2016

Determining Small Business Cybersecurity Strategies to Prevent Data Breaches

Jennifer Saber
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Jennifer Saber

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. Jaime Klein, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Greg Banks, Committee Member, Doctor of Business Administration Faculty

Dr. Richard Johnson, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2016

Abstract

Determining Small Business Cybersecurity Strategies to Prevent Data Breaches

by

Jennifer A. Saber

MBA, University of Massachusetts, 2003

BS, Newbury College, 1999

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

October 2016

Abstract

Cybercrime is one of the quickest growing areas of criminality. Criminals abuse the speed, accessibility, and privacy of the Internet to commit diverse crimes involving data and identity theft that cause severe damage to victims worldwide. Many small businesses do not have the financial and technological means to protect their systems from cyberattack, making them vulnerable to data breaches. This exploratory multiple case study, grounded in systems thinking theory and routine activities theory, encompassed an investigation of cybersecurity strategies used by 5 small business leaders in Middlesex County, Massachusetts. The data collection process involved open-ended online questionnaires, semistructured face-to-face interviews, and review of company documents. Based on methodological triangulation of the data sources and inductive analysis, 3 emergent themes identified are policy, training, and technology. Key findings include having a specific goal and tactical approach when creating small business cybersecurity strategies and arming employees with cybersecurity training to increase their awareness of security compliance. Recommendations include small business use of cloud computing to remove the burden of protecting data on their own, thus making it unnecessary to house corporate servers. The study has implications for positive social change because small business leaders may apply the findings to decrease personal information leakage, resulting from data breaches, which affects the livelihood of individuals or companies if disclosure of their data occurs.

Determining Small Business Cybersecurity Strategies to Prevent Data Breaches

by

Jennifer A. Saber

MBA, University of Massachusetts, 2003

BS, Newbury College, 1999

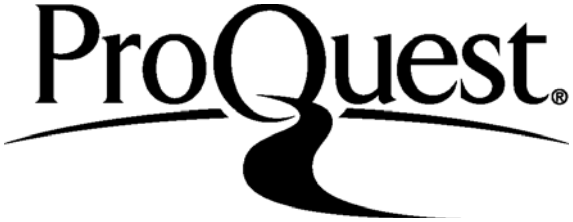
Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

October 2016



Dedication

To my husband, Shaun, you are my partner in life and are always supportive. Even though you keep asking me how much longer it is until the end of my schooling, you are always there to lend an ear when I am in full-stress mode. Your enduring love and encouragement have made it possible for me to take this doctoral journey.

Acknowledgments

From the beginning of my collegiate career, I have worked full-time during the day and attended classes at night. It took me 10 years to complete my Master of Business Administration degree, which was possible in part through the guidance and support of past and present professors. Attending college at night helped me to gain a great appreciation of fellow students who are in the same position. Specific to my Walden experience, I would like to acknowledge fellow students Annie Roman and Lee Marlais. The three of us made a bond at our first residency that I trust will last a lifetime.

Dr. Ron McFarland, my Walden chair, has been a driving force for me to complete my doctoral study. If it were not for his persistent pressure to keep forging ahead, I fear I might not have been able to get through this process. When Dr. McFarland took a leave of absence, my new chair assignment became Dr. Jaime Klein. Dr. Klein and I became kindred spirits. She has the same drive and energy as I do to get the job done. I am forever thankful to have met and worked with Dr. Klein; she was always there to give me the push I needed to complete this study.

Dr. Gregory Banks, my Walden second committee member, has always provided me with quick and valuable feedback on my doctoral study. I value all of his reviews of my study, which allowed me to make the necessary changes to continue the journey. Dr. Richard Johnson, my Walden University research reviewer, was instrumental in providing feedback for me to transform my doctoral study from good to great. He is a very thorough reviewer, for which I am grateful.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Technological advances have brought an onslaught of cybercrime, wherein criminals attempt to victimize firms or individuals through theft of personal information (Anandarajan, D'Ovidio, & Jenkins, 2013). Cybercriminals have the ability to penetrate mobile devices, computers, bank accounts, and credit cards (Holt, 2013). Cybercrime has the potential to upset the confidence that consumers, professionals, and governments have toward an organization (Vande Putte & Verhelst, 2013). Determining effective cybersecurity strategies for small businesses may lead to the protection of their systems from data breaches.

Background of the Problem

The introduction of the Internet in the early 1990s provided a new way for organizations to do business. The Internet enabled multiple categories of public and private sector establishments to run their firms using online electronic data interactions (Bernik, 2014). Danger arose when disgruntled employees executed cybercrimes, physically damaging their employers' computers (Neghina & Scarlat, 2013). Writing in 2013, Flowers, Zeadally, and Murray classified cybercrimes in two categories: (a) those that involved targeted computer devices or networks and (b) those that involved the use of a computer to target private networks.

Cybercrime has affected all areas of society, from government and business to the public sector (Hyman, 2013). For small businesses, technology has enhanced operational efficiency and increased profitability (Chao & Chandra, 2012). The Internet offered small

businesses means for competing in a larger market, which made small businesses more reliant on technology to store their data (Ghobakhloo & Hong Tang, 2013).

Small firms do not have the resources, finances, and security infrastructure that larger companies possess (Harris & Patten, 2014). Small business personnel may assume that their technology is safe, as they do not receive notifications about attacks or threats, which is why many small business attacks remain undetected (Harsch, Idler, & Thurner, 2014). Many small businesses lack awareness and knowledge about the threats of cyberattacks. This lack of awareness has contributed to the vulnerability of small businesses, suggesting small businesses do not appear to be concerned about their assets (Harsch et al., 2014).

Problem Statement

In the United States, the average cost of enterprise cybercrime attacks is $11.56 million annually (Internet Crime Complaint Center, 2013). American companies spend $5.3 billion yearly to combat cybercrime; these efforts have stopped an estimated 69% of all cyberattacks (Bloomberg Government, 2012). Twenty percent of small companies rely on their security business unit to handle insider attacks, compared with 62% of larger organizations (Pricewaterhouse Coopers, 2014). In a small business, information security and compliance can often be the part-time job of a single individual (Bedwell, 2014). The general business problem is that many small business security resources are scarce or unavailable. The specific business problem is that some small business leaders lack the cybersecurity strategies necessary to protect their systems from data breaches.

Purpose Statement

The purpose of this qualitative exploratory multiple case study was to explore the cybersecurity strategies that small business leaders used to protect their systems from data breaches. The targeted population for this study included five leaders of small companies located in the Middlesex County region of Massachusetts who had successfully implemented cybersecurity strategies to protect their systems from data breaches. The population for this study was appropriate, as researchers have found that the majority of small businesses do not place appropriate investments in cybersecurity (Densham, 2015; Hayes & Bodhani, 2013). The study's implications for positive social change include the potential for decreasing theft of sensitive, protected, or confidential data. Further, implementing cybersecurity strategies in small businesses may reduce the loss of personally identifiable information.

Nature of the Study

Researchers use the qualitative methodology to identify the perspectives of participants (Posey, Roberts, Lowry, & Hightower, 2014). I used the qualitative methodology to explore the cybersecurity strategies that small business leaders used to protect their systems from data breaches. Use of this research method assisted me in the development of themes and concepts acquired from the participants' language and responses to open-ended questions, as recommended by Percy, Kostere, and Kostere (2015). An online questionnaire containing open-ended questions allowed me to identify themes from their responses, as proposed by Graebner, Martin, and Roundy (2012). The qualitative method enabled me to determine the views, opinions, and insights of the

participants and explore their issues, claims, and concerns. The quantitative method was not appropriate for this study, as quantitative researchers gather quantifiable data essential in statistical analysis, and the objective of this study was to achieve a more profound understanding of how reality appears to individuals. Conducting an online questionnaire containing open-ended questions provided participants with the means to preserve their anonymity and supply honest responses, as proposed by Takey and de Carvalho (2015).

Researchers use the qualitative exploratory case study design to investigate particular and complex phenomena from a real-world perspective (Graebner et al., 2012; Yin, 2013). An investigation through an exploratory case study allowed me to conduct probing research, ask *how* or *why* questions, and understand the features of real-life events, as suggested by Yin (2013). Small, Maher, and Kerr (2014) suggested that ethnography entails understanding the cultural behaviors of participants. As it was not necessary to understand the cultural behaviors of the study participants, ethnography was not an appropriate design for this study. Grounded theory would have involved the development of theories upon conducting personal interfaces with small business leaders (Lo, 2014). Developing theories though personal interfaces with participants was not the goal of this study; thus, grounded theory was an inappropriate design. The focus of phenomenological design is on the lived experiences of participants (Cunliffe, 2011). Given that the aim of this study was to obtain information on the cybersecurity strategies small business leaders use to protect their systems from data breaches, the use of phenomenological design was not appropriate, as it would have entailed a focus on lived

experiences. The Delphi technique, as posited by Snape et al. (2014), involves group decision-making development. The development of small business leaders, cybercrime policies, or group consensus was not the goal of this study, thus making the Delphi technique an inappropriate design.

Research Question

The overarching research question for this study was as follows: What cybersecurity strategies do leaders of small businesses implement to protect their systems from data breaches?

Interview Questions

The following interview questions for this qualitative exploratory case study were designed to gain information about effective cybersecurity strategies that protect systems from data breaches:

1. What are your views concerning the importance of cybersecurity strategies to protect systems from data breaches at your small business?
2. What cybersecurity strategies are in place to protect systems from data breaches at your small business?
3. How are cybersecurity strategies to protect systems from data breaches circulated to employees at your small business?
4. What are your views on how employees recognize the importance of cybersecurity strategies for your small business?
5. What do you think is the best way to circulate cybersecurity strategies to employees of your small business?

6. What is the process for employees to report a potential cyber threat to the leader of the small business?
7. How do you respond to internal cyber threats made against the company?
8. How do you respond to external cyber threats made against the company?
9. Has your business experienced internal cyber threats? If yes, can you describe the risk and action taken to mitigate?
10. Has your business experienced external cyber threats? If yes, can you describe the risk and action taken to mitigate?

Conceptual Framework

The focus of this study was the exploration of cybersecurity strategies for small business leaders to improve the protection of their systems from data breaches. Two conceptual frameworks informed this study. Von Bertalanffy's (1972) general systems theory was used to understand the strategies small business leaders need to protect their systems from data breaches, and Cohen and Felson's (1979) routine activities theory was used to address issues that provide the foundation for cybercrime activities.

Von Bertalanffy (1972) introduced general systems theory in 1937, further developed the theory in 1949, and revisited it in 1972 (Drack & Schwarz, 2010). Key constructs of general systems theory include function, structure, and process (Drack & Schwarz, 2010). In 2015, systems thinking theory was used in the exploration of public and private partnership projects (Loosemore & Cheung, 2015). Systems thinking theory was the basis for viewing the entirety of organizational systems, which held propositions

for the exploration of experiences (Drack & Schwarz, 2010). Identifying participant experiences was essential to improving the protection of systems from data breaches.

Complementing systems thinking theory, Cohen and Felson (1979) established routine activities theory to explain crime, as an event, as it related to space and time (Kigerl, 2012). Key concepts within routine activities theory include a potential offender, a target, and the absence of protection (Kigerl, 2012). In 2015, usage of routine activities theory was the basis of an investigation of gang and nongang online criminal behaviors (Pyrooz, Descker, & Moule, 2015). Identifying participant experiences of crime as an event may provide information on potential cybercrime motivation regarding attacks on their systems.

Operational Definitions

Definition of important terminology ensures that the reader has a clear understanding of the usage of terms throughout a study. Definitions for 10 essential terms related to the world of cybersecurity are below:

Cyber: Cyber refers to the domain of intersecting technology networking systems under the operation of nations, societies, and institutions (Williams, 2014).

Cyberattack: A cyberattack is a deliberate action taken to alter, disrupt, deceive, degrade, or destroy computer systems or networks, in order to gain entry to the information and programs resident in these systems or networks (Caplan, 2013).

Cybercrime: Cybercrime refers to criminal acts committed by using electronic communication networks and information systems against explicit targets or targeted networks and systems (Lagazio, Sherif, & Cushman, 2014).

Cybersecurity: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment, the organization, and user assets (Von Solms & Van Niekerk, 2013).

Cyber warfare: Cyber warfare is a virtual condition that occurs if a nation state propels a cyberattack with the intention of accomplishing a military objective (Robinson, Jones, & Janicke, 2015).

Cyber weapons: Cyber weapons are computer codes for use with the intention of intimidating or inflicting physical, functional, or mental harm to structures, systems, or living beings (Valeriano & Maness, 2014).

Data breach: A data breach is an incident that comprises unauthorized access to sensitive, protected, or confidential data, resulting in the compromise of the confidentiality, integrity, and availability of the data (Sen & Borle, 2015).

Data leakage: Data leakage occurs as insiders commit diverse crimes, including theft of personally identifiable information, intellectual property, and sensitive or classified information, as well as transfer of such information to an unauthorized third party (Huth, Chadwick, Claycomb, & You, 2013).

Information system: Information systems are the balancing networks of hardware and software that establishments use to collect, filter, process, create, and distribute data (Burinskiene & Pipirienė, 2013).

Insider threat: An insider threat occurs when a trustworthy individual gains control to abuse one or more rules in a specified cybersecurity policy, thus causing the trusted entity to abuse power (Wall, 2013).

Assumptions, Limitations, and Delimitations

The assumptions, limitations, and delimitations section of a study contains a discussion of the weaknesses inherent within the study. Examining common assumptions allows for realistic expectations. An assumption is something the researcher accepts as true without concrete proof (Leedy & Ormrod, 2015). Examining the limitations or potential weaknesses and problems within a study allows for preparation for events that are out of the researchers' control, as suggested by Leedy and Ormrod (2015). In contrast, examining delimitations allows researchers to define the parameters for a study, as proposed by Leedy and Ormrod.

Assumptions

The first assumption in this study was that participants would be willing to complete the online questionnaire containing open-ended questions. The second assumption was that the respondents to the online questionnaire would supply honest and truthful answers concerning cybersecurity at their business. The third assumption was that a subset of three respondents would participate in semistructured face-to-face interviews. The final assumption was the responses to the online questionnaire and semistructured face-to-face interviews would allow for sufficient common theme development involving cybersecurity practices at small businesses.

Limitations

The principal limitation of the study was that my professional position as senior vice president of information technology at an information security organization had the potential to influence the research approach and analysis of the data. A second limitation arose from engaging an initial sample of five small business leaders to act as participants. A third limitation was retaining a subset sample of three small business leaders to serve, as participants might not have been representative of the entire firm arena. The final limitation was that small business leaders might not have had the appropriate knowledge to make informed responses surrounding their cybersecurity practices.

Delimitations

The main delimitation of the study was that the data collection involved small business leaders rather than in-house information security specialists. The second delimitation was the constraint of the initial sample size to five small business leaders. The third delimitation was the restriction of the subset sample to three small business leaders. The last delimitation was that the geographical area of the study was the Middlesex County region of Massachusetts, which was chosen for accessibility and convenience purposes.

Significance of the Study

The significance of this doctoral study resided in the effort to explore effective cybersecurity strategies for small businesses that are necessary to improve the protection of systems from data breaches. The analysis may contribute to knowledge regarding cybersecurity practices essential for small businesses to avoid potential data breaches and

attacks. With the influx of cybersecurity threats, including malware links and attachments in email messages, even the most knowledgeable professionals have made mistakes that lead to data breaches (Densham, 2015). Implications for positive social change include the potential for some small business leaders to accelerate the adoption of cybersecurity practices to protect their systems from data breaches. Increasingly, small businesses are the targets of cyberattacks that have the potential to shut down their operations if not prevented (Hayes & Bodhani, 2013).

Contribution to Business Practice

By offering cybersecurity practice awareness to the small business sector, I hope to contribute to the body of knowledge on business practices. My primary focus in conducting the research was the protection of small business systems from data breaches. Data encryption and access controls are traditional methods of securing information (Sun & Wang, 2013). For small firms with limited security budgets, data protection has not been sufficient to ward off cyberattacks. Raising awareness is a deliberate method of protecting small business data. Security incidents at one small business have adverse effects on that small business and its competition (Kolfal, Patterson, & Yeo, 2013). Informed business practices have built understanding for small business leaders to arm themselves with appropriate knowledge and subsequently improve the protection of their data to avoid the damaging results of a cyberattack.

My secondary focus in conducting the research was to fill gaps in the understanding and practice of security in small businesses. In the past, researchers focused on security in large corporations, neglecting to isolate the small business as an

important topic within the literature. The need for informed decision-making practices has grown, as business in cyberspace occurs at a relatively low cost (Roesener, Bottolfson, & Fernandez, 2014).

Data protection is critical for internal and external processes, whether a small business maintains data on local systems or online (Caruson, MacManus, & McPhee, 2012). Small business leaders may perceive their business size as unattractive to the cybercriminal, but the opposite is true; cybercriminals view small businesses as easy marks for attack, due to their limited security budgets (Hayes & Bodhani, 2013). Proactively protecting systems from data breaches should be at the forefront of the literature to inform small business leaders' strategy.

Implications for Social Change

As businesses have become increasingly reliant on information and communication technology, damage to these systems has had significant consequences for society (Vande Putte & Verhelst, 2013). Many critical business processes delivered through information technology systems and Internet connections are at risk and require solutions. Crucial business processes managed via databases containing confidential data have remained vulnerable (Vande Putte & Verhelst, 2013). Criminal intrusions into the smallest databases have created dire consequences for the owners of the databases and those who have private information in the databases.

This study may serve as a tool for social change in providing knowledge as a resource for small business leaders to accelerate the adoption of cybersecurity practices to protect their systems from data breaches. Densham (2015) proposed that assuming that a

data breach will occur should be the crucial first step toward awareness for a firm. With the creation of cybersecurity strategies, small businesses may reduce data breaches and safeguard private information from outflow.

A Review of the Professional and Academic Literature

A critical analysis of the literature informed my research for this qualitative study and helped me identify cybersecurity strategies that small business leaders implement to protect their systems from data breaches. My primary focus was investigating cybersecurity issues and their effect on businesses. The goal of this qualitative exploratory case study was to study five small business leaders in the Middlesex County region of Massachusetts. I built the foundation of this case study on the premise that effective cybersecurity strategies have originated with awareness of the need to expect a data breach (Densham, 2015). I developed the research design to include five small business leaders in diverse industries comprising online, franchise, and retail establishments.

I performed a review of the literature on cybersecurity strategies, which encompassed books, conference papers, peer-reviewed journal articles, dissertations, websites, and corporate and government reports. The specific themes that emerged from the literature review included Internet crime, computer crime, cybercrime, e-crime, data breaches, phishing, computer viruses, small business, cybersecurity strategies, qualitative case study, qualitative research, general systems theory, and systems thinking theory. The primary databases used were the Walden University Library, ABI/INFORM Complete, Academic Search Complete, ACM Digital Library, Business Source Complete,

Computers and Applied Sciences Complete, EBSCO eBooks, Emerald Management, IEEE Xplore Digital Library, ProQuest Central, SAGE Premier, ScienceDirect, Taylor and Francis Online, and Thoreau Multi-Database Search.

The total number of references for this study included (a) 10 books, (b) two conference papers, (c) 132 peer-reviewed journal articles, (d) eight non-peer-reviewed journal articles, and (e) four reports. Of the 156 total study references, 132 (85%) were peer reviewed, and 139 (89%) were published within 5 years of expected Chief Academic Officer approval. The literature review contained 85 of the total 156 references for this study. Of the 85 literature review references, 71 (84%) were peer reviewed, and 75 (88%) were published within 5 years of expected Chief Academic Officer approval.

Cybercrime can affect many areas of technology. Herein, the literature review includes information on four main themes: (a) cybercrime's financial effects, (b) cybercrime's legal effects, (c) cybercrime's sexual effects, and (d) cybercrime's social effects. For a detailed investigation of the study topic, each main theme included related subthemes. The subthemes for cybercrime's financial effects were (a) cash, (b) laundering, (c) prevention, and (d) strategies. The subthemes for cybercrime's legal effects were (a) police, (b) reality, (c) responsibility, and (d) rules. Cybercrime's sexual effects subthemes encompassed (a) challenge, (b) consequences, and (c) restitution. Cybercrime's social effects subthemes consisted of (a) cyberbullying, (b) community, and (c) fraud. The cybercrime themes were chosen to highlight the impact on small business; the primary theme was cybercrime's financial effects.

Cybercrime's Financial Effects

Cash. Bensted (2012) argued that international counterterrorist financing actions have increased since September 11, 2011. Chambers-Jones (2013) echoed this idea, asserting that financial crime through the Internet presents a constant technological danger due to the growth of virtual environments. Lack of targeted surveillance and coordination with Internet service providers (ISPs) has produced challenges for efforts to prevent terrorist financing actions on the Internet (Bensted, 2012). Chamber-Jones emphasized that applying physical laws to virtual environments is impossible. Bensted (2012) asserted that the development of an international standard to detect online terrorist financial activities should become a task for the United Nations.

Bernik (2014) extended the thoughts of Bensted (2012), evaluating financial activities via investments in the protection of organizations against cybercrime. Through cost model utilization, Bernik inspected data from global organizations and governments to discover the factual causes of each loss. The internal cost in Bernik's model involves detection, investigation, escalation, containment, recovery, and ex-post response. External consequences in the model include costs of information loss or theft, business disruption, equipment damage, and lost revenue.

Bernik (2014) confirmed that knowledge of costs empowered businesses to manage expenses and implement suitable measures. Companies performing such actions experienced increased levels of cybersecurity and better resilience to cybercrime. Organizations that invested in approaches aimed at providing protection and security, as well as developing employee culture and awareness to foster adoption of personal

protection mechanisms, were in a better position to prevent and overcome potential threats.

Security vendors McAfee Intel Security and Symantec Corporation reported, comparable to Bernik's (2014) cost model, variations of the financial costs of cybercrime (Hyman, 2013). Symantec Corporation reported that cybercrime costs the world $110 billion annually (Hyman, 2013). McAfee Intel Security reported worldwide cybercrime costs of $1 trillion yearly (Hyman, 2013). McAfee Intel Security attributed the difference between its figures and those of Symantec Corporation to the former's focus on both malicious and accidental data losses for businesses worldwide.

Hyman (2013) agreed with cybercrime researchers who blamed methodologies of surveys toward exaggerating the numbers on the high side, while others faulted artificially inflated cybercrime statistics to scare people into purchasing antimalware software. Anderson et al. (2012) claimed that a large portion of cybercrime costs is for the purchase of antivirus software. Anderson et al. recommended that a coalition of software and hardware vendors conduct cost reporting. Hyman supported the Anderson et al. suggestion as valid and proposed that companies should stop spending money calculating cybercrime, and instead spend it on the police.

Lagazio et al. (2014) prepared a multilevel approach founded on system dynamics methodology, measuring the financial costs of cybercrime. Important factors in determining the costs of cybercrime are (a) changes in companies' strategic priorities, (b) customer trust and loyalty as key objectives, and (c) market position in relation to competitors. Lagazio et al. determined that the approach companies use to protect their

business interests and market positioning can drive the costs of cybercrime. Similar to Bensted (2012), Lagazio et al. surmised that the outcomes of weak policing and international frameworks for tackling cyberattacks increased the cost of cybercrime.

Shackelford (2012) analyzed the financial effects of cyberattacks on organizations, U.S. law applicable to data breaches, and cyber risk insurance. Shackelford reported that identity theft costs consumers more than $5 billion per year and costs businesses another $48 billion per year. Shackelford noted that fraud is a significant issue, with over $1.8 billion in fraud claims reported in 2008. Another cyber issue, advanced persistent threats, can be a more serious threat to a company's bottom line.

Shackelford (2012) identified cyber risk insurance as a tool to manage liability exposure and mitigate the hazard of cyberattacks. Insurance policies cover losses from cyberattacks and data breaches. Shackelford indicated that investment in cyber risk insurance should be a recommendation to businesses to enhance cybersecurity. Shackelford recommended that a company's first investment in cybersecurity be in network and infrastructure, including firewalls, encryption, and intrusion detection. Cyber risk insurance is a tool used to return losses that result from cyberattack, but proactive cyber strategies should always be the starting point (Shackelford, 2012).

