2020

Effective Strategies Small Business Leaders Use to Address Ransomware

William Jason Tuttle
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

William Jason Tuttle

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. Franz Gottleib, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Janie Mayo, Committee Member, Doctor of Business Administration Faculty

Dr. Lisa Cave, University Reviewer, Doctor of Business Administration Faculty

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

Walden University
2020

Abstract

Effective Strategies Small Business Leaders Use to Address Ransomware

by

William Jason Tuttle

MS, Keller Graduate School, 2015

BS, DeVry, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

March 2020

Abstract

Small business leaders face a wide range of cybersecurity threats. Ransomware is a specific cybersecurity threat that cybercriminals can use to deny small business leaders' access to data in exchange for a ransom payment. Grounded in routine activity conceptual framework, the purpose of this qualitative multiple case study was to explore effective strategies small business leaders use to address ransomware. Data were collected from 5 leaders of small businesses in the southeast region of the United States. Data sources included interviews and archival documents. Data were analyzed using Yin's 5 step process. The analysis revealed 3 primary themes: ransomware strategy, support structure, and cybersecurity awareness. Managers and leaders of small businesses could potentially benefit from this research by applying strategies that emerged from the identified themes to prevent victimization from ransomware. The implications for positive social change include the potential to support the local economy and to prevent and mitigate the spread of ransomware to protect confidential and sensitive consumer information.

Effective Strategies Small Business Leaders Use to Address Ransomware

by

William Jason Tuttle

MS, Keller Graduate School, 2015

BS, DeVry, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

March 2020

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Small business leaders who rely on information systems as a critical component of their business face a spectrum of cybersecurity threats. The cybersecurity threat of ransomware denies small businesses access to their data in exchange for a ransom payment. The threat of ransomware attacks continues to escalate through computer vulnerabilities while criminal business models become more sophisticated (Young & Yung, 2017). The foundation of this study is the challenges faced by leaders of small businesses in protecting their information systems from the escalating use of ransomware.

Background of the Problem

The background of the problem consists of a specific type of cybersecurity threat to business. Ransomware is a type of cybersecurity threat that, once activated, prevents legitimate users from accessing their information systems until they pay a ransom (Brown, 2016). The criminal actors involved demand a ransom in return for access to business data (Choudhary, Zavarsky, & Lindskog, 2016). Victims typically pay ransoms with a difficult-to-trace electronic cryptocurrency (Brown, 2016). Complaints regarding infections from ransomware continue to rise (Federal Bureau of Investigation, 2016; Internet Crime Complaint Center, 2016). The success rate of infection is evidence that security models to protect against ransomware are inadequate. Reactive security models fail to provide adequate protection from the threat of cryptoviral ransomware extortion attacks (Young & Yung, 2017). Inadequate planning, preparation, and training for addressing ransomware can cause a small business to encounter operational disruptions, affecting business continuity and causing reputational damage. Small businesses may

benefit from knowledge and strategies to protect their information systems from ransomware. I have provided the background to the problem, and the focus of the study. In the following paragraphs, I discuss the problem statement, purpose statement, nature of the study, research questions, interview questions, conceptual framework, operational definitions, assumptions, limitations, and delimitations, and the significance of the study. Finally, I provide a review of the professional and academic literature.

Problem Statement

Ransomware has become a significant cybersecurity threat to business (Choudhary et al., 2016). Globally, new cases of ransomware infection grew to a rate of over 100,000 daily during the first few months of 2016 (Federal Bureau of Investigation, 2016), with over $2.4 million in losses and 2,673 total complaints for 2016 in the United States (Internet Crime Complaint Center, 2016). The general business problem is that many small business cybersecurity resources fail to protect information systems. The specific business problem is that some small business leaders lack the cybersecurity strategies necessary to protect their information systems from ransomware.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the cybersecurity strategies some small business leaders use to protect their information systems from ransomware. The targeted population for this study was five small business leaders located in the Knox County region of Tennessee who successfully implemented cybersecurity strategies to protect their information systems from ransomware. The study's implications for positive social change include the potential for increasing

employment opportunities in the region and supporting the local economy by protecting information systems from ransomware. Furthermore, small business leaders may realize their value as a cybercrime target and consider implementing stronger cybersecurity controls to prevent and mitigate the spread of ransomware to protect confidential and sensitive consumer information.

