, and (d) geographic location. The main delimitation of the study could affect data collection involving small business owners rather than the IT specialist. Second, in conducting an interview, body language illustrates the nondisclosure of information in the interviewee (Yin, 2017). Third, delimitation may include the constraints of the sample size of only six small manufacturing business owners. Finally, the midwestern region of the United States was chosen for convenience and size of the population.

## Significance of the Study

### Contribution to Business Practice

The findings of the study may contribute to managerial strategies used by small business organizations to combat cybercrime. Using strategic measures and the collaboration of senior management, the goal of preventative strategies is to ensure the protection of the organization's assets and data from hackers (Arora, 2016). Concurrent with the globalization of business, organizations conduct business transactions worldwide through the use of information technology (IT), which can leave them vulnerable to unauthorized access to their networks (Herley, 2014). Through the exploration of risk

factors, small business owners can implement new strategies and processes to reduce their vulnerabilities (Arora, 2016). For example, the organization could develop and deploy strategies and processes to protect the financial assets, data, and intellectual property (Aiken et al., 2016). The findings of this study could offer small business owners proactive protection against cyberattacks on the organization and thus prevent or reduce the resultant recovery costs.

**Implications for Social Change**

Cybercrime affects businesses, individuals, and society. Cybercriminals create sites to buy and sell stolen data, contribute access to infected computers, and writing tools (i.e., coding programs) for the theft of data, distributing cash flow for the criminals (Holt, Smirnova, & Chua, 2016). These activities cost organizations and society billions of dollars annually due to the vulnerability of networks, lack of strategies, operational measures for prevention, and efficiently tackling cyberattacks (Asghari, van Eeten, & Bauer, 2015). Symantec Norton investigators reported an annual loss of $110 billion by cybercriminals (Asghari et al., 2015). With the current era of online processing, society relies increasingly on information technology, which gives the cybercriminals with an expanding platform to launch potential cyberattacks (Hutchings & Holt, 2017).

The social impact of cybercrimes could cause economic disruptions, consumer trust, disruption of productivity, and attainable infiltration of National Security and the country's infrastructure (Quigley, Burns, & Stallard, 2015). The increase in online shopping, banking, and social media with the use of IT, mandates a secure internet environment to protect viable information from exposure to cybercrimes. The findings,

conclusions, and recommendations from the study could contribute strategic measures against cyberattacks (i.e., acquiring assets, personnel or classified material, and economic information), creating a secure and safer online environment for society.

## A Review of the Professional and Academic Literature

Cybercrime continues to grow as technology affects businesses, the economy, and society (Alkhateeb, 2016). Business leaders rely on computer technology, e-commerce, and smart devices for sending and receiving business information and carrying out transactions (Manworren, Letwat, & Daily, 2016). With the increase of globalization and the use of (IT), businesses implement protective measures and strategies to combat cybercriminal attacks and thus protect their assets, intellectual property, as well as customers' personnel information (Manworren et al., 2016). Cybercriminals commit acts of a violation through the employment of a computer (Quigley et al., 2015). The sole purpose is to illegally gain entrance into a computer or database to manipulate and steal data by corrupting an individuals' equipment (Quigley et al., 2015). For small manufacturing businesses, the importance of security strategies is crucial due to the ability of the Black Hat Community, malware developers, and new techniques developed by hackers to steal and sell information (Alkhateeb, 2016).

The critical analysis of the literature provided an extension of the qualitative study to enable me to identify the concepts of cybercrime and possible managerial strategies small manufacturing business owners can implement to protect themselves from data breaches. By investigating the concepts of cybercrimes, types of cybercrime and business strategies, and applications applied to the business problem, the study may

provide small manufacturing business owners with practical measures to combat cybercrime. The goal of the multicase qualitative study was to study four business owners in the midwestern region of the United States. According to the Small Business Association, small manufacturing companies consist of 1-500 employees (SBA, 2017). The recruitment of four business owners with 66-180 employees provided a compelling overview and understanding of the managerial strategies that organizations use to prevent cyberattacks of the organizations. The purpose of this qualitative multicase study was to explore the managerial strategies of small manufacturing business' owners to shore up their vulnerabilities and protection of their financial assets, data, and intellectual property.

**Search Strategy**

For the literature review, I used the following databases: Google Scholar, Galilei Scholar, Ulrich, SAGE Premier, Science Direct, ABI /Inform Complete, and government websites. The following keywords were used: cyberattacks, cybercriminals, cybercrimes, cybersecurity, information security, management strategies, organizational culture and structure, prevention strategies, small businesses, internal and external strategies, general systems theory, and systems thinking theory and action theory.

The total number of references for this study included two books and 167 peer-reviewed journal articles. Of the 169 total study references, 155 (91%) met the requirements of publication within five years of the study's estimated approval date by the Chief Academic Officer. Of the 80 literature review references, 74 (92%) were peer-reviewed and published within five years of the study's estimated approval date by the by the Chief Academic Officer.

I developed a conceptual research model for the literature review (Figure 1), illustrating the various concepts that small manufacturing owners' encounter daily to combat cybercrime. The small manufacturing owners must secure their networks from unauthorized intrusions and implement effective managerial strategies.

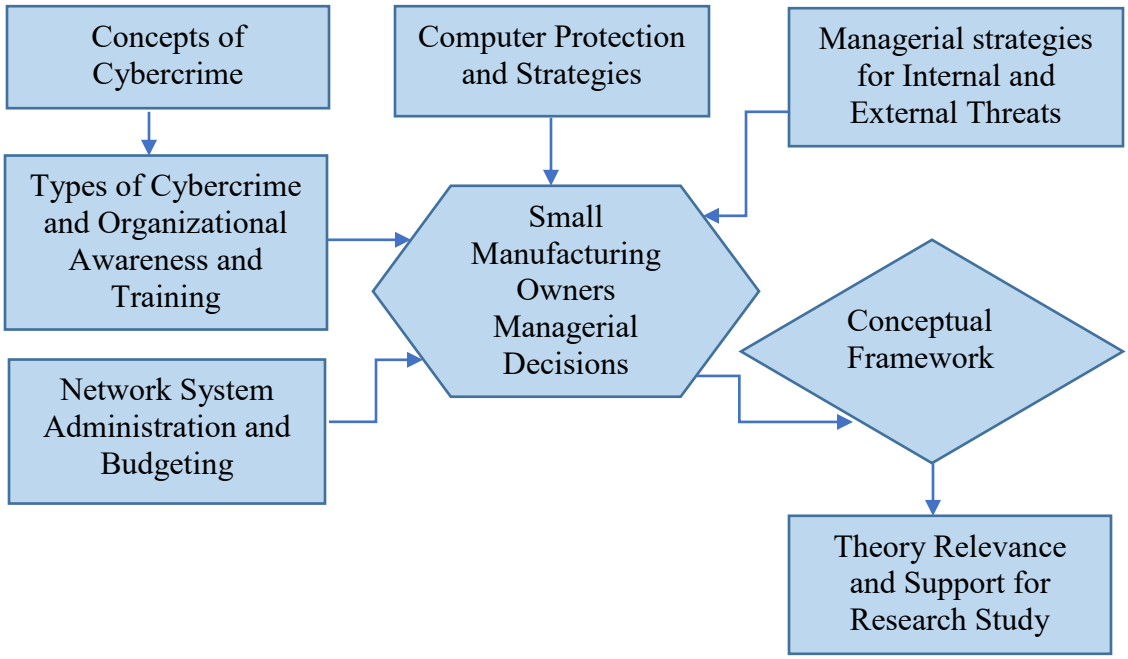


*Figure 1*. Conceptual research model of the literature review

The breach of a business's network could potentially lead to the intrusion of customers, vendors, and other partner's organization's vital information (Asghari et al., 2015). The chain reaction costs organizations and society billions of dollars annually due to the vulnerability of networks and lack of strategic measure towards prevention of cyberattacks (Asghari et al., 2015). The confidentiality of financial data and personnel information also influences the concern of customers, questioning the organization's standards of ethics, practices, and protection of their confidential information (Hutchings & Holt, 2017). Cybercriminals create sites to buy and sell stolen data and code to access

infected computers (Hutchings & Holt, 2017). The cybercriminal uses writing tools to infiltrate the computer network to steal data, using the information to sell or furnish the criminal with lucrative cash flow (Hutchings & Holt, 2017). In 2012, Norton Symantec antivirus program reported monetary losses of more than $110 billion through theft by cybercriminals (Asghari et al., 2015). The cybercriminal uses the internet for criminal intent. Through strict confidential tactics, the black-hat community reduces the risk of exposure of their identification (Alazab, 2015). Hackers steal and sell information to other hackers through anonymity techniques (Alazab, 2015). Cybercrimes include two forms of risk in cyberspace: (a) risk to hosting illegal websites on pirate servers; and (b) risk to information related to counterfeit products (Samtani, Chinn, Chen, & Nunamaker, 2017).

Small business owners should consider implementing strategic measures to fight cybercrime due to the increasing presence of individuals using cyberspace and the increase in the number of attacks and victimization (Shamsi, Zeadally, & Nasir, 2016). The first group, cybertrespass, includes acts involving the crossing of established boundaries into cyberspace, such as cybervandalism, spying, and terrorism (Shamsi et al., 2016). The second group, cybertheft, refers to a range of different types of appropriation taking place within cyberspace, such as theft of cyber credit, cybercash, and cyberpiracy (Shamsi et al., 2016).

Dupont (2017) noted cybercriminals participate in the criminal activity for financial gain, recognition, power, loyalty to others in the cybercrime organization, and their political beliefs. The consumer suffers the most extensive damage (i.e., identity

theft) due to financial loss and credit card companies that do not cover the losses (Hovav, 2014). The understanding of the phenomenon and continuous efforts on long-term strategies for prevention, detections, and attempted fraud, demands efforts for deterrence of cyberattacks (Holt et al., 2016). The world spends an enormous amount of money to prevent cybercrime, and companies continue to invest in computer programming to create credible firewalls to prevent access to their networks (Herley, 2014). Small businesses require continuous efforts to enlist managerial strategies to protect their financial assets and data, intellectual property, as well as customer information from the possibilities of cyberattacks.

**Types of Cybercrime and Business Strategies**

The implications of computer technology and cyberattacks enable an array of methods employed by the cybercriminals to obtain critical information from a business by infiltrating the firewall of their system. Customers' personnel data, financial data, and intellectual property can cause a company to fail (Cavusoglu, Cavusoglu, Son, & Benbasat, 2015). Businesses around the globe use technology to process, store, and transfer information when buying products or services, involving financial transactions in a matter of seconds (Lee & Lee, 2015). The biggest concern for companies is the capability to protect their data and financial assets from potential security risks, including the use of mobile devices (Romanosky, 2016). In 2013, the breach of Target's systems caused the theft of 70 million customers' personal information and 40 million credit cards, illustrating the lack of improper IT security (Cavusoglu et al., 2015). This section explores types of cyberattacks and business strategies to prevent attacks on small

businesses with limited IT support and budgets. The absence of an adequate IT budget is a primary concern for small businesses.

**Hacking.** Hacking by cybercriminals is an external and unpredicted event for monetary gain by selling and buying of customers' private data. However, the unauthorized breach can affect the internal platform of the business having damaging consequences, and exposure to the company's and customers' private data (Banal & Zahedi, 2015). Breach of the customers' information may lead to a lack of trust, especially for sales in the online environment (Banal & Zahedi, 2015). Banal and Zahedi (2015) noted the lack of confidence by the customer could result in devastating damages for the company, causing sales to drop and the possibility the business may fail (Banal & Zahedi, 2015). In many incidents, the small business does not realize the hacking incident occurred until it is too late. The irredeemable damage to the IT equipment costs the business downtime and thousands of dollars to replace the system with useful security technologies, such as firewalls, anti-virus software, and an intrusion detection system (Cavusoglu et al., 2015). If the IT system ensures configuration correctly to the business's security requirements, the next step is to hire an IT specialist to sustain the system from future attacks (Cavusoglu et al., 2015).

**Viruses, worms, botnets, and denial of service attacks.** The botnet can carry malicious viruses, denial-of-service attacks, spam, phishing, and click fraud, infecting the operating system of businesses (Mansfield-Devine, 2016). The cybercriminals recruit other criminals to aid in accessing the organizations operating system (Mansfield-Devine, 2016). Once the cybercriminal gains access to the system, the criminal extracts

information to sell to other cybercriminals (Mansfield-Devine, 2016). The importance to adopt new security software when it comes available is essential to prevent future attacks and prevention of infections from other users in the network (Srinidhi et al., 2015). The indirect attacks eventually target other systems through the deployment of worms or botnet, causing large-scale attacks and the ability to spread malicious viruses (Srinidhi et al., 2015). Once the botnet compromises the computer network, the attacker can remotely control the system through spreading spam, denial of service, stealing personnel confidential information, and other malicious activity (Bertino & Islam, 2017).

**Trojan horses and malware.** The sophistication of the cybercriminal uses a small piece of computer software called a shellcode to download and install malware automatically to a victim's system (Herath et al., 2014). Malware software includes Trojan horses, viruses, spyware, and other unwanted software (Herath et al., 2014). The cybercriminals can deploy two types of techniques: (a) social engineering or (b) drive-by download (Jang-Jaccard & Nepal, 2014). In *social engineering*, the victim is manipulated to download and install the malware, whereby, through *drive-by download*, tricks the victim into downloading and installing fictitious antivirus software through a fake web page (Jang-Jaccard & Nepal, 2014). Once the installation of the shellcode occurs, the malware incorporates viruses, including Trojan downloaders and spyware that deploys a botnet to infect the system and distribute denial of service or spamming techniques (Jang-Jaccard & Nepal, 2014). Often a pop-up window appears on the computer screen, informing the user of vulnerabilities to their system, in an attempt of

tricking the victim to download antivirus software or run a scan of the system (Jang-Jaccard & Nepal, 2014).

**Phishing and spam through email.** The number one sector for a variety of cybercrime affecting victims is through email authentication service. Through phishing, spam techniques, and schemes, the cybercriminal can access email to obtain personnel and financial information, leaving users and businesses vulnerable to identity theft and fraud (Herath et al., 2014). In 2009, Symantec reported 12.7 trillion spam messages, accounting for approximately 89% of all email messages received by individuals, businesses, and the financial sector (Herath et al., 2014). For example, cybercriminals employed a method of emailing the victims to obtain all the banking information, including username, password, cell phone number, and ATM card number (Leukfeldt, 2014). By communicating with the victim via telephone conversation, the cybercriminals obtain all the available information to access their account(s) (Leukfeldt, 2014). Leukfeldt (2014) noted the criminal then transfers the victim's money to another account called a *money mule account* to ensure the transaction does not leave a digital money trail. The withdrawal of the money occurs within a few minutes, leaving no trace of the violation (Leukfeldt, 2014). Many times, the cybercriminal uses a forged email containing a URL to a fake website, which appears as a legitimate site (Tan, Chiew, & Wong, 2016). With the recent online banking platforms, consumers and small businesses should promptly investigate the email by contacting the banking institution for verification to avoid victimization of the cybercriminals (Moghimi & Varjani, 2016).

**Identity theft and credit card fraud.** The use of the internet for banking, shopping, and social media continues to provide cybercriminals with a primary source of income through identity theft. Once the cybercriminal obtains an individual's personal information, such as name, address, date of birth and social security number, they apply the information to commit identity theft and sell the information to other cybercriminals (Clough, 2015). With further exploration of the victim, the cybercriminal can potentially obtain credit reports and financial institution information, whereby, transferring large sums of money electronically (Clough, 2015). Identity theft encompasses other forms of fraudulent behavior by the cybercriminal, including money laundering, drug trafficking, tax evasion, and terrorism (Samtani et al., 2017).

Many businesses and individuals use mobile phones, tablet, and other electronic devices to conduct business transactions or for personal use (Clough, 2015). Over 96% of the world's population use mobile devices, and over 1 billion individuals actively use social media networks, such as Facebook, LinkedIn, and other social forums (Samtani et al., 2017). Governments, financial institutions, and businesses furnish an online service platform, moving away from direct contact with the customer to online transactions and communications worldwide (Clough, 2015). Identity theft enables cybercriminals to access information to steal welfare and social security benefits and apply for credit cards (Kahn & Liñares-Zegarra, 2016). In some cases, the cybercriminal can order new checks to a new address, obtain loans in the victim's name, or use the victim's name to apply for a fake identification card (Kahn & Liñares-Zegarra, 2016).

## Applications to the Applied Business Problem

**Network system administration and budgeting.** Most attacks perpetrated by cybercriminals require international enforcement efforts (Topham, Kifayat, Younis, Shi, & Askwith, 2016). Businesses need to recognize all successful attacks executed by cybercriminals on a global scale (Asghari et al., 2015). The existence of globalization demands to implement strong security measures. Small businesses must recognize cyberattacks and respond by improving their security technologies (Asghari et al., 2015). Organizations need to institute cybersecurity as a requirement to promote prosperity and sustainability for their business. Unfortunately, organizations struggle with insufficient budgets for cybersecurity protection (Young, Lopez Jr., Rice, Ramsey, & McTasney, 2016). Small businesses do not share the same core values as larger corporations because of the lack of cost-effective budgeting (Young et al., 2016). Cyber-resilient organizations focus on leadership and processes to learn from mistakes and adapt approaches through layered security control to manage security risks (Young et al., 2016).

Organizations and individuals worldwide spend billions of dollars annually on cybersecurity, and yet computer systems are less secure than a decade ago (Jang-Jaccard, & Nepal, 2014). Although many organizations use cryptography to protect financial data and assets, they still experience successful cyberattacks and breach of sensitive information (Jang-Jaccard, & Nepal, 2014). Improperly trained employees are a significant risk due to little or no technical knowledge of complicated operating systems (Asghari et al., 2015). Organizations rely on the assurance their network security furnishes the protection necessary to prevent attacks through the implementation of sound

security policies, allowing proactive measures in managing cyberthreats (Asghari et al., 2015). The importance of learning and adapting defenses begins with promoting education in cybersecurity of every individual in the organization and their responsibility to security (Asghari et al., 2015).

The business' network may lack regular programming and system requirements to protect the organization from potential attacks due to an insufficient IT budget. The consensus among companies is a concern for top management to become involved in strategic decision-making with the IT department to implement cybersecurity (Soomro, Shah, & Ahmed, 2016). The major reasons to implement effective cybersecurity includes the business organization's system, connection to the internet, and protection of both the internal or external information (Young et al., 2016). Cybercriminals who devote enough time and resources to invade a company's network can steal an enormous amount of valuable information (Soomro et al., 2016). In fact, the most valuable information to a cybercriminal is the external data: (a) client credit cards, (b) passwords, (c) sales records, (d) vendor lists, and (e) emails (Young et al., 2016). A major part of any company's strategic planning to prevent security breaches involves securing current operations and building a defense against future attacks (Soomro et al., 2016). Management engagement to implement effective risk management strategies includes employees with capabilities and experience (Young et al., 2016). Many small businesses lack effective training programs or employees with expertise in cybersecurity (Young et al., 2016). Due to limited IT budgets to hire competent IT employees, small businesses employ third-party

cybersecurity providers for the protection of the organization's mainframe and security of organization' sensitive data (Young et al., 2016).

Organizational managers, whether department managers or business owners of small businesses need constant collaboration with the IT department or third-party providers to influence the prevention of cybercrime or cyberattacks (Hutchings & Holt, 2017). Topham, Kifayat, Younis, Shi, and Askwith, (2016) reported senior managers replied to the awareness of internal cybersecurity threats and actual incidents in a case study. Managers across the globe in most industries, except for banking institutions and energy firms, are ignorant of insider threats (Topham et al., 2016). Many managers view the job towards security the responsibility of the IT department (Hutchings & Holt, 2017). A significantly small number of executives recognize the importance of detecting unusual employee behavior, such as visiting inappropriate websites, and the urgency of obtaining an advanced warning of an attack (Mansfield-Devine, 2016). Nearly, two-thirds of internal and external IT professionals find it challenging to persuade executives, board members, or owners of organizations about risk factors and adequate budgeting for prevention measures (Brewer, 2016). A small number of IT departments receive guidance from top management concerning the most vital informational assets, the level of acceptable risk, and investment towards prevention of attacks (Brewer, 2016).

The most critical activities executives require of their IT departments is the process of monitoring all traffic in and out of the network via the internet or portable device. Soomro, Shah, and Ahmed (2016) noted all employees must follow the organization's security policies, and report any unusual behavior, violation, or

unacceptable issue to implement immediate corrective action. The organization must demand consistent implementation of network defense procedures and protocols as an operational priority. The organization must ensure employees never have access to sensitive data and update the user's accounts frequently (Soomro et al., 2016). Finally, the importance of frequent assessments and implementing company training programs, including seminars for executives, aids in understanding the significance and prevention of cyberattacks (Brewer, 2016).

**Computer protection and strategies.** The public's perception and vulnerabilities towards cybercrime and internet security remain a concern to combat cybercrime. A published report from the security company Kaspersky Lab reported individuals exposed to phishing attacks amounted to 3.7 million between 2012 and 2013 (Lim, Park, & Lee, 2016). The House of Lords Science and Technology reported an increase in cybercrime, calling it the 'new playground' for criminal activity (Wall, 2008). Although the victimizations occurred, many individuals do not report the incidents (Konradt, Schilling, & Werners, 2016). The advancement of new malicious code produced by cybercrimes illustrates the need for internet security, and the public's demand for provision of new laws implemented by the criminal justice system (McMahon, Bressler, & Bressler, 2016). The internet provides a platform for highly skilled cybercriminals to focus on profit from the inappropriate behavior and illegal activities (Konradt et al., 2016). The increased volume of people using cyberspace includes individuals for personal, business, and legal transactions on a global level (Eddolls, 2016). The importance of understanding the vulnerability and loss of data leads

to the significance of mandating new regulations and security policies on a global level (Wall, 2008). Cybersecurity requires implementation of adequate controls on the federal, state, and local governmental levels for protection of organizations, the economy, and the public (Eddolls, 2016).