Hayes and Bodhani (2013) identified small to medium-sized enterprises (SMEs) as increasingly targeted by online threats. Cybercriminals actively look for opportunities to mark these soft targets. SMEs with limited information technology (IT) resources have not placed appropriate investments in cybersecurity. In cases in which medium-sized to large enterprises (MLEs) have maintained business relationships with SMEs,

cybercriminals have attacked the SME as the perceived weaker link. Hayes and Bodhani implied that leaders of SMEs do not understand cybersecurity as an issue for them, perceiving cybersecurity as a challenge only for large enterprises. They suggested that SMEs were increasingly the target of cybercrime for those criminals trying to target larger enterprises, concluding that large enterprises could play a role in providing cybersecurity assistance to their SME partners.

Laundering. Laundering money via the Internet is a crime that terrorist organizations continue to use (Hunt, 2011). Cyber laundering is achievable using electronic cash and the Internet to legitimize criminal funds. Hunt (2011) examined money-laundering laws of the United States and reviewed attempts made by the United Nations, the G7, the Organization of American States, and the Council of Europe to stop cyber laundering. Review of U.S. law revealed loopholes that identified methods to close the gaps.

Hunt (2011) asserted that the U.S. Congress should increase the coverage of current acts to incorporate cyber laundering practices and the use of the Internet by terrorist organizations. This action would require adjustments to the existing U.S. Code but could expand current law to include electronic currency and online banks as regulatory tools that fall under the classification of financial institutions. Lawmakers should draft legislation that closes loopholes in current laws. Hunt argued that if governments were to increase pressure on terrorist supporters, then reductions in their financing would decrease.

Broadhurst, Grabosky, Alazab, and Chon (2014) reviewed variants in the organization of cybercrime. They determined that most organized cybercrime involved the work of experienced specialists who employed their knowledge through criminal activity. Criminal groups also exploited digital technology in pursuit of criminal purposes. Similar to Hunt (2011), Broadhurst et al. noted inadequate empirical evidence to establish that organized crime groups dominated cybercrime. Broadhurst et al. explained McGuire's typology of cybercrime groups, which encompassed six types of group assembly. The six groups identified were swarms, hubs, clustered hybrids, extended hybrids, hierarchies, and aggregates. Broadhurst et al. reflected that complexity theory, a derivative of systems theory, helped to describe the dynamic nature and collective behavior of cybercrime groups.

Philbin and Philbin (2013) identified malware in the forms of data deletion, data theft, and data manipulation. The primary motivations of cyber warfare include economic and political control of information. The combatants in cyber war are mathematicians using information as an agent, many times in the use of algorithms as weapons to exploit information. Behind the mathematicians, private organizations serve as proxies for cyberattacks. The use of these private organizations occurs covertly to avoid detection. The United States, under Homeland Security Presidential Directive HSPD-7, owns critical infrastructure (Hunt, 2011; Philbin & Philbin, 2013).

Beginning in the early 1990s, the rate of online property crime (OPC) rose through increased incidence of forms of identity theft, credit card theft and fraud, and cyberattacks (Tcherni, Davies, Lopes, & Lizotte, 2015). Tcherni et al. proposed an

alternate assessment of property crime trends and delivered gaps in crime reporting and accounting about online property crimes. Victims of cybercrime could now report the offenses to their local police department or the Internet Crime Complaint Center (IC3). Tcherni et al. estimated that victims do not report 20% of OPC. Deriving the actual costs of traditional property crime versus OPC will remain difficult if OPC continues to go uncounted.

Tcherni et al. (2015) indicated that one OPC can entail multiple compounded offenses. For example, stealing credit cards counts as one illegal act, but using the credit cards results in the criminal committing more crimes. The same may be true for victims, in that a crime may be committed against one or many victims. Available data indicating OPC as a growing concern show that a standard is needed for counting OPC data. Tcherni et al. identified a gap that could help criminologists reevaluate the central methodologies for quantifying a crime.

Prevention. Herley (2014) presented information on the threat model of sufficient defense against security and cybercrime. The first premise of Herley's model indicates that if protecting against all attacks is necessary and sufficient, then failure to do everything is the equivalent of doing nothing. Second, in a system where everything is necessary, trade-offs are not conceivable. Third, the premise that there is only a determinate amount of known attacks is plainly advantageous to the defender. Finally, Herley implied that if the threat model pertains to everybody, it is difficult to explain why not everyone experiences a hack every day.

Herley (2014) offered modifications to the threat model of sufficient defense when he added a threat model of necessary and sufficient conditions. For example, it is necessary and sufficient to defend against all attacks. The threat model should distinguish between fixed financial gain and endless financial gain, or between zero and nonzero cost. Herley recognized that cybercriminals inflicted the most harm with attacks that were repeatable and where they continuously located and monetized targets. When groups of targets (such as small businesses) underwent profitable exploitation, this warranted additional countermeasures.

Lee (2014) analyzed the problems of small and medium-sized businesses (SMBs) regarding industrial security and suggested strategic solutions for SMBs. Low-security awareness and financial difficulties made it difficult for SMBs to build an effective security management system that would protect the company from industrial espionage and leakage of its technology. The growing dependence of SMBs on networks such as the Internet placed SMBs at risk of technology leakage through hacking or comparable methods. There was a need for new measures to confront and control information security risks (Herley, 2014; Lee, 2014). In developing such measures, Lee suggested, SMBs should engage online security control services and technology deposit systems to mitigate leakage risks.

Prakash and Singaravel (2015) illustrated possible methods of protecting sensitive data. They defined sensitive data categories as medical, census, voter registration, social network, and customer information. Prakash and Singaravel offered a personalized anonymization approach to protecting data that preserved privacy. Such an approach may

remove any trace of the electronic publishing of data to its final destination. Privacy limitations of existing methods include similarity and background knowledge attacks.

Prakash and Singaravel (2015) proposed a three-phase personalized anonymization method to address privacy issues; this method includes three checks and a system of balances. Prakash and Singaravel then used U.S. Census data to test their proposed data privacy model. Prakash and Singaravel suggested that the personalized anonymization approach could prevent homogeneity attacks and that its speed could provide better proficiency.

Shields, Gibson, and Smith (2013) examined aspects of the psychology of people in the United States that have hindered the successful and consistent practice of certain security behaviors. As part of the investigation, Shields et al. built on a study by Mitnick and Simon (2011) in which the human factor was presented as security's weakest link. Shields et al. replicated efforts from a study by Ng, Kankanhalli, and Xu (2009), using the 1960 Rosenstock health belief model for theoretical insights. The premise of the model suggests that a person's beliefs will predict his or her actions. This model makes it possible to distinguish the perceived susceptibility and severity of a threat. Shields et al. stated that self-efficacy, perceived benefits, and perceived susceptibility predicted computer users' security behavior. Cues to action and perceived severity were not significant, which aligned with the Rosenstock model.

Todd and Rahman (2013) offered a cost-effective approach to information security for small businesses. They suggested that small businesses do not have sufficient resources available to secure their systems in the same manner as large organizations.

Todd and Rahman provided a method for creating, implementing, and enforcing an information security plan at low cost to small businesses. To carry out this plan, Todd and Rahman reported 10 inexpensive, or free, security measures for quick implementation:

1. Know your equipment, in terms of maintaining an asset list.
2. Stay ahead and identify all possible methods of attachment for a network.
3. Learn from mistakes, or study past threats to be able to predict future attacks.
4. Prioritize your security concerns by identifying what will have the greatest negative impact on the business.
5. Control access to the network and virtual private networks used for remote employee access.
6. Test firewalls to protect from intrusion.
7. Provide access to systems only when necessary.
8. Backup systems frequently and have a backup of the backup.
9. Train users to be suspicious of emails from senders they do not know, including never opening attachments from a suspicious party.
10. Alert remote workers to remain mindful of their equipment and do not allow anyone to use the equipment when working remotely (p.2).

Todd and Rahman (2013) argued for small businesses to utilize the steps and create a security-minded culture. Upon completion of a comprehensive security analysis, organizations would be able to create a practical budget plan. The security analysis contained components of assessment, requirements, policies, and procedures. The

rationale behind the cost-effective measures implemented common sense approaches (Shields et al., 2013; Todd & Rahman, 2013).

Strategies. The application of an information security culture transformed how employees interacted with information assets (Alhogail & Mirza, 2014). In starting a program, possible employee behavior exhibited resistance, fear, or confusion. Through a review of change management principles from existing literature, Alhogail and Mirza combined facets of each principle into a comprehensive multistep framework. The multistep change management framework included management support, analysis of the culture, change agents team, the sufficiency of resources, communication, focus groups and workshops, motivation, training, involvement and ownership, and success measures and milestones. Success in establishing and managing an information security culture started from top management going down to every employee.

Bamrama, Singh, and Bhatt (2013) evaluated cyberattack strategies of cybercriminals targeting banks. Cyberattack criminal approaches included spoofing, brute force attack, buffer overflow, and cross side scripting. Bamrama et al. accessed various cyberattack strategies of public and private sector banks and reviewed different cyber defense strategies and their correlation with cyberattacks. They argued financial institutions should adopt adequate security measures during financial transactions from internal databases. Encryption of confidential and high-risk data was necessary during transmission over insecure channels. Consumer education was appropriate, in collaboration with government and other private agencies, to thwart cyberattacks (Alhogail & Mirza, 2014; Bamrama et al., 2013).

Bolton (2013) reviewed the cybercrime strategies in terms of how organizations and governments proactively implant cybersecurity measures. Bolton noted chronic issues that resulted in significant corporate failures followed with tighter regulations, e.g., the Sarbanes-Oxley Act. The magnitude of cybercrime warranted stringent domestic and global regulations to limit the events. Many companies have not utilized proactive measures, such as cyber insurance (Bolton, 2013; Shackelford, 2012). Organization leaders and board of directors were encouraged to promote cybersecurity as a strategic issue.

Bolton (2013) defended the process of assessing risks, starting with the basics, then gaining an understanding of the critical devices and systems support critical processes. Cybersecurity roadmaps were central for an organization to increase its understanding of changing factors in cybersecurity, thus allowing them to address those changes proactively. When organizations employed the roadmap framework, they had the potential to reduce the impact of imminent and more inclusive regulatory requirements.

Chang (2014) analyzed security requirements based on business processes to prevent technology leakage. Without these processes, a data breach within the manufacturing industry could affect national security. Chang discovered types of technology leakage included blueprints of products, pictures, and images. The means for technology leakage was portable storage devices; email, printed material, mobile and digital cameras. Similar to Alhogail and Mirza (2014), Chang emphasized basic organizational security environment implementation is not correct in all major companies and SMEs.

Siponen, Mahmood, and Pahnila (2014) developed a model to explain employee obedience of company security policies. The new method combined elements of the protection motivation theory, the theory of reasoned action, and the cognitive evaluation theory. Siponen et al. undertook this research to decrease internal security threats to businesses through a synthesis of the theoretical frameworks. The synthesis included the assessment of threats and coping, gauging behavior intention as a verdict of how the employee will conform to policies, and the concept of reward as a positive motivator of compliance. Employee attitude and intention to comply with security policies had a significant impact on their actual obedience. The outcome revealed top-level management gained greater compliance when employees are mindful of company security policies (Bolton, 2013; Siponen et al., 2014).

Vande Putte and Verhelst (2013) utilized their knowledge and experience with operational risk management and business continuity management to explain cybercrime challenges about risk management. The upstream standard risk model level helped identify the cause, incident, and impact, which related to business, reputation, and finance zones. The downstream layer of the standard risk model identified control and mitigation measures, which included avoiding, manage, and transfer. Types of cybercrime incidents that affected business continuity were distributed denial of service attacks, infrastructure system attacks that erase and destroy, and infrastructure system attacks that steal or alter information. Vande Putte and Verhelst implied the usage of the standard risk model provided the business with areas to fill potential risk gaps.

Cybercrime's Legal Effects

Police. Technology has been in a continuous state of progression, which in turn has advanced cybercriminal behaviors. Legislative efforts to fight cybercrime may lack efficiency and improvement to keep up with cybercriminals. Cade (2012) recognized if global laws do not advance and take precedence, a catastrophic cyber event would ensue. Cade evaluated three proposals for combating cybercrime at an international level: (a) extend universal laws, (b) to use treaty law to bind domestic statutes, and (c) the adoption of international penal codes. Cade concluded that the lack of launching a universal jurisdiction over cybercrime continues to leave the world in a vulnerable position, where cybercriminals threaten individuals, economies, and nations.

Holt and Bossler (2012) acknowledged that law enforcement faced sizeable challenges when dealing with cybercrime. Many officers were not prepared to investigate cybercrime incidents due to lack of training or interest. The authors examined the connections that predict patrol officer interest in cybercrime training and investigations. Special attention is on the demographic, cybercrime exposure, and computer training of the officers. Officers with greater computer skills showed interest in cybercrime training and investigation.

Flowers, Zeadally, and Murray (2013) argued cybersecurity remains one of the most persistent national security issues challenging countries around the world. Cybersecurity topics included areas of Internet governance and jurisdiction, national security, and critical infrastructure protection. No country has completely solved the issues associated with cybercrime (Cade, 2012; Flowers et al., 2013). Flowers et al.

(2013) suggested the United States continues to attempt a balance between privacy and security.

The theft of intellectual property via the Internet was a primary concern, and it appeared law enforcement was becoming more successful in pursuing offenders (Flowers et al., 2013; Holt & Bossler, 2012). Flowers et al. (2013) argued that neither consumer protection, nor protection of the nation's critical infrastructure fared well in the 112th Congress. These continued concerns opened the door for future researchers to explore and discover the necessity of drafting existing laws, in such a way to anticipate changes in the cyber threat landscape.

Givens and Busch (2013) asserted that the federal government lacked an organized method to post cyber incident mitigation. The Department of Defense (DOD) and the Department of Homeland Security (DHS) worked collaboratively on cybersecurity initiatives. Their close ties allowed hackers to exploit an electronic vulnerability in one agency's network to gain access to another agency's system. Givens and Busch proposed a unified policy that would include cyber preparedness, incident response and recovery, offensive and defensive cyber warfare, public-private sector coordination, and citizen education on cyber threats.

Givens and Busch (2013) endorsed the logic of integrating federal approaches to post cyber incident mitigation. Greater legal integration for the DOD and DHS, as a bridge for the cultural differences between the two organizations, would affect the technology used by both agencies. Givens and Busch determined an urgent need to integrate and streamline the federal approach to cybersecurity. In part, appropriate

funding is essential for local and state cybersecurity plans, and the level to which these initiatives interface with federal programs. Further, Givens and Busch recognized the U.S. dependency on IT would keep the cybersecurity policy topic a significant issue for years to come.

Reality. Stuxnet, discovered in June 2010, was the first suspected instance of computer code or malware employed as a use of force. Stuxnet was only the beginning, two other targeted cyber espionage computer viruses emerged: Duqu in September 2011, trailed by Flame in May 2012. Flame, considered the most dangerous computer virus, and gathered intelligence from computers in Lebanon, the United Arab Emirates, the West Bank, and Iran (Farwell & Rohozinski, 2012). Such cybercrime instances led to a new era of an international trust. Nuclear weapons, primarily used to restrain, differed from cyber weapons. Using force as a means of protection remained the challenge. To date, there is no internationally accepted definition of force applicable to cybercrime. Farwell and Rohozinski (2012) surmised that state-to-state commitment would outline a new reality and necessitate new strategic controls to battle cybercrime.

Caplan (2013) analyzed the rising dependence on cyber infrastructure that opened the way to new national security threats against the DHS. Caplan pinpointed the United States should consider cyber as a war-fighting domain along with land, sea, air, and space. The United States was and remains more susceptible to cyberattacks, due to its high dependence on cyber controlled systems to run critical national infrastructure. The growing reliance on cyber infrastructure opened the gate to new national security threats against the United States.

Caplan (2013) indicated legislation aiming to protect the United States from cyberattack should be the result of private and government infrastructures. The intentional creation of the Cyber Security Act of 2012 is to protect the United States from cyberattack, but failed to secure enough votes to move forward in Congress. Caplan warned, as Internet usage continues to increase, every facet of U.S. society will progressively rely upon cyberspace. The recommendation to pursue an active cyber strategy is to guard U.S. networks against malicious activity.

A shift in focus evolved from cybercriminals to cyberspace weapons, military, and intelligence service (Caplan, 2013; Filshtinskiy, 2013). The largest change in cybercrime business happened when criminals moved from selling goods to establishing services. Computer crime became an industry comparable to weapons trafficking and drug trafficking (Filshtinskiy, 2013). Cybercriminal trade portals offered services to send unsolicited messages, writing malware, and abuse resistant hosting for other criminals. Filshtinskiy (2013) asserted that cybercrime services were available to anyone who wanted to purchase them. Criminals advertised hacking a private email address for $50, forged identity documents for $30, and custom-built malware for $1,500. The contention arose as successful arrests of cybercrime providers were rare, and declared that society's exposure to cybercrime was the result of the lack of appropriate defenses.

Pawlak and Wendling (2013) analyzed the trends in the governance of cyberspace and their effects on governments and global regulatory establishments. Assortments of impending threats posed considerable challenges to current global governance structures. Such structures were often lacking, in contrast to the vigorously evolving cyberspace.

Pawlak and Wendling reported acquiring a profound understanding of the condition and the activities behind policymaking was the first step in a more deliberate distribution of inadequate resources.

One issue that arose in the development of cybersecurity strategies was the ease of attacks in contrast to detection and prevention (Filshtinskiy, 2013; Pawlak & Wendling, 2013). Policymakers faced a difficult challenge, when decision-making processes were slower than the speed of technological advances. Increasing cybersecurity resources came with a high cost, which deters policy makers, as there was limited availability of data to reflect how investments delivered results.

Harsh regulations had adverse effects on the economy and businesses, which were necessary for research and development of new technologies (Pawlak & Wendling, 2013). In addressing threats to a state's survival, many states followed two corresponding courses of action: Developing military cyber competencies, and confidence building measures to improve harmonization between states. Pawlak and Wendling (2013) proposed the driving force of governmental regulations required policy, legal, or technological considerations. Involvement in rule creation rarely included all stakeholders (public administration, businesses, citizens, the research community, or relevant international players). A comprehensive formulated strategic policy-making process allows governments to keep up with the quickly progressing nature of cyber threats.

Berriz (2014) examined the problem of cybersecurity in the United States. The United States was not giving appropriate attention or funding to countermeasures. As a

result, the nation's intelligence and personal information is in severe security risk. The Cyber Intelligence Sharing and Protection Act (CISPA) provided an amendment to the National Security Act of 1947. CISPA defined a cyber threat as an effort to degrade, disrupt, or destroy a system or network, or theft or misappropriation of private or government information, intellectual property, or personally identifiable information. Additional amendments to CISPA allowed for lawsuits against the government in the case of any violation of the government's use of private information.

Berriz (2014) argued that even though a cyberattack had not severely hurt the U.S. economy or infrastructure, it was only a matter of time. The government's twofold strategy aimed at improving the nation's cybersecurity by improving resilience to cyber incidents, and reducing the cyber threat. The DHS planned to secure cyberspace by releasing actionable cyber alerts, investigating and arresting cybercriminals, and educating the public on the prevention of cyberattack by staying safe online. Similarly, the Secret Service created a unit specifically dedicated to cyberattacks and cybercriminals called the Electronic Crimes Task Force.

Berriz (2014) maintained that the U.S. government was doing very little to protect valuable information from potential enemies. Definitive steps toward preventing cyberattack continued to be necessary, to protect the U.S. government, country, and citizens. Promoting information sharing remained the most important and efficient step the United States could take in preventing cyberattacks from enemies. Berriz stressed the importance for agreement on the best methods to tackle cybersecurity in a legislative

manner. As a result, the United States could potentially further its position as a secure world power.

Sun and Wang (2013) examined cloud computing, related to SMEs, as an essential element of efficiency and competitiveness. Sun and Wang proposed a model to solve the problem of data security in cloud computing, which addressed the SME data integrity issue. The security features of the proposed model included encryption and decryption of data, ciphertext retrieval, and integrity verification. Data encryption and decryption components requested keys from a keys management component. The keys management component retrieved information of keys and ciphertext from the cloud storage system. Sun and Wang indicated their proposed model was a method to solve the problem of data security in the cloud, as the model adopts effective encryption mechanisms to protect users' data.

Responsibility. Healey (2011) suggested that cyber defenders continuously struggle to determine the source of harmful cyberattacks. Examination of cyber defense progress is through the acceptance of national policy makers to know the responsibility for an attack. Healey proposed a range of state responsibility, linking attrition to the needs of policy makers. The range of state responsibility included 10 categories to help researchers gain knowledge in the cybercrime areas of

- State-prohibited;
- State-prohibited-but-inadequate;
- State-ignored;

- State-encouraged;
- State-shaped;
- State-coordinated;
- State-ordered;
- State-rogue-conducted;
- State-executed; and
- State-integrated (p. 59).

Healey claimed policymakers waste too much time fixating on what started the attack, versus who was to blame for the attack. Healey's views opened the discussion to change the direction of thinking to a more stable and secure cyberspace.

Caruson et al. (2012) examined cybersecurity policies in five areas: (a) internal and external cyberattacks, (b) perceived cyber threats to agency operations, (c) current cybersecurity policies, (d) urgency of reactive measures, and (e) potential roadblocks to the development of cybersecurity plans. For perceived cyber threats, IT professionals rated each threat as more serious than an IT generalist or IT specialist, thus displayed disconnects among the three groups. Caruson et al. showed that local governments required more policy making and employee education in the area of cybersecurity. Similar to Healey (2011), Caruson et al. noted a lack of cybersecurity awareness cannot be a budgetary issue, and local offices should collaborate with the private sector to fill gaps in resources and knowledge.

Advances in data protection in conjunction with the growing popularity of cloud computing emphasized strains amid data protection regulators, businesses, and computer science communities (Desai, 2013). Data protection laws focused on data not leaving a country or a region, while cloud computing relied on the movement of data on a continuous basis. Desai analyzed the creation of laws that respected political interests and drew on the best insights of computer science, finding intensified data security was achievable. Media attention concerning security breaches raised concerns that the largest threat to unauthorized access was at data centers, which become a target to experience a breach. Losing computers and thumb drives was another way data could disappear, more so than through a data center. Governments, companies, and computer scientists would need to collaborate to create a data security system for the 21st century, as data security laws progressed.

Hult and Sivanesan (2013) advocated strengthening cyber resilience through a strong focus on leadership, people, and process. They offered a checklist of questions to ask executives, in order to obtain an accurate measurement of their cyber resilience effectiveness:

1. What level of assurance does an executive have?
2. What is the position of cybersecurity in the organization?
3. What is the sponsorship of cybersecurity by the organization?
4. How accomplished is the leadership team(s) leading the cyber resilience function(s)?

5. How do business continuity, IT, physical security, cybersecurity, and risk operation disciplines currently collaborate in the organization?
6. Is the cybersecurity function high performing?
7. How mature is the organization in its exercising and learning capability?
8. How does the organization currently get assurance for the effectiveness of the cyber response capability?
9. Does the organization have an understanding of the bedrock cybersecurity assumptions that it makes (p. 113)?

For each question, Hult and Sivanesan determined which responses could provide particular cyber resilience strategies and tools for executives to utilize within their organizations.

Raiyn (2014) investigated cyberattacks as the biggest threat for homeland security. Types of cyberattacks included distributed denial of service, access attacks, and malicious attacks. An overview of a state of the art cyberattack detection strategy included embedded programming, agent-based software engineering, and artificial intelligence approaches. These detection approaches were proactive with applications installed at the network layer, and on client machines, with the ability to detect and stop an intrusion. Raiyn recommended a system-type model infrastructure with four layers: (a) home agent for monitoring, (b) social agent for suspect objects detection, (c) mobile agent for searching for suspect objects, and (d) mobile agent for tracking suspect objects. The continuous evolution of cyberattack detection was necessary to overcome

cybercriminals, who continuously developed their hacking strategies (Healey, 2011; Raiyn, 2014).