Nature of the Study

I used a qualitative method to explore strategies that small business leaders use to protect their information systems from ransomware. Researchers espouse using the qualitative method to observe, understand, and explore a phenomenon (Goldberg & Allen, 2015). Researchers in quantitative research attempt to answer a question by using numbers for quantifying, measuring, and comparing the data (McCusker & Gunaydin, 2015). Mixed method research is relevant when the goal of the researcher is to combine the use of quantitative and qualitative methods (Abro, Khurshid, & Aamir, 2015). The quantitative and mixed method approaches are not appropriate because my objective was to explore the business problem qualitatively and not to conduct a quantitative analysis.

I used a case study design to explore viewpoints about the cybersecurity strategies of small business leaders. Case study design is appropriate in business settings where there is a potential benefit from gathering viewpoints from different perspectives and analyzing participants' experience with phenomena (Turner & Danks, 2014). A purpose of phenomenological design is to explore the meanings of participants' lived experiences (Wilson, 2015). The phenomenological research design was not appropriate for this study because exploring the meanings of lived experiences does not allow for a focused

examination of the business problem. In ethnographic research, the researcher must explore the culture of participants to become part of the social environment (Gelling, 2014). An ethnographic research design was not appropriate, as becoming immersed in the culture was outside the scope of this study. In narrative research, the objective is to understand lived experiences using others' words or descriptions (Joyce, 2015). Narrative research may offer a much wider description of events and behaviors than needed. Because I intended to explore strategies for mitigating ransomware from multiple data sources, I used a multiple case study design rather than other qualitative designs.

Research Question

What cybersecurity strategies do some small business leaders use to protect their information systems from ransomware?

Interview Questions

1. What strategies do you use to protect your information systems from ransomware?
2. How did you assess the effectiveness of your strategies for protecting your information systems from ransomware?
3. What were the key barriers to implementing the strategies for protecting your company from ransomware?
4. How did you address the key barriers to implementing the strategies for improving your protection against ransomware?

5. What other information could you add that might be applicable to the strategies that small business owners use to protect their information systems from ransomware?

Conceptual Framework

Cohen and Felson (1979) developed the routine activity theory to explain crime as an event that occurs in space and time. Routine activity theory was applicable to my study, as small business leaders may use routine activity theory as a framework to understand how effective protection against ransomware can prevent infection. Routine activity theory is a well-established criminological theory that serves as the basis for examining cybercrime offenses and victimization (Leukfeldt & Yar, 2016). I used routine activity theory as the foundation of my conceptual framework because it related to developing prevention strategies to address victims and attackers in the cybersecurity realm against ransomware. The following key constructs underlie routine activity theory: (a) potential offender, (b) target, and (c) absence of protection (Cohen & Felson, 1979). Applying the conceptual framework led to an understanding of the findings from this study because ransomware requires an actor as the ransomware offender, a target for the ransomware payload, and a lack of protection against the payload for the ransomware to cause damage. Adequate protection prevents a bad actor from compromising a robust system. The absence of adequate protection enables perpetrators to compromise a previously clean information system with a ransomware payload. The conceptual framework served as an appropriate lens to understand managerial actions to protect against cyberattacks.

Operational Definitions

The following includes definitions of terms used throughout this study.

Bitcoin: Bitcoin, created in 2009, is a pseudo-anonymous cryptographic electronic currency (Ortolani, 2016).

Blockchain: The blockchain is a public ledger containing the pseudo-anonymous Bitcoin addresses with every associated Bitcoin transaction (Ortolani, 2016).

Capable guardianship: Capable guardianship consists of technical capable guardianship (an example is antivirus software) and personal capable guardianship (a person with high technical knowledge and capable of anticipating threats thereby reducing target accessibility; Leukfeldt & Yar, 2016).

Cryptovirology: Researchers from Columbia University coined the term cryptovirology to describe the study of offensive cryptoviral technology consisting of malware and cryptography (Young & Yung, 2017).

Guardianship: Guardianship is synonymous with protection, while researchers commonly expand the definition to include other elements such as surveillance and the role of surveillance in preventing crime (Vries & Gelder, 2015).