One primary concern for many countries is cyberterrorism that poses a threat of sabotage to the power grids, financial institutions, air traffic control, and other infrastructures. The sophistication of cybercrime has increased in recent years with the abilities to paralyze nations (Stockton & Golabek-Goldman, 2014). The U.S. government continues to take proactive measures to prevent cyberterrorism and promotes standards of prosecution, especially after the 911 attack on the World Trade Center (Stockton & Golabek-Goldman, 2014). The importance of prosecution of cybercriminals can help prevent attacks in the nation and abroad requires domestic criminal laws and global cooperation between nations (Stockton & Golabek-Goldman, 2014). Stockton and Golabek-Goldman (2014) noted the 911 attack sparked the interest of the U.S. Department of Homeland Security to initiate the National Cyber Security Division. The division addressed the cyberthreats to government and corporate computer systems, and the understanding of cybercrime and crimes facilitated by a network (Stockton & Golabek-Goldman, 2014). Cybercrime exists when a perpetrator gains access to a computer system without the owner's permission (Aiken et al., 2016). The cybercriminal exceeds the scope of authorization through graining accesses, modifying, or destroying data without permission (Aiken et al., 2016). The cybercriminal's techniques to gain illegal access to the computer system include the use of botnets, viruses, and worms to

hack, steal data, and to send e-mail code to obtain sensitive information (Asghari et al., 2015).

U.S. Homeland Security plays a significant role in enhancing the capabilities of the role of cybersecurity professionals (Park, Kim, & Chang, 2016). The goal of creating a capable workforce is to develop a national cybersecurity workforce and address the demands for effective cybersecurity (Park et al., 2016). The onset of cybercriminals has created a demand for education and strategies to meet the vulnerabilities of cybercrime (Burley, Eisenberg, & Goodman, 2014). The IT profession needs to meet these challenges through continuous education. Companies require hiring knowledgeable and skillful IT employees and offer incentives to retain the employees, such as promotions and a series of positive career ladders (Burley et al., 2014). Through the education and acceptable skills of the IT trade, understanding significant problems and approaches can lead to better cybersecurity and promote public trust (Choi et al., 2014). Presently, the technical workforce requires well-trained cybersecurity professionals (Burley et al., 2014). The need for education in cybersecurity requires expectations of more than one to two years of education to meet the demands of a competent IT department (DeSouza & Valverde, 2016). The extensive knowledge allows the technician to understand and implement coding for systems protection (Burley et al., 2014). The present certification programs offered by technical institutions and colleges lack the knowledge and skills its graduates need for effective strategies in fighting cybercrime (Burley et al., 2014). The type and number of attacks have increased through the sophistication of the breach and the extent of the number of individuals affected by the attacks in the last decade

(Landwehr, 2015). Vulnerabilities continue to increase in businesses, vendors, and suppliers' networks, infiltrating customers and other connections to the company's network system (Landwehr, 2015).

The regulations to prosecute cybercriminals discussed by many governments includes (a) implementing new laws, (b) stronger penalties of existing laws, (c) attention to updating new laws, and (d) adaptation of alternatives of new regulation (Park et al., 2016). However, cybercrimes require definitions regarding the informational, networked, and globalized transformation of deviant criminal behavior through networked technologies (Choucri, Madnick, & Ferwerda, 2014). Global leaders need to agree on an asymmetric definition of cybercrimes to create global policing (Park et al., 2016). Present day cybercrimes use computers to gather information and aid other cybercriminals within the network, known as *traditional crimes* (Samtani et al., 2017). The significant concern for businesses and individuals consists of *computer integrity crimes*, such as hacking, cracking, spying, denial of service, and the use of viruses and Trojans (Samtani et al., 2017). The most significant cybercrime for businesses encompasses *computer-related crimes*, whereby, victims experience theft of cash, goods, or services. Phishing enables fee fraud in the online sale environment, as well as, theft of intellectual property (Samtani et al., 2017).

**Computer protection and managerial strategies.** The importance of the study encompasses managerial strategies employed by small businesses to combat cybercrime. Through strategic measures of collaboration between the chief financial officer (CFO) and the chief information officer (CIO), the goal of necessary preventative protection of

the organization's assets and data ensures preventative measures of intrusion of hackers and potential cybercrimes (Hyman, 2013). With globalization on the rise, even small businesses conduct transactions worldwide through the usages of information technology, leaving them vulnerable to the intrusion of their network (Herley, 2014). The examination of management strategies and the importance placed upon risk factors of sensitive information offers insight for small businesses (Aiken et al., 2016). Through the implementation of a significant budget, strategies, and collaboration between the chief financial officer and chief information officer offers protection of the organization's financial assets, data and intellectual property (Aiken et al., 2016).

Many companies use electronic commerce (e-commerce) to conduct business transactions with contractors, vendors, and customers for payments of services rendered, materials purchased, or products sold to the consumer (Kaur, Pathak, Kaur, & Kaur, 2015). The characteristic of the virtual economy as a business activity uses the electronic banking system for conducting transactions (Kaur et al., 2015). The virtual economy process offers the efficiency of transaction time and convenience, demanding organizations to implement secure firewalls for protection to eliminate the possibility of a breach (Wang & Li, 2014). The e-commerce system, prevalent in the marketplace, present potential cyberattacks of private information, leading to a high risk of victimization of vital information (Kaur et al., 2015). The importance of implementing strategic measures of the organizational network to protect the financial data and asset of the organization is critical. Small businesses, not immune to cyberattacks, call for the

implementation of a protective measure of the internal and external preventative strategies.

Cyberthreats, a top concern for business, is a primary concern for protecting financial data and assets. Many companies realize the severity of cybercrime and the importance of the implicit understanding of security and weakness of their IT department (Aiken et al., 2016). In 2013, cyberattack cost the world economies between $300 billion and $1 trillion (Aiken et al., 2016). The organization must focus on the primary weaknesses of their business practices, culture, and IT systems (Yang, 2015). The importance of internal audits and strategies of proactive administrators enhances the organization to implement innovations for the protection of the businesses' vital information (Piper, 2014). The primary threats include denial of service attacks and data security breaches. Therefore, organizations must recognize breaches and implement secure firewalls and continue to update their antivirus software to prevent attacks (Piper, 2014). It is crucial to run security checks and conduct a system backup daily. One major important safety issue includes intellectual data, such as patents, engineering designs, and other potential information of value, leading organizations to create a failsafe security system to protect all vital data (Piper, 2014).

Placing the importance of an efficient IT department in business promotes growth and prosperity. However, senior and executive managers still minimize their involvement, especially in aiding the IT department to engage managerial strategies to prevent breaches, cybercrimes, fraud, and omission to mistakes (Arief & Adzmi, 2015). New attitudes of management to understand the IT department can aid in the success of

the day-to-day operations to enhance a relationship vantage of success (Arief & Adzmi, 2015). All businesses need government policies to aid organizations in the development of an economic model, national regulations, and laws for companies to adopt secure systems to fight cybercrimes (Landau, 2014). Many businesses find the expense more significant than they can afford to budget for an efficient IT department. Regardless, the issue of privacy and security affects both the U. S. and nations abroad, looking for answers to protect data accessibility of networks by cybercriminals (Landau, 2014).

**Conceptual Framework**

The purpose of this qualitative multiple case study was to explore the managerial strategies of small manufacturing business owners to protect their financial assets, data, and intellectual property against cybercrime. The management and performance of business excellence deal with economic, ecological, and social challenges (Tickle, Mann, & Adebanjo, 2016). Small to large organizations have experienced some form of cybercrime, including worms, Trojan horses, phishing, botnets, and other illegal activities by cybercriminals to sabotage and attack the organization's systems (Vande Putte, & Verhelst, 2014). Globalization affects the complexity of an organization and components (i.e., task, people, structure, and technology), demanding a systematic approach for the organization to succeed and prosper (Vermeulen, 2015).

The initial explanation of the conceptual framework indicates the evolution of the general system theory from the biological view to the sociological view, and finally, to the viewpoint of the connection to the business, society, economic resources, and the control processes within the system's environment. The systems thinking and action

theory incorporates the control factors businesses use to understand the system and subsystems. The theory acknowledges the processes, adaptation in defining the properties of the business's system and response to its environment (Checkland, 2012).

**The general systems theory.** Von Bertalanffy (2008) introduced the general systems theory and explicitly acknowledged the role of interactions among components produce organized complexity. Von Bertalanffy (2008) noted the wholeness characteristics of the system, traditionally studied in physics and chemistry of organisms, is the examination of the living systems as open to change through the exchange of matter and energy within the systems and its environment. While von Bertalanffy (2008) expressed the system as viewing it through the lens of scientific behavior, the system endures by focusing on an exact science (e.g., biophysics and biochemistry), and the methodological principle of a mechanistic view. When the condition reaches a steady state, it becomes independent of the initial conditions and only decided by the rates of reaction of the parameters of the system (Adams, Hester, Bradley, Meyers, & Keating, 2014). However, Zenko, Rosi, Mulej, Mlakar, and Mulej (2013) stated systems theory describes a part of reality and a viewpoint of a scientific discipline, including holism of thinking, decision-making, and action for the survival of humanity and society through success in any human activities. Therefore, to understand the contribution of social responsibility and human activities can help to solve current crises to maintain an organization's systems as a daily practice.

**Sociological theory.** Emile Durkheim and Max Weber applied the principles of biological organisms to human social systems in the late 19th and early 20th centuries

(Drissel, 2012). The transformation of the world's economic systems and the relationship to the social structures provided an evolution of the *information revolution* (Drissel, 2012). In the late 19th and 20th century, the expansion of socioeconomic changes (e.g., industrialization, urbanization, capitalization, and bureaucratization) led to the industrial revolution (Drissel, 2012). The phenomena of the socioeconomic changes accounted for an open system to maintain themselves with the exchange of materials within the environment and a continuous change of their components (Valentinov, 2014). With the first invention of the computer in the mid-1940s, the evolution of the information revolution changed dramatically in relationship to socioeconomics and new technological advancements (Drissel, 2012). The mass proliferation of personal computers, word processing software, the internet, e-mail, and related information technologies of the late 1900s and early 2000s centuries, influenced the sociological theories of Durkheim and Weber (Drissel, 2012). The concept of a steady state signifies the ongoing exchange of matter and energy between the system and the environment, including the equilibrium at a steady state to initiate progress (Valentinov, 2014).

The systemic integrity and view of the world included ethics, as well as, technical advancements (Rousseau & Wilby, 2014). The struggle between morals and scandalous behavior for the gain of power and globalization launched the attention, commitment and efforts in the examination of moral reasoning (Rousseau & Wilby, 2014). Durkheim and Weber believed that human beings experience a unique social reality not experienced by other organisms, sharing the same morals and values (Drissel, 2012). Both theorists found the information revolution included economic changes and social responsibility

due to the transformation of the social impact of technological changes and the influences of the internet (Drissel, 2012).

**Systems thinking and action theory.** According to Checkland (2012), systems thinking and action theory includes the fundamentals and connection of business, society and economic resources, and the control processes within the system's environment. Checkland noted the four conditions for serious systems thinking and action includes (a) the acknowledgment of the system and the subsystems, (b) the process of communications within the system, (c) adaptation to change, and (d) defining the emergent properties of the systems environment. To achieve adaptation, both the system and environment necessitate several possibilities of control processes to initiates change with definable properties, resulting in characteristics of the system or interest of the system in relationship to its environment and society. Checkland further explained to understand and argue for the real existence of emergent properties; one must justify the system including many subsystems that function as part of a more extensive system. Notably, the system and environment adapt through the process of communications. Checkland noted if an action for adaptation persists, the system demands several possibilities of control processes to initiates change. The definable emergent properties result in characteristics of the system for the system to adapt to the environmental changes (Checkland, 2012). One of the most critical components of the system within the business is the strategic measures the company implements in its technology to combat vulnerabilities of cybercrime and protection to the organization's system.

Organizations require understanding cybercrimes and cybersecurity issues due to the globalization of many enterprises in the marketplace. Recently, small businesses now fall victim to cybercrimes due to lack of security and risk management strategies (Hanus & Wu, 2016). Due to the number and sophistication of cyberattacks, the accounting profession finds managing and protecting data as a top technological priority, including managing IT risks, protection of private information, and preventing fraudulent activity in a prompt response (Conteh & Schmick, 2016). Checkland (2012) focused on the organizational system adapting to change and maintain the changes in adaptation to its environment. The organizational system and all the sub-systems work together to maintain unity and adaptation to any internal or external changes. The urgency of protecting financial assets and data rely on the implementation of strategic management practices from the top executives down to the lower level employees for the survival of the business.

**Cybercrime Strategies and Systems Thinking and Action Theory**

Globalization and technological advancements remain a concern with the manner in which businesses conduct transactions in present-day society. The systems thinking and action theory contain a layered structure (i.e., subsystems) as part of the whole system. The subsystems work together to ensure the processes of the system perform and adapt to the changing environment (Checkland, 2012). By monitoring the system, either through automatic processes or by human beings, the system adapts to pertinent threats to allow corrective actions (Checkland, 2012). The primary concern of internal technological protection strategies includes the employees, monitoring system, raising

employee awareness, mobile devices security, and employing rigorous subcontracting processes (Conteh & Schmick, 2016). If a threat is known, the management processes can deploy preventative measures to control and prevent further damage (Baskerville, Spagnoletti, & Kim, 2014). If a threat is new and unknown or unexpected, management processes need to respond to control and repair any damages of the threat promptly (Baskerville et al., 2014). Checkland (2012) noted action is vital to confront the changes in its environment and take immediate measures to protect the system.

**Screening new employees and monitoring.** Organizations should enlist analytical interview techniques and screening processes to ensure the honesty of recruits. These include criminal background checks, misrepresentations of educational skills, and useful interview questions (Padayachee, 2016). To reduce internal cybertheft by employees, employers should consider offering competitive wages and compensation packages (Zhurin, 2015). Zhurin (2015) reported a significant management problem of not monitoring employees results in $200 billion in losses in U.S. businesses every year. Small business experience internal scams by employees through falsified invoices for regularly order goods without consent from the organization (Moghimi & Varjani, 2016). Checkland (2012) noted if the organization needs to implement changes to the internal environment, such as employee compensation packages, it can protect itself from internal failure. No two employees are alike, and the social phenomena continue to change, creating new adaptations to modify the system and subsystems of the internal environment (Checkland, 2012). Through adaptation and evolution of the system, business leaders need to inform employees of monitoring for cyber activity using time

stamps, security checks, monitoring use of flash drives, and malware warnings (Conteh & Schmick, 2016).

**Adopt a robust insider policy.** Small businesses are more likely to experience internal fraud and scams by employees (Moghimi & Varjani, 2016). Small businesses should demand employees to participate in a non-risk policy, aiding in the elimination of carelessness, negligence, or mishaps to eliminate the possibility of employee fraud (Padayachee, 2016). Small businesses often deal with inadequate accounting controls, allowing scams and fraud to prosper (Moghimi & Varjani, 2016). The small business lacks the resources and capabilities to implement security measures to detect employee fraud (Moghimi & Varjani, 2016). The central issues of internal attacks come from individuals that access the organization's assets for malicious purposes or those that unwittingly create vulnerabilities (Padayachee, 2016). The individuals can include employees, contractors, or suppliers of computer services (Padayachee, 2016). Therefore, the non-risk policy demands an understanding of all employees, at all levels in the organization to deal with its internal environment. The policy creates a different way of thinking and defines parameters to improve the environment by removing a layer of internal scrutiny (Checkland, 2012; Upton & Creese, 2014). The policy may include options for warning messages, policy violations, reinforced seminars, internal communications campaigns, and informational videos on cyberattacks (Brewer, 2016).

**Raise awareness.** Upton and Creese (2014) encouraged organizations to provide cybersecurity training programs to teach employees to recognize inappropriate cyber activity. The training programs should teach employees about major cyber activities,

such as phishing, phony emails, and malware intrusions (Brewer, 2016). The business should encourage employees to report unusual behavior or prohibited technologies, such as portable hard drives, and suspicious behavior by outside individuals, such as vendors or suppliers (Brewer, 2016). Organizations need to understand the system as an adaptive whole, surviving in its environment from change and potential risks (Checkland, 2012). In systems thinking theory, the function of each part, when adequately linked to one another, needs constant monitoring of each performance through monitoring all parts of the system (Checkland, 2012). Adams and Makramalla (2015) reported across 13 countries, 45% experienced breaches due to employee negligence. Cybersecurity awareness programs and skills training is essential to protect the business from potential cyberattacks and reduce the financial burden on small businesses (Adams & Makramalla, 2015).

**Mobile devices.** The propagation of the smartphone in recent years causes significant concerns due to the platform to check e-mail, containing contact list, and allowing the users to run hundreds of applications (Moussa, 2015). The global sales of mobile smartphones increase 55% on an annual basis (Markelj & Bernik, 2015). While many businesses use smartphones and tablets to improve productivity and efficiency of the workforce, misuse of the equipment can cause infection to the system through downloading of information to in-house computers attached to the mainframe (Moussa, 2015). A smartphone or tablet, if used without the protection of security applications or for personal use, can transfer malware and other threats (i.e., spyware, viruses, botnets, and other malicious attacks) to the business's mainframe (Markelj & Bernik, 2015).

More than 50% of employees use company smartphones for personal and business purposes (Markelj & Bernik, 2015). Tam, Feizollah, Anuar, Salleh, and Cavallaro (2017) noted approximately 98% mobile devices worldwide reported malware infections in 2015. Checkland (2012) noted the key to achieving adaptation to change, communication between the system and its environment is essential. Organizations must monitor the processes to adapt to the modification of the environment (Checkland, 2012). Therefore, it is paramount for businesses to consider implementing policies and employee training of smartphones to prevent failure of the other sub-systems and the technology of the organization.

**Employ rigorous subcontracting processes.** Small businesses should seek out partners and suppliers with the same risk appetite and culture of the organization. The most efficient strategy for defusing cyberattacks is to use the protective technologies available and resolve issues that may present opportunities for employees, partners, vendors, contractors, and suppliers (Manworren et al., 2016). Systems not only interface with the global environment, but they also interface with each other (Checkland, 2012). To modify security between systems, the assumptions of one subsystem must guarantee the safety of the other (Houser, 2015). The goal involves strategies to engage employee programs, to illustrate acceptable and unacceptable behaviors, reminding them by protecting the organization leads to protecting their jobs (Houser, 2015). Implementing strict guidelines for usage of the computer system is essential for the protection of the company's data and assets. For example, in 2013, Target experienced 40 million customers' card numbers and 70 million of individuals' personal data stolen due to one of

the company's refrigeration vendors (Manworren et al., 2016). The policy mandates implementation for all employees, business partners, contractors, vendors, and suppliers, along with regular data security audits. Notably, any participants of the subsystems contribute functionality to the system and its environment (Checkland, 2012). Therefore, the organization expects the same security measures from its business partnerships.

**Electronic commerce.** Electronic commerce (e-commerce) used in external business processes aids in business-related activities, such as processing customer payments, suppliers, vendors, contractors, and other parties involved in the business transactions (Wang & Li, 2014). Due to globalization, even small businesses use e-commerce for convenience, transaction efficiency, business cooperation, and virtual production for sales (Wang & Li, 2014). Small businesses, frequently targeted due to the perceived notion the company lacks security or implementation of IT security processes (Alkhateeb, 2016). Cybercriminal activity results in monetary gain through illicit activities, including online banking transfers, credit card purchases, or accessing the business's networks (Manworren et al., 2016). The small business using e-commerce requires adequate protection from hackers to keep their network secure through a proactive and reactive security strategy (August, August, & Hyoduk, 2014). The emerging properties of the sub-system (i.e., e-commerce) can affect the system, sub-systems, and the environment if adaptations for change do not exist (Checkland, 2012). For example, in 2012, 63 Barnes and Noble bookstores experiences a breach of its branches, including branches in New York City, Miami, Chicago, and Florida (Alkhateeb, 2016). Not only does a breach of e-commerce affect the business, but also

the customers may experience identity theft due to the data collected, processed, and stored electronically (Checkland, 2012; Kahn & Liñares-Zegarra, 2016).

**Collaboration.** Accounting managers or chief financial officers (CFOs) demand proactive cooperation with the chief information officer (CIO) and IT personnel to develop a stronger, comprehensive data protection plan. Through collaboration, the development of a defensive plan aids in the prevention of cybercrimes (Holtfreter & Harrington, 2014). With the rise of cybercrimes, public accounting firms, businesses, and other organizations acknowledge how their data and their clients or customers' data remains safe when stored, moved, and processed (Conteh & Schmick, 2016). Holtfreter and Harrington (2014) noted the small businesses connection to the internet could face failure due to potential risks of a breach. The sophistication of the cybercriminals and theft continues to increase in the global markets (Conteh & Schmick, 2016). The U.S. Department of Justice disclosed an estimated $57.6 million in damages have incurred since 2005 in ransomware, whereby, consumers paid $100-$200 to regain access to personal and business computer systems (Chaudhry, 2017). In 2015 alone, Chaudhry (2017) noted this type of fraud was an estimated cost of $24 million to the public and businesses in ransom. Many small businesses do not understand the importance of an IT budget or hiring a reputable IT representative to monitor their system (Lanz, 2014). Lanz (2014) noted the IT department needs to plan for the likelihood of a breach of their customer information. Checkland (2012) noted failure to the system relies on the protection of its components (i.e., subsystems). Small businesses need to recognize the interdependencies of political and social environments and maintain protective security

measures through the implementation of managerial functions (Doh, Lawton, Rajwani, & Paroutis, 2014).