Roesener et al. (2014) explained the current authorities, roles, and responsibilities of U.S. agencies, and detailed how these authorities, roles, and responsibilities needed modification to protect the U.S. national security interests. Cyberspace remained a vulnerable security interest, as a globally interconnected digital information and communications infrastructure. Due to the ease and low cost of conducting operations in cyberspace (compared to the physical domains of air, land, sea, and space), as well as the concealment allowed by this virtual domain, cyber threats and attacks became more dominant and as dangerous as do those in physical domains.

The negative impact on U.S. national interests and the lives and assets of U.S. citizens, gave rise for government preparation and protection in the virtual domain equal to those in the physical domain. The Obama administration modified the agency roles with Presidential Policy Directive 21, which stated the DHS retains the responsibility to coordinate Federal Government responses to significant cyber or physical incidents affecting critical infrastructure. Roesener et al. (2014) contended the DHS should retain responsibility for securing critical infrastructure in the physical domain. Further, they suggested the reduction in DHS's cybersecurity role should include the consequence management portion for effects after a cyberattack that results in physical damage.

Rules. Before the threat of nation crippling cyberattacks, organizations handled their cyber risks in isolation. Tikk (2011) presented the inception of international organizations, introducing new cybersecurity policies that expanded the conception of

cybercrime. The 10 rules for cybersecurity focused on working solutions that arose from conversations with cyber incident handling experts. The 10 rules included territory, responsibility, cooperation, self-defense, data protection, and duty of care, early warning, and access to information, cyber criminality, and mandate. Tikk stressed that the 10 rules were a framework of key ideas and areas that were worthy of integration into an all-inclusive legal methodology to cybersecurity.

Iasiello (2013) examined how the U.S. government handled cybersecurity and offered a proposal for coordinating cyberattacks. The U.S. government does not have one group that leads the cybersecurity effort. Instead, 16 intelligence agencies and numerous civilian and military organizations worked separately to warn of emerging cyber threats. Iasiello proposed a centralized domestic cybersecurity effort, which would reduce redundant cyber related homeland security missions in the U.S. government. Iasiello claimed the presidentially nominated cybersecurity coordinator should provide tactical level cybersecurity guidance domestically and internationally.

All U.S. cybersecurity strategies began with the presidentially nominated coordinator, and then trickled down to DHS. The DHS is the primary agency in charge of U.S. cybersecurity, and would have the authority to engage support from the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the DOD. Iasiello (2013) argued that his proposal would only work if each agency allowed the cybersecurity coordinator and the NSA to lead the cybersecurity responsibility.

Continuing his work, Iasiello (2014) compared the lack of transparency and visibility in cyberspace that allowed for the development of deterrence measures. Iasiello

defined cyber deterrence as a strategy to sustain the status quo, indicating intentions to dissuade aggressive cyber activity for fear of greater retaliation and offered two types of deterrence. The first type of deterrence is deterrence by punishment, applied to cyberspace in the form of digital actions such as a retaliatory cyber strike. The second type of deterrence is deterrence by denial, discourages or frustrates attacks with robust, proactive, and costly defenses. Steps that occurred in a precise order for cyber deterrence strategies were successful.

Cyber deterrence objectives intended to decrease the threat of cyberattacks to a tolerable level at an acceptable cost. Iasiello (2014) emphasized that thousands of cyberattacks transpire daily, which insinuated excessive struggle in differentiating serious threats from minor ones. Cyber deterrence by punishment included many unknown variables and immature tactics to make it a favorable course of action. Cyber deterrence by denial was successful in a limited capacity with network defenders. Iasiello reflected that organizations should evaluate current security policies to determine the effectiveness, while flexible security plans should consider the active realm of cyberspace and include targets and measures to attain objectives in a timely fashion.

Strikwerda's (2014) definition of virtual cybercrime involved the usage of simulation to commit a crime. Strikwerda researched whether criminal law should be a regulatory agency for virtual cybercrime and studied four dimensions of the law, including philosophical, legal-economic, pragmatic, and constitutional aspects. The philosophical dimension linked to legal ontology, which is the categorization of items under the law. The legal-economic dimension related to the costs and benefits of using

criminal law. The pragmatic dimension referred to the overall capacity of the criminal justice system to rule over information and communication technologies. The constitutional dimension signified the burdens imposed on the central freedoms of citizens. The pragmatic dimension applied to the instances of virtual cybercrime, while the constitutional dimension was the least applicable.

Colesniuc (2013) explored the necessity of building cyberspace as a secure environment similar to the manner of building societies. Cybersecurity was required to ensure the safety of cyberspace from any form of threat. Threats varied, from stealing secret information from national companies and government institutions, to attacking vital infrastructure that revealed the private information of a single person. Colesniuc indicated that governments have the greatest responsibility to protect the critical information infrastructure (CII) and can leverage knowledge from business and academia to accomplish the task.

Colesniuc (2013) emphasized nine core CII sectors for protection: (a) chemical, (b) emergency services, (c) communications, (d) financial services, (e) energy, (f) information technology, (g) nuclear reactors, materials, and waste, (h) transportation systems, and (i) water and waste systems. Colesniuc argued that no system will ever be infallible, but understanding the everyday threats to organizations may permit effective security management.

Cybercrime's Sexual Effects

Challenge. Cambria (2012) focused on a private organization certified to dispense Internet domain names for the adult Internet industry. The Internet Corporation

for Assigned Names and Numbers used its authority to set rules for assigning adult industry domain names by limiting them to the .xxx extension. Cambria argued the limitation placed a strain on the adult Internet market, as .xxx suggested sexually explicit content. The domain name design is comparable to a standard phone number. The creation of domains with the extension of .com, .net, .org, and .edu are for easy identification. Through registration of an adult-themed .xxx domain, the registrant authorized the monitoring, reporting, and conceivable prosecution of any content that implied the existence of child pornography. Cambria stated online pornographic providers should investigate all potential possibilities to guard their interest, both from an economic and rights positioned perspective.

The establishment of online offending presented a specialized phenomenon (Cambria, 2012; Donner, Jennings, & Banfield, 2014a). Researchers on criminality postulated that online offenders exhibited one class of deviant behavior during their life, which corresponded with Gottfredson and Hirschi's (1990) general theory of crime. The general adaptability of offenders offered an experiential test of whether online offenders specialized in cybercrime.

Utilizing the data collection of 502 undergraduate college students, Donner et al. (2014a) examined the extent to which college students commit off-line offending, as compared with online offending. Results from a series of bivariate and multivariate analysis designated support for theorizing online offending is not a specialty, but part of a general offending behavior. Donner et al. reported that law enforcement agencies needed

better policies to detect and investigate online crime, while intensification of processes could heighten the apprehension and punishment of online criminals.

Donner, Marcum, Jennings, Higgins, and Banfield (2014b) explored whether an individual's level of self-control was significant when compared to his or her involvement in an online deviance beyond digital piracy. Forms of an online deviance included identity theft, sex crimes, and illegal download of copyright material (songs, movies, software). Prior studies of online deviance, conducted by Buzzell, Foss, and Middleton (2006), have uncovered demographic correlations of age, sex, and race.

Theories used to explain cybercrime are routine activities theory, social learning theory, and low self-control theory. When focused on the 1990 low self-control theory from Gottfredson and Hirschi (1990), the most common act of deviance was illegal downloading and uploading of copyright materials. Low self-control has positive and significant correlation with acts of an online deviance (Donner et al., 2014b).

Cyberspace remained an attractive realm for criminals, as Internet users have limited knowledge in combating cybercrime. Incidents about cybercrime included identity theft, credit card fraud, and child pornography. Cybercrime is a complex phenomenon, with global confrontation as the only method of handling the problem (Nuredini, 2014). Nuredini recommended local institutions and international establishments work together to fight cybercrime, suggesting the war against cybercrime was the duty of society as a whole. Cooperation between national and international agencies, as well as the increase of public awareness, can reduce cybercrime.

Consequences. Grov, Gillespie, Royce, and Lever (2011) built on existing research that focused on the impact of online sexual activities (OSA). Prior studies placed attention to female partners of male OSA users, but yielded no information of how men recognized their female partners OSA. Grov et al. analyzed an online sub-sample of 8,376 adults in committed relationships, who reported having used the Internet to access adult materials. The multimethod research sought to examine and explore gender variances in worries about romantic partners' OSA, feelings of personal growth in sexual exploration, and influence on real-life sexuality. Grov et al. emphasized positive and negative effects of OSA in committed relationships, where negative effects outweighed positive effects.

Henry and Powell (2015) suggested a growing phenomenon in the use of new technologies to facilitate sexual violence and harassment online. Technology facilitated sexual violence and harassment (TFSV) consisted of six different forms:

1. The unauthorized creation and distribution of sexual images;
2. The creation and distribution of sexual assault images;
3. The use of a carriage service to procure a sexual assault;
4. Online sexual harassment and cyberstalking;
5. Gender-based hate speech; and
6. Virtual rape (p. 759).

Henry and Powell focused their examination on TFSV against adult women by adopting a social constructivist approach.

One such means TFSV was an issue presented as absenteeism of proficient guardianship. When TFSV was in direct relation to physical violence, police could take immediate action. Exceptions to this were evident in the case of sexual solicitation and exploitation of children, or the bullying and harassment of children online. Henry and Powell (2015) suggested TFSV was an age-specific issue of vulnerability, where young people can have protection from online predators. The law was not ready to address TFSV due to the fast pace of technology change. Attention to the unique harms victims experience could help attain legislative and cultural change. TFSV is a crime that necessitates a response from the individual, organization, and societal level (Henry & Powell, 2015).

Holt and Bossler (2014) examined the current literature on forms of cybercrime and the theoretical frameworks utilized to address the issue. They discovered technology allowed facilitation of new crimes that were not otherwise probable. The new crimes included the circulation of malicious software, hacking that can cause considerable economic harm, and the loss of sensitive personal data and intellectual property.

Holt and Bossler (2014) explored existing literature on various forms of technology-enabled crime issuing Wall's (2001) four-category cybercrime typology: (a) cyber trespass, (b) cyber deception and theft, (c) cyber porn and obscenity, and (d) cyber violence. Cyber trespass occurred when an individual is attempting to access a computer system, network, or data source without the permission of the system owner, thus violating the boundary of ownership. Cyber deception and theft comprised the use of the Internet to steal information or illegally obtain objects of worth from an individual or

corporation. Cyber porn and obscenity involved a range of sexual expression accessed via computer-mediated communications and distribution of sexually explicit materials online. Cyber violence included the ways individuals can cause harm in a real or virtual environment, such as stalking, harassment, and bullying online. Holt and Bossler claimed that researchers should evaluate under-examined practices of cybercrime offending and victimization.

Marcum, Higgins, and Ricketts (2014) explored the cyberstalking activities of adolescents under the age of 18 and assessed the predictors of their behaviors. Marcum et al. used the general theory of crime and social learning theory as the basis to understand predictor cyberstalking behavior. Marcum et al. performed this study to provide a richer representation of adolescents who participate in cyberstalking and to predict such behaviors. Low self-control and peer deviance links to the cyberstalking behavior of adolescents (Donner et al., 2014b; Marcum et al., 2014). Individuals with a high level of intelligence had a greater probability of committing cyberstalking (Marcum et al., 2014).

Restitution. Child pornography was, and remains, a tragedy of the technology age. The child pornography industry nearly disappeared during the 1980s. With the evolution of the Internet, child pornography evolved into a multibillion dollar business. Reiss (2011) examined if persons convicted of nonproduction child pornography, such as distribution, receipt, and possession, should have to pay restitution to the children whose images are in their custody. Reiss deducted that the U.S. Supreme Court decisions had little bearing on the majority of cases of child pornography victims. Reiss defended the

call for uncommon solutions, such as a victim compensation fund that would help victims recover emotionally and ease the strain on court systems.

Targets of cybercrime ranged from governments, corporations, to individuals. Common cybercrime presented the perpetrators committed the offense using a computer or other online or electronic platform. Näsi, Oksanen, Keipi, and Räsänen (2015) used routine activities theory, developed by Cohen and Felson (1979), to explore characteristics and predictors of cybercrime victimization at the individual level, while focusing on adolescents. At the individual level, forms of cybercrime included sexual solicitation or harassment, identity theft, defamation, fraud, or phishing. Näsi et al. aimed to provide new information regarding young Internet users, while examining the perception of exposure to cybercrime victimization and the components that affect those adverse occurrences of the adolescents.

Nobles, Reyns, Fox, and Fisher (2014) reported cyberstalking as a moderately studied area in criminology, with no agreement on whether cyberstalking characterizes a form of stalking or a new criminal phenomenon. Nobles et al. defined cyberstalking by using responses from individuals' experiences with harassing communications from the Internet. Nobles et al. revealed substantial variances amid stalking and cyberstalking victims, including some self-protective behaviors adopted, the length of contact with their stalker, financial costs of victimization, and perceived fear at onset. Individuals, who realized they were a victim of cyberstalking, were more likely to protect themselves. The public could benefit from cyberstalking education to recognize the signs and equip themselves with techniques for prevention (Nobles et al., 2014).

Tener, Wolak, and Finkelhor (2015) provided a qualitative, experiential typology of offenders who commit sex crimes against adolescents in the online realm. The offenders included in the study met the adolescent online or in person. Tener et al. based their analysis on grounded theory framework and focused on consistent comparisons for 75 of the 2,009 arrest narratives in the Third National Juvenile Online Victimization study. During the analysis, the development of four offender characteristics is: (a) patterns of online communication, (b) offline and online identity, (c) relationship dynamics with the victim, and (d) levels of sex crime expertise. Four additional typologies of offenders include: (a) the experts, (b) the cynical, (c) the affection-focused, and (d) the sex-focused. Understanding the sex-criminal typology was important when assessing and delivering the intervention to offenders and victims (Tener et al., 2015).

Cybercrime's Social Effects

Cyberbullying. In October 2006, cyberbullying became a national news headline when the suicide of a 16-year old occurred due to repetitive bullying through social networking sites. Cyberbullying was defined as the "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices" (Navarro & Jasinski, 2012, p. 81). Navarro and Jasinski recognized the criticality for scholars to continue researching predictors of cyberbullying, as technology continued to evolve. In part, their use of routine activities theory was to evaluate cyberbullying experiences.

Navarro and Jasinski (2012) obtained cyberbullying data by conducting phone interviews with 935 teens and their parents from the Pew Internet and American Life Project website. Interviewers asked questions relating to offline and online activities and

experiences. Results of the research determined victim gender was significant in the likelihood of experiencing cyberbullying, while adolescent females were at greater risk for experiencing cyberbullying than adolescent males. Navarro and Jasinski suggested teens engaged in the act of cyberbullying while conducting harmless activities, with instant messaging reported as the most dangerous youth online activity. Remarkably, many teens never reported incidents of cyberbullying to an authority.

Stewart and Fritsch (2011) presented an overview of the cyberbullying problem and defined characteristics of cyberbullying. Early on, bullying by electronic means became a mounting issue. Cyberbullying produced disturbances to educational environments and severe psychological and physical results for victims. Stewart and Fritsch focused on the progressively predominant problems of cyberbullying amid adolescents, and emphasized distinguishing cyberbullying from other types of cybercrime. Cyberbullying was not directly a part of any penal codes, but many of its actions can be indicative of standing statutes. Stewart and Fritsch stressed that school districts, in conjunction with law enforcement agencies, have a role in combating cyberbullying.

Chan-Mok, Caponecchia, and Winder (2014) studied the treatment of workplace bullying. Considerations were on health and safety legislation, as it applies to workplace bullying. Through case study design, comparisons of health and safety laws, risk management theoretical views, and legal cases, there was an attempt to clarify the management of workplace bullying. Chan-Mok et al. used Crawshaw's 23 terms to identify workplace bullying. In a review of the health and safety law applied to legal

studies, continuous findings revealed that workplace bullying was only punishable if it was a repeated offense. A repeated offense was in direct opposition to the health and safety law that indicated employers should ensure employees reduce exposure to any risks. The standards of repeated exposure to workplace bullying conflicted with legal principles courts maintained to enforce health and safety law (Chan-Mok et al., 2014).

Fahie and Devine (2014) conducted a study that included victims of workplace bullying who work, or have worked, in primary schools. They integrated key concepts of Foucault's (2002) theory of power and Davies' (2006) theory of subjectification for their formulation of the bullying analysis. Through qualitative research, Fahie and Devine analyzed 24 in-depth interviews conducted with self-identified workplace bullying victims. Participants revealed the nature of the bullying behavior, the outcomes for themselves, and the outcomes for the primary school community.

Fahie and Devine (2014) also questioned the participants about the strategies they used to cope with workplace bullying. Fahie and Devine ascertained their work is consistent with the Namie and Namie (2003) model, where four main dimensions of the effect of workplace bullying emerged: (a) psychological, (b) physical, (c) social, and (d) economic. Fahie and Devine reported that when a person was a victim of workplace bullying, they found it hard to view it as anything else.

Hong, Chien-Hou, Hwang, Hu, and Chen (2014) investigated the relationship between positive affect, perceived organizational innovation climate, the experience of being the recipient of cyberbullying, and psychological responses to cyberbullying. Hong et al. utilized the self-evaluation theory as a research model, and demonstrated that

cyberbullying incidents were not prevalent in the high-tech industry. For those few that were a victim of cyberbullying, Hong et al. concluded every bullied victim felt psychological and mental abuse.

Similar to Hong et al. (2014), Langos (2015) discussed the potential harm of cyberbullying, founded on original empirical research and a crime seriousness framework applied to traditional crimes. Langos's analysis provided theoretical awareness into the related harms of each form of cyberbullying. Forms of cyberbullying for analysis included happy slapping, masquerading or impersonation, denigration, harassment, and exclusion.

Langos (2015) described an account of the Feinberg (1984) harm principle as justification for criminalizing wrongful conduct. By using the Feinberg harm principle, Langos ranked each form of cyberbullying. The research demonstrated forms of cyberbullying at different levels of harm. Langos determined, based on the principle of harm, not all forms of cyberbullying warrant criminalization. Happy slapping, denigration through sexual or intimate image or video recording, and cyberstalking represented the most severe forms of cyberbullying.

Community. A form of social community, as addressed by Wellborn (2012), is the establishment and use of undercover profiles made by educators on social networking websites, such as Facebook or MySpace. When a teacher created a fabricated profile and became a friend of one of their unaware students, the teacher had a complete view of the student's life. As social networking use by high school and college students continued to increase, these occurrences also continued to rise.

For the educator to face criminal charges, the definition of mandatory rules and regulations of the social networking website was required. Courts have repeatedly ruled all rights lie with the computer owner. In a civil setting, courts may enforce a violation of website owner terms of service, but are less likely to do so in a criminal setting. Wellborn (2012) indicated that educators should understand the undercover use of social networking websites is a bad idea; educators should not add the threat of jail time to their list of professional challenges.

Another form of social community is the bring your own device (BYOD) phenomenon. BYOD allowed employees to bring personally owned technology to their workplaces. Gaff (2015) researched BYOD from a productivity improvement and employer risk perspective. BYOD can make a company's IT systems and data more vulnerable to malicious activity. For example, BYOD occurred when a company allowed an employee to utilize their personal mobile device to receive corporate email. Companies to institute a formal BYOD policy, to ensure the security of its systems, protect the confidentiality of its corporate information, and respect the privacy of its employees (Gaff, 2015).

Gaff (2015) reported that permitting employees to use their personally owned devices for work-related purposes might increase productivity. Recommended employer BYOD policies contained information for acceptable devices for use, nonsupport of the device, installation of virus security application, and a stipulation that the employee owns the device and is solely responsible for the device. Gaff proposed a firm's attorney should create the BYOD policy, to avoid potential litigation. When companies did not have a

formal BYOD policy, they opened the doors for potential cyberattack. The potential for company data leakage heightened, when an employee's personal device did not have the proper encryption certificate for secure retrieval of corporate email. Those who do not recognize the need for encryption and email protection, on personal (or corporate) mobile devices, can leave themselves vulnerable for cyberattack (Gaff, 2015).

Holt (2013) applied Best and Luckenbill's (1994) framework of social organization to the social community of openly available web forums, where individuals bought and sold stolen financial intelligence. The Best and Luckenbill framework concentrated on relations amid individuals and groups and the transactions in which they participate. Within the framework, the basis of deviance presented the concept of transactions and the focus of behavior.

Mutual association and participation were clear as the forums expedited connections between interested individuals to sell or acquire data. At the individual level, participants operated in relaxed, mutual connotation, and principally alone or in peer groups with a narrow division of labor (Holt, 2013). Participants in stolen data forums functioned at various stages of deviant sophistication. Holt urged law enforcement agencies to work together globally to ensure responsible criminals are detected and brought to justice.

Posey et al. (2014) assessed the social community of company insiders and their knowledge of information security efforts. Reviews of the beliefs underwent comparison alongside the mindset of information security professionals. Usage of the protection motivation theory was to analyze group views of how insiders become protective agents

against organizational information security threats. Categorization of assessments determined threat appraisal or coping appraisal characteristics. Posey et al. argued that insiders are not oblivious to the consequences their actions have on internal information security efforts. Motivating factors for insiders were financial gain and retribution. Posey et al. emphasized security professionals should strive to leverage the social influence and loyalty of insiders when designing security-training programs.

Schilke, Reimann, and Cook (2013) investigated the social community of trust recovery after a trust breach takes place. Schilke et al. examined why some types of relationships recover better from a trust breach than others. Schilke et al. hypothesized that the longer the relationship, the better chance of trust recovery after a trust breach. Examination of two behavior tests against their hypothesis were online and in a laboratory. The first test consisted of 100 participants that completed an eight-question survey of questions related to general trust. The second test included 22 members that underwent an MRI while engaged in the behavior task of gambling. Schilke et al. explained the length of a relationship would ease the trust recovery level when trust break occurs.

Fraud. The Federal Computer Fraud and Abuse Act (CFAA) banned evident computer-related conduct if harms exceed $5,000 in a single year (Kain, 2013). The CFAA covered hackers, but not employee-hackers. The identification of an employee-hacker is that of a former staff member that takes computer data and uses it in an anticompetitive method after leaving the company (Cheng, Li, Li, Holm, & Zhai, 2013). Delivery of split rulings for such behavior was derivative of state courts (Cheng et al.,

2013). Kain (2013) discussed the divisions between the courts, where unauthorized access to data was a violation in some jurisdictions without repute to the ensuing exploitation of the data.

The CFAA granted three broad access violations: (a) intentionally accessing a computer without authorization to obtain information, (b) intentionally accessing a protected computer without authorization and recklessly causing damage, and (c) intentionally accessing a protected computer without authorization to cause damage. Kain (2013) observed implications to CFAA as it related to employee-hackers and the meaning of authorized access. State courts are likely to have cases appealed to the Supreme Court, as CFAA leaves much to interpretation.

Anandarajan et al. (2013) compared U.S. data breach notification statutes. Drawing upon the state rulings, Anandarajan et al. provided a conceptual definition of severity of data breach notification statutes throughout the United States. The conceptual definition was derivative of proportions central to the model and for creating the Data Breach Notification Statute Index (DBNSI). The DBNSI indicated which of the exacted state data breach statutes were most effective and least effective. Additionally, Anandarajan et al. used Cohen and Felson's (1979) routine activities theory to investigate if DBNSI is beneficial in understanding the role of the state.

Anandarajan et al. (2013) established routine activities theory to examine the incidence of crime by reviewing the circumstances surrounding the events of the offense. Cohen and Felson (1979) asserted three characteristics were necessary for a crime to occur: (a) a motivated offender, (b) a suitable target for victimization, and (c) the absence

of a capable guardian against the violation. Anandarajan et al. declared that routine activities theory served as a useful theoretical lens for understanding how technology shifts affect a wide variety of criminal offenses, such as identity theft and unauthorized use of personally identifiable information.

Deibert (2012) investigated rising despondency of cyberspace, and identified six driving forces:

1. Cloud computing;
2. Expansion of cyber users from the global South;
3. Economy of cybercrime;
4. Espionage, sabotage, and warfare;
5. State involvement in cyberspace governance; and
6. The industrial sector of cybersecurity protection (p. 262).

Deibert contended that few citizens outside of the United States realized that if their data storage is with Google, even if the location of those machines is in the users' local country, they are subject to the U.S.A. Patriot Act. With Google's headquarters located in the United States, the U.S.A. Patriot Act compels Google to turn over their data when required, regardless of data storage location.