**Cloud computing application.** Small businesses continuously seek innovations to compete in the global marketplace due to changes in the economic business environment. The ability to use technology requires high quality and speed of information, providing a modern means of communication worldwide. Through this means, small businesses need safe, inexpensive ways to store critical financial data. Manoj and Bhaskari (2016) noted a reasonable manner of storing and protecting financial data and assets in a technological structure is cloud computing, whereby, buying an information structure tailored for the business's storage platform. Small businesses lack funding for technical equipment and software to protect financial assets and data, and one inexpensive option to store vital information is cloud technology (Stergiou, Psannis, Kim, & Gupta, 2018). Notably, one primary concern is the safety and security of cloud technology. The new technology leads organizations to question the validity of security (Chang, Ramachandran, Yao, Kuo, & Li, 2016). Utilization of the cloud promotes further attacks, as the new storage facilitate an easy target for the cybercriminal due to security issues (Stergiou et al., 2018). Checkland (2012) noted each functional part linked to others, if unstable in its environment, it may cause internal failure, demanding constant monitoring of performance to adapt to changes affecting the whole system.

**Added value of systems thinking theory and action.** Checkland (2012) noted the importance of the correlation between the system and the subsystems of the business environment is essential for the protection of the entire system. While I discussed several

different subsystems within the system, cybercrime affects several other areas of concern, such as firewall protection, encryption, password protection, and many others. Due to many problematical situations, business systems research is interested not only in the thinking process but also the proactive action resulting from the thought process (Checkland, 2012). The course of action taken from the discovery of problems to the recovery process remains essential to maintain and sustain the business from the possibility of failure. Checkland (2012) noted four fundamental factors involved in the system, the environment, and real-world actions includes the following conditions:

- Emergent Properties: The core justification for the ideas of the system;
- Adaptation: An exploration of the complexity of the real-world and existence in the environment;
- The process of Inquiry: Perceiving the real-world and understanding the soft system thinking process; and
- Define the Methodology: Engage in the process of defined action research and recovery research to validate criteria for a course of action and thinking during the research for positive results.

Checkland (2012) noted the ideas of system thinking create an avenue to resolve real-world problems as a practical tool. The existence of cybercrime affects business, economics, and society. Needless-to-say, in the environment of business and social aspects, technology touches everyone around the globe. Technology continues to change at a constant rate with new software and hardware, cell phones, computers and other gadgets, which plague our lives for convenience. However, businesses, society, and

governments regularly struggle with cybercrime and the repercussions of cyberattacks daily, creating new proactive measures to disarm the criminals. In this proposed study, I explored the strategies small manufacturing companies use to combat the vulnerabilities of cybercrime to protect their financial data, assets, and intellectual property, producing useful results.

## Transition

The common application of IT around the globe, requires that businesses depend on computers, mobile phones, and other devices connected to the internet. The devices connect to the internet via networks and wireless platforms. This enables computers to collect, store, and transmit information anywhere in the world in a matter of seconds. Because of the transactional activity using the internet, financial information and data require complex systems of security and risk management to protect an organization's most valuable assets and data. While many organizations benefit from advancements in IT, the cybercriminals continue to identify new ways to steal financial assets and data from vulnerable companies and then sell these assets. Through learning from other organizations' mistakes, many businesses may make changes to their network system to protect the organization and the public from potential cyberattacks.

Organizational risk factors plague every business worldwide, which, in turn, affect partners, contractors, vendors, consumers, and society. Technological advancement continues to transform methods of payment and organizational business models to improve operational efficiency, resulting in the reduction of risk factors when conducting business globally. But organizations struggle with the risk of cybercrimes

due to the increasing use of mobile computing, internet transactions, social networking, and cloud-based services. The importance of implementing strategic measures to combat these risk factors remains a significant concern for small organizations. If they fail to protect themselves, the consequences could be dire. Strategic and preventative measures, internal and external, ensure the protection of the organization's data and assets against hackers and cybercrimes. As the sophistication of cybercriminals increases, the need for advancements in cybersecurity is the primary concern. In this study, I explored the strategies and solutions used by small manufacturing companies to protect their financial assets, data, and intellectual property against cybercrimes.

Section 2 covers the following topics: role of the researcher, participants, research method, research design, population and sampling, data collection instruments, data collection and organization technique, data analysis, the reliability and validation of the study procedures and reporting.

In Section 3 of the study, I present the findings, applications to professional practice, implications for social change, recommendations for action, recommendations for further research, reflections, summary, and conclusion of the study. The data collected in Section 3 of the study pertains to managerial strategies to combat the vulnerabilities of cybercrime for small manufacturing companies, thereby, protecting the financial assets and data of the organizations.

## Section 2: The Project

In this qualitative case study, I explored the effectiveness of the managerial strategies of small manufacturing businesses in the midwestern region of the United States to combat cybercrime. I collected data from four small business owners via interviews using open-ended questions. Understanding the experiences of small manufacturing business owners with cybercrimes and their managerial strategies could help create effective strategies to prevent breaches to their system and protect vital assets. Section 2 of the study addresses the following topics: (a) restatement of the purpose, (b) role of the researcher, (c) research participants, (d) research method and design, (e) population and sampling, (f) ethical research, (g) data collection instruments, techniques, organization, and analysis, and (h) reliability and validity.

### Purpose Statement

The purpose of this qualitative multiple case study was to explore the managerial strategies of small manufacturing business' owners to protect their financial assets, data, and intellectual property against cybercrime. I explored the managerial strategies implemented by four small manufacturing business owners who successfully prevented cybercrimes in the midwestern region of the United States. Cybercrime affects the businesses sector, society, and global economies. The implications of the study for social change include (a) the elimination of cybercrimes, including the theft of confidential data and assets; (b) the protection of customers' information in the business' networks; and (c) the prevention of breaches by implementing effective managerial strategies to protect

individuals in society. Other businesses may use the information to improve their strategies.

## Role of the Researcher

The qualitative researcher explores a different dimension of the social world through exploration of how and why the phenomenon of the study impacts social processes, and the significance of the study (Berger, 2015). Furthermore, it is important to understand the concerns that may be mitigated to enhance the reliability and validity of the study (Yin, 2017). The qualitative researcher factors the findings into its analysis to constitute a compelling argument about the study (Berger, 2015). I attempted to go beyond basic research to provide an in-depth understanding of a phenomenon through open-ended questions and observations during the interview, while avoiding bias. As a manager of an accounting firm, we were the victims of cybercrime. I worked with the IT experts to rectify the problem.

According to the U. S. Department of Health and Human Services (1979), the three core ethical principles indicated in the Belmont Report include respect for persons, beneficence, and justice. First, the researcher must protect the autonomy of all human subjects and treat them with respect, providing each participant with the voluntary consent and adequate, truthful information regarding the participation in the research. Secondly, the researcher must apply the principles of beneficial action towards the participant by doing no harm, maximizing practical benefits, and minimizing potential damage. Lastly, the researcher must ensure reasonable justice requiring fairness in distribution to each participant. The researcher must provide reasonable, non-

exploitative, and well-considered procedures that are administered fairly and equally to each participant, treating each participant with the same basic ethical principles and guidelines while conducting the research (HHS, 1979).

The qualitative researcher provides the participant with a consent a form containing (a) information and disclosure agreement, (b) comprehension of the research subject and participation, and (c) valid consent of voluntary participation in the study (HHS, 1979). I plan to have all participants send an email with the words, "I consent," assuring each participant of their confidentiality as contributors. The consent form provides information, so the participants have an understanding of the study, procedures, and addresses the ethical standards outlined in the Belmont Report (Fiske & Hauser, 2014). All the collected data remains stored in a fireproof, lock box for five years until the final destruction of the data.

The responsibility of the researcher to avoid bias includes to strive for the highest standards of research, not falsifying information, avoiding deception, and accepting the responsibility of producing their own work (Yin, 2017). To mitigate bias, the researcher must remain the data collection instrument and not separate themselves from the research (Fusch & Ness, 2015). The qualitative researcher must recognize their personal lens (i.e., the personal view of the world) to listen and interpret the behaviors of the participants (Fusch & Ness, 2015). I focused on the interview questions as indicated in Appendix C through exploring the managerial strategies to prevent cybercrime with the understanding my beliefs, expectations, and cultural values could prejudice the study. The researcher must ensure accuracy, credibility, and follow the protocol when interviewing to reduce

bias while collecting data (Yin, 2017). After reviewing and interpreting the interview transcripts, I used member checking to ensure the accuracy and credibility of the collected data.

The interview process in a multicase study requires the utilization of an audiotaped recording. The protocol includes a set of open-end questions, reflecting inquiry of a set of questions for the case study instruments for analysis to support or not support the primary research question of the study (Yin, 2017). I followed the interview protocol by providing each participant with an overview of the case study, the data collection procedure, the data collection questions, and follow the same guideline in the examination and reporting my findings (see Appendix D). The importance of following the same protocol increases the reliability of the case study research and provides the researcher with guidelines to maintain obtaining the same data of each participant in a multicase study (Yin, 2017).

## Participants

The participants for the multicase study include four business owners of small manufacturing companies in the midwestern region of the United States who used successful strategies to combat cybercrime. For the purposes of the study, the definition of a small manufacturing business is 500 or fewer employees (SBA, 2017). Due to the extensive range of employees in a small manufacturing business, I interviewed four business owners with a range of 66-180 employees, who have not experienced breaches or cybercrime. The participants, small manufacturing owners (i.e., sole proprietorship),

experienced in the day-to-day operations of the company, can provide a definitive account of managerial strategies to combat potential breaches and cybercrime.

I obtained 90 small manufacturing businesses containing the owners' name, email address, location, and the number of employees from the U.S. Small Business Administration online database, using the classification codes for manufacturing companies, located in the midwestern region of the United States. The U.S. Small Business Administration district office provided the links to the Dynamic Small Business Search website and the Table of Small Business Size Standards: Matched to North American Industry Classification System Codes (SBA, 2017). Yin (2017) noted that gaining access to key organizational leaders for recruitment and documentation to collect pertinent information of the potential participants is essential for the validity of the study. The prospective participants will receive an invitation via email (see Appendix B) to take part in a face-to-face interview. I provided a clear understanding of the subject matter for the study, the interview process, and data collection to equip the participant with an understanding of the study focus and the phenomenon to obtain participants.

Establishing a working relationship with the participants is essential from the initial contact with a written invitation of communication, noting the interview time consist of one hour (Yin, 2017). As the researcher, one must maintain a relationship with the participants of transparency, respect, and trustworthiness (Nadal et al., 2015). The goal of the relationship is to explore the essential managerial strategies small manufacturing business owners apply to combat vulnerabilities of cybercrimes for the protection of financial assets and data. To establish a positive working relationship, I

provided a copy of the informed consent form, via email, to the potential participants I chose from the Dynamic Small Business Search website to participate in the study. The informed consent form provides all the information that pertains to the study. Once I confirm the participants of the study, I scheduled a face-to-face interview with each participant at an available time and in a comfortable setting chosen by the participants. Yin (2017) noted the researcher should maintain a comfortable atmosphere for the participant as an observer to promote trustworthiness during the interview. I established a collaborative working relationship with each participant through professional interaction and conduct each interview in a complementary manner by showing mutual respect.

## Research Method and Design

The participants for this multicase study included four business owners of small manufacturing companies in the midwestern region of the United States who understand managerial strategies to combat cybercrime. For the purposes of the study, the definition of a small manufacturing business is 500 or fewer employees (SBA, 2017). Due to the extensive range of employees in a small manufacturing business, I interviewed four business owners with a range of 66-180 employees, who have not experienced breaches or cybercrime. The participants, small manufacturing owners, can provide a definitive account of cyberattacks and breaches.

### Research Method

I chose the qualitative research method, aligning the exploration of the managerial strategies small manufacturing owners can implement to protect their assets and data

from cyberattacks and breaches. The basis of qualitative research is an interpretation of the experiences through inductive data analysis, focusing on the details or themes with a lens that explores motives and actions of a problem in its real-world context (Lewis, 2015; Yin, 2017). The qualitative methodology approach uses multiple data collection sources and enables a better understanding of the phenomenon, presenting a more convincing and accurate portrayal of the situation and analysis of the business problem (Hays, Wood, Dahl, & Kirk-Jenkins, 2016). A quantitative approach limits an understanding of the phenomenon, while the qualitative approach entails the specific experiences of the participants (McCusker & Gunaydin, 2015). McCusker and Gunaydin (2015) noted the mixed method approach offers a cumulative body of knowledge, cutting across several methodologies, thereby, creating a more in-depth understanding to develop the triangulation of qualitative and quantitative data. However, mixed methodology hinges on the research question, purpose, and context, and may not present the findings through quantitative methodology (i.e., experiment and a field study) to develop a holistic presentation of the phenomenon (McCusker & Gunaydin, 2015).

The consideration of quantitative research, from a human observational perspective, focuses on the review of a particular behavior to determine statistical data and not recurring issues in social and behavioral sciences research (McCusker & Gunaydin, 2015). The intent of the study is to gain a deeper understanding of small manufacturing business owners' managerial strategies as they pertained to protecting their organization from data breaches. A quantitative numerical analysis would not supply an inquiry to answer the research question of this study. Mixed methods research

is a combination of qualitative and quantitative analysis and lacks incommensurability of the research question, purpose, and context of the study (McCusker & Gunaydin, 2015). A mixed-methods approach is not appropriate for this study, as the use of quantitative data would not have provided comprehensive answers to the research question.

Therefore, to thoroughly explore the research question and the organizations' response to the issue of cybercrime and breaches, I chose a qualitative research method to explore the social and behavioral aspects of the study. Qualitative research can provide insights into new ways of working and practices, evolving from interactions and influence on multiple levels of an organization (Barnham, 2015). The concepts of cybercrime and the managerial strategies small manufacturing companies employ to deal with business, social, and economic resources, exploring cases bound by time and activity involving procedures over a period of time.

**Research Design**

The five qualitative traditional research methods for inquiry include biography, phenomenology, grounded theory, ethnography, and case studies (Lewis, 2015). Narrative research can provide individual stories and sheds light on the individual's experiences and how they see themselves (Lewis, 2015). Thus, to fully understand an organization in narrative research, the researcher needs to observe the contextual nature of the work of the individual (Barnham, 2015). Therefore, narrative research would not comply with this study due to an examination of the organization and its functioning parts and not a study of an individual's view of their life experiences.

Phenomenology determines a participant's experience, and a common theme of several individuals lived experience (Lewis, 2015). The phenomenological design might provide insight into the study if the focus relied on lived experiences of small manufacturing business cybersecurity professionals. I considered a phenomenological research design. However, the phenomenological research design is the exploration of lived experiences and beliefs (Lewis, 2015). The goal of this study was to explore the managerial strategies small business owners use to combat breach and provide adequate cybersecurity. Therefore, the phenomenological design is not appropriate for this study.

Grounded theory is used to identify intervening factors, moving beyond description to generate a theoretical explanation (Lewis, 2015). The primary conception of the grounded theory is the participants help to shape or develop a theory (Barnham, 2015). The grounded theory focuses on a process or action through a distinct phase over a period of time (Barnham, 2015). Grounded theory is not an appropriate design for this study because the study encompasses conducting personal interfaces with small business owners and the managerial strategies they implement to eliminate breaches and does not focus on creating a theory.

Ethnographic researchers focus on an entire cultural-sharing group (Lewis, 2015). They mainly explore the shared and learned patterns, behaviors, beliefs, and language in the environment of the cultural group (Barnham, 2015). They explore the unique characteristics of a specific group and the dynamics of the cultural system to understand members' behaviors (Barnham, 2015). The ethnography research method is not an

appropriate design for this study because it is not necessary to understand or study the cultural behaviors of the participants.

The case studies method is intended to explore an in-depth understanding of several entities experiencing the same phenomenon within a real-life setting (Yin, 2017). The basis of qualitative case studies is an interpretation of the experiences of individuals regarding a particular event bounded by time and place (Yin, 2017). The qualitative case study design is the appropriate form of research for the study due to the exploration of the phenomenon of cybercrime and the vulnerabilities small manufacturing businesses face to employ strategies for the prevention of breaches. In a case study, the researcher explores the multiple units within the case, such as an entire business organization (Yin, 2017). Qualitative case study research is the approach of studying people in their environment to discover the significance of their experiences (Cope, 2014). Qualitative research allows an understanding of the knowledge and beliefs of the subjects of the study (McCusker & Gunaydin, 2015). The qualitative case study design is the appropriate method for the study due to the exploration of the phenomenon of cybercrime and the vulnerabilities small manufacturing businesses face to employ strategies for the prevention of breaches. I explored a real-life situation through a collection of data from small manufacturing business owners to provide effective managerial strategies for eliminating cybercrime.

In this qualitative multicase study, I collected data through semistructured face-to-face interviews and review of the company's managerial strategy documentation. Data saturation occurs when no new themes or codes emerge from the data collected (Fusch &

Ness, 2015; Yin, 2017). To reach saturation, while I planned to interview six participants, I met my goal of saturation with four participants. The participants in this study may include up to 12 small business owners who would provide data through a face-to-face interview containing open-ended questions. Member checking of each participant provides verification of the data collected and any other information the participant may provide for the validity of the study (Hays et al., 2016). Member checking ensures the data collected through the interview process is accurate and credible (Hays et al., 2016). Through the application of triangulation of multiple sources of data, it enhances the reliability of results and the procurement of data saturation (Fusch & Ness, 2015).

## Population and Sampling

The population for the study is small manufacturing business owners from the midwestern region of the United States. To understand the population, the definition of small business is 500 or fewer employees (SBA, 2017). The state of Wisconsin is the second highest manufacturing concentration of all states in the United States, with more than 9,200 manufacturing companies (WEDC, 2016). Southeastern Wisconsin ranks third in the number of small manufacturing businesses (SBA, 2017). Justifying the population demonstrates saturation within the dataset (Gentles, Charles, Ploeg, & McKibbon, 2015). Within qualitative research, the population and sample size, measured by the depth of data rather than frequencies, whereby, selection of participants should consist of the best to answer the research topic (Cho & Lee, 2014). I recruited participants by obtaining the owners' name, email address, location, and the number of

employees from the U.S. Small Business Administration online database, using the classification codes for manufacturing companies, located in the midwestern region of the United States (see Appendix A). The prospective participants received an invitation via email to take part in a face-to-face interview (see Appendix B). The email also included the informed consent form to provide all the information that pertains to the study. All participants successfully implemented managerial strategies to combat cybercrime and breaches and are willing to provide information about the topic of this study.

Purposeful sampling for the qualitative case study is appropriate if the participants interviewed have knowledgeable information about the phenomenon and topic of the study (Elo et al., 2014). Cho and Lee (2014) stated purposeful sampling indicates selecting information-rich cases strategically and purposefully. Purposeful sampling involves identifying and selecting individuals or groups of individuals, who especially exhibit knowledge or experience with the phenomenon of interest (Palinkas et al., 2015). I selected a purposeful sample of 12 business owners from the population of small manufacturing companies the midwestern region of the United States from the Dynamic Small Business Search website provided by the SBA. The selection of potential participants provides information to conduct purposeful sampling to recruit participants and those meeting the eligibility for the study. The eligibility of each participant for the study must include business owners (i.e., sole proprietorships) who have successfully implemented managerial strategies to prevent breaches and cybercrime, and who are willing to share in-depth knowledge and contribute to the exploration of the business problem of this study.

The appropriate sample size for the qualitative researcher requires structured guidelines for rigor to estimate the sample size (Gentles, Charles, Ploeg, & McKibbon, 2015). It is important to note the sample size of the participants require generating focus on information regarding the research question (Cleary, Horsfall, & Hayter, 2014). Notably, the sample size should provide convincing information about the same phenomenon to reach validity and saturation of the data (Cleary et al., 2014). Yin (2017) noted the sample size depends on the complexity of the study topic and the depth of the data collected. In a case study, the sample size can consist of 4-15 participants to reach saturation (Gentles et al., 2015). I interviewed four business owners with 66-180 employees with six open-ended questions. Eligible participants for this study include small business owners who have not experienced breaches by successfully implementing managerial strategies and are willing to participate in a face-to-face interview to contribute information for this study. While I had planned to interview six participants, I met the goal of saturation by interviewing four participants, whereby, I did not receive any additional information.

Failure to reach data saturation impacts the quality of the research and impedes content validity (Fusch & Ness, 2015). To reach data saturation, the researcher must acquire enough information whereby no further coding is necessary for the study (Fusch & Ness, 2015). Data saturation occurred when no additional themes or categories arise from the collected data (Fusch & Ness, 2015; Yin, 2017). The necessity of researchers is the approach to reach saturation to maintain the validity of the study (Yin, 2017). Researchers realize data saturation exists when no new findings are relevant to the

purpose of the study (Fusch & Ness, 2015). The achievement of data saturation signifies the optimal sample size (Elo et al., 2014). To reach saturation, while I planned to interview six participants, I met the goal of saturation by interviewing four participants.