Deibert (2012) claimed regulation and control of cyberspace is crucial on a daily basis. Criminals are no longer young men creating viruses in their basement. Cybercriminals are now highly professional transnational enterprises worth billions annually. Espionage, sabotage, and warfare present high-level cyber breaches against governments, private companies, and other infrastructure. The OpenNet Initiative

estimated as many as 960 million people are living in jurisdictions that censor the Internet, which equals 47% of the entire Internet population worldwide. Market estimates have grown to tens of billions of dollars annually. Deibert proposed a distributed approach where governments self-limit and check each other's behavior in mutually transparent ways.

Huth et al. (2013) documented four new approaches to address components of the problem of data leakage and insider threats, with the objective of decreasing the harm malicious insiders can inflict on an organization. Preventing, detecting, and responding to data leakage transmitted by authorized user or insider threats was among the most difficult challenges facing security researchers and professionals. Malicious insiders continued to succeed in harming organizations by leaking sensitive information. A malicious insider threat occurs when an employee or business partner, who has access to an organization's network, intentionally misuses their access for a negative effect on the confidentiality or integrity of the organization's information.

Insider threats categorizations are technical, social, or socio-technical. Insider threats focused on motivations, organizational culture, and workplace reporting. The description of data leakage outlined different types of crimes perpetrated by insiders, including theft of personally identifiable information, theft of intellectual property, or for an insider to pass sensitive or classified information to an unauthorized third party. Huth et al. (2013) revealed three stages of data leakage and theft: (a) obtaining access, (b) downloading data, and (c) sharing data. Common motivations for insider data leakage included revenge or for-profit means.

Kraemer-Mbula, Tang, and Rush (2013) explored the globalization of credit card fraud and identity theft within the digital ecosystem conceptual framework. Kraemer-Mbula et al. developed a framework to contribute a new perspective of how cybercriminals innovate, organize, and operate. Emphasis focused on how law enforcement agencies change to combat the growing cybercrime trend. Credit card fraud (illicit use of stolen credit cards and credit card details) and identity theft (using someone's personal details without their knowledge) was the focus of the study. Particularly relevant to this study, Kraemer-Mbula et al. acknowledged that small businesses might be particularly vulnerable to cybercrime, as they may not have full knowledge of how their IT systems function.

The outline of the cybercrime value chain has three basic activities: (a) detecting vulnerabilities, (b) infection and distribution, and (c) exploitation. Data harvesting and exploitation were the two essential credit card fraud and identity theft activities in financial cybercrime. Discussion of potential tools for cybercriminals included the loyalty, business-process-outsourcing, hybrid, and Internet-based business models. Kraemer-Mbula et al. (2013) concluded that digital business ecosystems provided a holistic framework to analyze the cybercrime industry from a variety of angles. Kraemer-Mbula et al. recommended their framework had the potential to assist law enforcement efforts to identify the types of data required to capture players and events of cybercrime.

Reyns (2013) explored routine activities theory about crimes where the offender and victim do not come into physical contact. Comparable to Anandarajan et al. (2013), Reyns used Cohen and Felson's (1979) routine activities approach to examine physical

contact crimes. In 2003, Eck and Clarke expanded routine activities theory to explain crimes where the victim and offender do not interact at the same physical location. Reyns expanded on the theoretical framework and analyzed online routines and identity theft.

Reyns (2013) accessed the relationships between individuals' online routine activities (banking, shopping, downloading), individual characteristics (gender, age, employment), and a perceived risk of identity theft victimization. Reyns suggested individuals, who used the Internet for banking, email, or both, were 50% more likely to become victims of identity theft. Online shopping and downloading increased chances of victimization by 30%. Males and older individuals with high incomes were more likely to experience victimization. Reyns identified routine activities theory, originally written for physical contact crimes, could apply to noncontact crimes.

Transition

Small business leaders experienced the same cybersecurity threats as large corporations, yet many small businesses continue to struggle to protect their systems from data breaches. The purpose of this study was to provide small business leaders with cybersecurity strategies they can implement to improve the protection of their systems from data breaches. The research design of this study was a qualitative exploratory case study. The population for this study included small business leaders from the Middlesex County region of Massachusetts. Small business leaders participated in an online questionnaire containing open-ended questions and semistructured face-to-face interviews. Those leaders chosen were most suitable to identify the cybersecurity

strategies needed to protect their systems from data breaches. For methodological triangulation purposes, a review of company documents was performed (Yin, 2013).

The background of the problem and problem statement encompassed the consequences cybercrime has on small businesses. In particular, those small businesses that do not have cybersecurity strategies in place run a significant risk to their operations and continued survival. The purpose statement identified the proposed research design as an exploratory case study and provided details of the target population and format of the open-ended questions. The overarching research question guiding the focus of the study asked, "What cybersecurity strategies do leaders of small businesses implement to protect their systems from data breaches?"

In Section 1, I discussed the conceptual framework that was used to develop the study. Systems thinking theory materialized as the main framework for the study, after a review of the available professional and academic literature. The creation of systems thinking theory was from a comprehension of how items work including functionality, structure, and processes. Significant within systems thinking theory was the allowance of explanations of strategies and experiences. Routine activities theory is the secondary conceptual framework for this study. The usage of routine activities theory was to explain crime concerning space and time. Additionally, usage of routine activities theory was to explore the means in which a criminal may commit a crime.

Also within Section 1, I offered a list of operational definitions to provide readers of the study a precise meaning of terms. Assumptions, limitations, and delimitations offerings distributed the risks, weaknesses, and parameters for the study. The significance

of the study contributed to the business practice and implications for social change. The final element of Section 1 included a comprehensive review of the professional and academic literature concerning cybersecurity's financial, legal, sexual, and social effects.

In Section 2, I describe the role of this researcher, participants, research method, research design, and population and sampling. Additional pertinent details include the data collection instruments, data collection technique, data organization technique, and data analysis. Reliability and validity discussions ensue, ending with a transition and summary of the section.

Section 3 of the study includes a presentation of the findings, applications to professional practice, and implications for social change. Additional discussions offer recommendations for action and recommendations for further research. The study closes with reflections, summary, and conclusion elements.

Section 2: The Project

The focus of this qualitative exploratory case study was exploring the effectiveness of small business cybersecurity strategies that safeguard systems from data breaches. I collected data from small business leaders using an online questionnaire containing open-ended questions, as well as semistructured face-to-face interviews with a subset sample of three of the participants. Understanding small business leaders' experiences of cybersecurity strategies may aid in the creation of efficient plans to protect their systems from data breaches. Section 2 of this study addresses the (a) restatement of the purpose; (b) role of the researcher; (c) research participants, method, and design; (d) population and sampling; (e) ethical research; (f) data collection instruments, techniques, organization, and analysis; (g) reliability; and (h) validity. Section 3 of this study follows with a presentation of the research findings.

Purpose Statement

The purpose of this qualitative exploratory multiple case study was to explore the cybersecurity strategies that small business leaders used to protect their systems from data breaches. The targeted population for this study included five leaders of small companies located in the Middlesex County region of Massachusetts who had successfully implemented cybersecurity strategies to protect their systems from data breaches. The population for this study was appropriate, as researchers have found that the majority of small businesses do not place appropriate investments in cybersecurity (Densham, 2015; Hayes & Bodhani, 2013). The study's implications for positive social change include the potential for decreasing theft of sensitive, protected, or confidential

data. Further, implementing cybersecurity strategies in small businesses may reduce the loss of personally identifiable information.

Role of the Researcher

For this qualitative exploratory case study, I was the primary data collection instrument as the sole researcher in the data collection process. Qualitative researchers should display poise, equality, and comprehensiveness in their data analysis and interpretation (Leedy & Ormrod, 2015). The secondary data collection instrument was an online questionnaire containing open-ended questions to gather themes, which I distributed electronically to each participant. The purpose of creating open-ended questions was to return results containing abundant descriptions of lived experiences (Giles & Yates, 2014). I have great familiarity with the topic of effective cybersecurity to improve the protection of systems from data breaches. My profession as senior vice president of information technology for a leading vendor in the security industry provides me with a wealth of understanding of the subject.

Regarding ethics, I ensured that all participants in the online questionnaires and semistructured face-to-face interviews were cognizant about and agreed to the nature of this study, as suggested by Leedy and Ormrod (2015). Informed consent forms were collected from each participant before their involvement in the study; participants also received written assurance of their confidentiality as contributors (see Appendix A). Ethical standards applied throughout the study were in alignment with the principles outlined in the Belmont Report (Fiske & Hauser, 2014).

To mitigate bias, I defined reasonable beliefs, expectations, and cultural values that could prejudice the study, as recommended by Leedy and Ormrod (2015). Researchers cannot inject themselves into a study, or the result of the investigation will be biased (Brayda & Boyce, 2014). Viewing the data through a personal lens allowed me to acknowledge potential personal beliefs and outlooks that could distort interpretations. The rationale for the online questionnaire format was to allow participants to provide immediate feedback and to minimize researcher misinterpretation (Salmons, 2015). In an attempt to gain honest information from participants, I employed an online questionnaire containing open-ended questions. The online format provided a contemporary form of technology that delivered structure and confidentiality for the respondents (Salmons, 2015). A subset sample of three small business leaders, who indicated that they had successfully addressed the business problem within their online questionnaire responses, also partook in semistructured face-to-face interviews.

Participants

I gathered data through a questionnaire that contained open-ended questions, with initial question delivery in an online format. I did not implement a pilot study, as the theme development transpired from the online questionnaire and semistructured face-to-face interview responses. The initial online open-ended questionnaire aligned with the nature of the topic as a technology-based tool (Salmons, 2015). The eligibility criteria, as recommended by Reybold, Lammert, and Stribling (2013), indicated that study participants must be small business leaders located in the Middlesex County region of Massachusetts. The strategy for gaining access to potential participants was to obtain

their names and email addresses from the Massachusetts district office of the U.S. Small Business Administration.

I sent a written letter of request for information via Federal Express to the director of the Massachusetts district office in order to obtain a list of at least 100 Middlesex County small businesses (see Appendix C). Prospective participants received an invitation via email; I received five acceptances to complete the initial online open-ended questionnaire. From the initial participant list, a subset sample of three small business leaders partook in the semistructured face-to-face interviews.

Establishing a working relationship with the participants was essential from the onset of the first written invitation communication (Yin, 2013). The relationship was one of transparency, respect, and trustworthiness, as proposed by Wolgemuth et al. (2015). The goal of the relationship was to explore and discover effective cybersecurity strategies for improving the protection of systems from data breaches. Confirmed participants supplied their preferred method of communication, which I observed throughout the study (see Appendix A). Telephone, email, or other technology communication options were available at the participant's discretion for discussion purposes only.

Research Method and Design

The basis for the selection of the research method and design of this study was derivative of the research question, requirement, and objectives, as suggested by Khan (2014). The goal of the study was to ascertain cybersecurity strategies that small business leaders can apply to advance the safety of their systems from data breaches. The qualitative exploratory case study research method and design provided the structure for

the study. Data collected from small business leaders through an online questionnaire containing open-ended questions, followed by semistructured face-to-face interviews with a subset sample of three of the five participants, helped me to understand the strategies to secure participants' systems.

Research Method

The qualitative research method aligned with the aim of this study to explore cybersecurity strategies that small business leaders can implement to protect their systems from data breaches. The basis of qualitative research is interpretation of the experiences of individuals regarding a particular event (Khan, 2014). The discovery of cybersecurity strategies for small business leaders to implement was reliant on understanding how they interpreted the protection of their systems. Yilmaz (2013) defined qualitative research as an evolving approach to studying people in their familiar environment to discover the significance they attach to their experiences. Through the online questionnaire, small business leaders had an opportunity to share their cybersecurity experiences. Qualitative research allowed for an understanding of the knowledge and beliefs of the subjects of the study (Yilmaz, 2013).

I collected initial responses from the participants by using an online questionnaire, as recommended by Percy et al. (2015). In qualitative analysis, themes emerged from the data (Bendassolli, 2014). Knowledge and understanding of the topic allowed for the development of categories from participant experiences (Percy et al., 2015). Exploration of the data from each online questionnaire allowed me to construct the overarching themes to develop a categorical code database. A combination of the data from all

participants revealed consistent patterns. Synthesizing the topics provided a full picture of the data collected regarding the research question, as recommended by Percy et al. (2015).

I considered the use of quantitative and mixed-methods research approaches for this study. Quantitative research, from a human observational perspective, focuses on the review of a particular behavior to determine frequency or rating (Leedy & Ormrod, 2015). The intent of this study was to gain a deeper understanding of small business leaders' cybersecurity strategies as they pertained to protecting their systems from data breaches. A quantitative numerical analysis would not have supplied a thematic result to answer the research question of this study. Mixed methods research is a combination of qualitative and quantitative analysis to derive completeness (Leedy & Ormrod, 2015). A mixed-methods study is relatively complex and requires extensive time and energy from the researcher (Leedy & Ormrod, 2015). A mixed-methods approach was not appropriate for this study, as the use of quantitative data would not have provided comprehensive answers to the research question.

Research Design

Qualitative research designs include ethnography, grounded theory, phenomenology, the Delphi technique, and case study. I explored each qualitative research design for its applicability in this study. Upon review, I found that an exploratory case study was the most appropriate qualitative design for this study. The focus of this study was exploring small business leaders' strategies and experiences as recommended by Yin (2013). Exploratory case study allowed for the investigation of

cybercrime strategies in small businesses in a real-world context, where there may not be a single set of outcomes.

In ethnography, researchers immerse themselves in the environment of the cultural group they are studying for a particular period to understand members' behaviors (Small et al., 2014). Participant observation allows the ethnographer to grasp the point of view of the group under study. It is not the aim of the ethnographic researcher to understand a phenomenon, but rather to immerse themselves in the atmosphere of their subjects to collect data about behaviors (Small et al., 2014). Ethnography was not an appropriate design for this study, as it was not necessary to understand cultural behaviors of the participants.

Grounded theory allows researchers to develop theories through the course of recognizing categories via personal interactions (Chittem, 2014). Researchers using the grounded theory design submerge themselves into the effort to understand the social world to perform actions of theoretical sampling, data collection, coding, memos, and writing (Lo, 2014). The goal of this study was to explore the strategies that small business leaders use for cybersecurity. Grounded theory was not an appropriate design for this study, as it was not the goal to develop theories upon conducting personal interfaces with small business leaders.

Phenomenology involves a descriptive stance, wherein the researcher seeks to describe the essence of experiences (Gill, 2014). Phenomenology includes the interpretive examination of human experiences of being (Gill, 2014). Researchers who use the phenomenological design conduct participant interviews to identify common

themes of experiences (Gill, 2014). The phenomenological design might have been useful for this study, if the focus had been on the lived experiences of the small business cybersecurity professional. Serious deliberation occurred as I considered a phenomenological research design. Phenomenology is the exploration of lived experiences and beliefs (Cunliffe, 2011). Given that the goal of this study was to obtain strategies of small business leaders to maintain their companies' cybersecurity, the use of phenomenological design was not appropriate.

The Research and Development Corporation established the Delphi technique for technology forecasting (RAND Corporation, 1967). The assumptions made by some users of the Delphi technique suggest that group consensus carries greater weight than an individual view (Snape et al., 2014). Some researchers perceive the Delphi technique as unsatisfactory due to the forced nature of the group consensus, and due to the exclusion of individual opinion expansion (Snape et al., 2014). As the goal of this study was not the development of small business leaders, cybercrime policies, or group consensus, the Delphi technique was not an appropriate design.

In this qualitative exploratory case study, data collection took place through online questionnaires, semistructured face-to-face interviews, and review of company documents. Data saturation occurred when no new themes or codes were achievable from the data collected (Ando, Cousins, & Young, 2014). The participants in this study included five small business leaders who completed an online questionnaire containing open-ended questions. Thematic coding of the responses from the online questionnaire was the basis for a codebook (Ando et al., 2014). A subset sample of three participants

from the initial five partook in semistructured face-to-face interviews to gain additional information to reach data saturation.

Population and Sampling

The population for this study was small business leaders from the Middlesex County region of Massachusetts. From the population, a purposeful sample of five participants who successfully addressed the business problem partook in an online questionnaire containing open-ended questions. From the purposeful sample of five participants, a subset sample of three small business leaders partook in semistructured interviews via face-to-face discussions. Purposeful sampling is appropriate for qualitative studies to collect data from participants who are knowledgeable about the research topic (Elo et al., 2014). The appropriateness of the sample size in a qualitative study is dependent upon the context of the study (Kasim & Al-Gahuri, 2015). There exists no uniform unbiased sample size for qualitative research, which is suitable for a case study (Molenberghs et al., 2014). The exploratory case study design was applicable for the analysis, as multiple participant responses allowed for replication of the results and data saturation, as suggested by Yin (2013).

I selected a purposeful sample of five small business leaders from the population of small business leaders from the Middlesex County region of Massachusetts. Purposeful sampling involved gaining knowledge-rich data from participants who had successfully addressed the business problem, which aligned with the purpose of the study (Reybold et al., 2013). A subset of three participants from the five small business leaders in the purposeful sample partook in semistructured face-to-face interviews. Eligible

participants in the study were small business leaders who had successfully addressed the business problem and were willing to contribute to an online questionnaire containing open-ended questions and semistructured interviews in a face-to-face setting. The online questionnaire took approximately 30 minutes to complete. For participants in the semistructured face-to-face interviews, the process was no longer than 60 minutes in duration, and the location was at the discretion of the participants.

Data saturation occurred when no additional themes or categories were derived from the data (Ando et al., 2014). Researchers can realize data saturation when no new findings are relevant to the purpose of the study (Kasim & Al-Gahuri, 2015). The achievement of data saturation signifies the optimal sample size (Elo et al., 2014). In qualitative studies, when the sample size is illustrative of the target population and is information rich, readers may relate the results to comparable conditions (Percy et al., 2015). Five open-ended questionnaires were sufficient to provide the majority of themes and codes necessary in qualitative research, as recommended by Ando et al. (2014). Additional semistructured face-to-face interviews, after the identification of three core themes, did supply modifying classifications for a more generalized result, as suggested by Ando et al. (2014). In this study, I fulfilled data saturation when it became ineffective to create new themes and categories that added to the purpose of the study, as recommended by Kasim and Al-Gahuri (2015). I did not conduct a pilot study, as theme development transpired through the analysis of data from online questionnaires and semistructured face-to-face interviews.

Ethical Research

Ethical protection of participants is a critical component of research studies. I sought the permission of the Walden University Institutional Review Board (IRB), to commence the research portion of this study. Upon selection of the potential research site and participants, I obtained the permission of the study site from the prospective companies for inclusion in the study. Upon the receipt of permission from the companies, and after the IRB granted permission to initiate the study, I sent an informed consent form to prospective participants. The informed consent form includes details of the study, participant rights, and instructions to indicate acceptance to partake in the research (Ando et al., 2014; Khan, 2014). Participants voluntarily agreed to contribute in the study by replying to the original email of the informed consent form (see Appendix A) with the words "I consent".

Participants could withdraw from the study or interview process at any time without penalty by simply contacting me via email or telephone. Participants did not receive incentives to partake in the study or interview process. Establishment of identity protection of research contributors and confidentiality of interview data for not less than 5 years adhered to IRB standards before exploration initiation (Fiske & Hauser, 2014).

Guaranteeing the protection of individuals' names and company information occurred through a masking process to preserve confidentiality and privacy (Khan, 2014). Labeling participant names represented the participant as a random number, and a random letter represented company names. Storage of an electronic scan of executed informed consent is on a password protected flash drive, with the original paper copies

immediately shredded after scanned. Data from the online questionnaires and semistructured face-to-face interviews are stored electronically on a password protected flash drive for no longer than 5 years from the date of interview. After 5 years, all electronic informed consent forms, interview data from the password protected flash drive, and destruction of the flash drive will be through secure measures.

Data Collection Instruments

In this qualitative exploratory case study, I was the primary data collection instrument, with an online tool being the secondary instrument. Five small business leader participants answered 10 open-ended questions via usage of the Survey Monkey online tool as proposed by Elo et al. (2014). Each question was open-ended to allow participants to share their thoughts and detailed experiences (Khan, 2014). The 10 open-ended questions related to von Bertalanffy's (1972) systems thinking theory (see Appendix B).

Upon completion of the online questionnaire by the five small business leaders that had indicated they successfully addressed the business problem via their acceptance of the Informed Consent Form (see Appendix A), a subset sample of three participants partook in semistructured face-to-face interviews to gain additional data regarding their cybersecurity strategies. The subset semistructured face-to-face interview was the final information gathering session, where I asked the small business leaders to elaborate on the initial 10 questions they responded to via the online format. Yin (2013) recommended methodological triangulation of interview data with various sources for additional variables of interest. For methodological triangulation points, an examination of company

documents transpired to strengthen the validity of the study as suggested by Yin (2013). The objective of the data collection instruments was to obtain participant opinions and viewpoints concerning effective cybersecurity strategies to protect their systems from data breaches (Khan, 2014). Through the responses of the participants, I was able to reveal the effectiveness of the cybersecurity strategies in their small businesses.

The reliability and validly of the data collection instrument is essential in qualitative studies to minimize bias and subjectivity (Pozzebon & Rodriguez, 2014). Demonstration of the reliability of a case study is by repeating the same data collection method by another researcher that will achieve the same result (Pozzebon & Rodriguez, 2014; Yin, 2013). To realize reliability, in this case study, I prepared complete documentation of all research steps and procedures and ensured the research method and design were consistent throughout the study. Validity refers to the correctness of the findings as defined by the researcher and participants (Elo et al., 2014). Participants of this study received a full transcript of their responses to the online questionnaire to confirm their responses were accurate. Participants of the semistructured face-to-face interviews received a full transcript of my interpretation of their responses, which allowed them to perform member checking, confirming my understanding of their interviews responses was accurate.

Data Collection Technique

The data collection technique for this qualitative case study was a three-stage process. The first phase of data collection was from five participants who answered 10 open-ended questions in an online format. Within the Informed Consent Form (see

Appendix A), each of the five participants that accepted to be in the study did so by agreeing that they had successfully addressed the business problem. The online qualitative data collection employed the acquisition of error-free transcripts that were date and time stamped (Wilkerson, Iantaffi, Grey, Bockting, & Rosser, 2014). Survey Monkey was the online tool selection, where data collection occurred without interaction to diminish researcher input and bias (Morison, Gibson, Wiggington, & Crabb, 2015). Online data collection provided an advantage that allowed for greater participant openness due to observed anonymity, which applied to the sensitive topic of cybercrime (Wilkerson et al., 2014). A disadvantage of online data collection might exist if participants did not have access to a computer (Wilkerson et al., 2014).

The online questionnaire provided anonymity for participant responses. The Survey Monkey tool identified the Internet Protocol (IP) address of each responder. I did not utilize any IP search methods to discover the responders' location. The population of small business leaders in this study contributed via an email message, which ensured they had access to a computer. Each participant received an invitation, sent via email, which included a website link for access to complete the questionnaire. Upon completion of the online questionnaire, the participants clicked a submit link, and the data was saved securely via the Survey Monkey online tool.

After 1 week from the date of sending the email invitation, I checked to see the number of responses to the online questionnaire. After another week, I engaged two more potential participants from the list of Middlesex County small businesses. I continued this action until I secured five questionnaire responses. Probing follow-up questions were via

semistructured face-to-face interviews with a subset sample of three small business leaders. I added a section at the end of the online questionnaire asking respondents to supply their email address if they would like to participate in the second phase of the data collection.

The second phase of data collection was from semistructured interviews in a face-to-face setting. Three participants of the five respondents contributed in the semistructured face-to-face interviews. The subset sample of three participants partook in semistructured interviews in a face-to-face format to gain additional details from their responses to the original 10 questions. An advantage of the semistructured face-to-face interview offered participants the opportunity to expand their strategies and beliefs of the research topic (Khan, 2014). A disadvantage of the semistructured face-to-face interview would have occurred if the question delivery were in a biased manner (Yin, 2013).

The semistructured face-to-face interview was at the date, time, and location of choice of the participant in agreement with their availability (Yin, 2013). With prior participant permission, a recording device captured the dialogue of each semistructured face-to-face interview. During each semistructured face-to-face interview, I maintained the following ordinal process:

1. Introduce the research topic;
2. Explain the consent form (see Appendix A);
3. Present the recording device;
4. Emphasize confidentiality;
5. Gain verbal approval from the participants to record the interview;

6. Confirm the interview would take no longer than 60 minutes;
7. Encourage participants to answer questions to their ability; and
8. Thank each participant upon completion of the interview for the contribution to the study.

The final stage of data collection involved an organizational document review; the participants provided the organizational documents. I asked participants to share their companies' current cybersecurity strategies. The application of online questionnaire transcripts, semistructured face-to-face interview transcripts, and company documents was necessary to use methodological triangulation as a process to collect data from various sources (Yin, 2013). Methodological triangulation is appropriate for case study research to achieve substantial and precise results and to support the rigor of the discoveries from each data collection technique (Yin, 2013). In addition to the online questionnaires and semistructured face-to-face interviews, small business leaders were able to share their current cybersecurity strategy documents thus allowing me to secure additional data for the process of methodological triangulation.

Before data collection started, I requested permission from the IRB. Upon approval from the IRB, data collection process commenced. Participants received an informed consent form for their review and execution (see Appendix A). Upon receipt of executed informed consent forms, I spoke to each participant via telephone to introduce the study. Each participant then received an email containing a link to the questionnaire via an online format. Upon completion of the online questionnaire, participants received an electronic password-protected copy of their individual transcript. The participants

reviewed their transcript for accuracy, intended meaning, and interpretation of their responses, as a method of transcript review (Welch, Grossaint, Reid, & Walker, 2014). Once each participant provided approval of their transcript, I extracted the transcript data from the Survey Monkey tool and imported the data into the NVivo software program.

The subset sample of three participants received a telephone call asking for their involvement in the semistructured face-to-face interview phase. The scheduling of semistructured face-to-face interviews commenced upon securing a subset sample of three participants. Recording and transcription occurred for each semistructured face-to-face interview. Each of the semistructured face-to-face interview participants received an email containing a password-protected copy of their transcribed interview, which contained my interpretation of the interview. The semistructured face-to-face interview participants performed member checking of their transcript for correctness, interpretation, and deliberate connotation of the discussions (Welch et al., 2014). Once each participant supplied written approval of their transcript, I imported the transcript data into the NVivo software program.

Data Organization Technique

The collection of data for this qualitative exploratory case study was from participant responses to an online questionnaire containing open-ended questions and semistructured face-to-face interviews. Those participants completing the online questionnaire typed in their answers directly into the Survey Monkey tool. Upon participant transcription review and written agreement, response extraction occurred from Survey Monkey for subsequent import into NVivo software (Welch et al., 2014).

Capturing the replies for the semistructured face-to-face interviews was via a recording device. I used the Microsoft Word software tool to type the transcription of each interview recording. I provided each respondent with a password-protected file, containing a copy of the interview transcript, for his or her review and written approval as proposed by Welch et al. (2014). Upon respondent approval, the transcription extraction occurred from Microsoft Word for subsequent import into NVivo software.

Computer-assisted analysis tools, such as NVivo, were effective for organizing data and saving time (Chittem, 2014). NVivo was the qualitative data analysis software tool used for importing and coding data (Edwards-Jones, 2014). NVivo also provided advanced features for planning, storing, managing, collating, analyzing, and presenting data (Edwards-Jones, 2014). For this qualitative case study, an import of all participant data took place into NVivo for thematic coding as suggested by Ando et al. (2014). Upon transcript upload into NVivo, each transcript received a random number assignment to designate the participant name and random letter assignment to designate participant business name. Random number and letter assignment preserved the confidentiality of each participant and company (Khan, 2014).

I provided every participant of this qualitative case study all-necessary means to protect their right to privacy as recommended by Leedy and Ormrod (2015). Participants' right to privacy included all measures to protect their identity, company name, and any raw data derived from their online questionnaires and face-to-face interviews (Yin, 2013). Storage of an electronic scan of all executed informed consent forms received was stored on a password protected flash drive, with the original paper copies immediately

shredded after scanning. All participant data from the online questionnaires and semistructured face-to-face interviews will be stored electronically on a password protected flash drive for no longer than 5 years from the date of the interview. The destruction of all electronic informed consent forms and interview data will occur from the password protected flash drive, and demolition of the flash drive will take place using secure means, after a 5-year term passes from the time of collection.

Data Analysis

Data analysis in qualitative studies is a generalization practice where the researcher places particular meanings to the data collected via thematic coding to derive conclusions (Leedy & Ormrod, 2015). For this qualitative case study, an online questionnaire containing 10 open-ended questions enabled me to gather data:

1. What are your views concerning the importance of cybersecurity strategies to protect systems from data breaches at your small business?
2. What cybersecurity strategies are in place to protect systems from data breaches at your small business?
3. How are cybersecurity strategies to protect systems from data breaches circulated to employees at your small business?
4. What are your views on how employees recognize the importance of cybersecurity strategies for your small business?
5. What do you think is the best way to circulate cybersecurity strategies to employees of your small business?

6. What is the process for employees to report a potential cyber threat to the leader of the small business?
7. How do you respond to internal cyber threats made against the company?
8. How do you respond to external cyber threats made against the company?
9. Has your business experienced internal cyber threats? If yes, can you describe the risk and action taken to mitigate?
10. Has your business experienced external cyber threats? If yes, can you describe the risk and action taken to mitigate?

Upon collection of the data from five respondents during the online questionnaire, a subset of three respondents participated in semistructured face-to-face interviews. I conducted the semistructured face-to-face interviews to gain additional details to the responses small business leaders made on the online questionnaire. The goal of the data analysis was to answer the research question: What cybersecurity strategies do leaders of small businesses implement to improve the protection of their systems from data breaches?

To answer the research question, I inputted responses from the online questionnaires and semistructured face-to-face interviews to NVivo software for thematic coding. NVivo software is a qualitative data analysis tool used by researchers to code data into themes (Edwards-Jones, 2014). NVivo software does not code data automatically into themes, but allows the researcher to visualize the data and make a determination of common themes (Edwards-Jones, 2014). The coding of the themes

enabled the discovery of similar experiences of each participant (Leedy & Ormrod, 2015).

Case study research is appropriate when exploring multiple sources of data to determine the foundation of a phenomenon (Keutel, Michalik, & Richter, 2014). Methodological triangulation in this study commenced after the thematic coding of participant responses. Additional forms of data for methodological triangulation reviewed include organizational documents that revealed the current cybersecurity strategies in place at small business leader establishments. Methodological triangulation substantiated the equivalent outcome of the thematic coding of responses (Yin, 2013). Correlation of themes related to participant cybersecurity strategies, existing small business, cybersecurity policy literature, systems thinking theory, and routine activities theory.

The key themes from the data correlated to von Bertalanffy's (1972) systems thinking theory. Systems thinking theory offered understanding, as to how systems influence one another within a whole. In organizations, systems consisted of individuals, arrangements, and practices that work jointly to create a robust or feeble business (Loosemore & Cheung, 2015). The premise of systems thinking allowed participants to share experiences concerning cybersecurity strategies, in order to improve the protection of systems from data breaches.

When examining the data within the systems thinking theory, construction of themes matched the (a) function, (b) structure, and (c) process of cybersecurity strategies used by small business leaders (Ing, 2013). Supplementing systems thinking theory, Cohen and Felson (1979) established routine activities theory. Routine activities theory

explained crime as an event that highlights its relation to space and time and emphasizes its ecological nature and implications (Kigerl, 2012). Examining the data through a routine activities theory lens allowed for the building of themes about potential cybercriminal motivation regarding attacking small business systems.

Reliability and Validity

Reliability signifies the repeatability of the results, and validity denotes the accuracy of the data (Barry, Chaney, Piazza-Gardner, & Chavarria, 2014; Grossoehme, 2014). 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, 2013). Both reliability and validity were necessary for this qualitative study, ensuring the data was factual and truthful.

Reliability

Reliability represents the degree in which duplication and replication of the study results occur by an alternative researcher (Pozzebon & Rodriguez, 2014). A mode of establishing reliability is for the researcher to record the entire research process (Grossoehme, 2014). For this study, I documented all research procedures from beginning to end. I maintained a research journal where I accurately reported all phases of data collection, data analysis, and data interpretation as suggested by Grossoehme (2014).

Listing each criterion used to select participants in the research journal achieved dependability, the stability of data over time (Elo et al., 2014). Each participant reviewed

and approved their transcribed responses to maintain member checking for accuracy of the data. Creditability reflected reliability via the detailed identification and description of each participant in the research journal (Elo et al., 2014). Participants examined their online questionnaire responses as part of transcription review and performed member checking of my interpretation of their semistructured face-to-face interview to establish member checking. For methodological triangulation, an analysis of participant specific small business company strategy documents occurred to reinforce the creditability of the results as recommended by Yin (2013).

Transferability is the level of reassigning the findings to a new set of participants (Elo et al., 2014). Transferability in this study returned reliability, as the results reflected small businesses only. The documentation of the research provided transferability of the results to a fresh set of participants in various industries of small businesses. Confirmability referred to truth in which the results reflect that of the participants' response (Pozzebon & Rodriguez, 2014). To establish confirmability, participants performed a transcription review of their online questionnaire responses and examined their semistructured face-to-face interviews to ensure I correctly interpreted their intended meanings.

Data saturation transpired when no further themes or categories were noticeable in the data (Ando et al., 2014). Researchers can reach data saturation when no new findings are pertinent to the purpose of the study (Kasim & Al-Gahuri, 2015). In this study, data saturation occurred when it became unproductive to generate new themes and

categories that related to the purpose of the study as proposed by Kasim and Al-Gahuri (2015).

Validity

The objective of validity in qualitative research is to ensure the truthfulness of the research findings (Pozzebon & Rodriguez, 2014). Researchers aiming to achieve research validity should ensure they describe and understand the topic of study in its entirety (Grossoehme, 2014). Yin (2013) documented three tests of validity in case studies were (a) construct validity, (b) internal validity, and (c) external validity.

Construct validity is a test for how an instrument measures an unobservable characteristic of the sample under study (Leedy & Ormrod, 2015). For validity achievement, the construction of the open-ended questions encouraged behavioral responses from the small business leaders, as it relates to their cybersecurity strategies. I also tested construct validity against the identified themes from the data and compared them to the purpose of the study.

Internal validity is a check for the establishment of how the findings map to the phenomenon of the research question (Yin, 2013). For achievement of internal validity, employment of member checking ensued throughout the research process. Before the commencement of thematic coding, participants performed a transcription review of their online questionnaire responses for correctness. Semistructured face-to-face interview participants performed member checking to ensure I accurately interpreted their intended meanings. Upon completion of data analysis, I shared the initial findings with the participants for their examination as suggested by Grossoehme (2014). Participants

reviewed the preliminary results for accuracy and confirmation of captured meanings of their responses.

External validity is a test of the generalizability of the findings as it relates to other studies (Yin, 2013). Within the Informed Consent Form (see Appendix A), each of the five participants that accepted to be in the study did so by agreeing that they had successfully addressed the business problem. To establish external validity, I used a purposeful sampling method to identify a sample of five small business leaders. Purposeful sampling is a system to attain knowledge-rich data to match the purpose of the study (Reybold et al., 2013). For increased external validity, a subset sample of three participants occurred from the original five small business leader sample. Usage of the subset sample was to ensure participants chosen from the purposeful sample allowed for the gathering of additional information-rich data (Robinson, 2014).

I examined company documents to strengthen the validity of the study and to use methodological triangulation as a process to collect data from various sources as recommended by Yin (2013). Methodological triangulation was necessary to support the same findings from each data collection method (Yin, 2013). Methodological triangulation is a process that enables the exploration of different data sources, which provides rich, robust, and comprehensive results (Yin, 2013). The discovery of online questionnaire transcripts, semistructured face-to-face interview transcripts, and the company strategy documents was essential to use methodological triangulation as a process to collect data from various sources (Yin, 2013). Methodological triangulation

was applicable for this case study research, and helped me reach significant and accurate results as suggested by Yin (2013).

Transition and Summary

The purpose of this qualitative exploratory case study was to explore effective cybersecurity strategies for small business leaders to protect their systems from data breaches. Data collection for the study was a three-step process including an online questionnaire containing open-ended questions, semistructured interviews in a face-to-face setting, and review of participant organizational documents. In the first and second step, I used an online questionnaire and semistructured face-to-face interviews to collect data and explore the approaches and experiences of the participants. In the third step, I triangulated the data by reviewing participants' documents that outlined current small business cybersecurity strategies.

I used the purposeful sampling technique to select five small business leaders from the Middlesex County region of Massachusetts. A subset of three participants from the original five small business leader sample participated in semistructured face-to-face interviews. Before data collection, I obtained permission from the IRB to begin the research. Data collection of online questionnaires and semistructured face-to-face interviews underwent transcription and review by participants for accuracy. When final transcription was complete, I imported all data into the NVivo qualitative data analysis software tool to organize and code the data into themes.

In Section 2 of this study, I supplied pertinent study research information including the role of the researcher, research method and design, population and

sampling, ethical issues, data collection techniques, and analysis. Additional discussion in Section 2 of this study related to the reliability and validity of the study. Section 3 of the study follows with a presentation of the findings, applications to professional practice, and implications for social change. Additional dialogue in Section 3 pertains to action and further research recommendations. Study reflection, summary, and conclusion elements conclude the study.

Section 3: Application to Professional Practice and Implications for Change

The objective of this qualitative exploratory multiple case study was to explore the cybersecurity strategies that small business leaders use to protect their systems from data breaches. This section of the study contains a presentation of the findings, applications to professional practice, implications for social change, and recommendations for action and further research. This section of the study concludes with reflections, summary, and conclusions.

Introduction

The purpose of this qualitative exploratory multiple case study was to explore the cybersecurity strategies that small business leaders use to protect their systems from data breaches. Online open-ended questionnaires from five small business leaders from the Middlesex County region of Massachusetts produced an abundance of data. Semistructured face-to-face follow-up interviews with three of the five small business leaders yielded significant additional data. I reviewed the questionnaires, interview transcripts, and documents provided by the small business leaders as part of this study. The analysis resulted in the identification of 83 codes and three major themes.

From my analysis of the data, the three major themes that emerged were (a) policy, (b) training, and (c) technology. The three central themes are comparable to findings of past and present research on the topic of cybersecurity strategies that small business leaders use to protect their systems from data breaches. Additionally, my findings support the conceptual frameworks of Von Bertalanffy's (1972) general systems theory and Cohen and Felson's (1979) routine activities theory. In this section of this

study, I confirm the connection between the identified themes derived from the data to the primary and secondary conceptual frameworks.

Presentation of the Findings

The presentation of the findings of this study addresses the overarching research question: What cybersecurity strategies do leaders of small businesses implement to protect their systems from data breaches? Five online open-ended questionnaires and three semistructured face-to-face interviews, with follow-up member checking for all transcripts, provided the data from the participants. The population for this study was small business leaders from the Middlesex County region of Massachusetts. From the population, a purposeful sample of five participants who were knowledgeable about the research topic completed an online questionnaire containing open-ended questions (Elo et al., 2014). From the purposeful sample of five participants, as suggested by Robinson (2014), a subset sample of three small business leaders participated in the semistructured face-to-face interviews, which increased information-rich data.

Each participant's involvement in this study was voluntary. All participants replied with "I consent" to an emailed informed consent form, in which they agreed to contribute to the study, answer an open-ended online questionnaire, and be audiotaped for semistructured face-to-face interviews. I used methodological triangulation to support the responses of the contributors through the review of company documents obtained from willing participants, as recommended by Yin (2013). I uploaded an import of all data collected to NVivo software, which allowed me to analyze the data in a visual manner to code the data into themes, as recommended by Edwards-Jones (2014). Theme

development aligned with the conceptual frameworks and literature review provided in Section 1 of this study.

The conceptual framework for this study was von Bertalanffy's (1972) systems thinking theory, which I supplemented with Cohen and Felson's (1979) routine activities theory. Systems thinking theory allowed me to examine the data regarding themes matching the (a) function, (b) structure, and (c) process, as suggested by Ing (2013), of the cybersecurity strategies used by small business leaders. Usage of routine activities theory enabled the construction of themes about potential cybercriminal motivation regarding attacking small business systems, as proposed by Kigerl (2012).

Previous research on the cybersecurity strategies that leaders of small businesses use to protect their systems from data breaches was deficient in academic depth based on the literature review in Section 1 of this study. Due to the limited information available about strategies that small business leaders use to protect their systems from data breaches, research opportunities are available. The data collected from the open-ended online questionnaires and semistructured face-to-face interviews answered the overarching research question: What cybersecurity strategies do leaders of small businesses implement to protect their systems from data breaches?

Three major themes pertinent to the research emerged from my data analysis: (a) policy, (b) training, and (c) technology. For confidentiality purposes, I referred to each small business leader participant in this study with a letter and a number (2B, 3C, 4D, 6F, and 7G). Table 1 is an illustration of the frequency of codes, which led to the creation of the three major themes for this study.

Table 1

Frequency of Major Themes

Major theme	*N*	% of frequency of codes
Policy	44	53.01%
Training	24	28.92%
Technology	15	18.07%

Note. *n*= frequency.

Theme 1: Policy

The first major theme in this study resulting from my data analysis was the concept of policy. The concept of policy involves the importance of small businesses having a cybersecurity policy in place. Participants expressed the need to have a cybersecurity policy for their small businesses. Some of the participants had a formal cybersecurity policy for their company. Relevant comments included the following:

> Cybersecurity policies were factored into the development of our software and operations. (7G)
>
> The strategies for the policy must be around business growth and customer data protection. (2B)

These comments aligned with the systems thinking theory framework, as Loosemore and Cheung (2015) found that viewing an organization as an interrelated system allowed for understanding of the interaction of all elements.

Routine activities theory was the secondary conceptual framework used for this study, which aligned with the theme of policy. Kigerl (2012) posited that routine

activities theory included the absence of protection. Relevant cybersecurity policies responses included the following:

> We maintain secure hardware and software systems. (3C)
>
> We are starting to look at it like a customer would look at it from the outside. (7G)

Such statements, as related to routine activities theory, depicted small business leaders as understanding that they remained targets and as implementing cybersecurity strategies to protect their systems from data breaches.

Table 2 is an illustration of the frequency of codes directly related to the theme of policy. Prior literature on cybersecurity policies suggested that companies performing actions experienced increased levels of cybersecurity and better resilience to cybercrime (Bernik, 2014). Participants agreed that cybersecurity strategy and data protection were key to protecting their systems from external threat. This aligns with current literature, wherein merely applying IT best practices is inadequate for the unique small business custom network (Young, Lopez, Rice, Ramsey, & McTasney, 2016).

Table 2

Frequency of Codes Directly Related to Theme 1: Policy

Code	*N*	% of frequency of codes
Cybersecurity strategy	30	55.56%
Data protection	12	22.22%
External threats	12	22.22%

Note. *n* = frequency.

Cybersecurity strategy. Participant responses and company policy documents showed that cybersecurity strategies were of the utmost importance to the successful small business leader. Small businesses have increasingly become the target of cyber threats, which has increased their awareness and action (Hayes & Bodhani, 2013). Cybersecurity strategies varied between participants as a reflection of the ways in which they did business, the need to follow DOD protocols, and the amount of information they shared with employees. Relevant responses revealed the following:

> There are three prongs in our cybersecurity strategy, which has a specific goal and tactical approach. (2B)
>
> We do not possess or retain any classified material and follow the U.S. National Industry Security Program Operating Manual. (4D)
>
> We have a least privilege and need to know policy, which provides our employees with the least amount of information they need to know to get their job done. (7G)

Comparable to participant responses, Grossman and Schortgen (2016) found that building security policies cultivated professional skills and allowed a small organization to have distinctive positioning.

Data protection. The existing literature related to data protection is consistent with participant responses and company documents reviewed in this study. The growing dependence of small businesses on the use of networks opened up the risk of cyberattack (Lee, 2014). Love and Roper (2015) found that small business data protection strategies differed from those of larger firms, where the focus was more often on speed to market. Upon review of the findings, it is clear that all participants were highly mindful of data

protection and had found methods to protect their data securely, particularly as doing so was crucial to their business survival. Respondents recognized that they were subject to cyberattack and indicated using such services as Dropbox, a cloud file storage service. Relevant responses included the following:

> The best security measure is not to put any critical data on a network. (6F)
>
> Data is collected from customers and stored in the cloud. (2B; 4D; & 7G)

A shared statement from all participants indicated that they stored employees' personal information at their place of business in a secure area instead of in the cloud. According to company policy documents, employees' personal information was stored on encrypted computers at the business location, with paper copies stored in a locked cabinet.

External threats. In relation to external threats, participant responses and company documents identified weakness in the findings of previous research. Todd and Rahman (2013) suggested that small businesses had insufficient resources to secure their systems in the same manner as large corporations. In contrast, all participants voiced the same response: They had not experienced any external threats to their company. Some participants noted that they had experienced potential malware and phishing attacks, but their systems had thwarted the attacks. An alternate viewpoint revealed the following:

> Some of the scams are more sophisticated, and those are the ones you have to be careful of. (6F)

Company documents were clear on what to do to report security incidents, with steps indicating whom to contact and what actions to perform if an employee believed that a system was experiencing external threats. Current literature on the topic of external

threats was consistent with the study findings. Small business leaders implemented protective measures when they trusted that the measures were effective, their outlook toward online protection was optimistic, and they thought they were responsible for their online security (Jansen, Veenstra, Zuurveen, & Stol, 2016).

Theme 2: Training

The concept of training was the second major theme in this study. The theme of training involves the importance of small businesses training their employees to be aware of cybersecurity threats. Participants in this study shared their employee cybersecurity training programs. Some of the participants noted that they had formal training programs, while others mentioned that their training was informal. The responses included the following:

> All of our people go through security training on an annual basis. (4D)
>
> We just did our first training of our employees and contractors in January 2016 for the information security policy. (7G)

The responses from the participants aligned with the main conceptual framework of systems thinking theory, as it relates to the theory's key constructs of function and process (Drack & Schwarz, 2010). All participants expressed that the process of training was a necessary function that enabled their employees to work in a manner that was mindful of potential cyber issues that could damage company systems.

The supplemental routine activities theory framework also aligned with the theme of training. Pyrooz et al. (2015) reviewed online identity and behavior as a way of understanding malicious activity on the Internet, referring to the routine activities theory

propositions of presence of a target and absence of protection. In the participant responses, it was evident that each small business leader understood that the business remained a target of potential cyberattack. Through training programs, each small business leader ensured that there was no absence of protection in the company. One of the participants expressed a sense of urgency about empowering and arming employees:

> It is a game you have to constantly stay on top of, because you know it's out there. (6F)

Table 3 is an illustration of the frequency of codes directly related to the theme of training. Prior literature on cybersecurity training emphasized that establishing a security culture starts with top management and continues down to every employee (Alhogail & Mirza, 2014). In participant responses, it was apparent that small business leaders agreed that they must lead the charge of cybersecurity training for their employees. The consensus across responses revealed that employers' leadership and employee's appreciation are relative to the importance of protecting company data. This aligned with current literature, as researchers have found that management-led cybersecurity training increases the appeal, comprehension, and memorability of security information (Zhang-Kennedy, Chiasson, & Biddle, 2016).

Table 3

Frequency of Codes Directly Related to Theme 2: Training

Code	*N*	% of frequency of codes
External threat measures	32	50.79%
Training employees	17	26.98%
Employee awareness	14	22.22%

Note. *n*= frequency.

External threat measures. Participant responses and company policy documents were consistent with existing literature on external threat measures. Core activities of cybersecurity external threat measures were (a) detecting vulnerabilities, (b) thwarting infection and distribution, and (c) foiling exploitation (Kraemer-Mbula et al., 2013). The core cybersecurity activities were in agreement with external threat measures, as participants shared similar external threat measures:

> Prevent them, neutralize them, and fight back with special programs. (2B)
>
> Investigate the reported or detected threat, isolate as necessary, and disclose if customer data is affected, as documented in their cybersecurity policies. (7G)

Common among all participants was the installation of security products on their servers to stop virus intrusion and to shut down their networks at the first sign of cyberattack. Participants' external threat measures were also in agreement with the current literature, which stresses the need to create and maintain cyber defensive and preventative procedures to defend organizations (Shafqat & Masood, 2016).