The interview process caters to the interviewees' availability, allowing accurate data collection through open-ended questions and the possibility of follow-up questions to provide clarity and validation for the study (Houghton et al., 2015; Yin, 2017). As the primary data collection instrument, the researcher collects data in a natural setting (Nadal et al., 2015). A natural setting assists in performing data analysis that is inductive and deductive to establish patterns and themes (Elo et al., 2014). The process of the face-to-face interview provides visual clues, such as the loss of nonverbal data, contextual data, and distortion of verbal data (Goodman-Delahunty, Martschuk, & Dhami, 2014). By promoting a comfortable, natural surrounding is necessary to gain the participant's confidence and support, encouraging the interviewee to contribute knowledgeable and substantial data (Goodman-Delahunty et al., 2014). It is essential to create an asymmetric power relationship between the interviewer and the interviewee to conduct an effective interview (Robinson, 2014). In an interview setting, it is vital to allow the interviewee to contribute to the study through providing details about their experiences, expectations, and predicaments about the particular interview topic through interviewing a conversation, rather than an interrogation (Robinson, 2014). The face-to-face interview setting provides the human factor for forming a relationship between the interviewee and interviewer (Goodman-Delahunty et al., 2014).

The interview process in the qualitative multicase study could include four to six participants (Gentles et al., 2015). With the understanding of the definition of small manufacturing companies provided by the SBA (2016), I interviewed four business owners with 66-180 employees. The reasoning behind selection from the number of employees could illustrate how the managerial strategies of the organization conflict with cybercrime and breaches. However, upon recruitment, I plan to interview more participants, if needed, to reach data saturation. The interview process follows the protocol (see Appendix D) to provide dependability and validity of the study.

## Ethical Research

The process of designing and researching a qualitative multicase study demands ethical standards during several phases of research, including ethical issues of sensitive information of participants (Yin, 2017). Approval from the Institutional Review Board (IRB) follows the ethical standards and requirements before the collection of any data from participants. Qualitative researchers deposit anonymized data that meet standardized requirements relating to its format and ethical consent (Nadal et al., 2015). For example, the researcher requires specific conditions in allowing access to their data (Nadal et al., 2015). After the IRB granted permission to initiate the study, I emailed the prospective participants (see Appendix B), inviting them to participate in the study.

All interviews with the participants require information of the purpose of the interview, the subject matter of the study, the procedure of data collection, and as found in the informed consent form. The informed consent form includes details of the study, participant rights, and instructions to indicate acceptance to partake in the research. The

informed consent form assures the researcher and the participants of anonymity and confidentiality of the information provided, privacy, and security of the data (Nadal et al., 2015). Through via email, each participant voluntarily agreed to contribute to the study by replying to the original email of the informed consent form with the words "I consent."

The participant may withdraw from the study without penalty by merely contacting me via email or telephone with the assurance of the destruction of all documentation as outlined in the informed consent form. Participants will not receive incentives or any monetary payments to partake in the study and interview process. I addressed the ethical standards of the Walden University Institutional Review Board (IRB), following the process to ensure meeting the ethical standards prior, during, and after conducting the research. Through the IRB process, I received approval number 12-26-17-0506262 before collecting data.

All participants will receive a code to protect their anonymity with the identification codes of P-1, P-2, P-3, and P-4. As stated in the Belmont Report, the researcher requires following the three core ethical principles (a) respect for persons, (b) beneficence, and (c) justice for every participant (HHS, 1979). The correct procedures for collecting the relevant research to conduct the multicase study of participants must meet the requirements of the same phenomenon. I secured all forms, field notes, transcripts, and data collected in a locked box for five years and subsequently destroy by burning all documentation, the password-protected flash drive and any other information in my fire pit.

## Data Collection Instruments

I am the primary data collection instrument in this qualitative multicase study. The primary data collection instrument consists of a semi-structured interview. I interviewed at least six small manufacturing business owners and ask six open-ended questions (see Appendix C). The open-ended questions allow the participants to share their experiences and more in-depth understanding of the nature or meaning of everyday experiences (Tran, Porcher, Falissard, & Ravaud, 2016). Each participant will share specific experiences and strategies to combat cybercrime of the organization's processes and procedures. The participants respond to the open-ended questions as they wish, and the researcher may probe their responses (McIntosh & Morse, 2015). The six open-ended questions related to Checkland (2012) systems thinking and action theory (see Appendix C) and to gain answers to the study's research question. The information obtained from participants can generate focused information of the research questions to enable a convincing account of the phenomenon (Yin, 2017).

The face-to-face semi-structured interview and observations with each participant provide data regarding experiences of data breaches and implemented managerial strategies of the organization. While conducting the interview, the researcher must remain unbiased, eliminating any personal characteristics (i.e., gender, race, age, personal experiences and beliefs, political and ideological stances, and emotional responses) to the participant (Berger, 2015). It means turning the researcher lens back onto oneself and removing bias by providing a natural setting to allow the participant to feel free to share their experience of the phenomenon (Berger, 2015). After the interview process, I

requested any documentation of managerial strategies to prevent breaches and cybercrime attacks (See Appendix D).

When a researcher analyzes data from archival documents, interviews, and observations, they reveal patterns and themes (Nadal et al., 2015). By combining a convergent of evidence through methodological triangulation, examination of company documents helps to strengthen the validity of the study (Yin, 2017). The objective of the data collection instruments is to obtain significant and pertinent information from each participant, providing rich, thick data (Fusch & Ness, 2015). The interview responses from each participant, managerial strategy documentation, and observations provide significant information concerning effective strategies to protect their systems from data breaches.

I conducted each interview, in the same manner, to ensure reliability and validity by following an interview protocol (see Appendix D). Demonstration of the reliability of a case study is by repeating the same data collection method achieving the same result (Yin, 2017). To maintain reliability, the researcher must prepare and complete the documentation through the same research steps and procedures and remain constant throughout the study to minimize error and bias (Kihn & Ihantola, 2015). I followed the same protocol (see Appendix D) for each interview, maintaining effective note-taking and observation during the interview process.

Member checking is a critical component of qualitative research to assess the accuracy and validity of the data provided by the participant and helps to eliminate bias (Yin, 2017). Though member checking, the researcher maintains the correctness of all

documentation of every participant (Elo et al., 2014; Fusch & Ness, 2015). Participants of the semi-structured face-to-face interviews will receive a full transcript of my interpretation of their responses. Member checking provides accuracy for the researcher, and the representation of a participant's subjectivity (Thomas, 2017). The importance of ensuring the credibility, dependability, confirmability, and transferability of a study, member checking is essential to conduct the research reliably to gain a full understanding of the investigated phenomena (Hays et al., 2016). I used member checking to verify the participant's answers and ensure the accuracy of the data collected. I conducted member checking by sending a copy of the analysis via email a week after the initial interview and set up a follow-up telephone interview for verification of the information to ask for feedback on the reported data.

## Data Collection Technique

The data collection techniques for this qualitative multicase study includes a collection of data through six interviews with owners of small manufacturing companies, observations during the interviews, and organizational documentation illustrating the managerial strategies to combat cybercrime. With open-ended questions, the researcher can explore the phenomenon spontaneously, asking additional questions by creating a relaxed atmosphere to develop a conversation with the participant (Percy, Kostere, & Kostere, 2015). Percy, Kostere, and Kostere (2015) noted that open-ended questions encourage the participant(s) to provide depth and vitality, which increases the validity of the study by collecting rich data for analysis. The face-to-face interview provides visual observations, such as body language and facial expressions, providing the researcher with

information about the ease or uneasiness of the interview (Goodman-Delahunty et al., 2014).

Yin (2017) noted the interview process facilitates consistency, reliability, and unity, and requires following the same protocol. It is important to note that the researcher must remain bias and objective while conducting an interview (Berger, 2015). A disadvantage of the semi-structured face-to-face interview could occur if the question delivery is in a biased manner (Yin, 2017). Also, the participant may decline on answering a question due to feeling uncomfortable with a recording device (Yin, 2017). Another disadvantage includes the comfort level of divulging information, whereby, providing incomplete data (Goodman-Delahunty et al., 2014).

The semistructured face-to-face interview of each participant includes a selected date, time, and location of choice in agreement with their availability (Yin, 2017). I contacted each chosen participant for an interview with an agreed date, time, and location to conduct the interview (see Appendix A). I provided each participant with a copy of the informed consent form for their records, which explains the background information, procedures, voluntary nature of the study, risks, and benefits of participating, assurance of no promise of payment or gift, privacy issues, and my contact information. I followed the same protocol for each interview (see Appendix D).

I converged my evidence through the utilization of methodological triangulation. To promote the convergence of evidence, I included open-ended interviews transcripts, organizational documentation regarding managerial strategies implemented, and field notes of observations during the interview processes. Credibility can enhance the study

with triangulation, which uses several methods to study one phenomenon (Hays et al., 2016). Data triangulation strengthens the validity of the study (Yin, 2017). Methodological triangulation is appropriate for the multicase study research to achieve substantial and precise results to support reliability, validity, and rigor through discoveries of each data collection technique (Hays et al., 2016).

After the transcription of the interviews, I conducted member checking with each participant to confirm the data collected during the interview process. At the completion of data analysis, the researcher requests feedback or member check from the participants to validate the conclusions, promoting accuracy of the interpreted data (Cope, 2014). The importance of the validity of the study relies on providing research of correctness in the reporting of the findings through member checking (Kihn & Ihantola, 2015). Member checking provides the opportunity to ask further questions as a measure of trustworthiness and establishes credibility (Harvey, 2015). I conducted member checking by contacting the participant through a phone interview, if necessary, to verify the data collected is accurate unless I receive an email verifying the one to two-page summary is correct. After member checking, I imported the transcribed data into the NVivo programs for coding and finding themes.

## Data Organization Technique

The collection of data for this qualitative multicase study is from six small manufacturing business owner's responses through a face-to-face interview with open-ended questions. I used a handheld recorder with an integrated USB flash drive, allowing connection to my computer for easy transcription. I needed to prepare by understanding

how the handheld recorder works, enabling successful recordings of the face-to-face interviews with all the participants. I saved each participant's interview on a different USB flash drive labeled with the correlating identification code. Recording the interview allows the researcher to focus on the content of the interview easier to transcribe verbatim (Jamshed, 2014). I used a transcription software (i.e., Naturally Speaking Dragon) to save time and review the transcription to promote correctness of all transcriptions. Once again, the importance of understanding the software enables successful transcription of all interviews. I used a transcription software to save time. I saved all information on a removable hard drive to prevent loss of the data collected or technical problems.

After the transcription of the original interview and member checking, the researcher establishes the credibility of the data (Harvey, 2015). Member checking maintains the correctness of all documentation of every participant (Elo et al., 2014; Fusch & Ness, 2015). I conducted member checking by sending a copy of the analysis (i.e., one to two-page summary) via email a week after the initial interview. I set up a follow-up interview via telephone call, if necessary, to verify the data collected is accurate unless I receive an email from the participant that the verifying the summary is correct. Member checking ensures the data collected through the interview process is accurately recorded and transcribed (Hays et al., 2016).

After performing the follow-up member checking interview (i.e., scheduled phone interview), I imported all documentation into NVivo software. With the use of computer-assisted tools, such as NVivo, the researcher can categorize vast amounts of data (Yin, 2017). Nvivo software analyzes a set of data, comparing and contrasting codes, themes,

and subsequent findings (Sotiriadou, Brouwers, & Le, 2014). The software offers the process of two outputs: (a) a coded data set and (b) a node system, providing an index of the significant and subsidiary categories of coded data (Woods, Paulus, Atkins, & Macklin, 2016). The software locates and ensures any issue described in the findings, and not the perception of just one person, but confirms the participants had the same opinion (Hays et al., 2016). NVivo helps a researcher manage and organize data, including interview transcripts, documents, and survey responses (Wood et al., 2016). The software analyzes sets of data, providing an insight to help develop conclusions (Sotiriadou et al., 2014). I secured all forms, field notes, transcripts, USB flash drives, and data collected in a locked box for five years and destroyed by burning the papers and deleting all electronic files.

## Data Analysis

Case study research is appropriate for exploring multiple sources of data to help determine the foundation of a phenomenon (Houghton et al., 2015). Yin (2017) stated the utilization of multiple sources of evidence in a case study allows the researcher to explore a broad range of evidence and convergence of lines of inquiry. Yin (2017) noted the analytical techniques enables patterns to emerge and help to strengthen the validity of the study. Through triangulation, the researcher can explore three sources of information to strengthen the construct validity of a study (Mayer, 2015; Yin, 2017). Methodological triangulation correlates people, time and space through examining data from multiple collections of data methods (Fusch & Ness, 2015). I used methodological triangulation through a collection of data from open-ended interviews, company documentation of

strategies used to combat cybercrime, and field notes of observations during the interview processes. Methodological triangulation involves the utilization of multiple methods of data collection experiencing the same phenomenon (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014).

Data analysis relies on the ability of the researcher attaining enough data to reach saturation. Fusch and Ness (2015) agree the general principles of saturation include (a) no new data, (b) no new themes, (c) no new coding, and (d) ability to replicate the study. While I interviewed four participants, Fusch and Ness (2015) noted choosing the most significant participants providing rich and thick data is more important than sample size to reach data saturation. I selected participants that have successfully implemented managerial strategies used to prevent breaches and protected the organization from cybercrime attacks. To reach data saturation, the researcher needs collecting rich, thick data through relevant data collection methods (Fusch & Ness, 2015). To reach saturation, I interviewed four participants until there were no new themes, no new data, and no new coding.

The method of collection of data from the study includes six open-ended questions in a face-to-face interview with six small manufacturing business owners to gather the data (see Appendix C). Upon completion of each face-to-face interview using a handheld Olympus digital voice recorder, I transferred the data into my computer system via USB drive from the recorder. I transcribed the taped interview data by utilizing Nuance Dragon Speech Recognition Software. The goal of methodological

triangulation analysis of the face-to-face interviews, the organization's archival strategic records, and interview observations collected to answer the research question.

Member checking in qualitative research is informative feedback or respondent validation to help improve the accuracy, credibility, and validity of the data received from an interview or another source of information provided by the participant of the study (Harvey, 2015). The member checking is a critical component of qualitative research to assess the accuracy, reliability, and validity of the data provided by the participant and helps to eliminate bias (Yin, 2017). To ensure validity and creditability of the information gained through the interview processes, I completed member checking of each interview.

I used NVivo computer-assisted software to analyze the data. The tool and guidance help the researcher to code data into themes and serves as an able assistant and reliable tool (Yin, 2017). NVivo software does not provide code data automatically into themes but allows the researcher to visualize the data and determine common themes (Zamawe, 2015). However, the software allows the researcher more creativity and relieves the researcher the burden of manual coding (Zamawe, 2015). NVivo offers a coding comparison function to check the consistency and reliability of the coding process (Woods et al., 2016). After coding all the data, I explored the prominent themes for further analysis of the data to identify existing themes.

The key themes from the data correlated to Checkland (2012) systems thinking and action theory offer an understanding of how each part of the system influence one another, and initiates change to adapt to its environment. Organizations consist of

employees, technology, and procedures working together to create a successful business, reduce potential risk, and promote sustainability (Helfat & Karim, 2014). The routines of management include involvement in planning, initiating, and implementing change, strategic assessments and planning (Helfat & Karim, 2014). The most critical components of the system within the business is the strategic measures the company implements in its technology to combat vulnerabilities of cybercrime and protection to the organization's system. When examining the data within the systems thinking and action theory, I propose the following four themes require examination: (a) organizational policies, (b) IT structure, (c) assessment and action, and (d) managerial strategies.

The potential themes correlated with Checkland (2012) systems thinking and action theory and the relationship to the research question enable me to find the key themes. Systems thinking and action theory offers an understanding of the influence of the subsystems and the whole system of the organization. Checkland (2012) noted the ideas of system thinking and action creates an avenue to resolve real-world problems as a practical tool. Systems thinking and action theory in relationship to an organization comprised of people, processes, and technologies working together to achieve a common goal (Loosemore & Cheung, 2015). The premise of systems thinking and action allows the participants to share experiences concerning managerial strategies to combat cybercrime to improve the protection of the organization's financial asset and data.

When examining the data within systems thinking and action theory, among the developed themes, I expect to find the following four themes: (a) organizational policies, (b) IT structure, (c) assessment and action, and (d) managerial strategies. While systems

thinking and action theory dictates the concept of the system and environment, routine activities theory explained crime as an event that highlights its relation to space and time and emphasis on victimization (Shabnam, Faruk, & Kamruzzaman, 2016). Consumers increasingly use technology to shop and find products at discounted rates, and 60% of the United States population now buy more items online at least once per fiscal quarter (Holt & Bossler, 2014). Identity theft victimization occurs when a motivated cybercriminal and suitable target intersect within a network characterized by low level of security (Golladay & Holtfreter, 2017). Network connection and lack of security features are more likely to identity theft (Golladay & Holtfreter, 2017). Routine activity theory places emphasis on characteristics, whereby, businesses need to protect and assess customer's activities to prevent victimization (Shabnam et al., 2016).

## Reliability and Validity

### Reliability

Reliability signifies the replication of the tests results, and validity indicates the accuracy of the data (Yin, 2017). Reliability encompasses four criteria of (a) dependability, (b) creditability, (c) transferability, and (d) confirmability (Elo et al., 2014). Validity involves tests of (a) construct validity, (b) internal validity, and (c) external validity (Yin, 2017). Both reliability and validity, necessary for the qualitative study, ensures the data is accurate and trustworthy.

### Reliability

Dependability refers to the stability of data over time and under different conditions (McCusker & Gunaydin, 2015). The interaction between the researcher, the

research, collected data, and a high level of accuracy enables the dependability of the data presented (Thomas, 2017). One specific method to ensure dependability includes member checking. The researcher seeks to establish dependability through trustworthiness by reporting the process of content analysis accurately through data collection method, sampling strategy, and the selection of data analysis techniques (Hays et al., 2016). I followed the same research protocol (see Appendix D), along with journal notations, and explored the re-occurring themes of each participant. Trustworthiness is essential in all stages of research, including the preparation phase, the organization phase, and reporting phase (Elo et al., 2014).

Member checking in qualitative research is informative feedback or respondent validation to help improve the accuracy, credibility, reliability, and dependability of the data received from an interview or another source of information provided by the participant of the study (Harvey, 2015). The member checking is a critical component of qualitative research to ensure the data provided by the participant is dependable and helps to eliminate bias (Yin, 2017). The study has dependability if the process of selecting, justifying, and applying research strategies, procedures, and methods are clearly explained and evaluated efficiently by the researcher (McCusker & Gunaydin, 2015). I conducted member checking by sending a copy of the analysis via email a week after the initial interview and set up a follow-up telephone interview for verification of the information to ask for feedback on the reported data.

## Validity

For a qualitative study to be credible and trustworthy, the data must be sufficiently descriptive and include a precise description of the participants, activities, interactions, and the interview setting (McCusker & Gunaydin, 2015). Triangulation is used to confirm the data to enhance credibility and ensure the data gathered from the participant is complete (Hays et al., 2016). Triangulation compares data from multiple sources to explore the extent of verification of the findings (Yin, 2017). I used methodological triangulation analysis of the face-to-face interviews, the organization's archival strategic records, and interview observations collected to answer the research question. If the data is consistent, it increases confidence in the credibility of the findings (McCusker & Gunaydin, 2015; Yin, 2017). I ensured the participants I recruit have successfully implemented managerial strategies to prevent breaches and cybercrime.

Along with triangulation, I conducted member checking with each participant. Member checking ensures the data collected through the interview process is accurately recorded and transcribed (Hays et al., 2016). To achieve validity, the use of the open-ended questions promotes behavioral responses from the small manufacturing business owners in connection with managerial strategies used to combat cybercrime (see Appendix C). I tested the credibility of the data collected through member checking, and triangulation of the data to increase confidence in the credibility of findings.

Transferability is achieved if the findings of a qualitative study are transferable to other similar settings (Hays et al., 2016). A thick description of the setting, context, people, actions, and events studied is needed to ensure transferability in qualitative

studies (Hays et al., 2016). Furthermore, transferability and the relationship of saturation refers to the categories or themes are fully accounted for and tested to produce validity, whereby, a theory can emerge (Elo et al., 2014). Methodological triangulation is necessary to support the findings from each data collection method (Yin, 2017). I used the interview, observations, and member checking to strengthen the validity and transferability of the study to ensure findings related to my research question and promote future research about cybercrime in small businesses.

Transferability of a qualitative study results if the findings are transferable to other similar settings. The importance of transferability allows other researchers to expand on the study or develop a new theory (Elo et al., 2014). Through the findings from the study, I provided small manufacturing businesses with information from the study to promote effective managerial strategies to combat cybercrime and provide information for further research.

Confirmability or member checking is based on the analysis of the collected data and explored to confirm the findings, based on the data, is logical, verified with clarity (Pozzebon, Rodriguez, & Petrini, 2014). Before the commencement of thematic coding, I conducted member checking by sending a copy of the analysis via email a week after the initial interview and set up a follow-up telephone interview for verification of correctness and validity. Confirmability distinguishes how the findings relate to the phenomenon of the research question (Yin, 2017). To achieve confirmability, member checking of each interview ensures the validity of the research process (Hays et al., 2016). Member checking provides the opportunity to ask further questions as a measure

of trustworthiness and establishes validity (Harvey, 2015). Open-ended questions encourage the participant(s) to provide an in-depth of information, and through member checking, it increases the validity of the study through collecting rich data for analysis (Percy et al., 2015).

Member checking the transcriptions provide confirmability and trustworthiness of the collected data (Fusch & Ness, 2015; Harvey, 2015). Furthermore, member checking provides accuracy of the data collected, interpretation, and validation of the data furnished by each participant, which is a critical tool to establish confirmation and credibility (Harvey, 2015). After transcription of the initial interview, I scheduled a phone interview with each participant to verify the accuracy of the interpreted data and any other pertinent information for analysis.

The validation of the qualitative study is to ensure data saturation. Data saturation provides validity in a qualitative study, which is like a statistical validity in a quantitative study. In a qualitative case study, the researcher asks *how* and *what* questions (Yin, 2017). Failure to reach data saturation impacts the quality of the research and impedes content validity (Fusch & Ness, 2015). To reach data saturation, the researcher must acquire enough information, whereby, no further coding is necessary for the study (Fusch & Ness, 2015). If data saturation does not occur, the study has a negative impact on the validity of one's research (Yin, 2017). It is important to note the sample size of the participants require generating focused information regarding the research question and provide convincing information of the same phenomenon to reach validity and saturation of the data (Cleary et al., 2014). Furthermore, the qualitative research must understand

the concept of the *personal lens* to enable data saturation, whereby, understanding the information presented by the participant is imperative, and the researcher is the data collection instrument (Fusch & Ness, 2015).

Purposeful sampling for the qualitative researcher requires selection of information-rich data from participants with experience and knowledge of the phenomenon of interest to promote saturation (Palinkas et al., 2015). I recruited business owners of small manufacturing companies, who have not experienced cybercrime and the managerial strategies they successfully use to prevent future breaches. The importance of these elements and the willingness of the participants to provide information-rich data should promote data saturation.

Another method to reach data saturation for the qualitative researcher is the interview process and the number of interviews (Fusch & Ness, 2015). Furthermore, the importance of structuring the interview questions and asking the same questions for all participants is essential to reach data saturation (Fusch & Ness, 2015). As listed in Appendix C, I have six open-ended questions to ask the participants. Furthermore, I have created an interview protocol (see Appendix D) to conduct each interview in the same manner.

Finally, the triangulation methodology uses multiple methods of data collection, such as interviews, observations, field notes, and organizational documentation (Cope, 2014). Methodological triangulation ensures data is rich in depth using multiple relevant sources to promote saturation (Fusch & Ness, 2015). Through triangulation, data saturation is reached by the examination of different levels and perspectives of the

explored phenomenon, ensuring the richness of the data is met (Fusch & Ness, 2015). I analyzed the data from the face-to-face interviews, the managerial strategies records, and interview observations to answer the research question.

## Transition and Summary

The focus of this qualitative case study is to explore the effectiveness of managerial strategies of four small manufacturing businesses in the midwestern region of the United States to combat the vulnerabilities of cybercrime. I collected data from small business owners by conducting interviews containing open-ended questions of four participating companies. Understanding small manufacturing business owners' experiences with cybercrimes and managerial strategies may aid in the creation of effective strategies to protect vital data and prevent breaches to their system. Before data collection, I completed my oral defense and obtained permission from the IRB to begin the research.

Section 2 of the study provides the case study research information include (a) the role of the researcher, (b) participants, (c) research method, (d) research method and design, (e) population and sampling, (f) ethical research, (g) data collection instruments and techniques, (h) data analysis, and (i) the reliability and validity of the study.

Section 3 of the study presents the findings, applications to professional practice, implications for social change, recommendations for action, recommendations for further research, reflections, summary, and conclusion of the study. The data collected in Section 3 of the study pertains to managerial strategies to combat the vulnerabilities of

cybercrime for small manufacturing companies, whereby, protecting the financial assets, data, and intellectual property of the organizations.

Section 3: Application to Professional Practice and Implications for Change

## Introduction

The purpose of this qualitative multiple case study was to explore the managerial strategies of small manufacturing business owners to protect their financial assets, data, and intellectual property against cybercrime. The population for this study included four small manufacturing business owners who successfully prevent cybercrimes in the midwestern region of the United States. The four owners provided the findings through interviews, followed by member checking of all the transcripts, and strategic documentation. The methodological triangulation included the interviews, exploration of company documents, and observation of each participant during the interview.

NVivo 12 Pro allowed visualizing the data through visualization outputs such as charts, mind maps, word clouds, and comparison diagrams as they relate to Checkland's systems thinking and action theory. Through the combination of the interview data, literature review, and conceptual framework, I discovered the managerial strategies that the participants used to eliminate breaches and cybercrimes. Four themes emerged from the research: (a) organizational policies, (b) IT structure, (c) managerial strategies, and (d) assessment and action.

In Section 3, I provide the findings of the study to explore the managerial strategies small manufacturing business owners implement to combat cybercrimes for the protection of financial assets, data, and intellectual property. Section 3 also includes the application to professional practice, implications for social change, recommendations for action and further study, along with reflections and conclusions.

## Presentation of the Findings

The presentation of the findings of this study addresses the overarching research question: What managerial strategies do small manufacturing business owners implement to combat cybercrimes for the protection of financial assets, data, and intellectual property? Four themes emerged: (a) organizational policies, (b) IT structure, (c) managerial strategies, and (d) assessment and action. The findings validate, disconfirm, or extend knowledge, and I connect the findings to new literature and the conceptual framework used for this study. I used the case study interview protocol (see Appendix D), and analyzed the recorded interviews and transcription using NVivo 12 Pro research software to identify emerging themes. The findings validate, disconfirm, or extend knowledge, and I connect the findings to new literature and the conceptual framework used for this study. Table 1 illustrates the demographic information of the four participating small manufacturing business owners. The table provides the number of the employees of each participant in the manufacturing industry.

Table 1

*Demographic Information about the Business*

| Participant | Participant's Comment | | | |
|---|---|---|---|---|
| | Case 1 | Case 2 | Case 3 | Case 4 |
| Code Name | P-1 | P-2 | P-3 | P-4 |
| Number of Employees | 180 | 160 | 150 | 66 |

The participants provided consistent answers to the interview questions and correlated with the conceptual framework, literature review findings, and triangulation, helping me identify the themes through the data analysis process.

**Theme 1: Organizational Policies**

The organizational climates shaped by its founders and most importantly by the management or leaders decide the rules and policies for the employees to follow. Many organizations provide an employee handbook defining the policies and procedures of the business, ensuring ethical behavior and practice of their employees (Ford, Piccolo, & Ford, 2017). As part of the organizational policies, an organization's ethical climate is shaped by its founders and modified by management as the organization grows, and most importantly by the leaders who decide alteration to its rules and policies (Lau, Tong, Lien, Hsu, & Chong, 2017). Employees are more committed to the organizations when the ethical values mirror those of its leaders (Lau et al., 2017). Organizations should enlist analytical interview techniques and screening processes to ensure the honesty of recruits (Padayachee, 2016). These include criminal background checks, misrepresentations of educational skills, and useful interview questions (Upton & Creese, 2014). Organizations must recognize the significance of knowledgeable employees as valuable assets to influence prosperity, maximize economic value, and improve the effectiveness of the organization (Alsharo, Gregg, & Ramirez, 2017). Team effectiveness towards employee achievement in the organization enables a collaborative effort by all employees for the organization's growth and prosperity (Alsharo et al., 2017). Affective commitment is a typical response toward a positive work environment.

Virtual environments make it challenging due to day-to-day informal interactions and nonverbal communications, which may be lost in web-based communications, relying on building and sustaining trust (Ford et al., 2017). In systems thinking and action theory, the function of each part, when adequately linked to one another, needs constant monitoring of each performance through monitoring all parts of the system (Checkland, 2012). The four participants created tiers between each department for effective security and monitoring of the employees. Checkland (2012) noted if the organization needs to implement changes to the internal environment, such as employee compensation packages, it can protect itself from internal failure. No two employees are alike, and the social phenomena continue to change, creating new adaptations to modify the system and subsystems of the internal environment (Checkland, 2012).

The four participants conducted background checks of the employees. However, only 50% signed a nondisclosure or confidentiality agreement. Through adaptation and evolution of the system, business leaders need to inform employees of monitoring for cyber activity using time stamps, security checks, monitoring use of flash drives, and malware warnings (Upton & Creese, 2014). Only 50% of the organizations allow the employee to use the company's computer system for personal use but block specific sites. The other 50% only allow the employees to use their own personal devices. However, the organizations recognize their responsibility in providing clearly defined policies and the mission of the business to instill trust among the employees (Ford et al., 2017). A defined organizational mission gains employees' trust. The most important aspect of collaboration between the management team and the employee bonds a relationship

between knowledge sharing, trust, and effectiveness in an organization's success in a virtual setting.

Table 2 contains the participants' statements about their Organizational Policies between the employees and management and their business practices

Table 2

*Theme 1: Organizational policies*

| Participant | Participant's Comments |
|---|---|
| P-1 | The organization has a tight screening process for new employees and does background checks on employees. All employees must sign a noncompliant agreement and nondisclosure agreement. The organization has a limited number of individuals to have access to the system in terms of banking and the financial accounting department through the utilization of tiers between departments. The organization has a good traditional system of internal financial controls where only a few individuals have control of the financial transactions. The organization handles the intellectual property by limiting what they give to their customers. The employees may not use the organization's computer system for personal use. |
| P-2 | The organization conducts a screening process for new employees and does background checks on new employees. The organization does have limited access to the system to protect the intellectual property from employee theft. The organization implemented the tiers for login and access for the different departments. Employees may use their own personal devices, but they cannot connect to the employer's network. They do have a clause in the employee handbook that each employee must sign-off on, but it is not really enforced. The organization does block specific sites where the employee will receive a forbidden message, but they must report it to IT. |
| P-3 | The organization conducts a background check of new employees. The employees sign a confidentiality agreement. The organization set up tiers to provide security between different internal departments, allowing access to specific information to authorized individuals. Every department can only access the information they need to perform |

*(table continues)*

| Participant | Participant's Comments |
|---|---|
| | their task with access through password protection to the specific files they use daily. The employee may use the computer for personal use, but they block specific sites. The employee with smartphones, tablets, and laptops include security software for those within the business and those who travel on business for the organization. |
| P-4 | The organization conducts a background check of new employees. The employees do not sign a confidentiality agreement. The organization feels all the employees possess high integrity and values. The organization set up tiers between the different departments. The organization does not have a system to protect the intellectual property from employee theft. Employees can connect to the internet during lunch to check email or do online shopping but do stop them from entering unsecured sites. The organization is not concerned with the employees accessing the internet for personal use. Employees that travel can only use devices the organization provides for their use and the software extended to the devices are secure, and the software is up-to-date. |

**Theme 2: IT Structure**

With globalization on the rise, even small businesses conduct transactions worldwide through the usages of information technology, leaving them vulnerable to the intrusion of their network (Tajpour et al., 2016). The virtual economy process offers the efficiency of transaction time and convenience, demanding organizations to implement secure firewalls for protection to eliminate the possibility of a breach (Wang & Li, 2014). The participants in this study understand the importance of the use of more than one firewall for protection. Two of the participants use several firewalls in place, and two of the participants use two firewalls. Firewalls include filtering rule to implement network segments or tiers between different departments according to application control policies (Tsuchiya, Fraile, Koshijima, Ortiz, & Poler, 2018). Software defined network (SDN)

makes it possible to modify the network by creating segments without reconfiguring the existing networks to minimize network attacks (Tsuchiya et al., 2018). Cyberthreats, a top concern for business, is a primary concern for protecting financial data and assets by establishing and maintaining the firewall(s) of their system. Many companies realize the severity of cybercrime and the importance of the implicit understanding of security and weakness of their IT system (Aiken et al., 2016).

The primary threats include denial of service attacks and data security breaches. The denial-of-service (DoS) uses malicious code to attack or reduce network reliability (Li, Zhang, Xia, & Yang, 2018). The DoS attack reduces the system's performance through blocking the flow of information from the sender to the receiver (Li et al., 2018). The DoS attack does not require the system's information and well-suited in a shared network (Li et al., 2018). In 2017, cybercriminals launched Global ransomware and DoS attach which cost $5 billion (Thornton-Trump, 2018). Kaspersky Labs reported from January to September 2016 the attack increased three-fold to attacks occurring every 40 seconds (Thornton-Trump, 2018). Therefore, organizations must recognize breaches, implement secure firewalls, and continue to update their antivirus software to prevent attacks (Piper, 2014). Systems not only interface with the global environment, but they also interface with each other (Checkland, 2012). Checkland (2012) noted the key to achieving adaptation to change, communication between the system and its environment is essential. Organizations must monitor the processes to adapt to the modification of the environment (Checkland, 2012). Manager of businesses demand strong links between systems thinking, and action approaches their goals and recognizes the importance of

sustainability (Cavana & Forgie, 2018). It is crucial to run security checks, update all software, and conduct a system backup daily, ensuring the firewalls sustain protection of the system.

All four of the participants backup their systems daily and applied the relevant patches to stop potential breaches. One of the most critical components of the system within the business is the strategic measures the company implements its technology to combat vulnerabilities of cybercrime and protection to the organization's system. The subsystems work together to ensure the processes of the system perform and adapt to the changing environment (Checkland, 2012). By monitoring the system, either through automatic processes or by human beings, the system adapts to pertinent threats to allow corrective actions (Checkland, 2012). If a threat is new and unknown or unexpected, management processes need to respond to control and repair any damages of the threat promptly (Baskerville et al., 2014). With the understanding the emergent properties of potential breaches, the businesses should examine the system from multiple views, including the subsystems to ensure protection from cyber attacks.

While online cybercriminals have become more organized, businesses, governments, and society lack consistency and sustainability. Part of the problem lies in securing new products and services (Paquet-Clouston, Décary-Hétu, & Bilodeau, 2018). Most firms are directly at risk of a breach if they do not have an actionable software inventory (McGraw, 2018). Security depends on writing code, which can prove to be difficult, time-consuming and costly (Paquet-Clouston et al., 2018). Many organizations rely on software which includes vulnerabilities, leading to situations of incorporating

malicious code, such as ransomware (Paquet-Clouston et al., 2018). It is essential to choose the best software, as well as ensuring that everyone in the organization is using current releases and fixing discovered problems (McGraw, 2018). Checkland (2012) noted action is vital to confront the changes in its environment and take immediate measures to protect the system. For all four of the participants, the importance of applying patches and updating their software to their systems is crucial. Moreover, the four participants hired an IT consultant to ensure their network security. By monitoring the system, either through automatic processes or by human beings, the system adapts to pertinent threats to allow corrective actions (Checkland, 2012). Therefore, due to the global use of the internet, businesses, and society need to work together against cybercriminals through securing their networks with credible software to prevent potential breaches.

The ideal contribution to protect the businesses network from potential breaches and protection of the company's assets is cyber liability insurance. Many companies have purchased cyber liability insurance to cover economic losses or damage from the vulnerability of cybercrime and breaches. Because the internet of things (IoT) involve the business' use of the internet and network structure, companies have purchased cyber liability insurance as an addition to their property insurance or from another insurance vendor (Lu, Niyato, Privault, Jiang, & Wang, 2018). The National Institute for Standards in Technology reported the common vulnerability to a business' IT structure is the impact of the threats made to their network (Baldwin, Gheyas, Ioannidis, Pym, & Williams, 2017). By providing financial protection against service outage (i.e., denial-of-service),

cyber insurance ensures the business for financial compensation (Lu et al., 2018). Checkland (2012) noted if an action for adaptation persists, the system demands several possibilities of control processes to initiates change. The definable emergent properties result in characteristics of the system for the system to adapt to the environmental changes (Checkland, 2012). While many businesses hire an IT consultant to contribute risk management services, the service provider's service agreement limits their liability (Lu et al., 2018). Therefore, cybersecurity insurance aids to cover the gaps in the service provider agreement and insurance coverage to cover the company's loss in case of a substantial breach (Franke, 2017). While all four participants have hired an IT consultant, two of the participants carry cybersecurity insurance through their property insurance. Notably, the two participants voiced concerns about cybersecurity and the possibility of purchasing more insurance. The primary concern is the excessive cost of the insurance and the IT budget for the company.

As technology continues to develop innovations, small businesses try to implement new security measures to protect their data, assets, and intellectual property through authentication devises. The organization must focus on the primary weaknesses of their business practices, culture, and IT systems (Yang, 2015). Over the years, businesses have embraced innovative technology to maintain security within the organization (Satterfield, 2018). More companies are turning to biometrics, such as the key fob as an alternative to security (Waggett, 2016). The four participant us a key fob for the employees to enter the building. The participants stated when the employee enters the building; it sends information of the name of the employee and a time stamp to the

network. Many organizations take advantage of the new biometric for secure authentication mechanisms (Waggett, 2016). By monitoring the system, either through automatic processes or by human beings, the system adapts to pertinent threats to allow corrective actions (Checkland, 2012). Checkland (2012) noted action is vital to confront the changes in its environment and take immediate measures to protect the system. Based on risk factors business organizations face in a digital world, businesses continue to explore new options for IT security, such as biometrics.

Table 3 contains the participants' statements about their organizational policies of the IT Structure and their business practices.

Table 3

*Theme 2: IT Structure*

| Participant | Participant's Comments |
|---|---|
| P-1 | The organization instills tight internal controls for processing financial information, banking transactions, and the Human Resource department. The organization has an Internal IT department with a strong manager and uses a traditional infrastructure, including multiple firewalls. They use security software, anti-malware, and anti-virus software. The organization uses encryption software. For security measures, the organization created a network of departmental tiers which require password protection and login scrip between the different departments. They update all software daily, conduct daily backups of transactions, and blocks all unauthorized internet sites. The IT department installs patches when need and conduct a penetration test daily. The employees use a Key Fob to enter the building. The organization invests in cyber liability insurance with the organization's property insurance. |
| P-2 | The organization's external strategies consist of five firewalls and use McAfee encryption. They run security checks daily with 24-hour IT support from a consultant that is on site two days a week but monitors |

*(table continues)*

| Participant | Participant's Comments |
|---|---|
| | the system 24-7 and informs the IT manager if there is an issue. The organization has an Internal IT department with an active manager. They have multiple firewalls with a cloud base mainframe and back-up off-site. The organization uses Microsoft NAV as the organization's platform, security software, anti-malware, and anti-virus software. They created a network of departmental tiers and a separate network for extremely confidential information, along with password protection and login scrip between the different departments. The organization uses McAfee encryption, McAfee malware program, McAfee web root, and Hitman Pro to protect their system. The IT department updates all software, runs daily backups, blocks all unauthorized internet sites, and installing patches when needed. The employees use a Key Fob to enter the building. They hired an IT Consultant to check the system weekly. |
| P-3 | The IT department maintains the system to prevent any breaches of the system. The organization uses Microsoft NAV product for all our data collection, with two firewalls for the security of all the company's PCs, tablets, and phones. They use TrendMicro for spam filtering from the internet. The organization created departmental tiers with password protection and login scrip between the different departments. They implemented an electronic naming system. The organization invests in cyber liability insurance with the organization's property insurance. The IT department conducts daily backups, blocks all unauthorized internet sites, and installs patches when needed. The employees use a Key Fob to enter the building. They hired an IT Consultant checks the system weekly. |
| P-4 | The organization feels secure with their security measures between the IT department and the external consultant. The organization has two firewalls and uses Microsoft NAV as the organization's platform. The organization uses security software, anti-malware, and anti-virus software. The organization created a business accounting platform and departmental tiers with password protection and login scrip between the different departments. The IT department update all software, blocks all unauthorized internet sites, conducts daily backups and installs patches when needed. The employees use a Key Fob to enter the building. They hired an IT Consultant checks the system every two weeks. |

**Theme 3: Managerial Strategies**

Cyber threats, a top concern for business, is a primary concern for protecting financial data and assets. Many companies realize the severity of cybercrime and the importance of the implicit understanding of security and weakness of their IT department (Aiken et al., 2016). The primary threats include denial of service attacks and data security breaches. Therefore, organizations must recognize breaches and implement secure firewalls and continue to update their antivirus software to prevent attacks (Piper, 2014). The primary concern of internal technological protection strategies includes the employees, monitoring system, raising employee awareness, mobile devices security, and employing rigorous subcontracting processes (Conteh & Schmick, 2016). The managerial strategies small business choose can make or break the organization. Strategic management involves the consideration of resources and an assessment of the internal and external environments. Checkland (2012) noted action is vital to confront the changes in its environment and take immediate measures to protect the system.

Organizations should enlist analytical interview techniques and screening processes to ensure the honesty of recruits. These include criminal background checks, misrepresentations of educational skills, and useful interview questions (Padayachee, 2016). Small businesses are more likely to experience internal fraud and scams by employees (Moghimi & Varjani, 2016). Small businesses should demand employees to participate in a non-risk policy, aiding in the elimination of carelessness, negligence, or mishaps to eliminate the possibility of employee fraud (Padayachee, 2016). The central issues of internal attacks come from individuals that access the organization's assets for

malicious purposes or those that unwittingly create vulnerabilities (Padayachee, 2016). To reduce internal cybertheft by employees, employers should consider offering competitive wages and compensation packages (Zhurin, 2015).

Checkland (2012) noted if the organization needs to implement changes to the internal environment, such as employee compensation packages, it can protect itself from internal failure. No two employees are alike, and the social phenomena continue to change, creating new adaptations to modify the system and subsystems of the internal environment (Checkland, 2012). Through adaptation and evolution of the system, business leaders need to inform employees of monitoring for cyber activity using time stamps, security checks, monitoring use of flash drives, and malware warnings (Conteh & Schmick, 2016). Businesses need to screen new employees and monitor their system to prevent individuals that may go beyond fulfilling their assigned responsibilities (BaMaung, McIlhatton, MacDonald, & Beattie, 2018). In some cases, newly hired employees, someone whom the organization entrusts, may engage in insider activity by accessing secure areas or within the system (BaMaung et al., 2018). Through the uses of knowledge of the organization and system, the employee could cause harm or theft (BaMaung et al., 2018). While all the participants do background checks on employees, only two have them sign a nondisclosure agreement. However, they felt monitoring the employees was not necessary because the group of individuals working for them possessed trustworthy qualities.