Training employees. Training employees was a common trend among the

participant responses and company policy documents. Holt and Bossler (2012) found a positive relationship between cybercrime exposure, computer training, and computer proficiency. As one participant reflected,

> We have the training, we give a document to people coming onboard, offer official training online live, and record the video. (7G)

All participants offered a form of cybersecurity training to their employees. Many provided the employee with exposure and education on understanding and preventing cyberattacks. Cybersecurity training was at the top of the list for some small business leaders. One respondent revealed,

> If there were some training courses for small businesses, definitely security should be one of the things. (6F)

Cybersecurity training programs increased information security awareness and had a significant effect on employee attitudes toward policy compliance (Sohrabi Safa, Von Solms, & Furnell, 2016).

Employee awareness. From participant responses and company documents, prior research is compatible regarding employee awareness. Organizational leaders that promote an employee culture and awareness of cybersecurity were in a better position to prevent and overcome potential threats (Bernik, 2014; Lee, 2014). The responses revealed these employers recognized employee awareness helped perform their jobs and protected their assets; alternatively, a violation of policy would alternatively carry consequences:

> My employees are aware of the importance as it directly impacts their ability to

perform their job duties. (3C)

The employees all recognize and appreciate the importance of protecting our data. (6F)

Violations of policy carry consequences up to termination. (7G)

The findings were clear; each participant believed employee awareness is a fundamental component in the war against cybercrime and armed their employee accordingly. Organizational cybersecurity countermeasures, such as training and policy communication, strengthened employee awareness and influenced information system misuse (Rocha Flores & Ekstedt, 2016).

Theme 3: Technology

The third major theme in this study was the topic of technology. The theme of technology is the importance of small business' dependence on hardware and software. Participants in this study shared what they felt are serious cyber situations, forms of technology they use to run their business, and information concerning business size as a deterrent. The urgency was clear from this response:

Cyber warfare is real and we are under attack, positively and absolutely, from foreign countries. (4D)

Related to technologies participants used to run their business, all participants maintained relationships with vendors to have their data in the cloud.

When it comes to the size of the company, participant responses are mostly in alignment with the main conceptual framework of systems thinking theory where

structure defines components, function defines the outcome, and process defines the activities required to produce the result (Ing, 2013).

> We are a small company, and I do not think that there is much here people would be interested in, but you never know. (6F)

From the technology perspective, all participants utilized components of technology, as a means of business functionality to achieve the desired result of no exposure to cyberattacks.

Within the complementing conceptual framework of routine activities theory, participant responses were in general alignment with the theme of technology. Criminal activity occurred, per routine activities theory, when a person motivated to commit crime encountered a suitable victim in an environment lacking protection (Anandarajan et al., 2013). It was apparent that each participant understood there remained a threat; highly motivated cyber offenders viewed small businesses as a suitable target. Suitable targets are viewable as those who lack the appropriate protection to thwart an attack. From the findings, the small business leader was using technology to place their data in the hands of large cloud vendors that had the resources to protect the data.

Table 4 is an illustration of the frequency of codes directly related to the theme of technology. Prior literature on technology in small businesses depicted technology as a means to advance and prevent cybercrime (Lagazio et al., 2014). Participants revealed using cloud vendors to store their data, which demonstrated their understanding of technology to prevent cybercrime. This aligned with the current literature, where benefits of using cloud computing for small businesses encompassed the ability to use powerful

IT infrastructure and software, and free up limited resources in all areas of the company's business, including cybersecurity (Cleary & Quinn, 2016).

Table 4

Frequency of Codes Directly Related to Theme 3: Technology

Code	*N*	% of frequency of codes
Cyber warfare	7	43.75%
Cloud (based company)	5	31.25%
Size does not matter	4	25.00%

Note. *n*= frequency.

Cyber warfare. Participant responses and company documents were inconsistent on the concept of cyber warfare. Prior literature from Philbin and Philbin (2013) on the topic of cyber warfare suggested mathematicians use information as an agent, by algorithms as a weapon, to combat cyber warfare. Only one participant mentioned cyber warfare:

> Cyber warfare cascades down to guys like us and they have already demonstrated they are a very skilled generation. (4D)

The findings are limited for the concept of cyber warfare as only one participant shared information about the topic and there is no mention in any of the company documents. Current research by Pipyros, Mitrou, Gritzalis, and Apostolopoulos (2016) denoted a growing amount of cyberattacks has altered cyberspace into a battleground, which carried cyber warfare as a fifth dimension of war.

Cloud (based company). Cloud (based company) was an overwhelmingly

recurrent trend within the small business participant responses. Sun and Wang (2013) assessed cloud computing as a vital component of efficiency and competitiveness for the small business, as it can solve issues of data security. Relevant responses included the following:

> There are no corporate servers in their network environment. (4D)
>
> We are a software as a service (SaaS) company and all of our service data, our customer data, is out in the cloud. (7G)

Participants had mixed responses when it came to ensuring their cloud vendor has appropriate cybersecurity policies. Senarathna, Yeoh, Warren, and Salzman (2016) revealed that privacy and security aspects have less impact on the decision-making of small businesses in the adoption of cloud computing.

Size does not matter. When it comes to the size of business, about the probability of a cyberattack, participants had mixed responses. According to Hayes and Bodhani (2013), a small business leader may attribute their business size as unattractive to the cybercriminal. Cybercriminals viewed the small business as easy marks for attack due to their limited security budgets. The divergent participant responses had little effect on their agreement that cybersecurity strategies were necessary for small business:

> When it comes to being a small business, given the nature of what we do, there are certain situations where people very much could want to be targeting us. (4D)
>
> We are just so small that I don't think we are that much of a choice target. (6F)

Hess and Cottrell (2016) agreed with the majority of participant responses that small business leaders should embrace the approach that threat management is an essential

investment in the business's future.

Summary of the Findings

The overall research findings in this study were consistent with the purpose and significance of the study. The three themes that emerged from the data analysis were (a) policy, (b) training, and (c) technology. Participant online open-ended questionnaires, semistructured face-to-face interviews, and company cybersecurity policy documents guided the themes. Each theme related to both systems thinking theory and routine activities theory. Shown in Tables 2, 3, and 4 are the frequency of codes for each main theme. Each recurrent code and central theme was significant to answer the research question of: What cybersecurity strategies do leaders of small businesses implement to protect their systems from data breaches? The themes that emerged from this study may be factors considered critical for small business leaders to realize the importance of implementing cybersecurity strategies in their organizations.

Applications to Professional Practice

The findings of this study contribute important methods for small business leaders to implement successful cybersecurity strategies and protect their systems from data breaches. The findings were significant for the small business leader that would like to enhance their existing cybersecurity strategy. The first major contribution of this research for the professional practice of business surrounded the topic of policy. The subject of policy encompassed cybersecurity strategies, data protection, and external threats. Employing cybersecurity strategies provided a way for a small business to maintain distinctive positioning in their marketplace (Grossman & Schortgen, 2016). As revealed

in the findings, having a specific goal and tactical approach was key for small business cybersecurity strategies. Engaging the least privilege and need to know mindset, when building or enhancing cybersecurity strategies, is one way of securing company data from the employees. Providing employees access to only the information they need to know to perform their duties reduced the risk of data breaches.

Data protection strategies in small businesses varied from that of larger firms (Love & Roper, 2015). The common thread revealed organization size is not a factor when it comes to protecting data. Protecting data was crucial to business survival. Methods of data protection included refraining from placing any critical data on the company network and using cloud providers to store data. Such methods of data storage were a way to protect the data from external threats. While the small businesses in this study shared that they had not experienced an external threat, they realized they are responsible for their online security as posited by Jansen et al. (2016). Small businesses that used cloud vendors to store their data placed the security responsibility on the large cloud provider. Where the small business had limited funds to protect their data accurately, the large cloud providers specialized in such services.

The second major contribution of this research for the professional practice of business encompassed the topic of training. The subject of training involved external threat measures, training employees, and employee awareness. Common in the findings is the prevention, neutralization, and battling of external threats using appropriate programs. Small businesses that produced and upheld cyber defensive and preemptive methods ensured the protection of their data (Shafqat & Masood, 2016). Protecting systems from

external threats required small business leaders to utilize the means to detect and isolate the threat. Participants noted the use of third-party software assisted in the external threat battle. Training employees was another way to defend against external threats.

Cybersecurity training increased employee awareness, and in turn armed employees with skills toward security compliance (Sohrabi Safa et al., 2016). Employee training methods included offering cybersecurity documentation, online training programs, and video recordings. Such training increased employee awareness to prevent and overcome potential threats (Bernik, 2014; Lee, 2014). For reinforcing employee cybersecurity awareness, it is essential to provide relevant training and policies (Rocha Flores & Ekstedt, 2016). Some small business leaders found it necessary to reinforce employee awareness that violations of company cybersecurity policies and training may result in employment termination.

The third major contribution of this research for the professional practice of business covered the topic of technology. Technology included cyber warfare, cloud (based company), and size does not matter topics. The growing rate of cyberattacks has changed cyberspace to a cyber war battlefield (Pipyros et al., 2016). One participant, who enforced the seriousness of cybersecurity, also spoke of cyber warfare. Cyber warfare may be a battle fought by larger outlets, but remains a fight that can filter down to the small business. Small businesses remain vulnerable in the event of cyber war but can reduce their vulnerability if they place their data in the hands of a cloud provider. Being a cloud (based company) was popular among small businesses when it lends to their efficiency and competitiveness (Sun & Wang, 2013).

Placing data in the cloud allowed the small business to utilize the cybersecurity measures of the larger based cloud provider. Cloud computing enabled small businesses to remove the worry of protecting data on their own, and made it unnecessary to house corporate servers. Using a cloud provider closed the door for attack on a different scale. Small businesses attributed their size as unattractive to cybercriminals, but the cybercriminals viewed small businesses as easy targets due to their limited security budgets (Hayes & Bodhani, 2013). Participants had mixed responses on the possibility of experiencing a cyberattack due to their size. One thing was clear from the results; all participants agreed that cybersecurity was a necessary investment in their businesses future (Hess & Cottrell, 2016).

Within these findings, I will be able to offer small business leaders practical approaches for the professional practice of business, which created or enhanced cybersecurity strategies and protected their systems from data breaches. Additionally, small business leaders, who have been unable to formulate cybersecurity strategies, gained a new awareness about the necessity of protecting their systems from cyberattack. Small business leaders realized policy, training, and technology could safeguard their systems from data breaches.

Implications for Social Change

Small business leaders that accelerated the adoption of cybersecurity practices to protect systems from data breaches provided a clear path of acceptance and awareness, as a critical first step when safeguarding their data. Areas of application included policy, training, and technology. Densham (2015) suggested that a company's recognition of

assuming a data breach will occur should be the crucial first step to awareness. Through the implementation of cybersecurity strategies, small businesses may diminish data breaches and safeguard private information from looming cyberattacks.

Small business leaders, who created or improved their cybersecurity strategies, benefitted from a proactive stance that builds awareness from knowledge, education, and instruction. Maintaining cybersecurity policies increased levels of cybersecurity and upheld a strong resilience to cybercrime (Bernik, 2014). When businesses escalated their dependence on IT, the impairment of these systems can affect the greater society (Vande Putte & Verhelst, 2013). In particular, leakage of personal information, resulting from a data breaches, affected the livelihood of the individuals or companies who experienced the disclosure of their data.

Training employees was a fundamental component in the war on cybercrime. Small business leaders would be remiss to overlook the investment in cybersecurity training for their employees. Establishing a cyber aware employee culture must flow from top management down to every member of the company (Alhogail & Mirza, 2014). Cybersecurity training created employee recognition and appreciation to protect the companies' data. Technology advanced and prevented cybercrime (Lagazio et al., 2014). Small businesses, which used cloud computing, experienced the benefits of the large cloud vendor. This alone freed up resources and provided greater means to invest in cybersecurity. Cloud computing was beneficial for small businesses, as it freed up limited resources in the area of cybersecurity (Cleary & Quinn, 2016).

Recommendations for Action

The first recommended action for small business leaders is to have a cybersecurity policy. The creation of a cybersecurity policy enables the small business leader to formulate cybersecurity strategies to protect themselves from data breaches and external threats. Small businesses are wholly responsible for their online security (Jansen et al., 2016). The small business leader should consider the least privilege and need to know attitude about data access for their employees. The suggested small business cybersecurity policy should contain methods of data protection. Security software, or placing their data in the cloud, ensured they reduced their vulnerability to external threats.

The second recommended action for small business leaders is to offer cybersecurity training programs for themselves and their employees. Fostering a culture of security is achievable when the training starts with top management and flows down to every employee (Alhogail & Mirza, 2014). Cybersecurity training programs include topics of how to prevent, counteract, and combat external threats.

Cybersecurity training programs that consisted of documentation, online training, and video recordings ensure employee awareness. Recommended documentation include methods of what employees need to know to prevent, counteract, and combat a pending cyberattack. When small business leaders lack cybersecurity expertise, online training using a third party that is an expert in the area of cybersecurity is effective. Recording the online training is appropriate and allows employees to practice and reinforce their

cybersecurity knowledge. Strengthening employee awareness of cybersecurity arms them with the information they needed to avoid system abuse (Rocha Flores & Ekstedt, 2016).

Technology is the third recommended action for small business leaders. Cyber war is and remains a serious threat to all business types and sizes (Pipyros et al., 2016). A small business must protect themselves; the use of a cloud service is recommended to provide that protection, and help combat cyber war. Popularity for the use of cloud providers has grown for the small business, when it contributes to their efficiency and competitiveness (Sun & Wang, 2013).

Using a cloud service allows the small business to secure their data behind the walls of a large provider, one that has the resources and finances to protect the data more securely. Where some small business leaders thought that size does not matter when it comes to being the target of cyberattack, cybercriminals realize a small business portrays a prime target because of their limited security budgets (Hayes & Bodhani, 2013). Using a cloud service to protect data provides the small business leader the benefits of large company security protection and greater peace of mind that their data will be secure.

Small business leaders represent the relevant audience for the results of this study. As an agent of social change, I am fully committed to ensuring the distribution of the study results to small business leaders via appropriate mechanisms. Such sharing mechanisms include offering the study population the opportunity to have the study sent to them via email, upon its acceptance and publishing. Several members of the population, including participants, have already requested a copy of the final approved

study. Small businesses need to create and maintain cybersecurity strategies to ensure they have unique positioning in their markets (Grossman & Schortgen, 2016).

Recommendations for Further Research

The creation and continuous improvement of cybersecurity strategies are essential to protect data from cyberattack. Herein, I present a significant contribution to existing literature, which included the cybersecurity strategies small business leaders used to protect their systems from data breaches. Cybersecurity strategies, in the form of policies, training, and technologies presented vital recommendations for small business cyberattack awareness, prevention, and isolation (Lagazio et al., 2014).

Limitations in this study included my professional position as senior vice president of information technology at an information security vendor. An untechnical researcher may yield additional results from a nontechnical perspective and offer small business leaders alternative methods to view cybersecurity strategies. Another limitation of this study is the small sample size of five small business leaders from the Middlesex County region of Massachusetts. I recommend future studies should expand to additional small business locations to yield additional results. Future researchers could start with investigating small businesses in other areas of Massachusetts, and then move on to additional regions in the United States.

I retained a subset sample of three small business leaders to take part in semistructured face-to-face interviews, which added a limitation to this study. Future studies might offer beneficial results if more participants partook in semistructured face-to-face interviews. While the results were abundant from the open-ended online

questionnaire, speaking to participants via the semistructured face-to-face interviews was a way to gather more information-rich data.

A final limitation of this study was assuming small business leaders have limited knowledge to make informed decisions surrounding their cybersecurity practices. As all participants in this study were small business leaders, their responses reflected their extensive knowledge in the area of their cybersecurity practices. Researchers that conduct further analyses in the field of cybersecurity strategies would be wise to continue the dialogue with the small business leader. Extending studies to the small business employees can provide additional insights.

Reflections

As a senior vice president of information technology for a leading information security vendor, I have distinctive experience on cybersecurity strategies for businesses of all sizes. When I began this study, I vowed that my professional cybersecurity knowledge would not lend to any personal bias when working with small business leaders. Specifically, I pledged to listen to what small business leaders had to say and not make any recommendations for them to create or improve their cybersecurity strategies. I found that keeping my personal bias out of the research was not difficult. By following the study protocol, participants performed member checking of their open-ended online questionnaire and semistructured face-to-face interview transcripts to ensure my interpretations were accurate. Participants were able to make any edits to the data transcribed to ensure their responses were correct when used for theme development.

Additionally, I was able to collect and review participant cybersecurity company documents to triangulate the data to substantiate the findings.

Reflecting back on my study, there are distinctive challenges in obtaining the number of small business leaders to conduct the research. I was able to acquire the population listing from the U.S. Small Business Administration, but it took close to four weeks to obtain the listing. From the population listing, I sent over 800 emails to prospective participants. An additional 7 days enabled me to secure the five participants. The data collection and analysis process moved quickly, once the participants gave their informed consent. All five small business leaders participating in this study were open and honest about their cybersecurity strategies, which provided the resultant themes and recommendations.

From the onset of this study, it was my professional opinion that many small businesses lacked the necessary cybersecurity strategies in place to protect their systems from data breaches. Since conducting the appropriate research, I am pleasantly surprised that small businesses do have proper cybersecurity strategies. Each participant in this study fully understood the need to protect his or her data. In addition, all study participants are successfully employing cybersecurity strategies, which should be reassuring to their employees and customers.

Conclusion

The objective of this qualitative case study was to explore the cybersecurity strategies small business leaders implement to protect their systems from data breaches. In Section 1 of this study, I provided the background of the problem, problem statement,

purpose statement, nature of the study, and research question about the consequences cyberattack can have on small businesses. Section 1 included a review of systems thinking theory and routine activities theory as the conceptual framework, operational definitions, assumptions, limitations, delimitations, the significance of the study, implications for social change, and a review of the professional and academic literature.

In Section 2 of this study, I provided details on the role of this researcher, participants, research method, research design, and data collection information. Open-ended online questionnaires and semistructured face-to-face interviews were the foundations of the collection of data for investigation. Cybersecurity policies and organizational documents from participants, in addition to using NVivo software, concluded the data collection.

In Section 3 of this study, I presented the findings, application to professional practice, and implications for social change. Section 3 contained recommendations for action and further research for cybersecurity strategies small business leaders can implement to protect their systems from data breaches. Section 3 concluded with a reflection of my research experience during this study.

Through data analysis, the three emerging themes included policy, training, and technology. The theme of policy offered details of cybersecurity strategies, data protection, and external threats. The training theme encompassed information of external threat measures, training employees, and employee awareness. The technology theme detailed cyber warfare, cloud (based company), and size does not matter. The most significant application to business practice in this study was the need for small businesses

to have a cybersecurity strategy that enforced the least privilege and need to know mindset about opening up data to employees. Implications for positive social change included using this study to offer awareness to small business leaders, who in turn may accelerate the adoption of cybersecurity strategies to protect their systems from data breaches.

Recommended actions ensuing from this study were for small business leaders to have a cybersecurity policy, offer cybersecurity training programs for themselves and their employees, and to consider cloud computing as a secure method of protecting data. Further research should encompass additional small business locations to yield additional results, and engage more participants to take part in semistructured face-to-face interviews. Finally, extending the research to small business employees, dedicated to information security, could provide additional insight into the area of small business cybersecurity strategies.

References

Alhogail, A., & Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical & Applied Information Technology, 64*(2), 540–549. Retrieved from http://www.jatit.org/volumes.php

Anandarajan, M., D'Ovidio, R., & Jenkins, A. (2013). Safeguarding consumers against identity-related fraud: Examining data breach notification legislation through the lens of routine activities theory. *International Data Privacy Law, 3*(1), 51–60. doi:10.1093/idpl/ips035

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eaton, M. J. G., Levi, M., . . . Savage, S. (2012, June). *Measuring the cost of cybercrime*. Paper presented at the 11th Annual Workshop on the Economics of Information Security, Berlin, Germany. Retrieved from http://weis2012.econinfosec.org/

Ando, H., Cousins, R., & Young, C. (2014). Achieving saturation in thematic analysis: Development and refinement of a codebook. *Comprehensive Psychology, 3*(4), 1–7. doi:10.2466/03.CP.3.4

Bamrama, A., Singh, G., & Bhatt, M. (2013). Cyber-attacks and defense strategies in India: An empirical assessment of banking sector. *International Journal of Cyber Criminology, 7*(1), 49–61. doi:10.2139/ssrn.2488413

Barry, A. E., Chaney, B., Piazza-Gardner, A. K., & Chavarria, E. A. (2014). Validity and reliability reporting practices in the field of health education and behavior: A review of seven journals. *Health Education & Behavior, 41*(1), 12–18. doi:10.1177/1090198113483139

Bedwell, P. (2014). Finding a new approach to SIEM to suit the SME environment. *Network Security*, *2014*(7), 12–16. doi:10.1016/S1353-4858(14)70070-4

Bendassolli, P. F. (2014). Reconsidering theoretical naiveté in psychological qualitative research. *Social Science Information*, *53*(2), 163–179. doi:10.1177/0539018413517181

Bensted, G. (2012). Hi terrorist financing and the Internet: Dot com danger. *Information & Communications Technology Law*, *21*(3), 237–256. doi:10.1080/13600834.2012.744222

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

Berriz, C. (2014). Cybersecurity and United States policy issues. *Global Security Studies*, *5*(3), 35–40. Retrieved from http://globalsecuritystudies.com/vol5iss3summer2014.htm

Best, J., & Luckenbill, D. S. (1994). *Organizing deviance* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Bloomberg Government. (2012). The price of cybersecurity: Big investments, small improvements (Data file). Retrieved from http://www.bgov.com/

Bolton, F. (2013). Cybersecurity and emergency management: Encryption and the inability to communicate. *Journal of Homeland Security & Emergency Management*, *10*(1), 1–7. doi:10.1515/jhsem-2012-0038

Brayda, W. C., & Boyce, T. D. (2014). So you really want to interview me? Navigating

"sensitive" qualitative research interviewing. *International Journal of Qualitative Methods*, *13*(1), 318–334. Retrieved from http://globalsecuritystudies.com/vol5iss3summer2014.htm

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology, 8*(1), 1–20. Retrieved from http://www.cybercrimejournal.com/

Burinskiene, A., & Pipirienė, V. (2013). Adoption of information systems by trade and manufacturing enterprises. *European Integration Studies*, *2013*(7), 168–176. doi:10.5755/j01.eis.0.7.4271

Buzzell, T., Foss, D., & Middleton, Z. (2006). Explaining use of online pornography: A test of self-control theory and opportunities for deviance. *Journal of Criminal Justice and Popular Culture, 13*(2), 96–116. Retrieved from http://www.albany.edu

Cade, N. W. (2012). An adaptive approach for an evolving crime: The case for an international cyber court and penal court. *Brooklyn Journal of International Law*, *37*(3), 1139–1175. Retrieved from http://www.brooklaw.edu/

Cambria, P. J., Jr. (2012). ICANN, the ".xxx" debate, and antitrust: The adult Internet industry's next challenge. *Stanford Law & Policy Review*, *23*(1), 101–118. Retrieved from http://journals.law.stanford.edu/

Caplan, N. (2013). Cyber war: The challenge to national security. *Global Security Studies*, *4*(1), 93–115. Retrieved from http://globalsecuritystudies.com/

Caruson, K., MacManus, S. A., & McPhee, B. D. (2012). Cybersecurity policy-making at the local government level: An analysis of threats, preparedness, and bureaucratic roadblocks to success. *Journal of Homeland Security & Emergency Management*, *9*(2), 1–22. doi:10.1515/jhsem-2012-0003

Chambers-Jones, C. (2013). Virtual world financial crime: Legally flawed. *Law & Financial Markets Review*, *7*(1), 48–56. doi:10.5235/LFMR7.1.48

Chan-Mok, J. O., Caponecchia, C., & Winder, C. (2014). The concept of workplace bullying: Implications from Australian workplace health and safety law. *Psychiatry, Psychology & Law*, *21*(3), 442–456. doi:10.1080/13218719.2013.829399

Chang, H. (2014). A study of security requirement demand survey analysis on manufacturing industry. *International Journal of Security & Its Applications*, *8*(1), 201–212. doi:10.14257/ijsia.2014.8.1.19

Chao, C. A., & Chandra, A. (2012). Impact of owner's knowledge of information technology (IT) on strategic alignment and IT adoption in US small firms. *Journal of Small Business & Enterprise Development*, *19*(1), 114–131. doi:10.1108/14626001211196433

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447–459. doi:10.1016/j.cose.2013.09.009

Chittem, M. (2014). Understanding coping with cancer: How can qualitative research

help? *Journal of Cancer Research & Therapeutics, 10*(1), 6–10. doi:10.4103/0973-1482.131328

Cleary, P., & Quinn, M. (2016). Intellectual capital and business performance. *Journal of Intellectual Capital, 17*(2), 255–278. doi:10.1108/jic-06-2015-0058

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. Retrieved from http://www.asanet.org

Colesniuc, D. (2013). Cyberspace and critical information infrastructures. *Informatica Economica, 17*(4/2013), 123–132. doi:10.12948/issn14531305/17.4.2013.11

Cunliffe, A. L. (2011). Crafting qualitative research: Morgan and Smircich 30 years on. *Organizational Research Methods, 14*(4), 647–673. doi:10.1177/1094428110373658

Davies, B. (2006). Subjectification: The relevance of Butler's analysis for education. *British Journal of Sociology of Education, 27*(4), 425–438. doi:10.1080/01425690600802907

Deibert, R. (2012). The growing dark side of cyberspace (. . . and what to do about it). *Penn State Journal of Law & International Affairs, 1*(2), 260–274. Retrieved from http://elibrary.law.psu.edu

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security, 2015*(1), 5–8. doi:10.1016/S1353-4858(15)70007-3

Desai, D. (2013). Beyond location: Data security in the 21st century. *Communications of the ACM, 56*(1), 34–36. doi:10.1145/2398356.2398368

Donner, C. M., Jennings, W. G., & Banfield, J. (2014a). The general nature of online and off-line offending among college students. *Social Science Computer Review* (0894439314555949), 1–17. doi:10.1177/0894439314555949

Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E., & Banfield, J. (2014b). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior, 34*, 165–172. doi:10.1016/j.chb.2014.01.040

Drack, M., & Schwarz, G. (2010). Recent developments in general system theory. *Systems Research & Behavioral Science, 27*(6), 601–610. doi:10.1002/sres.1013

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. *Crime Prevention Studies, 16*(2003), 7–30. Retrieved from http://www.popcenter.org/

Edwards-Jones, A. (2014). Qualitative data analysis with NVIVO. *Journal of Education for Teaching, 40*(2), 193–195. doi:10.1080/02607476.2013.866724

Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utriainen, K., & Kyngas, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open*, *4*(1), 1–10. doi:10.1177/2158244014522633

Fahie, D., & Devine, D. (2014). The impact of workplace bullying on primary school teachers and principals. *Scandinavian Journal of Educational Research, 58*(2), 235–252. doi:10.1080/00313831.2012.725099

Farwell, J. P., & Rohozinski, R. (2012). The new reality of cyber war. *Survival (00396338), 54*(4), 107–120. doi:10.1080/00396338.2012.709391

Feinberg, J. (1984). *Harm to others: The moral limits of the criminal law* (Vol. 1). New York, NY: Oxford University Press.