The primary concern of internal technological protection strategies includes the employees, monitoring system, raising employee awareness, mobile devices security, and

employing rigorous subcontracting processes (Conteh & Schmick, 2016). By monitoring the system, either through automatic processes or by human beings, the system adapts to pertinent threats to allow corrective actions (Checkland, 2012). The business should encourage employees to report unusual behavior or prohibited technologies, such as portable hard drives, and suspicious behavior by outside individuals, such as vendors or suppliers (Brewer, 2016). Cybersecurity awareness programs and skills training are essential to protect the business from potential cyber attacks and reduce the financial burden on small businesses (Adams & Makramalla, 2015). Technology continuously changes, and the organization should keep the employee informed of new malicious malware. A security policy instilled by the business can help prevent breaches (Williams, Levi, Burnap, & Gundur, 2018). Security threats include opening infected emails, visiting internet shopping sites, downloading infected files, and internet banking (Williams et al., 2018). Employee awareness of cyber threats through informal security reminders helps to save time and cost to the organization. Two of the participants provide informal security reminder of new malicious viruses. All the participants allow internet access for all employees. One participant addresses the issue in the employee handbook that each employee must sign-off on, but they do not enforced the poliy. Due to the complexity of the system, small business should not allow employees to use the internet for personal use, as well as allowing them to connect their personal devices to the system. Employees require awareness training to avoid malicious email or phishing scams.

Another security risk is the use of passwords in the business place. It is important to note that all the passwords require changing on a regular basis. The password should be challenging and kept confidential between users (i.e., smart passwords). Smart Passwords consist of a letter, capital letters, numbers, and symbols that have no affiliation with the person or business. Cybercriminals create sites to buy and sell stolen data and code to access infected computers (Hutchings & Holt, 2017). To avoid victimization, such as DoS, users should change their password regularly as a security measure (Am & Kim, 2018). Dupont (2017) noted cybercriminals participate in the criminal activity for financial gain, recognition, power, loyalty to others in the cybercrime organization, and their political beliefs. The determination to access a system is inevitable by the cybercriminal through the use of malicious code (An & Kim, 2018). Organizations must monitor the processes to adapt to the modification of the environment (Checkland, 2012). All four participants instruct their employee to change their passwords, and each department is password protected. It is essential the organization create a weekly awareness for all employees and departments to change their Smart Passwords to eliminate security risks.

Organizations must monitor the processes to adapt to the modification of the environment (Checkland, 2012). All four participants instruct their employee to change their passwords, and each department is password protected. It is essential the organization create a weekly awareness for all employees and departments to change their Smart Passwords to eliminate security risks. 50% of the participants use encryption software for company emails. Only one participant allows very few employees to have

VPN (Virtual Private Network) to connect to the networks to access corporate resources when away from the office. Whereby, two of the participants only allow the owner of the company to use the VPN to access the corporate resources away from the office securely.

Biometric technology, a smart authentication, is a solution to combat usability and provides more security for the organization (Sinno, 2018). All four participants use key fobs and other security devices, such as logins and password protection. While key cards and fob keys are used in businesses today, the expansion of biometrics technology offers security options of fingerprint identification, facial recognition and voice recognition to vascular scanning and heartbeat recognition (Sinno, 2018). In fact, adding biometric fingerprint and voice recognition technology can reduce risks, rather than using password protection (Hill, 2018). The policy creates a different way of thinking and defines parameters to improve the environment by removing a layer of internal scrutiny (Checkland, 2012). Moreover, as technology continues to change, biometrics may offer security to provide authentication for different levels of assurance. As small businesses grow, the importance of security, both internal and external, weighs heavily on business owners, especially in protecting the organization's data, assets, and intellectual property.

One significant aspect of protecting the network is setting up tiers between each department to keep confidential data secure, such as protecting Human Resources and the Accounting Department. Small business owners should consider implementing strategic measures to fight cybercrime due to the increasing presence of individuals using cyberspace and the increase in the number of attacks and victimization (Shamsi, Zeadally, & Nasir, 2016). While every employee uses a login username and password to

gain access to the system, only specific individuals can access specific files and document to perform their work (Brar & Kumar, 2018). For security measures, the organization requires to setup classifications of confidential information to protect the organization from cyber attacks (Brar & Kumar, 2018). Checkland (2012) noted the importance of the correlation between the system and the subsystems of the business environment is essential for the protection of the entire system. To ensure the security of the organization confidential information, IT must assess the system to understand the risks of potential threats (Aminzade, 2018).

Due to many problematical situations, business systems research is interested not only in the thinking process but also the proactive action resulting from the thought process (Checkland, 2012). The course of action taken from the discovery of problems to the recovery process remains essential to maintain and sustain the business from the possibility of failure. The organization's network consists of interacting layers (i.e., tiers) allowing a flow of information through the network, and through username and password distinguishes the specific tier the individual can obtain access (Baycik, Sharkey, & Rainwater, 2018). While the layers provide security within the organization of unwanted users to access secure or confidential information, the cybercriminal can access the system through the use of a botnet (Bertino & Islam, 2017). Once the botnet compromises the computer network, the attacker can remotely control the system through spreading spam, denial of service, stealing personnel confidential information, and other malicious activity (Bertino & Islam, 2017).

Therefore, organizations must recognize breaches continue to update their antivirus software to prevent attacks. All four participants use interacting layers or tiers to secure access between the departments within the organization. 50% of the participants implemented the Accounting Department on a separate network. For security measures of their networks, all four participants have hired an IT Consultant who checks the system. One of the participants uses an IT consultant who monitors the system 24/7. Small businesses have become the new focus of cybercrime. Having proactive managerial strategies can protect the system and create solutions for cybersecurity.

Table 4 contains the participants' statements about their managerial strategies and their business practices.

Table 4

*Theme 3: Managerial Strategies*

| Participant | Participant's Comments |
|---|---|
| P-1 | The organization conducts a tight screening process for new employees and background checks. The organization allows employees to connect to the public internet, guest access with their own devices, but ae not allowed to use their servers. The employees change their passwords weekly. Furthermore, the organization blocks unsecured sites. The organization does not use encryption software. The organization created a network of departmental tiers which require password protection and login scrip between the different departments. The employees cannot connect to the organization's system from home. Employees use a Key Fob to allow employees to enter the organization's building. The organization hired an IT Consultant who checks the system weekly. |
| P-2 | The organization requires the employee, contractors, and vendors to sign a confidentiality and nondisclosure agreement with the |

*(table continues)*

| Participant | Participant's Comments |
|---|---|
| | organization. Each department is password protected and changed regularly. The organization uses encryption software for emails dealing with company business. The organization allows employees to connect to the public internet. The organization expects the blueprints from their customer protected when sent to their vendors. The organization has set up tiers to limit access to the different departments, such as the accounting department and Human Resources. The organization has limited rights to specific information, whereby, the extremely confidential material on a separate network. The organization has limits to access to different departments on specific drives. The organization does have a shared drive that only incorporates worksheet and workbooks that people are working in daily with nonproprietary of specific information, such as data entry. The accounting department is on a separate network. Employees use a Key Fob to allow employees to enter the organization's building. The organization only allows very few employees to have VPN (Virtual Private Network) to connect to the networks to access corporate resources when away from the office. The organization hired an IT Consultant who monitors the system 24/7. |
| P-3 | The organization conducts a backup of the system daily and feel the system is secure from breach by using their own IT employees and the consultant to oversee the security measures of the system. The organization filters any spam from the internet and feels pretty secure with the performance of their present system. The organization instructs employees to change their password regularly. The organization uses encryption software for company emails. The organization has limits to access to different departments on specific drives using tiers. The Accounting department is on a separate network. Only the owner of the company can use the Virtual Private Network (VPN), allowing to securely connect to the networks to access corporate resources when away from the office. The organization uses an encryption program to provide more security for the receipt of the email or fax. Employees use a Key Fob to allow employees to enter the organization's building. The organization hired an IT Consultant who checks the system weekly. |
| P-4 | The organization departments are password protected. It is set up with the financial institution secure site. The contractors and vendors do not |

*(table continues)*

| Participant | Participant's Comments |
|---|---|
| | have access to the organization's system. The organization intellectual property is held on all their servers and with the two firewalls. The organization uses a business accounting platform for accounts payable, accounts receivable and created different tiers so the different department cannot access different departmental areas. The organization uses an encryption program to provide more security for the receipt of the email or fax. Only the owner of the company can use the Virtual Private Network (VPN), allowing to securely connect to the networks to access corporate resources when away from the office. Employees use a Key Fob to allow employees to enter the organization's building. The Key Fob knows what employee and what time they have entered the building. The organization hired an IT Consultant who checks the system weekly. |

**Theme 4: Assessment and Action**

Globalization and technological advancements remain a concern in the manner in which businesses conduct transactions in present-day society. The existence of cybercrime affects business, economics, and society. Many small businesses realize the reliance on IT for their business practices. They understand the implication of effective IT practices to prevent failure of their systems, and in some cases, failure of the business. Cybercrime cost $315 billion in damages worldwide in 2015 (Weishäupl, Yasasin, & Schryen, 2018).

The importance of sustainability of the organization demands continuous assessment and action of the business practices. Checkland (2012) noted four fundamental factors involved in the system, the environment, and real-world actions. First, the Emergent Properties consist of the core justification for the ideas of the system. Second, Adaptation demands exploration of the complexity of the real-world and existence in the environment. Third, the Process of Inquiry perceives the real-world and

understanding the soft system thinking process. Finally, Defining the Methodology which engages the process of the defined action research and recovery research to validate criteria for a course of action and thinking during the research for positive results. Checkland (2012) noted the ideas of system thinking create an avenue to resolve real-world problems as a practical tool. The impact of cybercrime and potential breaches of small business calls for immediate assessment and action to maintain the sustainability of the business.

Many small businesses realize the importance of expanding their IT budgeting to avoid potential breaches and reduce vulnerabilities through improvements in monitoring their systems. Through investments in spyware detection, anti-malware, and other virus detection software, the organizations implement various security protection technologies to prevent data loss (Weishäupl et al., 2018). However, small business owners realize the difficulty budgeting for IT investments due to the costs third-party financial services, the rise of employee health care plans, and property insurance (Weishäupl et al., 2018). Moreover, with the changing economic environment, the consideration of IT planning and budgeting leads small business of the importance to re-examine the issues of additional investments in their IT protection (Weishäupl et al., 2018). With the rise of cybercrimes, public accounting firms, businesses, and other organizations acknowledge how their data and their clients or customers' data remains safe when stored, moved, and processed (Conteh & Schmick, 2016). Organizations need to understand the system as an adaptive whole, surviving in its environment from change and potential risks (Checkland, 2012). In systems thinking theory, the function of each part, when adequately linked to

one another, needs constant monitoring of each performance through monitoring all parts of the system (Checkland, 2012). Checkland (2012) noted action is vital to confront the changes in its environment and take immediate measures to protect the system. Three of the four participants voiced concern with the costs of budgeting for IT but realize the importance of expanding budgeting for either cybersecurity insurance or hiring an IT expert. The four participants are concerned with their firewalls and multi-server protection. Only two participant uses encryption software in their correspondences to their customer due to the nature of their business.

The number of cyberattacks presented establishes patterns in managerial strategies of business leaders about the preventative measures of cybercrimes to protect intellectual property. Protection of the financial data, assets, intellectual property, and personnel information remain critical for all organizations, understanding no one is immune to cybercrime (Aiken et al., 2016). Phishing enables fee fraud in the online sale environment and theft of intellectual property (Samtani et al., 2017). Small business owners reported that employee theft included cash, materials, goods, and intellectual property Kennedy, 2018). Although the efforts of necessary laws to protect patents and intellectual property exist, smaller businesses tend to use minor innovations to protect their intellectual property (Heikkilä & Lorenz, 2018). Small business experience negative consequences and financial issues from internal cybertheft (Kennedy, 2018).

All four of the participants voiced their concerns about potential employee theft of intellectual property through the methods of downloads of data with the use of a flash drive. The significant content of the intellectual property for all the participants include

plans and drawings of products or blueprints from customers. The organizations feel they need stronger security measures, such as installing software to protect their intellectual property and detection of downloads on the system. Two of the participants expect the contractors and vendors to have high-security measures in place to protect the information sent to their servers and protect the data. While one participant allows the technicians that travel with the blueprints, the organization would like to instill a more secure method of checking the blueprints in/out of the customer's intellectual property. The organizations are considering installing software to protect the intellectual property which detection of downloads on the system. Customers' personnel data, financial data, and intellectual property can cause a company to fail (Cavusoglu, Cavusoglu, Son, & Benbasat, 2015). Checkland (2012) noted if the organization needs to implement changes to the internal environment, such as employee compensation packages, it can protect itself from internal failure. No two employees are alike, and the social phenomena continue to change, creating new adaptations to modify the system and subsystems of the internal environment (Checkland, 2012). Through adaptation and evolution of the system, small business leaders need to monitor their systems using time stamps, security checks, use of flash drives and implement effective software which provides a warning of possible theft.

Many companies use electronic commerce (e-commerce) to conduct business transactions with contractors, vendors, and customers for payments of services rendered, materials purchased, or products sold to the consumer (Kaur, Pathak, Kaur, & Kaur, 2015). The characteristic of the virtual economy as a business activity uses the electronic

banking system for conducting transactions (Kaur et al., 2015). The most efficient strategy for defusing cyberattacks is to use the protective technologies available and resolve issues that may present opportunities for employees, partners, vendors, contractors, and suppliers (Manworren et al., 2016). Systems not only interface with the global environment, but they also interface with each other (Checkland, 2012). For example, in 2013, Target experienced 40 million customers' card numbers and 70 million of individuals' data stolen due to one of the company's refrigeration vendors (Manworren et al., 2016).

Only 50% of the participants demand the contractors and vendors to sign a confidentiality and nondisclosure agreement with the organization due to the nature of their business. Moreover, they are not allowed to connect the organization's network as a security measure. The policy mandates implementation for all employees, business partners, contractors, vendors, and suppliers, along with regular data security audits. Notably, any participants of the sub-systems contribute functionality to the system and its environment (Checkland, 2012). With the uncertainties of It technology, businesses should examine the qualification and the acceptable risk of their contractors, vendor, and suppliers (Mikkelsen & Johnsen, 2018). The business should sign a non-disclosure and confidentiality agreement with its contractor, vendors, and supplies to uphold data integrity and security (Nawawi & Salin, 2018). Therefore, small businesses should expect the same security measures from its business partnerships, as well as its contractors and vendors.

The importance of an Employee Educational Program company-wide could prevent breaches and cyberattack. The training programs should teach employees about major cyber activities, such as phishing, phony emails, and malware intrusions (Brewer, 2016). Security training programs for employees can reduce the possible number of breaches and infection to the network (Bozkus Kahyaoglu & Caliyurt, 2018). The awareness and reporting of cyber incidents by the employees can aid in handling potential breaches (Bozkus Kahyaoglu & Caliyurt, 2018). With sufficient budgeting, The Human Resources Department (HR) and IT department should ensure implementing awareness and educational training for all employees (Nawawi & Salin, 2018). The business should encourage employees to report unusual behavior or prohibited technologies, such as portable hard drives, and suspicious behavior by outside individuals, such as vendors or suppliers (Brewer, 2016). Organizations need to understand the system as an adaptive whole, surviving in its environment from change and potential risks (Checkland, 2012).

Cybersecurity awareness programs and skills training are essential to protect the business from potential cyber attacks and reduce the financial burden on small businesses (Adams & Makramalla, 2015). In attempts to combat breaches, organizations have begun to invest in Security Education Training and Awareness programs (Yoo, Sanders, & Cerveny, 2018). The program addresses employee compliance with security policies, secure user practices, and awareness training, providing assurance to reduce security breaches (Yoo et al., 2018). Security awareness training for employees can reduce the number of breaches from malicious viruses (Bozkus Kahyaoglu & Caliyurt, 2018). All

four of the participants had put thought into budgeting and providing an education program on cybercrime and prevention. Of the four participants, only one provides training for the accounting department. The importance of cybersecurity educational programs offered company-wide instills assurance to combat potential cyber attacks.

Table 5 offers the participants' statements about their business practices and potential changes of security measures through assessment and action.

Table 5

*Theme 4: Assessment and Action*

| Participant | Participant's Comments |
|---|---|
| P-1 | The organization is more concern with the design phase of some of their equipment and ways to protect the designs. The contractors and vendors must sign a confidentiality and nondisclosure agreement with the organization. The organization is concerned with the cost of budgeting for more cyber liability insurance and budgeting for IT security because it is costly. The organization does not have an excellent system to stop an employee to walk out with their intellectual property or a detection program if some employees download a lot of information. The organization has considered installing software to protect their intellectual property, and detection of downloads on the system as the company grows. The organization expects the contractors and vendors to have high-security measures in place to protect the information sent to their servers and protect the data. The organization uses encryption software. The organization is evaluating the cost of purchasing more cyber liability insurance. The organization is becoming more concern with the design phase of some of their equipment and ways to protect the designs. The organization is considering hiring a business security consultant to help with addressing the design of the security system. They want to engage an IT consultant to come in to assess the system and work with the IT department. The organization is interest in hiring an IT expert if in the future they experience a breach to their system. The organization would place more security with their contractors and suppliers in the future, but at this time thinks the business is small and is not vulnerable. However, the organization realizes the importance of more |

*(table continues)*

| Participant | Participant's Comments |
|---|---|
| | security for their IT system. The organization is thinking of implementing an employee awareness program and may implement an employee education program on cybercrime and prevention. |
| P-2 | The organization would like to extend stronger security to protect the customer's blueprints and on-going security with the employees and vendors. The organization expects the contractors and vendors to have high-security measures in place to protect the information sent to their servers and protect the data. The organization would like to implement a system to pinpoint theft of information by an employee with a flash drive. They use an encryption program to send correspondences to customers. They would like to implement a program to limit their access to the system and implement a legal recourse, such as the use of cyber insurance for more protection. The organization does not have an educational program in place but makes employees aware of suspicious emails and to report anything suspicious. The organization feels there is open communication between the staff and employees about suspicious activity. They try to keep them alert to new viruses and potential threats to the system. The organization does provide cybersecurity training for the accounting department. The organization would like to implement a system to pinpoint theft of information by an employee with a flash drive and implement a program to limit their access to the system and implement a legal recourse for more protection. The organization is concerned with the cost of budgeting but realizes the importance of budgeting of IT for the company. The organization is thinking of implementing an employee awareness program and may implement an employee education program on cybercrime and prevention. |
| P-3 | The IT department is planning to provide the organization with stronger security measures to protect their intellectual property. The primary organization concern is back-up due to having multiple servers because of the different departments in the company. Another concern is if their firewalls are up to date and working correctly to protect their system from a potential breach or denial of service. Although the cost of budgeting for IT is a concern, the organization realizes they need to examine a way to expand their budget. The company does not use an encryption program. The organization is looking into creating programming to protect their intellectual property. The organization thinks it would be a good idea to provide a training program and thinks |

*(table continues)*

| Participant | Participant's Comments |
|---|---|
| | it would be a good idea to provide a training program for employees, especially those that conduct the record keeping tasks, financial information, and sales departments employees. |
| P-4 | The organization is concerned with the firewalls needed for a reasonable cost that will eliminate any potential breaches. The organization is discussing updating the security of the intellectual property, but at this time the organization has not experienced any issues. However, the organization may implement a more secure manner of checking in and out of the customer's intellectual property by the technician that travel to perform repairs for the customer. The system for protecting the intellectual property is not reliable. The organization has considered installing software to protect their intellectual property as the company grows. The organization is considering hiring a business security consultant to help with addressing the design of the security system and engage a consultant to come in and assess the system and work with the IT department. The organization has an interest in hiring an IT expert in the future if they experience a breach to their system. The organization is considering placing more security with their contractors and suppliers in the future. They may consider changing the practice of allowing employees to access the internet for personal usage. |

## Applications to Professional Practice

The findings of this study may contribute to the examination and options for small business owners to implement successful managerial strategies to protect their systems from data breaches. The findings were significant for the small business owners to enhance their existing cybersecurity strategy. The study findings include four underlying themes: (a) organizational policies (b) IT structure, (c) managerial strategies, and (d) assessment and action. The first significant contribution of the research encompassed professional practices of the business and the organizational policies enact for the rules and policies the employees follow in the workplace. An added value to the business

includes the organization focuses on the people, positions, or practices (Glaister, Karacay, Demirbag, & Tatoglu, 2018). The practices associated with the performance of the business, ultimately rely on enacting policies to plan for the future and ensure the stability of the organization (Glaister et al., 2018). With the onset of cybercrime, the importance of managerial strategies to combat cybercrime and potential breaches require implementation of effective organizational policies. Virtual environments make it challenging due to day-to-day informal interactions and nonverbal communications, which may be lost in web-based communications, relying on building and sustaining trust (Ford et al., 2017). The organization recognizes their responsibility in providing clearly defined policies and the mission of the business to instill trust among the employees (Ford et al., 2017). If the small business addresses cybersecurity strategies with the employees, the small business can provide policies to protect and maintain the sustainability of the organization. The organization must provide each employee with the understanding of their performance and duties to prevent potential breaches.

The second contribution to enhance the reliability of the small business is the IT structure. All organizations rely on technology to conduct their business. Firewalls include filtering rule to implement network segments or tiers between different departments according to application control policies (Tsuchiya et al., 2018). The challenge for small businesses encompasses the concepts of cybersecurity, fighting cybercriminals from disrupting their system with malicious code. The mitigated risks that threaten the organization's firewall(s) include malware, viruses, botnets, and worms, disrupting the system and causing denial of services (Bertino & Islam, 2017). While the

business' firewalls can detect and prevent malware from penetrating the network, a hacker can use botnets consisting of malware to enter holes in the firewall (Cambou, Flikkema, Palmer, Telesca, & Philabaum, 2018). Businesses around the globe use technology to process, store, and transfer information when buying products or services, involving financial transactions in a matter of seconds (Lee & Lee, 2015). The biggest concern for companies is the capability to protect their data and financial assets from potential security risks, including the use of mobile devices and tablets (Romanosky, 2016). Moreover, cybercriminals sophistication of creating new malicious code creates a continuous challenge for small businesses to update their security defenses (Bozkus Kahyaoglu & Caliyurt, 2018).

Modern System-on-Chip (SoC) design integrates billions of transistors on to a single silicon chip, consist of various components such as microprocessors, hardware accelerators, memories, and input/output devices (Ray, Peeters, Tehranipoor & Bhunia, 2018). The SoC powers several devices, such as computer systems, smartphones, robots, automobiles, and electronic medical devices (Ray et al., 2018). The security assurance of modern computers is challenging due to the architecture of the design and preserving the integrity of the system (Ray et al., 2018). The challenge of cybersecurity persists the same between the hardware and the software of the system, causing organizations to re-think the structure of their system (Ammar, Russello, & Crispo, 2018). It is essential to choose the best software and ensure that everyone in the organization is using current releases and fixing discovered problems (McGraw, 2018).

The third contribution to provide security of the organization's data, assets, and intellectual property is the managerial strategies the small business requires to combat cybercrime and stop potential breaches. Small businesses should demand employees to participate in a non-risk policy, aiding in the elimination of carelessness, negligence, or mishaps to eliminate the possibility of employee fraud (Padayachee, 2016). Cybercrime affects business, Governments, economic resources, and society. One of the significant attacks recently was Ransomware. Small businesses should implement a response plan for cyberattacks (Hawkins, 2018). Businesses need to screen new employees and monitor their system to prevent individuals that may go beyond fulfilling their assigned responsibilities (BaMaung et al., 2018). Along with screening employees, the small business must ensure all employee follow a rigorous security policy and keep the employees informed of new malicious code and malware. Security threats include opening infected emails, visiting internet shopping sites, downloading infected files, and internet banking (Williams et al., 2018). The primary concern of internal technological protection strategies includes the employees, monitoring system, raising employee awareness, mobile devices security, and employing rigorous subcontracting processes (Conteh & Schmick, 2016). Security training programs for employees can reduce the possible number of breaches and infection to the network (Bozkus Kahyaoglu & Caliyurt, 2018). The small business should provide an employee awareness program to instruct employees on understanding potential threats and breaches. The course of action taken from the discovery of problems to the recovery process remains essential to maintain and sustain the business from the possibility of failure.

The fourth contribution to provide sufficient security measures for potential breaches includes assessment and action. Hawkins (2018) noted the stages of an effective response plan includes assessing the situation, locate the impact, action to attack, and analyze ways to improve the system. Because of the many problematical situations, business systems research is interested not only in the thinking process but also the proactive action resulting from the thought process (Checkland, 2012). The small business must maintain a level of performance mandates implementing assessment and action to maintain resilience to prevent breaches (Rothrock, Kaplan, & Van Der Oord, 2018). Many small businesses realize the importance of expanding their IT budgeting to avoid potential breaches and reduce vulnerabilities through improvements in monitoring their systems. Through investments in spyware detection, anti-malware, and other virus detection software, the organizations implement various security protection technologies to prevent data loss (Weishäupl et al., 2018). Moreover, with the changing economic environment, the consideration of IT planning and budgeting leads small business of the importance to re-examine the issues of additional investments in their IT protection (Weishäupl et al., 2018). As advancements and reliance on technology continue to encounter business and society, small businesses need to recognize the social environments and maintain protective security measures. The importance of sustainability of the organization demands continuous assessment and action of the business practices.

## Implications for Social Change

Cybercriminals create sites to buy and sell stolen data, contribute access to infected computers, and to write tools for the theft of data to distribute cash flow for the criminals (Hawkins, 2018). The cybercrime costs organizations and society billions of dollars annually due to the vulnerability of networks, lack of strategies, operational measures for prevention, and efficiently tackling cyberattacks (Ammar et al., 2018). Small businesses owners often overlook vulnerabilities of their network (Holt et al., 2016). Vulnerable networks may result in cybercriminals targeting the organization for theft of vital information (Weishäupl et al., 2018). The challenge for businesses encompass the concepts of cybersecurity, fighting cybercriminals from disrupting their system with malicious code. The mitigated risks that threaten the organization's firewall(s) include malware, viruses, botnets, and worms, disrupting the system and causing DoS (Bertino & Islam, 2017). While the business' firewalls can detect and prevent malware from penetrating the network, a hacker can use botnets consisting of malware to enter holes in the firewall (Cambou et al., 2018). Businesses around the globe use technology to process, store, and transfer information when buying products or services, involving financial transactions in a matter of seconds (Lee & Lee, 2015). The theft of vital data may lead to severe consequences for the survival of the small business (Aiken et al., 2016). Moreover, cybercriminals sophistication of creating new malicious code creates a continuous challenge for small businesses to update their security defenses (Bozkus Kahyaoglu & Caliyurt, 2018).

The implications for social change include the elimination or reduction of cybercrimes, theft of confidential data and assets, protection of customers' information in the business' networks, and prevention of future breaches through the implementation of effective managerial strategies to protect all individuals in society (Adhikari & Panda, 2018). The increased volume of people using cyberspace includes individuals for personal, business, and legal transactions on a global level (Eddolls, 2016). In 2013, cyberattack cost the world economies between $300 billion to $1 trillion (Aiken et al., 2016). While the business' firewalls can detect and prevent malware from penetrating the network, hackers can use malware of phishing to enter holes in the firewall (Cambou et al., 2018). Cybersecurity threats include opening infected emails, visiting internet shopping sites, downloading infected files, and internet banking (Williams et al., 2018).

The increase in online shopping, banking, and social media with the use of information technology, mandates a secure internet environment to protect viable information from exposure to cybercrimes (An & Kim, 2018). Small businesses should protect their network, not only for the security of their system but also the well-being of its customers (Cambou et al., 2018). It is critical to provide secure online services to a business' customers to instill gaining their trust in the organization (Plachkinova & Maurer, 2018). As small businesses ensure they remain competitive and meet customer demand, an increase in cybersecurity is a foremost concern to protect the customer (Cambou, 2018). If small businesses provide cybersecurity measures of their systems, cybercriminal may lose the battle of infiltrating their networks, thereby, protecting their

customers, reduce economic strain, and achieve sustainability through the confidence of society.

## Recommendations for Action

Small businesses should implement cybersecurity policies to prevent breaches into their systems. The organizations recognize their responsibility in providing clearly defined policies and the mission of the business to instill trust among the employees (Ford et al., 2017). The biggest concern for companies is the capability to protect their data and financial assets from potential security risks, including the use of mobile devices and tablets (Romanosky, 2016). Small business should instill a policy of not allowing the employees to connect their personally owned mobile devices to the organization's network, laptops, tablets, or any other company-owned device. The connections could cause a severe infection of the organization's network. Furthermore, employees should not be allowed to connect their devices to the network and not be allowed to access the internet through the company's network.

Small business should train employees continually to recognize potential breaches, inform them of new viruses, and cybercriminals new tactic used for potential attacks. Small businesses should implement a response plan for cyber attacks (Hawkins, 2018). Security threats include opening infected emails, visiting internet shopping sites, downloading infected files, and internet banking (Williams et al., 2018). Security training programs for employees can reduce the possible number of breaches and infection of the organization's network. The small businesses commitment to fighting

cybercrime not only begins with cybersecurity policies, but also the education of their employees, company-wide.

Most small businesses do not employ a full-time security officer for their company, nor do they budget the funds necessary to adopt an adequate security plan. The challenge of security persists the same between the hardware and the software of the system, causing organizations to re-think the structure of their system (Ammar et al., 2018). However, small businesses can design a simple security network, and as the company continues to grow, they can expand their network from the basics of security measures. Small businesses should implement the following procedures to protect their network.

- Back up critical data: The small business should backup all data daily including any data that is confidential and critical for business. The data should be kept in more than one location in case of a breach. I recommend a removable hard drive or a separate network, not connected to the internet.
- Keep track of devices: Small business should protect departmental workstations, especially those with crucial data. All mobile devices, laptops require constant monitoring and deletion of crucial information, and any stolen or lost device requires deactivation.
- Have an effective data recovery plan: Make sure the employees know how to retrieve data if backups are required. If a breach occurs, the employees must reach the data to keep the business running.

- Update all security software: All the software and programs used should be kept up to date. The new updates of software often have improved security measures to protect the data further. If updates, not performed daily, security issues could cause the software to malfunction, risking the loss of data and critical work, leaving the system vulnerable to potential breaches. The only way a small business can protect themselves from cybercrime is constant proactive measures.
- Take advantage of new business malware, spyware and firewall software programs: The small business should mandate a policy for each machine used in the company's business, including laptops, tablets, and cell phones. Each device requires up-to-date installed malware, spyware, and firewall software to help eliminate threats before they become problematic. I recommend the following useful software for small businesses: Malwarebytes anti-malware for business (Kleczynski, 2018), Spybot Search and Destroy business edition (Safer-Networking Ltd., 2018), and Sophos virus removal tool for business (Sophos Ltd., 2018).
- Software Reconfiguration: Application settings may need to be changed to support security policy changes or to achieve compliance with the existing policy.

Finally, small businesses should continue to monitor their system through assessment and actions to prevent potential breaches to their system. Small businesses should implement a response plan for cyber attacks (Hawkins, 2018). The small business

must maintain a level of performance mandates implementing assessment and action to maintain resilience to prevent breaches (Rothrock et al., 2018). The importance of sustainability of the organization demands continuous assessment and action of the business practices as they pertain to their network.

## Recommendations for Further Research

The advancement of technology affects small to large businesses. The contribution of this study provides information a small business may use to provide security measures to combat a breach. Regardless of the size of the organization, managerial strategies to protect the data, assets, and intellectual property is essential for potential cyberattacks. Small businesses should implement a response plan to prevent cyberattacks (Hawkins, 2018).

While I reached saturation with four participants, one limitation of this study exists on the number of employees (i.e., 66-180) of the small manufacturing businesses. The results of the study may provide managerial strategies to combat breaches to all size organizations. The state of Wisconsin is the second highest manufacturing concentration of all states in the United States, with more than 9,200 manufacturing companies (WEDC, 2016). Southeastern Wisconsin ranks third in the number of small manufacturing businesses (SBA, 2017). Justifying the population demonstrates saturation within the dataset (Gentles et al., 2015). While the information is significant in obtaining consistent findings in the Midwest, the study results may differ in other regions of the United States.

The study could obtain the information for the study through conducting a statewide online survey to obtain potential participant. However, although the results of conduction an open-ended survey may result in an abundance of participants, interviewing an individual in an open-ended interview produces more information-rich data through examination of body language or observing the participant's reluctance of providing more information. The process of the face-to-face interview provides visual clues, such as the loss of nonverbal data, contextual data, and distortion of verbal data (Goodman-Delahunty et al., 2014). The future researchers could obtain a database to examine countries around the globe who have experienced cybercrime. The information provided by the different countries could offer a global view of the managerial strategies used to combat potential breaches. The importance of the data may provide other managerial strategies for the increase of cybercrime.

The final assumption that small business owners may have limited knowledge of cybersecurity and the strategies they use to prevent breaches to their network. In this study, the business owner's responses provided recommendations for future action to prevent cybercrime and protect their network. Extending the study to interviewing the IT manager may offer more information and additional insight.

## Reflections

I conduct the interviews in a natural setting chosen by the participants which provided an environment in which they were comfortable in sharing information. It was easy to expand the questions in order to gain optimal information. The comfort level of the participants changed as exhibited by their body language when they did not want to

share more information. As the discussion continued with the participants, they made notes regarding specific topics of the conversation.

I obtained 90 small manufacturing businesses containing the owners' name, email address, location, and the number of employees from the U.S. Small Business Administration online database, using the classification codes for manufacturing companies. My search method to obtain small manufacturing owners provided 30 potential participants. However, many were not willing to participate in a face-to-face interview. I determined an online questionnaire would not yield the same results. However, I feel the face-to-face interview provided a better avenue to obtain knowledgeable and substantial data.

The participants of this study provided substantial information, illustrating effective strategies to protect their networks and prevent breaches. However, the small businesses must also implement employee training programs to train their employees to recognize cybercriminal tactics. Additionally, the organizations need to continuously update the software to combat the constant updates of malicious codes and tactics used by the cybercriminals to infiltrate the system. Cybersecurity protects customers and is necessary for the sustainability of the organization.

## Conclusion

Cybercriminals create sites to buy and sell stolen data, contribute access to infected computers, and sell writing tools for the theft of data, distributing cash flow for the criminals. These activities cost organizations and society billions of dollars annually due to the vulnerability of networks, lack of strategies, operational measures for

prevention, and effective measure to stop cyberattacks. For small manufacturing businesses, the importance of security strategies is crucial due to the ability of the Black Hat Community, malware developers, and new techniques developed by hackers to steal and sell information. Cybercriminals who devote enough time and resources to invade a company's network can steal an enormous amount of valuable information. Once the cybercriminal obtains an individual's personal information, such as name, address, date of birth and social security number, they apply the information to commit identity theft and sell the information to other cybercriminals. Small businesses should recognize the severity of cyberattacks and never underestimate the abilities of the cybercriminal and the potential of experiencing a breach of their network.

The estimated worldwide losses due to cybercrime cost billions of dollars annually, affecting governments, business organizations, and the public. The social impact of cybercrimes can cause economic disruptions, consumer trust, and disruption of productivity in business organizations. The challenge for businesses, governments, individuals, national security, and security of the infrastructure, and the economy is securing cyberspace. The increase in online shopping, banking, and social media with the use of information technology, mandates a secure internet environment to protect viable information from exposure to cybercrimes. Many small businesses must fight cybercrime to secure their organizations with proactive protection against cyberattacks and prevent or reduce resultant recovery costs. Through the exploration of risk factors, small business owners can implement new strategies, such as re-examining their

organizational policies, IT structure, managerial strategies, and assessment and action to reduce vulnerabilities through to protect their networks.

Small business should recognize their responsibility in providing clearly defined policies and the mission of the business to maintain its sustainability. Small businesses should instill an organizational policy, requiring all employees to sign a Confidentiality Agreement and provide cybersecurity awareness programs to help prevent and recognize potential cyberattacks. Many small businesses lack effective training programs for all employees, company-wide. Cybersecurity training enables all employee to recognize and report potential cyberattacks and breaches. Through significant budgeting, the organization could provide a training program with the aid of HR and IT. The whole organization needs to understand the potential threats and procedures to a cyberattack and create an atmosphere of assurance to reduce security breaches. Through the exploration of risk factors, small business owners can implement new strategies and processes to reduce vulnerabilities through assessment and action to protect their networks.

The primary threats to businesses include denial of service attacks and data security breaches. Therefore, organizations must recognize breaches and implement secure firewalls and continue to update their antivirus software to prevent attacks. It is crucial to run security checks and conduct a system backup daily. The most critical activities small businesses require of their IT departments is the process of monitoring all traffic in and out of the network via the internet or portable device. Due to limited IT budgets, small businesses lack the funding for extensive cybersecurity for the protection of the organization's mainframe and security of organization' sensitive data. The

organization must demand consistent monitoring of their network defense procedures and protocols as an operational priority. Through the exploration of risk factors, small business owners can implement new strategies and processes to reduce vulnerabilities through assessment and action to protect their networks. For the protection of their network, small business should back up critical information daily, keep track of all company devices, create an effective data recovery plan, update all security software, continue to research all new business malware, spyware, and firewall software programs, and continually educate its employees.

With globalization on the rise, even small businesses conduct transactions worldwide through the usages of information technology, leaving them vulnerable to the intrusion of their network. Small businesses require investment and budgeting in managerial strategies for prevention and strategic risk management to combat intrusions and strengthen their protection against the cybercriminals and potential breaches. Increased cybersecurity strategies are necessary to protect an organization's financial assets, data, and intellectual property. Therefore, small business owners need to implement managerial strategies to prevent breaches of their network and potential cybercrime attacks. Maintaining a level of performance mandates implementing protection the business needs to maintain resilience to prevent breaches for the organization's financial health. Managerial strategies for the company's financial health is to engage the entire organization concerning cybersecurity issue. Organizational resilience is about operating the business while fighting back and recovering. Maintaining the level of performance of the small business requires the ability to measure

an organization's digital resilience to maintain its financial health. The small business must maintain its goals of implementing effective strategies to protect partners, contractors, vendors, consumers, and society from the reaches of the cybercriminals to maintain the sustainability of the organization.

# References

Adams, K. M., Hester, P. T., Bradley, J. M., Meyers, T. J., & Keating, C. B. (2014). Systems theory as the foundation for understanding systems. *Systems Engineering, 17,* 112-123. doi:10.1002/sys.21255

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review, 2015*(1), 5-14. Retrieved from http://timreview.ca

Adhikari, K., & Panda, R. K. (2018). Users' information privacy concerns and privacy protection behaviors in social networks. *Journal of Global Marketing*, *31*, 96-110. doi:10.1080/08911762.2017.1412552

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*(4), 373-391. doi:10.1080/21582041.2015.1117648

Alazab, M. (2015). Profiling and classifying the behavior of malicious codes. *Journal of Systems and Software*, *100*, 91-102. doi:10.1016/j.jss.2014.10.031

Alkhateeb, S. (2016). Cyber crimes. *International Journal of Scientific & Engineering Research*, *7*(4), 918-929. Retrieved from http://www.ijser.org

Alsharo, M., Gregg, D., & Ramirez, R. (2017). Virtual team effectiveness: The role of knowledge sharing and trust. *Information & Management*, *54*, 479-490. doi:10.1016/j.im.2016.10.005

Aminzade, M. (2018). Confidentiality, integrity and availability–finding a balanced IT framework. *Network Security*, *2018*(5), 9-11. doi:10.1016/S1353-4858(18)30043-6

An, J., & Kim, H. W. (2018). A data analytics approach to the cybercrime underground economy. *IEEE Access*, *2018*, 26636-26652. doi:10.1109/ACCESS.2018.2831667

Arief, B., & Adzmi, M. A. B. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 2--defenders and victims. *IEEE Security & Privacy*, *13*(2), 84-88. doi:10.1109/MSP.2015.44

Arora, B. (2016). Exploring and analyzing internet crimes and their behaviours. *Perspectives in Science*, *8*, 540-542. doi:10.1016/j.pisc.2016.06.014

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. doi:10.1109/MSP.2015.110

August, T., August, R., & Hyoduk, S. (2014). Designing user incentives for cybersecurity. *Communications of the ACM*, *57*(11), 43-46. doi:10.1145/2629487

Baldwin, A., Gheyas, I., Ioannidis, C., Pym, D., & Williams, J. (2017). Contagion in cyber security attacks. *Journal of the Operational Research Society*, *68*, 780-791. doi:10.1057/jors.2016.37

BaMaung, D., McIlhatton, D., MacDonald, M., & Beattie, R. (2018). The enemy within? The connection between insider threat and terrorism. *Studies in Conflict & Terrorism*, *41*(2), 133-150. doi:10.1080/1057610X.2016.1249776

Banal, G. & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems, 71*, 62-77. doi:10.1016/j.dss.2015.01.009

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

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management, 51*, 138-151. doi:10.1016/j.im.2013.11.004

Baycik, N. O., Sharkey, T. C., & Rainwater, C. E. (2018). Interdicting layered physical and information flow networks. *IISE Transactions*, *50*, 316-331. doi:10.1080/24725854.2017.1401754

Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. *Qualitative Research, 15*, 219-234. doi:10.1177/1468794112468475

Bertino, E., & Islam, N. (2017). Botnets and internet of things security. *Computer*, *50*(2), 76-79. doi:10.1109/MC.2017.62

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, 33, 360-376. doi:10.1108/MAJ-02-2018-1804

Brar, H. S., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications*, *2018*, 1-11. doi:10.1155/2018/1798659

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

Brinkmann, S. (2016). Methodological breaching experiments: Steps toward theorizing the qualitative interview. *Culture & Psychology*, *22*, 520-533. doi:10.1177/1354067X16650816

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM*, *57*(2) 24-27. doi:10.1145/2556936

Cambou, B., Flikkema, P. G., Palmer, J., Telesca, D., & Philabaum, C. (2018). Can ternary computing improve information assurance?. *Cryptography*, *2*, 1-16. doi:10.3390/cryptography2010006

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A., J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum, 41*, 545-547. doi:10.1188/14.ONF.545.547

Cavana, R. Y., & Forgie, V. E. (2018). Overview and insights from 'Systems education for a sustainable planet'. *Systems, 6(1),*1-5. doi:10.3390/systems6010005

Cavusoglu, H., Cavusoglu, H., Son, J., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management, 52*, 385-400. doi:10.1016/j.im.2014.12.004

Chang, V., Ramachandran, M., Yao, Y., Kuo, Y. H., & Li, C. S. (2016). A resiliency framework for an enterprise cloud. *International Journal of Information Management*, *36*, 155-166. doi:10.1016/j.ijinfomgt.2015.09.008

Chaudhry, P. E. (2017). The looming shadow of illicit trade on the internet. *Business Horizons*, *60*, 77-89. doi:10.1016/j.bushor.2016.09.002

Checkland, P. (2012). Four conditions for serious systems thinking and action. *Systems Research & Behavioral Science, 29,* 465-469. doi:10.1002/sres.2158

Cho, J. Y., & Lee, E. (2014). Reducing confusion about grounded theory and qualitative content analysis: Similarities and differences. *The Qualitative Report, 19*, 1-20. Retrieved from http://nsuworks.nova.edu