Filshtinskiy, S. (2013). Cybercrime, cyberweapons, cyber wars: Is there too much of it in the air? *Communications of the ACM, 56*(6), 28–30. doi:10.1145/2461256.2461266

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*(38), 13675–13676. doi:10.1073/pnas.1414626111

Flowers, A., Zeadally, S., & Murray, A. (2013). Cybersecurity and US legislative efforts to address cybercrime. *Journal of Homeland Security & Emergency Management, 10*(1), 1–27. doi:10.1515/jhsem-2012-0007

Foucault, M. (2002). *Power. Essential works of Foucault 1954–1984* (Vol. 3). London, England: Penguin.

Gaff, B. M. (2015). BYOD? OMG! *Computer, 48*(2), 10–11. doi:10.1109/MC.2015.34

Ghobakhloo, M., & Hong Tang, S. (2013). The role of owner/manager in adoption of electronic commerce in small businesses: The case of developing countries. *Journal of Small Business & Enterprise Development, 20*(4), 754–787. doi:10.1108/JSBED-12-2011-0037

Giles, D., & Yates, R. (2014). Enabling educational leaders: qualitatively surveying an organization's culture. *International Journal of Organizational Analysis, 22*(1), 94–106. doi:10.1108/IJOA-11-2011-0526

Gill, M. J. (2014). The possibilities of phenomenology for organizational research.

Organizational Research Methods, *17*(2), 118–137. doi:10.1177/1094428113518348

Givens, A. D., & Busch, N. E. (2013). Integrating federal approaches to post-cyber incident mitigation. *Journal of Homeland Security & Emergency Management, 10*(1), 1–28. doi:10.1515/jhsem-2012-0001

Gottfredson, M., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.

Graebner, M. E., Martin, J. A., & Roundy, P. T. (2012). Qualitative data: Cooking without a recipe. *Strategic Organization*, *10*(3), 276–284. doi:10.1177/1476127012452821

Grossman, M., & Schortgen, F. (2016). Building a national security program at a small school: Identifying opportunities and overcoming challenges. *Journal of Political Science Education, 2016*(1) 1–17. doi:10.1080/15512169.2015.1103653

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

Grov, C., Gillespie, B., Royce, T., & Lever, J. (2011). Perceived consequences of casual online sexual activities on heterosexual relationships: A U.S. online survey. *Archives of Sexual Behavior, 40*(2), 429–439. doi:10.1007/s10508-010-9598-z

Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*(1), 97–114. doi:10.1108/IMCS-03-2013-0019

Harsch, A., Idler, S., & Thurner, S. (2014, May). *Assuming a state of compromise: A best practise approach for SMEs on incident response management*. Paper presented at the 2014 Eighth International Conference on IT Security Incident Management & IT Forensics, Washington, DC. doi:10.1109/IMF.2014.13

Hayes, J., & Bodhani, A. (2013). Cyber security: Small firms under fire. *Engineering & Technology, 8*(6), 80–83. doi:10.1049/et.2013.0614

Healey, J. (2011). The spectrum of national responsibility for cyberattacks. *Brown Journal of World Affairs, 18*(1), 57–70. Retrieved from http://www.bjwa.org/

Henry, N., & Powell, A. (2015). Embodied harms gender, shame, and technology-facilitated sexual violence. *Violence Against Women, 21*(6), 758–779. doi:10.1177/1077801215576581

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

Hess, M. F., & Cottrell, J. H. (2016). Fraud risk management: A small business perspective. *Business Horizons, 59*(1), 13–18. doi:10.1016/j.bushor.2015.09.005

Holt, T. J. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime, 14*(2–3), 155–174. doi:10.1080/17440572.2013.787925

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40. doi:10.1080/01639625.2013.822209

Holt, T. J., & Bossler, A. M. (2012). Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. *Cyberpsychology, Behavior & Social Networking, 15*(9), 464–472.

doi:10.1089/cyber.2011.0625

Hong, J.-C., Chien-Hou, L., Hwang, M.-Y., Hu, R.-P., & Chen, Y.-L. (2014). Positive affect predicting worker psychological response to cyber-bullying in the high-tech industry in Northern Taiwan. *Computers in Human Behavior, 30*(2014), 307–314. doi:10.1016/j.chb.2013.09.011

Hult, F., & Sivanesan, G. (2013). What good cyber resilience looks like. *Journal of Business Continuity & Emergency Planning, 7*(2), 112–125. Retrieved from http://www.theicor.org/

Hunt, J. (2011). The new frontier of money laundering: How terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them. *Information & Communications Technology Law*, *20*(2), 133–152. doi:10.1080/13600834.2011.578933

Huth, C. L., Chadwick, D. W., Claycomb, W. R., & You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. *Information Systems Frontiers, 15*(1), 1–4. doi:10.1007/s10796-013-9419-8

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

Iasiello, E. (2013). Fixing U.S. national cybersecurity: A modest proposal for swallowing pride and reducing egos. *Comparative Strategy, 32*(4), 301–307. doi:10.1080/01495933.2013.821843

Iasiello, E. (2014). Is cyber deterrence an illusory course of action? *Journal of Strategic Security, 7*(1), 54–67. doi:10.5038/1944-0472.7.1.5

Ing, D. (2013). Rethinking systems thinking: Learning and coevolving with the world. *Systems Research & Behavioral Science*, *30*(5), 527–547. doi:10.1002/sres.2229

Internet Crime Complaint Center. (2013). *2013 IC3 Annual Report* (Data file). Retrieved from http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

Kain, R. C. (2013). Federal computer fraud and abuse act: Employee hacking legal in California and Virginia, but illegal in Miami, Dallas, Chicago, and Boston. *Florida Bar Journal*, *87*(1), 36–39. Retrieved from http://www.floridabar.org/

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

Keutel, M., Michalik, B., & Richter, J. (2014). Towards mindful case study research in IS: A critical analysis of the past ten years. *European Journal of Information Systems*, *23*(3), 256–272. doi:10.1057/ejis.2013.26

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

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470–486. doi:10.1177/0894439311422689

Kolfal, B., Patterson, R. A., & Yeo, M. L. (2013). Market impact on IT security spending. *Decision Sciences*, *44*(3), 517–556. doi:10.1111/deci.12023

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online

innovation in the shadows? *Technological Forecasting & Social Change, 80*(3), 541–555. doi:10.1016/j.techfore.2012.07.002

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology, 35*(5), 368–379. doi:10.1080/0144929x.2016.1160287

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security, 45*(2014), 58–74. doi:10.1016/j.cose.2014.05.006

Langos, C. (2015). Cyberbullying: The shades of harm. *Psychiatry, Psychology & Law, 22*(1), 106–123. doi:10.1080/13218719.2014.919643

Lee, C.-M. (2014). The strategic measures for the industrial security of small and medium business. *The Scientific World Journal, 2014*, 1–4. doi:10.1155/2014/614201

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

Lo, C. O. (2014). Enhancing groundedness in realist grounded theory research. *Qualitative Psychology*, *1*(1), 61–76. doi:10.1037/qup0000001

Loosemore, M., & Cheung, E. (2015). Implementing systems thinking to manage risk in public private partnership projects. *International Journal of Project Management*, *33*(6), 1325–1334. doi:10.1016/j.ijproman.2015.02.005

Love, J. H., & Roper, S. (2015). SME innovation, exporting and growth: A review of existing evidence. *International Small Business Journal, 33*(1), 28–48.

doi:10.1177/0266242614550190

Marcum, C. D., Higgins, E., & Ricketts, M. L. (2014). Juveniles and cyberstalking in the United States: An analysis of theoretical predictors of patterns of online perpetration. *International Journal of Cyber Criminology, 8*(1), 47–56. Retrieved from http://www.cybercrimejournal.com/

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. New York, NY: John Wiley & Sons.

Molenberghs, G., Kenward, M. G., Aerts, M., Verbeke, G., Tsiatis, A. A., Davidian, M., & Rizopoulos, D. (2014). On random sample size, ignorability, ancillarity, completeness, separability, and degeneracy: Sequential trials, random sample sizes, and missing data. *Statistical Methods in Medical Research, 23*(1), 11–41. doi:10.1177/0962280212445801

Morison, T., Gibson, A. F., Wiggington, B., & Crabb, S. (2015). Online research methods in psychology: Methodological opportunities for critical qualitative research. *Qualitative Research in Psychology, 12*(3), 223–232. doi:10.1080/14780887.2015.1008899

Namie, G., & Namie, R. (2003). *The bully at work: What you can do to stop the hurt and reclaim your dignity on the job*. Naperville, IL: Sourcebooks.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: A multi-nation study. *Journal of Scandinavian Studies in Criminology & Crime Prevention, 16*(2), 203–210. doi:10.1080/14043858.2015.1046640

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum, 32*(1), 81–94. doi:10.1080/02732173.2012.628560

Neghina, D., & Scarlat, E. (2013). Managing information technology security in the context of cyber crime trends. *International Journal of Computers, Communications & Control, 8*(1), 97–104. Retrieved from http://journal.univagora.ro

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815–825. doi:10.1016/j.dss.2008.11.010

Nobles, M. R., Reyns, B. W., Fox, K. A., & Fisher, B. S. (2014). Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly, 31*(6), 986–1014. doi:10.1080/07418825.2012.723030

Nuredini, A. (2014). Challenges in combating cyber crime. *Mediterranean Journal of Social Sciences, 5*(19), 592–599. doi:10.5901/mjss.2014.v5n19p592

Pawlak, P., & Wendling, C. (2013). Trends in cyberspace: Can governments keep up? *Environment Systems & Decisions, 33*(4), 536–543. doi:10.1007/s10669-013-9470-5

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

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

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016). Cyberoperations and international humanitarian law. *Information & Computer Security, 24*(1), 38–52. doi:10.1108/ics-12-2014-0081

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51*(5), 551–567. doi:10.1016/j.im.2014.03.009

Pozzebon, M., & Rodriguez, C. (2014). Dialogical principles for qualitative inquiry: A nonfoundational path. *International Journal of Qualitative Methods*, *2014*(13), 293–317. Retrieved from https://ejournals.library.ualberta.ca/

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

Pricewaterhouse Coopers. (2014). *2014 US State of Cybercrime Survey*. Retrieved from http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf

Pyrooz, D. C., Descker, S. H., & Moule, J. R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly, 32*(3), 471–499. doi:10.1080/07418825.2013.778326

Raiyn, J. (2014). A survey of cyber-attack detection strategies. *International Journal of Security & Its Applications, 8*(1), 247–256. doi:10.14257/ijsia.2014.8.1.23

RAND Corporation. (1967). *Analysis of the future: The delphi method*. (Data file). Retrieved from http://www.rand.org/pubs/papers/P3558.html

Reiss, B. P. (2011). Restitution devolution? *St. John's Law Review, 85*(4), 1621–1652. Retrieved from http://www.stjohns.edu/

Reybold, L. E., Lammert, J. D., & Stribling, S. M. (2013). Participant selection as a conscious research method: Thinking forward and the deliberation of "emergent" findings. *Qualitative Research, 13*(6), 699–716. doi:10.1177/1468794112465634

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime & Delinquency, 50*(2), 216–238. doi:10.1177/0022427811425539

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

Robinson, O. D. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology, 11*(1), 25–41. doi:10.1080/14780887.2013.801543

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26–44. doi:10.1016/j.cose.2016.01.004

Roesener, A. G., Bottolfson, C., & Fernandez, G. (2014). Policy for US cybersecurity. *Air & Space Power Journal, 28*(6), 38–54. Retrieved from

http://www.airpower.maxwell.af.mil/article.asp?id=236

Salmons, J. (2015). *Qualitative online interviews* (2nd ed.). Thousand Oaks, CA: Sage.

Schilke, O., Reimann, M., & Cook, K. S. (2013). Effect of relationship experience on trust recovery following a breach. *Proceedings of the National Academy of Sciences, 110*(38), 15236–15241. doi:10.1073/pnas.1314857110

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

Senarathna, I., Yeoh, W., Warren, M., & Salzman, S. (2016). Security and privacy concerns for Australian SMEs cloud adoption: Empirical study of metropolitan vs regional SMEs. *Australasian Journal of Information Systems, 20*, 1–20. doi:10.3127/ajis.v20i0.1193

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons, 55*(4), 349–356. doi:10.1016/j.bushor.2012.02.004

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science & Information Security, 14*(1), 129–136. Retrieved from https://sites.google.com/site/ijcsis/

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

Siponen, M., Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information

security policies: An exploratory field study. *Information & Management, 51*(2), 217–224. doi:10.1016/j.im.2013.08.006

Small, W., Maher, L., & Kerr, T. (2014). Institutional ethical review and ethnographic research involving injection drug users: A case study. *Social Science & Medicine, 104*, 157–162. doi:10.1016/j.socscimed.2013.12.010

Snape, D., Kirkham, J., Britten, N., Froggatt, K., Gradinger, F., Lobban, F., Jacoby, A. (2014). Exploring perceived barriers, drivers, impacts and the need for evaluation of public involvement in health and social care research: A modified Delphi study. *BMJ Open, 4*(6), 1–11. doi:10.1136/bmjopen-2014-004943

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

Stewart, D. M., & Fritsch, E. J. (2011). School and law enforcement efforts to combat cyberbullying. *Preventing School Failure: Alternative Education for Children & Youth, 55*(2), 79–87. doi:10.1080/1045988X.2011.539440

Strikwerda, L. (2014). Should virtual cybercrime be regulated by means of criminal law? A philosophical, legal-economic, pragmatic and constitutional dimension. *Information & Communications Technology Law, 23*(1), 31–60. doi:10.1080/13600834.2014.891870

Sun, T., & Wang, X. (2013). Research of data security model in cloud computing platform for SMEs. *International Journal of Security & Its Applications, 7*(6), 97–108. doi:10.14257/ijsia.2013.7.6.10

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2015). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly, 2015*(1), 1–22. doi:10.1080/07418825.2014.994658

Takey, S. M., & de Carvalho, M. M. (2015). Competency mapping in project management: An action research study in an engineering company. *International Journal of Project Management, 33*(4), 784–796. doi:10.1016/j.ijproman.2014.10.013

Tener, D., Wolak, J., & Finkelhor, D. (2015). A typology of offenders who use online communications to commit sex crimes against minors. *Journal of Aggression, Maltreatment & Trauma, 24*(3), 1–19. doi:10.1080/10926771.2015.1009602

Tikk, E. (2011). Ten rules for cyber security. *Survival, 53*(3), 119–132. doi:10.1080/00396338.2011.571016

Todd, M. S., & Rahman, S. M. (2013). Complete network security protection for SMEs within limited resources. *International Journal of Network Security & Its Applications, 5*(6), 1–13. doi:10.5121/ijnsa.2013.5601

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research, 51*(3), 347–360. doi:10.1177/0022343313518940

Vande Putte, D., & Verhelst, M. (2013). Cyber crime: Can a standard risk analysis help in the challenges facing business continuity managers? *Journal of Business Continuity & Emergency Planning, 7*(2), 126–137. Retrieved from http://www.henrystewartpublications.com/

Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal, 15*(4), 407–426. doi:10.2307/255139

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. doi:10.1016/j.cose.2013.04.004

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal, 26*(2), 107–124. doi:10.1057/sj.2012.1

Wall, D. S. (2001). *Cybercrimes and the Internet*. New York, NY: Routledge.

Welch, D., Grossaint, K., Reid, K., & Walker, C. (2014). Strengths-based leadership development: Insights from expert coaches. *Consulting Psychology Journal: Practice & Research*, *66*(1), 20–37. doi:10.1037/cpb0000002

Wellborn, P. F. (2012). "Undercover teachers" beware: How that fake profile on Facebook could land you in the pokey. *Mercer Law Review*, *63*(2), 697–713. Retrieved from http://www.law.mercer.edu/

Wilkerson, J. M., Iantaffi, A., Grey, J. A., Bockting, W. O., & Rosser, B. R. S. (2014). Recommendations for internet-based qualitative health research with hard-to-reach populations. *Qualitative Health Research*, *24*(4), 561–574. doi:10.1177/1049732314524635

Williams, C. (2014). Security in the cyber supply chain: Is it achievable in a complex, interconnected world? *Technovation*, *34*(7), 382–384. doi:10.1016/j.technovation.2014.02.003

Wolgemuth, J. R., Erdil-Moody, Z., Opsal, T., Cross, J. E., Kaanta, T., Dickmann, E. M., & Colomer, S. (2015). Participants' experiences of the qualitative interview:

Considering the importance of research paradigms. *Qualitative Research*, *15*(3), 351–372. doi:10.1177/1468794114524222

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, *48*(2), 311–325. doi:10.1111/ejed.12014

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

Young, D., Lopez, 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*., *2016*(1), 1–15. doi:10.1016/j.ijcip.2016.04.001

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2016). The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human-Computer Interaction*, *32*(3), 215–257. doi:10.1080/10447318.2016.1136177

Appendix A: Informed Consent Form

You are invited to take part in a research study about determining cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The researcher is inviting small business leaders from the Middlesex County region of Massachusetts who have knowledge of the topic of cybersecurity strategies to be in the study. I obtained your name and contact information via the U.S. Small Business Administration Massachusetts district office. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part.

This study is being conducted by a researcher named Jennifer Saber, who is a doctoral candidate at Walden University.

Background Information

The purpose of this study is to explore the cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The targeted population will consist of leaders of small companies located in the Middlesex County region of Massachusetts whose systems are susceptible to data breaches. This population is appropriate for this study, as research suggests the majority of small businesses do not place appropriate investments in cybersecurity. Leaving their systems open to potential cyberattacks may result in data breaches. The implication for positive social change

includes the potential for some small business leaders to accelerate the adoption of cybersecurity practices to protect their systems from data breaches.

Procedures

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

- Complete an online questionnaire that contains 10 open-ended questions. The questionnaire will take approximately 30 minutes to complete.
- Be randomly selected to participate in a semistructured face-to-face interview that may take approximately 60 minutes. I will conduct the interview process. I will be taking notes on my computer and record the interview process to ensure data collection accuracy and will repeat your answers during the interview. Collected data will be coded to ensure privacy. I will be the only person with access to the completed information and will keep it in a locked cabinet.
- Supply company documents containing cybersecurity policies, if available.
- Provide your preferred method of communication with the researcher. Preferred methods of communication include telephone, email, or other technology communication methods.

Voluntary Nature of the Study

This study is voluntary. Everyone will respect your decision of whether or not you choose to be in the study. No one at Walden University will treat you differently if you

decide not to be in the study. If you decide to join the study now, you can still change your mind later. You may stop at any time.

Risks and Benefits of Being in the Study

Being in this type of study involve no known foreseeable risks of the minor discomforts that can be encountered in daily life. Being in this study would not pose risk to your safety or wellbeing.

The potential benefits from participating in this study may include an offering of awareness to the small business sector about cybersecurity practices, the protection of small business systems from data breaches, and by filling gaps in the understanding and practical nature of security practice in small businesses.

Payment

There will be no payment, thank you gifts, or reimbursements provided for being in this study.

Privacy

Any information you provide will be kept confidential. The researcher will not use your personal information for any purposes outside of this research project. Also, the researcher will not include your name or anything else that could identify you in the study reports. Data will be kept secure by:

- Storing an electronic scan of all executed informed consent forms on a password protected flash drive, with the original paper copies immediately shredded after scanned.
- All participant data from the online questionnaires and semistructured face-to-face interviews will be stored electronically on a password protected flash drive.
- Data will be kept for a period of at least 5 years, as required by the university.
- After the 5-year period, the destruction of the password protected flash drive will take place using secure means.

Contacts and Questions

You may ask any questions you have now. Or if you have questions later, you may contact the researcher via [redacted] or jennifer.saber@waldenu.edu. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 612-312-1210. Walden University's approval number for this study is 02-23-16-0460278 and it expires on February 22, 2017. Please print or save this consent form for your records.

Obtaining Your Consent

If you feel you understand the study well enough to make a decision about it, please indicate your consent by replying to this email with the words, "I consent". Your

response is appreciated within 5 business days of receipt of this email. Thank you in advance for your time and consideration of this study.

Appendix B: Interview Questions

1. What are your views concerning the importance of cybersecurity strategies to protect systems from data breaches at your small business?
2. What cybersecurity strategies are in place to protect systems from data breaches at your small business?
3. How are cybersecurity strategies to protect systems from data breaches circulated to employees at your small business?
4. What are your views on how employees recognize the importance of cybersecurity strategies for your small business?
5. What do you think is the best way to circulate cybersecurity strategies to employees of your small business?
6. What is the process for employees to report a potential cyber threat to the leader of the small business?
7. How do you respond to internal cyber threats made against the company?
8. How do you respond to external cyber threats made against the company?
9. Has your business experienced internal cyber threats? If yes, can you describe the risk and action taken to mitigate?
10. Has your business experienced external cyber threats? If yes, can you describe the risk and action taken to mitigate?