Choi, Y., Nam, J., Lee, D., Kim, J., Jung, J., & Won, D. (2014). Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics. *The Scientific World Journal*, *2014*, 1-15. doi:10.1155/2014/281305

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

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

Clough, J. (2015). Towards a common identity? The harmonisation of identity theft laws. *Journal of Financial Crime, 22,* 492-512. doi:10.1108/JFC-11-2014-0056

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

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

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. Retrieved from www.jatit.org

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

Doh, J. P., Lawton, T. C., Rajwani, T., & Paroutis, S. (2014). Why your company may need a chief external officer: Upgrading external affairs can help align strategy and improve competitive advantage. *Organizational Dynamics, 43*, 96-104. doi:10.1016/j.orgdyn.2014.03.003

Drissel, D. (2012). Cyberspatial transformations of society: Applying Durkheimian and Weberian perspectives to the internet. *International Journal of Technology, Knowledge & Society, 8*(3), 71-86. Retrieved from http://techandsoc.com

Dupont, B. (2017). Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale

cybercrime. *Crime, law and social change*, *67*, 97-116. doi:10.1007/s10611-016-9649-z

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

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *Sage Open, 4*(1), 1-10. doi:10.1177/2158244014522633

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

Ford, R. C., Piccolo, R. F., & Ford, L. R. (2017). Strategies for building effective virtual teams: Trust is key. *Business Horizons*, *60*, 25-34. doi:10.1016/j.bushor.2016.08.009

Franke, U. (2017). The cyber insurance market in Sweden. *Computers & Security*, *68*, 130-144. doi:10.1016/j.cose.2017.04.010

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

Gentles, S., Charles, C., Ploeg, J., & McKibbon, K. A. (2015, Nov.). Sampling in qualitative research: Insights from an overview of the methods literature. *Qualitative Report, 20*(11), 1772-1789. Retrieved from http://nsuworks.nova.edu

Glaister, A. J., Karacay, G., Demirbag, M., & Tatoglu, E. (2018). HRM and performance—The role of talent management as a transmission mechanism in an emerging market context. *Human Resource Management Journal*, *28*, 148-166. doi:10.1111/1748-8583.12170

Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, *12*, 741-760. doi:10.1080/15564886.2016.1177766

Goodman-Delahunty, J., Martschuk, N., & Dhami, M. K. (2014). Interviewing high value detainees: Securing cooperation and disclosures. *Applied Cognitive Psychology*, *28*, 883-897. doi:10.1002/acp.3087

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*, 2-16. doi:10.1080/10580530.2015.1117842

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

Hawkins, N. (2018). Resistance, response and recovery. *Computer Fraud & Security*, *2018*(2), 10-13. doi:10.1016/S1361-3723(18)30014-9

Hays, D. G., Wood, C., Dahl, H., & Kirk-Jenkins, A. (2016). Methodological rigor in Journal of Counseling & Development qualitative research articles: A 15-year review. *Journal of Counseling & Development*, *94*, 172-183. doi:10.1002/jcad.12074

Heikkilä, J., & Lorenz, A. (2018). Need for speed? Exploring the relative importance of patents and utility models among German firms. *Economics of Innovation and New Technology, 27*, 80-105. doi:10.1080/10438599.2017.1310794

Helfat, C. E., & Karim, S. (2014). Fit between organization design and organizational routines. *Journal of Organization Design 3*(2), 18-29. doi:10.7146/jod.16738

Henson, M., & Taylor, S. (2014). Memory encryption: A survey of existing techniques. *ACM Computing Surveys, 46*(4), Article #53, 1-26. doi:10.1145/2566673

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

Herley, C. (2014). Security, cybercrime, and scale. *Communications of the ACM, 57*(9)*,* 64-71. doi:10.1145/2654847

Hill, C. (2018). Biometrics becoming must-have for fraud prevention. *Biometric Technology Today*, *2018*(1), 9-11. doi:10.1016/S0969-4765(18)30012-2

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35,* 20-40. doi:10.1080/01639625.2013.822209

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior*, *37*, 353-367. doi: 10.1080/01639625.2015.1026766

Holtfreter, R. E., & Harrington, A. (2014). Will hackers win the battle? *Strategic Finance, 95*(7)*,* 27-34. Retrieved from http://www.imanet.org

Houghton, C., Murphy, K., Shaw, D., & Casey, D. (2015). Qualitative case study data analysis: An example from practice. *Nurse Researcher*, *22*(5), 8-12. doi:10.7748/nr.22.5.8.e1307

Houser, W. (2015). Could what happened to sony happen to us?. *IT Professional*, *17*(2), 54-57. doi:10.1109/MITP.2015.21

Hovav, A. P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Association for Information Systems, 34,* 893-912. Retrieved from http://aisel.aisnet.org/cais

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

Hyman, P. (2013). Cybercrime: It's serious, but exactly how serious? *Communications of the ACM, 56*(3), 18-20. doi:10.1145/2428556.2428563

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy, 5,* 87-88. doi:10.4103/0976-0105.141942

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*, 973-993. doi:10.1016/j.jcss.2014.02.005

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. doi:10.1007/s10693-015-0218-x

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. Retrieved from http://www.ijera.com

Kennedy, J. P. (2018). Asset misappropriation in small businesses. *Journal of Financial Crime*, *25*, 369-383. doi:10.1108/JFC-01-2017-0004

Kihn, L. & Ihantola, E. (2015). Approaches to validation and evaluation in qualitative studies of management accounting. *Qualitative Research in Accounting & Management, 12*, 230-255. doi:10.1109/QRAM-03-2013-0012

Kleczynski, M. (2018). Malwarebytes anti-malware for business [Computer software]. Retrieved from https://www.malwarebytes.com

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

Landau, S. (2014). Summing up. *Communications of the ACM, 57*(11), 37-39. doi:10.1145/2668901

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

Lanz, J. (2014). Cybersecurity governance: The role of the audit committee and the CPA. *CPA Journal*, *84*(11), 6-10. Retrieved from http:// www.cpajournal.com

Lau, P. Y. Y., Tong, J. L. T., Lien, B. Y. H., Hsu, Y. C., & Chong, C. L. (2017). Ethical work climate, employee commitment and proactive customer service performance: Test of the mediating effects of organizational politics. *Journal of Retailing and Consumer Services*, *2017*(35), 20-26. doi:10.1016/j.jretconser.2016.11.004

Lee, I., & Lee, K. (2015). The internet of things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*, 431-440. doi:10.1016/j.bushor.2015.03.008

Leukfeldt, E. (2014). Cybercrime and social ties. *Trends in Organized Crime, 17,* 231-249. doi:10.1007/s12117-014-9229-5

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice, 16,* 473-475. doi:10.1177/1524839915580941

Li, L., Zhang, H., Xia, Y., & Yang, H. (2018). Security estimation under denial-of-service attack with energy constraint. *Neurocomputing*, *2018*(292), 111-120. doi:10.1016/j.neucom.2018.02.086

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

Loosemore, M., & Cheung, E. (2015). Implementing systems thinking to manage risk in public private partnership projects. *International Journal of Project Management, 33,* 1325-1334. doi:10.1016/j.ijproman.2015.02.005

Lu, X., Niyato, D., Privault, N., Jiang, H., & Wang, P. (2018). Managing physical layer security in wireless cellular networks: A cyber insurance approach. *IEEE Journal on Selected Areas in Communications*, (in press). doi:10.1109/JSAC.2018.2825518

Manoj, S. K. A., & Bhaskari, D. L. (2016). Cloud forensics-A framework for investigating cyber attacks in cloud environment. *Procedia Computer Science*, *2016*(85), 149-154. doi:10.1016/j.procs.2016.05.202

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. doi:10.1016/S1353-4858(16)30104-0

Mansfield-Devine, S. (2016). Ransomware: Taking businesses hostage. *Network Security*, *2016*(10), 8-17. doi:10.1016/S1353-4858(16)30096-4

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, *59*, 257-266. doi:10.1016/j.bushor.2016.01.002

Markelj, B., & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications*, *20*, 84-89. doi:10.1016/j.jisa.2014.11.001

Mayer, I. (2015). Qualitative research with a focus on qualitative data analysis. *International Journal of Sales, Retailing & Marketing*, *4*(9), 53-67. Retrieved from http://www.ijsrm.com

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, *30*, 537-542. doi:10.1177/0267659114559116

McGraw, G. (2018). The new killer app for security: Software inventory. *Computer, 51*(2), 60-62. doi:10.1109/MC.2018.1451662

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research, 2*, 1-12. doi:10.1177/2333393615597674

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*(1), 26-37. Retrieved from https://www.abacademies.org

Mikkelsen, O. S., & Johnsen, T. E. (2018). Purchasing involvement in technologically uncertain new product development projects: Challenges and implications. *Journal of Purchasing and Supply Management*, (in press). doi:10.1016/j.pursup.2018.03.003

Moghimi, M., & Varjani, A. Y. (2016). New rule-based phishing detection method. *Expert systems with applications*, *2016*(53), 231-242. doi:10.1016/j.eswa.2016.01.028

Moussa, M. (2015). Monitoring employee behavior through the use of technology and issues of employee privacy in America. *Sage Open*, *5*(2), 1-13. doi:10.1177/2158244015580168

Nadal, K. L., Davidoff, K. C., Davis, L. S., Wong, Y., Marshall, D., & McKenzie, V. (2015). A qualitative approach to intersectional microaggressions: Understanding influences of race, ethnicity, gender, sexuality, and religion. *Qualitative Psychology*, *2*, 147-163. doi:10.1037/qup0000026

Nawawi, A., & Salin, A. S. A. P. (2018). Employee fraud and misconduct: empirical evidence from a telecommunication company. *Information & Computer Security*, *26*, 129-144. doi:10.1108/ICS-07-2017-0046

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

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

Paquet-Clouston, M., Décary-Hétu, D., & Bilodeau, O. (2018). Cybercrime is whose responsibility? A case study of an online behaviour system in crime. *Global Crime*, *19*, 1-21. doi:10.1080/17440572.2017.1411807

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. doi:10.1016/j.compeleceng.2016.04.001

Parker, K. L. (2014). The utility of cyberpower. *Military Review, 92*(3), 26-33. Retrieved from http://militaryreview.army.mil

Percy, W. H., Kostere, K., & Kostere, S. (2015). Generic qualitative research in psychology. *The Qualitative Report*, *20*(2), 76-85. Retrieved from https://nsuworks.nova.edu

Piper, A. (2014). Businesswide cybersecurity. *Internal Auditor, 71*(3), 38-43. Retrieved from https://iaonline.theiia.org

Plachkinova, M., & Maurer, C. (2018). Teaching case: Security breach at Target. *Journal of Information Systems Education*, *29*, 11. Retrived from http://jise.org

Pozzebon, M., Rodriguez, C., & Petrini, M. (2014). Dialogical principles for qualitative inquiry: A nonfoundational path. *International Journal of Qualitative Methods*, *2014*(13), 293–317. doi:10.1177/160940691401300114

Quigley, K., Burns, C., & Stallard, K. (2015). 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, *32*, 108-117. doi:10.1016/j.giq.2015.02.001

Ray, S., Peeters, E., Tehranipoor, M. M., & Bhunia, S. (2018). System-on-chip platform security assurance: Architecture and validation. *Proceedings of the IEEE*, *106*, 21-37. doi:10.1109/JPROC.2017.2714641

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

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

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*(2), 12-15. Retrieved from https://sloanreview.mit.edu

Rousseau, D., & Wilby, J. (2014). Moving from disciplinarity to transdisciplinarity in the service of thrivable systems. *Systems Research & Behavioral Science, 31,* 666-677. doi:10.1002/sres.2314

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. doi:10.1080/07421222.2017.1394049

Safer-Networking Ltd. (2018). Spybot search and destroy: Business user editions [Computer program]. Retrieved from https://www.safer-networking.org

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. doi:10.1080/07421222.2017.1394049

Satterfield, S. L. (2018). *Employee perceptions of effective training strategies* (Doctoral dissertation, Walden University). Retrieved from https://ezp.waldenulibrary.org. (Order no. 10808834).

Schneider, B., González-Romá, V., Ostroff, C., & West, M. A. (2017). Organizational climate and culture: Reflections on the history of the constructs in the Journal of Applied Psychology. *Journal of Applied Psychology*, *102*, 468-482. doi:10.1037/apl0000090

Shabnam, N., Faruk, M. O., & Kamruzzaman, M. (2016). Underlying causes of cyber-criminality and victimization: An empirical study on students. *Social Sciences, 5*(1), 1-6. doi:10.11648/j.ss.20160501.11

Shamsi, J. A., Zeadally, S., & Nasir, Z. (2016). Interventions in cyberspace: Status and trends. *IT Professional*, *18*(1), 18-25. doi:10.1109/MITP.2016.19

Sinno, S. (2018). How risk engines could solve a biometric dilemma. *Biometric Technology Today*, *2018*(5), 9-11. doi:10.1016/S0969-4765(18)30069-9

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. doi:10.1016/j.ijinfomgt.2015.11.009

Sophos Ltd. (2018). Sophos Virus removal tool for business [Computer program]. Retrieved from https://www.sophos.com

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. doi:10.1080/11745398.2014.902292

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

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964-975. doi:10.1016/j.future.2016.11.031

Stockton, P. N., & Golabek-Goldman, M. (2014). Prosecuting cyberterrorists: Applying traditional jurisdictional frameworks to a modern threat. *Stanford Law & Policy Review, 25,* 211-268. Retrieved from https://journals.law.stanford.edu

Taguchi, N. (2018). Description and explanation of pragmatic development: Quantitative, qualitative, and mixed methods research. *System, 2018* (in press), 1-10. doi:10.1016/j.system.2018.03.010

Tam, K., Feizollah, A., Anuar, N. B., Salleh, R., & Cavallaro, L. (2017). The evolution of android malware and android analysis techniques. *ACM Computing Surveys*, *49*(4), Article #76, 1-76. doi:10.1145/3017427

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. doi:10.1016/j.dss.2016.05.005

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave?. *Justice Quarterly*, *33*, 890-911. doi:10.1080/07418825.2014.994658

Thomas, D. R. (2017). Feedback from research participants: Are member checks useful in qualitative research?. *Qualitative Research in Psychology*, *14*, 23-41. doi:10.1080/14780887.2016.1219435

Thornton-Trump, I. (2018). Malicious attacks and actors: An examination of the modern cyber criminal. *EDPACS*, *57*(1), 17-23. doi:10.1080/07366981.2018.1432180

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

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

Tran, V. T., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of clinical epidemiology*, *2016*(80), 88-96. doi:10.1016/j.jclinepi.2016.07.014Upton, D. M., & Creese, S. (2014). The danger from within. *Harvard Business Review, 92*(9), 94-101. Retrieved from www.hbr.org

Tsuchiya, A., Fraile, F., Koshijima, I., Ortiz, A., & Poler, R. (2018). Software defined networking firewall for industry 4.0 manufacturing systems. *Journal of Industrial Engineering and Management*, *11*, 318-333. doi:10.3926/jiem.2534

United States Department of Health and Human Services (HHS). (1979). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research*. Retrieved from Department of Health, Education, and Welfare website: http://www.hhs.gov

U.S. Small Business Association. (2017). *Dynamic small business search.* Retrieved from SBA website: http://dsbs.sba.gov/dsbs/search/dsp_dsbs.cfm

U.S. Small Business Association. (2017). *Resource guide for small businesses: U.S. small business administration, Wisconsin.* Retrieved from SBA website: https://www.sba.gov/offices/district/wi/milwaukee

U.S. Small Business Association (SBA). (2017). *Summary of size standards by industry sector*. Retrieved from SBA website: https://www.sba.gov

U.S. Small Business Association (SBA). (2017). *Table of Small Business Size Standards: Matched to North American Industry Classification System Codes*. Retrieved from SBA website: https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf

Valentinov, V. (2014). The complexity-sustainability trade-off in Niklas Luhmann's social systems theory. *Systems Research & Behavioral Science, 31,* 14-22. doi:10.1002/sres.2146

Vande Putte, D., & Verhelst, M. (2014). Cyber crime: Can a standard risk analysis help in the challenges facing business continuity managers?. *Journal of Business Continuity & Emergency Planning*, *7*, 126-137. Retrieved from http://www.henrystewartpublications.com

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. doi:10.1002/bse.1804

Von Bertalanffy, L. (2008). An outline of general system theory. *Emergence: Complexity*

*& Organization, 1,* 134-165 doi:10.1093/bjps/I.2.134

Waggett, P. (2016). Risk-based authentication: Biometrics' brave new world. *Biometric Technology Today*, *2016*(6), 5-7. doi:10.1016/S0969-4765(16)30106-0

Waldrop, M. M. (2016). How to hack the hackers: The human side of cybercrime. *Nature*, *533*, 167-167. doi:10.1038/533164a

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology, 22,* 45-63. doi:10.1080/13600860801924907

Wang, B. & Li, J. (2014). Study on model of factor analysis applied in the risk management of electronic commerce enterprise. *International Journal of u-and e-Service, Science and Technology*, *7*(5), 263-270. doi:10.14257/ijunnesst.2014.7.5.23

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

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2018). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior*, (in press), 1-13. doi:10.1080/01639625.2018.1461786

Wisconsin Economic Development Corporation (WEDC) (2016). Industry leadership drives manufacturing advancements in Wisconsin. *Manufacturing Industry Profile* (INWIBIZ Publication No. 855). Retrieved from

http://inwisconsin.com/wp-content/uploads/2016/04/Manufacturing-Industry-Profile.pdf

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

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

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

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, *2018*(108), 107-118. doi:10.1016/j.dss.2018.02.009

Young, D., Lopez Jr, J., 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. doi:10.1016/j.ijcip.2016.04.001

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

Zenko, Z., Rosi, B., Mulej, M., Mlakar, T., & Mulej, N. (2013). General systems theory completed up by dialectical systems theory. *Systems Research & Behavioral Science*, *30*, 637-645. doi:10.1002/sres.2234

Zhurin, S. I. (2015). Comprehensiveness of response to internal cyber-threat and selection of methods to identify the insider. *Journal of ICT Research and Applications*, *8*, 251-269. doi:10.5614/itbj.ict.res.appl.2015.8.3.5

# Appendix A: Information Search Form

Owner's Name:

Organization Name:

Address:

Phone:

Email:

Sole proprietorship?

Number of Employees:

**If "I Consent":**

Interview Date and Time:

Appendix B: Email Invitation for Potential Participants

**RE: [RSVP] Are you willing to participate in a doctoral research project…**

Salutation:

My name is Doreen Maahs, and I am a doctoral candidate at Walden University. At this time, I am preparing my doctoral study on the topic of determining small manufacturing business managerial strategies used to prevent data breaches and combat cybercrime. As part of the doctoral study, I plan to conduct research necessary to answer my study research question of "What are the key managerial strategies small manufacturing business owners apply to combat vulnerabilities to cybercrimes for the protection of financial assets and data?" The purpose of this study is to explore the managerial strategies of small manufacturing business' owners to protect their financial assets, data, and intellectual property. I plan to explore the managerial strategies implemented by 6-12 small manufacturing business owners who successfully prevent cybercrimes in the midwestern region of the United States.

Cybercrime affects businesses, society, and the economy. It is estimated worldwide losses due to cybercrime cost approximately $1 trillion annually, affecting governments, business organizations, and the public. Roughly 86% of the most common cybercrime cases reported affect small to medium-sized enterprises. Researchers have found that security risks not only rely on its protection, but also the protection of its business partners, vendors, contractors, suppliers, and customers. This study can provide other small businesses with information to improve their strategies and prevent breaches and cybercrime.

**Can you please help?**

I have attached the *Informed Consent Form* to providing all the information that pertains to the study. Please indicate your consent by replying to the *Informed Consent Form* via email by providing the words, "I consent."

Many thanks in advance for your consideration.

Kind regards,

Doreen Maahs
Walden University Doctoral Candidate

## Appendix C: The Six Open-ended Interview Questions

The method of collection of data from the study includes six open-ended questions in a face-to-face interview with six small manufacturing business owners to gather the data:

1. What are your major concerns regarding managerial strategies to protect your systems from data breaches?
2. What are the managerial strategies you use to protect your financial assets, data, and intellectual property of possible cybertheft or breaches?
3. What internal and external managerial strategies has your organization developed and implemented to prevent theft or loss of financial assets, data, and intellectual property from cybercrime?
4. How are managerial strategies to protect your systems from data breaches engaged by employees?
5. What managerial strategies does your organization use to measure the effectiveness of the cybercrime prevention?
6. What additional information can you provide pertaining to managerial strategies to prevent breaches and cybercrime?

**Please note:** The researcher plans to take notes of observations during the interview.

## Appendix D: The Interview Process Protocol

The semi-structured face-to-face interview includes the following process:

1. Introduction of the research topic as stated in the "Informed Consent" form and provide a copy of the form;
2. Presentation of the recording device to the participant;
3. Assure the participant of confidentiality;
4. Confirm the interview process will take no longer than 60 minutes;
5. Encourage the participant to answer the questions to their best ability;
6. Note any expanding questions for future interviews to maintain reliability and validity in collection of data;
7. Note any observations during the interview;
8. Thank each participant at the end of the interview;
9. I will inform the participant that I will transcribe the interview from the audio recording and email them a one to two-page summary of the interview in a process call member checking, where they approve the data collected for analysis;
10. I will schedule a follow-up interview via telephone call if necessary to verify the data collected is accurate unless I receive an email from you that the verifying the summary is correct; and
11. Collect the organization's documentation of managerial procedures to prevent breaches, if available.