Appendix C: Request for Information

February 24, 2016

Mr. Robert H. Nelson

District Director, Massachusetts

U.S. Small Business Association

10 Causeway Street, Room 265

Boston, MA 02222

RE: Request for Information

Dear District Director Nelson,

My name is Jennifer Saber, and I am a doctoral candidate at Walden University. At this time, I am preparing my doctoral study for the topic of determining small business cybersecurity strategies to prevent data breaches. As part of the doctoral study, conduction of research is necessary to answer the study research question of what cybersecurity strategies do leaders of small businesses implement to protect their systems from data breaches.

My current employment is as senior vice president of information technology at an Internet security vendor in Woburn, Massachusetts. I am also fifty percent owner of a

small business in Lowell, Massachusetts. My town of residence is Chelmsford, Massachusetts. Due to my commitment to the state of Massachusetts, I believe researching our small businesses' cybersecurity strategies is key to their continued success.

To complete my doctoral study research, this letter is to request your support to provide a list of small businesses located within the Middlesex County region of Massachusetts. Specifically, business name, owner, address, phone number, and email address. The usage of the information will be to request the participation of small business leaders to complete an online questionnaire contain 10 open-ended questions.

I would like to thank you in advance for your assistance in supplying a list of small businesses for this important research topic. I am also happy to supply any additional information you may need. Please feel free to contact me at [redacted].

Sincerely,

Jennifer Saber

Appendix D: Participant 2B Informed Consent

Gmail by Google

Jennifer Saber <jennifer.saber@waldenu.edu>

Re: [RSVP Please] Are you willing to participate in a doctoral research project?

[redacted] Participant 2B Wed, Mar 30, 2016 at 8:47 AM

To: Jennifer Saber <jennifer.saber@waldenu.edu>

I consent

[redacted]

On Tue, Mar 29, 2016 at 12:13 PM, Jennifer Saber <jennifer.saber@waldenu.edu> wrote:

Hello!

I was wondering if you would be willing to participate in a doctoral study research project related to small business cybersecurity? I am looking for five small business leaders in the Middlesex County area to take a quick 10 question survey. Then, depending on the results, I may ask you to have a brief conversation with me.

As half owner of a small business in Middlesex County myself, I think it is very important to bring the topic of cybersecurity to our community. Please note that this study is about cybersecurity only, and your information (including responses) will remain private and confidential.

Can you help?
If yes, please take a moment to read the informed consent form below and reply with "I consent". If not, could you please reply back with "I cannot"?

Many thanks in advance for your consideration.

Kind regards,

Jennifer Saber
[redacted]

You are invited to take part in a research study about determining cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The researcher is inviting small business leaders from the Middlesex County region of Massachusetts who have knowledge of the topic of cybersecurity strategies to be in the study. I obtained your name/contact information via the U.S. Small Business Administration Massachusetts district office. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part.

This study is being conducted by a researcher named Jennifer Saber, who is a doctoral candidate at Walden University.

Background Information
The purpose of this study is to explore the cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The targeted population will consist of leaders of small companies located in the Middlesex County region of Massachusetts whose systems are susceptible to data breaches. This

population is appropriate for this study because research suggest the majority of small businesses do not place appropriate investments in cybersecurity thus leaving their systems open to potential cyber-attacks that may result in data breaches. The implication for positive social change includes the potential for some small business leaders to accelerate the adoption of cybersecurity practices to protect their systems from data breaches.

Procedure
If you agree to participate in this study, you will be asked to:

- Complete an online questionnaire that contains 10 open-ended questions. The questionnaire will take approximately 30 minutes to complete.
- Be randomly selected to participate in a semistructured face-to-face interview that may take approximately 60 minutes. I will conduct the interview process. I will be taking notes on my computer and record the interview process to ensure data collection accuracy and will repeat your answers during the interview. Collected data will be coded to ensure privacy. I will be the only person with access to the completed information and will keep it in a locked cabinet.
- Supply company documents containing cybersecurity policies, if available.
- Provide your preferred method of communication with the researcher. Preferred methods of communication include telephone, email, or other technology communication methods.

Voluntary Nature of the Study
This study is voluntary. Everyone will respect your decision of whether or not you choose to be in the study. No one at Walden University will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind later. You may stop at any time.

Risks and Benefits of Being in the Study
Being in this type of study involve no known foreseeable risks of the minor discomforts that can be encountered in daily life. Being in this study will not pose risk to your safety or wellbeing.

The potential benefits from participating in this study may include an offering of awareness to the small business sector about cybersecurity practices, the protection of small business systems from data breaches, and by filling gaps in the understanding and practical nature of security practice in small businesses.

Payment
There will be no payment, thank you gift, or reimbursements provided for being in this study.

Privacy
Any information you provide will be kept confidential. The researcher will not use your personal information for any purpose outside of this research project. Also, the researcher will not include your name or anything else that could identify you in the study reports. Data will be kept secure by:

- Storing an electronic scan of all executed informed consent forms on a password protected flash drive, with the original paper copies immediately shredded after scanned.
- All participant data from the online questionnaires and semistructured face-to-face interviews will be stored electronically on a password protected flash drive.
- Data will be kept for a period of at least 5 years, as required by the university.
- After the 5-year period, the destruction of the password protected flash drive will take place using secure means.

Contacts and Questions
You may ask any questions you have now. Or if you have questions later, you may contact the researcher via [redacted] or jennifer.saber@waldenu.edu. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 612-312-1210. Walden University's approval number for this study is 02-23-16-0460278 and it expires on February 22, 2017. Please print or save this consent form for your records.

Obtaining Your Consent
If you feel you understand the study well enough to make a decision about it, please indicate your consent by replying to this email with the words, "I consent". Your response is appreciated within 5 business days of receipt of this email. Thank you in advance for your time and consideration of this study.

Appendix E: Participant 3C Informed Consent

Gmail byGoogle

Jennifer Saber <jennifer.saber@waldenu.edu>

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

[redacted] Participant 3C Wed, Mar 30, 2016 at 2:34 PM
To: Jennifer Saber <jennifer.saber@waldenu.edu>

I consent

From: Jennifer Saber [mailto:jennifer.saber@waldenu.edu]
Sent: Wednesday, March 30, 2016 1:42 PM
To: undisclosed-recipients:
Subject: [RSVP Please] Are you willing to participate in a doctoral research project

Hello!

I was wondering if you would be willing to participate in a doctoral study research project related to small business cybersecurity? I am looking for five small business leaders in the Middlesex County area to take a quick 10 question survey. Then, depending on the results, I may ask you to have a brief conversation with me.

As half owner of a small business in Middlesex County myself, I think it is very important to bring the topic of cybersecurity to our community. Please note that this study is about cybersecurity only, and your information (including responses) will remain private and confidential.

Can you help?
If yes, please take a moment to read the informed consent form below and reply with "I consent". If not, could you please reply back with "I cannot"?

Many thanks in advance for your consideration.

Kind regards,

Jennifer Saber
[redacted]

You are invited to take part in a research study about determining cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The researcher is inviting small business leaders from the Middlesex County region of Massachusetts who have knowledge of the topic of cybersecurity strategies to be in the study. I obtained your name/contact information via the U.S. Small Business Administration Massachusetts district office. This form is part of a process called "informed consent" to allow you to understand

this study before deciding whether to take part.

This study is being conducted by a researcher named Jennifer Saber, who is a doctoral candidate at Walden University.

Background Information

The purpose of this study is to explore the cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The targeted population will consist of leaders of small companies located in the Middlesex County region of Massachusetts whose systems are susceptible to data breaches. This population is appropriate for this study because research suggest the majority of small businesses do not place appropriate investments in cybersecurity thus leaving their systems open to potential cyber-attacks that may result in data breaches. The implication for positive social change includes the potential for some small business leaders to accelerate the adoption of cybersecurity practices to protect their systems from data breaches.

Procedure

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

- Complete an online questionnaire that contains 10 open-ended questions. The questionnaire will take approximately 30 minutes to complete.
- Be randomly selected to participate in a semistructured face-to-face interview that may take approximately 60 minutes. I will conduct the interview process. I will be taking notes on my computer and record the interview process to ensure data collection accuracy and will repeat your answers during the interview. Collected data will be coded to ensure privacy. I will be the only person with access to the completed information and will keep it in a locked cabinet.
- Supply company documents containing cybersecurity policies, if available.
- Provide your preferred method of communication with the researcher. Preferred methods of communication include telephone, email, or other technology communication methods.

Voluntary Nature of the Study

This study is voluntary. Everyone will respect your decision of whether or not you choose to be in the study. No one at Walden University will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind later. You may stop at any time.

Risks and Benefits of Being in the Study

Being in this type of study involve no known foreseeable risks of the minor discomforts that can be encountered in daily life. Being in this study will not pose risk to your safety or wellbeing.

The potential benefits from participating in this study may include an offering of awareness to the small business sector about cybersecurity practices, the protection of small business systems from data breaches, and by filling gaps in the understanding and practical nature of security practice in small businesses.

Payment

There will be no payment, thank you gift, or reimbursements provided for being in this study.

Privacy

Any information you provide will be kept confidential. The researcher will not use your personal information for any purpose outside of this research project. Also, the researcher will not include your name or anything else that could identify you in the study reports. Data will be kept secure by:

- Storing an electronic scan of all executed informed consent forms on a password protected flash drive, with the original paper copies immediately shredded after scanned.

- All participant data from the online questionnaires and semistructured face-to-face interviews will be stored electronically on a password protected flash drive.
- Data will be kept for a period of at least 5 years, as required by the university.
- After the 5-year period, the destruction of the password protected flash drive will take place using secure means.

Contacts and Questions

You may ask any questions you have now. Or if you have questions later, you may contact the researcher via [redacted] or jennifer.saber@waldenu.edu. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 612-312-1210. Walden University's approval number for this study is 02-23-16-0460278 and it expires on February 22, 2017. Please print or save this consent form for your records.

Obtaining Your Consent

If you feel you understand the study well enough to make a decision about it, please indicate your consent by replying to this email with the words, "I consent". Your response is appreciated within 5 business days of receipt of this email. Thank you in advance for your time and consideration of this study.

Appendix F: Participant 4D Informed Consent

Gmail by Google

Jennifer Saber <jennifer.saber@waldenu.edu>

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

[redacted] Participant 4D Wed, Mar 30, 2016 at 4:18 PM

To: Jennifer Saber <jennifer.saber@waldenu.edu>

I consent.

Looking forward to it. Maybe I can learn something!

Waiting for the survey.

From: Jennifer Saber [mailto:jennifer.saber@waldenu.edu]
Sent: Wednesday, March 30, 2016 4:17 PM
To: undisclosed-recipients:
Subject: [RSVP Please] Are you willing to participate in a doctoral research project

Hello!

I was wondering if you would be willing to participate in a doctoral study research project related to small business cybersecurity? I am looking for five small business leaders in the Middlesex County area to take a quick 10 question survey. Then, depending on the results, I may ask you to have a brief conversation with me.

As half owner of a small business in Middlesex County myself, I think it is very important to bring the topic of cybersecurity to our community. Please note that this study is about cybersecurity only, and your information (including responses) will remain private and confidential.

Can you help?
If yes, please take a moment to read the informed consent form below and reply with "I consent". If not, could you please reply back with "I cannot"?

Many thanks in advance for your consideration.

Kind regards,

Jennifer Saber
[redacted]

You are invited to take part in a research study about determining cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The researcher is inviting small business leaders from the Middlesex County region of Massachusetts who have knowledge of the topic of cybersecurity strategies to be in the study. I obtained your name/contact information via the U.S. Small Business Administration Massachusetts district office. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part.

This study is being conducted by a researcher named Jennifer Saber, who is a doctoral candidate at Walden University.

Background Information

The purpose of this study is to explore the cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The targeted population will consist of leaders of small companies located in the Middlesex County region of Massachusetts whose systems are susceptible to data breaches. This population is appropriate for this study because research suggest the majority of small businesses do not place appropriate investments in cybersecurity thus leaving their systems open to potential cyber-attacks that may result in data breaches. The implication for positive social change includes the potential for some small business leaders to accelerate the adoption of cybersecurity practices to protect their systems from data breaches.

Procedure

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

- Complete an online questionnaire that contains 10 open-ended questions. The questionnaire will take approximately 30 minutes to complete.
- Be randomly selected to participate in a semistructured face-to-face interview that may take approximately 60 minutes. I will conduct the interview process. I will be taking notes on my computer and record the interview process to ensure data collection accuracy and will repeat your answers during the interview. Collected data will be coded to ensure privacy. I will be the only person with access to the completed information and will keep it in a locked cabinet.
- Supply company documents containing cybersecurity policies, if available.
- Provide your preferred method of communication with the researcher. Preferred methods of communication include telephone, email, or other technology communication methods.

Voluntary Nature of the Study

This study is voluntary. Everyone will respect your decision of whether or not you choose to be in the study. No one at Walden University will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind later. You may stop at any time.

Risks and Benefits of Being in the Study

Being in this type of study involve no known foreseeable risks of the minor discomforts that can be encountered in daily life. Being in this study will not pose risk to your safety or wellbeing.

The potential benefits from participating in this study may include an offering of awareness to the small business sector about cybersecurity practices, the protection of small business systems from data breaches, and by filling gaps in the understanding and practical nature of security practice in small businesses.

Payment

There will be no payment, thank you gift, or reimbursements provided for being in this study.

Privacy

Any information you provide will be kept confidential. The researcher will not use your personal information for any purpose outside of this research project. Also, the researcher will not include your name or anything else that could identify you in the study reports. Data will be kept secure by:

- Storing an electronic scan of all executed informed consent forms on a password protected flash drive, with the original paper copies immediately shredded after scanned.
- All participant data from the online questionnaires and semistructured face-to-face interviews will be stored electronically on a password protected flash drive.
- Data will be kept for a period of at least 5 years, as required by the university.
- After the 5-year period, the destruction of the password protected flash drive will take place using secure means.

Contacts and Questions

You may ask any questions you have now. Or if you have questions later, you may contact the researcher via [redacted] or jennifer.saber@waldenu.edu. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 612-312-1210. Walden University's approval number for this study is 02-23-16-0460278 and it expires on February 22, 2017. Please print or save this consent form for your records.

Obtaining Your Consent

If you feel you understand the study well enough to make a decision about it, please indicate your consent by replying to this email with the words, "I consent". Your response is appreciated within 5 business days of receipt of this email. Thank you in advance for your time and consideration of this study.

Appendix G: Participant 6F Informed Consent

Gmail byGoogle

Jennifer Saber <jennifer.saber@waldenu.edu>

Re: [RSVP Please] Are you willing to participate in a doctoral research project

[redacted] Participant 6F Wed, Mar 30, 2016 at 4:45 PM

To: Jennifer Saber <jennifer.saber@waldenu.edu>

I consent.

Regards,

[redacted]

On 3/30/2016 3:49 PM, Jennifer Saber wrote:

> Hello!
>
> I was wondering if you would be willing to participate in a doctoral study research project related to small business cybersecurity? I am looking for five small business leaders in the Middlesex County area to take a quick 10 question survey. Then, depending on the results, I may ask you to have a brief conversation with me.
>
> As half owner of a small business in Middlesex County myself, I think it is very important to bring the topic of cybersecurity to our community. Please note that this study is about cybersecurity only, and your information (including responses) will remain private and confidential.
>
> ***Can you help?***
> If yes, please take a moment to read the informed consent form below and reply with "I consent". If not, could you please reply back with "I cannot"?
>
> Many thanks in advance for your consideration.
>
> Kind regards,
>
> Jennifer Saber
> [redacted]
>
> ---
>
> You are invited to take part in a research study about determining cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The researcher is inviting small business leaders from the Middlesex County region of Massachusetts who have knowledge of the topic of cybersecurity strategies to be in the study. I obtained your name/contact information via the U.S. Small Business Administration Massachusetts district office. This form is part of a process called "informed consent" to allow

you to understand this study before deciding whether to take part.

This study is being conducted by a researcher named Jennifer Saber, who is a doctoral candidate at Walden University.

Background Information
The purpose of this study is to explore the cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The targeted population will consist of leaders of small companies located in the Middlesex County region of Massachusetts whose systems are susceptible to data breaches. This population is appropriate for this study because research suggest the majority of small businesses do not place appropriate investments in cybersecurity thus leaving their systems open to potential cyber-attacks that may result in data breaches. The implication for positive social change includes the potential for some small business leaders to accelerate the adoption of cybersecurity practices to protect their systems from data breaches.

Procedure
If you agree to participate in this study, you will be asked to:

- Complete an online questionnaire that contains 10 open-ended questions. The questionnaire will take approximately 30 minutes to complete.
- Be randomly selected to participate in a semistructured face-to-face interview that may take approximately 60 minutes. I will conduct the interview process. I will be taking notes on my computer and record the interview process to ensure data collection accuracy and will repeat your answers during the interview. Collected data will be coded to ensure privacy. I will be the only person with access to the completed information and will keep it in a locked cabinet.
- Supply company documents containing cybersecurity policies, if available.
- Provide your preferred method of communication with the researcher. Preferred methods of communication include telephone, email, or other technology communication methods.

Voluntary Nature of the Study
This study is voluntary. Everyone will respect your decision of whether or not you choose to be in the study. No one at Walden University will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind later. You may stop at any time.

Risks and Benefits of Being in the Study
Being in this type of study involve no known foreseeable risks of the minor discomforts that can be encountered in daily life. Being in this study will not pose risk to your safety or wellbeing.

The potential benefits from participating in this study may include an offering of awareness to the small business sector about cybersecurity practices, the protection of small business systems from data breaches, and by filling gaps in the understanding and practical nature of security practice in small businesses.

Payment
There will be no payment, thank you gift, or reimbursements provided for being in this study.

Privacy
Any information you provide will be kept confidential. The researcher will not use your personal information for any purpose outside of this research project. Also, the researcher will not include your name or anything else that could identify you in the study reports. Data will be kept secure by:

- Storing an electronic scan of all executed informed consent forms on a password protected flash drive, with the original paper copies immediately shredded after scanned.
- All participant data from the online questionnaires and semistructured face-to-face interviews will be stored electronically on a password protected flash drive.
- Data will be kept for a period of at least 5 years, as required by the university.

- After the 5-year period, the destruction of the password protected flash drive will take place using secure means.

Contacts and Questions
You may ask any questions you have now. Or if you have questions later, you may contact the researcher via [redacted] or jennifer.saber@waldenu.edu. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 612-312-1210. Walden University's approval number for this study is 02-23-16-0460278 and it expires on February 22, 2017. Please print or save this consent form for your records.

Obtaining Your Consent
If you feel you understand the study well enough to make a decision about it, please indicate your consent by replying to this email with the words, "I consent". Your response is appreciated within 5 business days of receipt of this email. Thank you in advance for your time and consideration of this study.

--

Appendix H: Participant 7G Informed Consent

Gmail byGoogle

Jennifer Saber <jennifer.saber@waldenu.edu>

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

[redacted] Participant 7G Wed, Mar 30, 2016 at 5:04 PM
To: Jennifer Saber <jennifer.saber@waldenu.edu>

I consent

From: Jennifer Saber [mailto:jennifer.saber@waldenu.edu]
Sent: Wednesday, March 30, 2016 3:50 PM
Subject: [RSVP Please] Are you willing to participate in a doctoral research project

Hello!

I was wondering if you would be willing to participate in a doctoral study research project related to small business cybersecurity? I am looking for five small business leaders in the Middlesex County area to take a quick 10 question survey. Then, depending on the results, I may ask you to have a brief conversation with me.

As half owner of a small business in Middlesex County myself, I think it is very important to bring the topic of cybersecurity to our community. Please note that this study is about cybersecurity only, and your information (including responses) will remain private and confidential.

Can you help?
If yes, please take a moment to read the informed consent form below and reply with "I consent". If not, could you please reply back with "I cannot"?

Many thanks in advance for your consideration.

Kind regards,

Jennifer Saber
[redacted]

You are invited to take part in a research study about determining cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The researcher is inviting small business leaders from the Middlesex County region of Massachusetts who have knowledge of the topic of cybersecurity strategies to be in the study. I obtained your name/contact information via the U.S. Small Business Administration Massachusetts district office. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part.

This study is being conducted by a researcher named Jennifer Saber, who is a doctoral candidate at Walden University.

Background Information

The purpose of this study is to explore the cybersecurity strategies leaders of small businesses use to protect their systems from data breaches. The targeted population will consist of leaders of small companies located in the Middlesex County region of Massachusetts whose systems are susceptible to data breaches. This population is appropriate for this study because research suggest the majority of small businesses do not place appropriate investments in cybersecurity thus leaving their systems open to potential cyber-attacks that may result in data breaches. The implication for positive social change includes the potential for some small business leaders to accelerate the adoption of cybersecurity practices to protect their systems from data breaches.

Procedure

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

- Complete an online questionnaire that contains 10 open-ended questions. The questionnaire will take approximately 30 minutes to complete.
- Be randomly selected to participate in a semistructured face-to-face interview that may take approximately 60 minutes. I will conduct the interview process. I will be taking notes on my computer and record the interview process to ensure data collection accuracy and will repeat your answers during the interview. Collected data will be coded to ensure privacy. I will be the only person with access to the completed information and will keep it in a locked cabinet.
- Supply company documents containing cybersecurity policies, if available.
- Provide your preferred method of communication with the researcher. Preferred methods of communication include telephone, email, or other technology communication methods.

Voluntary Nature of the Study

This study is voluntary. Everyone will respect your decision of whether or not you choose to be in the study. No one at Walden University will treat you differently if you decide not to be in the study. If you decide to join the study now, you can still change your mind later. You may stop at any time.

Risks and Benefits of Being in the Study

Being in this type of study involve no known foreseeable risks of the minor discomforts that can be encountered in daily life. Being in this study will not pose risk to your safety or wellbeing.

The potential benefits from participating in this study may include an offering of awareness to the small business sector about cybersecurity practices, the protection of small business systems from data breaches, and by filling gaps in the understanding and practical nature of security practice in small businesses.

Payment

There will be no payment, thank you gift, or reimbursements provided for being in this study.

Privacy

Any information you provide will be kept confidential. The researcher will not use your personal information for any purpose outside of this research project. Also, the researcher will not include your name or anything else that could identify you in the study reports. Data will be kept secure by:

- Storing an electronic scan of all executed informed consent forms on a password protected flash drive, with the original paper copies immediately shredded after scanned.
- All participant data from the online questionnaires and semistructured face-to-face interviews will be stored electronically on a password protected flash drive.

- Data will be kept for a period of at least 5 years, as required by the university.
- After the 5-year period, the destruction of the password protected flash drive will take place using secure means.

Contacts and Questions

You may ask any questions you have now. Or if you have questions later, you may contact the researcher via [redacted] or jennifer.saber@waldenu.edu. If you want to talk privately about your rights as a participant, you can call Dr. Leilani Endicott. She is the Walden University representative who can discuss this with you. Her phone number is 612-312-1210. Walden University's approval number for this study is 02-23-16-0460278 and it expires on February 22, 2017. Please print or save this consent form for your records.

Obtaining Your Consent

If you feel you understand the study well enough to make a decision about it, please indicate your consent by replying to this email with the words, "I consent". Your response is appreciated within 5 business days of receipt of this email. Thank you in advance for your time and consideration of this study.

Appendix I: Sample of Instrument

Small Business Cybersecurity

1. What are your views concerning the importance of cybersecurity strategies to protect systems from data breaches at your small business?

2. What cybersecurity strategies are in place to protect systems from data breaches at your small business?

3. How are cybersecurity strategies to protect systems from data breaches circulated to employees at your small business?

4. What are your views on how employees recognize the importance of cybersecurity strategies for your small business?

5. What do you think is the best way to circulate cybersecurity strategies to employees of your small business?

6. What is the process for employees to report a potential cyber threat to the leader of the small business?

7. How do you respond to internal cyber-threats made against the company?

8. How do you respond to external cyber threats made against the company?

9. Has your business experienced internal cyber threats? If yes, can you describe the risk and action taken to mitigate?

10. Has your business experienced external cyber threats? If yes, can you describe the risk and action taken to mitigate?

Click here to Submit