Ransomware: Ransomware is a form of cryptovirology used to extort money from victims (Young & Yung, 2017).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are commonly accepted as fact without any proof and made by researchers during study design, data capture, and interpretation of results (Niven &

Boorman, 2016). The first assumption for this study was that participants would have an interest and be willing to participate in the study. Another assumption was that participants would provide honest and truthful responses to interview questions. An additional assumption was that conducting face-to-face interviews and acquiring company documents would provide the information needed for thematic development. Another assumption was that responses provided by the participants would be substantial and address the research question. To mitigate these assumptions, I purposely selected participants, established positive relationships, and conducted interviews that lead to data saturation.

Limitations

Researchers define limitations of a study to account for known weaknesses and to provide transparency (Levy, Fabian, & Peters, 2015). One limitation was the continual evolution of ransomware and how effective strategies change over time. The effectiveness of ransomware improves as attackers create more sophisticated ransomware and exploit new vulnerabilities (Genç, Lenzini, & Ryan, 2017; Kharraz, Robertson, Balzarotti, Bilge, & Kirda, 2015). Another limitation was related to my constrained sample size, as small samples may not provide significant findings to transfer to other venues or businesses with strategies for coping with ransomware. Data saturation within qualitative research requires at least two case studies to justify the sample size for transferability with small samples (Boddy, 2016). An additional limitation was that the chosen participants consisted of small business leaders who may have lacked a priori knowledge required to answer the interview questions from the standpoint of an

information technology expert. It is possible for researchers to mitigate inherent limitations in case study research by combining research synthesis techniques (Levy et al., 2015).

Delimitations

Study delimitations consist of parameters, scope, and boundaries (Hernández-Flores et al., 2017). One delimitation of this study was chosen participants were small business leaders rather than information technology experts. Another delimitation of the study was the sample size of five small business leaders. An additional delimitation of the study was the geographic region of the study—the Knox County region of Tennessee.

Significance of the Study

The significance of this study is that small business leaders may become more informed about the implications of weak cybersecurity controls for compromising business operations. Small business leaders remain uninformed of the magnitude of the threat posed by ransomware (Fanning, 2015; Paulsen, 2016). Small business leaders may learn how to mitigate and strengthen their cybersecurity to lessen negative consequences stemming from ransomware attacks. Small business leaders might also gain the information they need to promote safety and stability in their locus of control, profitability, efficiency, and cost-effectiveness in responsibly managing cybersecurity risks associated with ransomware. Businesses leaders of larger firms with more sophisticated information systems than a small business might find it useful to adapt the strategies used by some small business leaders as mitigation strategies to combat

ransomware targeting small business information systems to subcomponents of larger and more complex information systems.

Contribution to Business Practice

The potential significance of this study to the practice of business is multifaceted. Small business leaders may have the opportunity to learn about securing their information systems from ransomware attacks. A strategic ransomware cybersecurity plan includes scenarios for the potential attack, steps taken during the attack, the post ransomware incident response, and defensive posturing (Bridget, 2016). Findings from this study may contribute to avoiding or mitigating the effects of ransomware and hardening existing information systems, as well as provide a foundation to create a strategic cybersecurity plan that may enable small business owners to address the threats from ransomware.

Implications for Social Change

The implications of this study to social change include increased public awareness about the transformative power of cybersecurity technologies and strengthened trust in universal cybernetworks. The potential adoption of a stronger security posture may support the protection of sensitive consumer information, while assurance promotes consumer trust in Internet commerce. Advancements in cybersecurity support the distribution of innovative technologies, which is a societal benefit (Yeoh, 2017). Also, positive social change might result from employment opportunities and effects on local economies by mitigating potential economic losses to small businesses originating from a ransomware infection.

A Review of the Professional and Academic Literature

The purpose of this qualitative multiple case study was to explore the cybersecurity strategies that small business leaders use to protect their information systems from ransomware. The purpose of this professional and academic literature review was to compare and contrast opposing positions and complementary research surrounding my research topic. The literature review begins with an expository of the applied conceptual framework of routine activity theory.

My sources for the literature review included journals available from academic databases, such as the Academic Search Complete/Premier, DeepDyve, EBSCOhost, Google Scholar, NASA's Astrophysics Data System Bibliographic Services, ProQuest, and SAGE. I accessed these electronic databases through the Walden University Library. I kept a research journal to document specific keywords for searching these databases and subscribed to peer-reviewed journals to track the latest research and trends related to my topic. Specific keywords include *1979 routine activity theory, Cohen and Felson*, *ransomware and business*, *routine activities, routine activity theory, routine activity theory and cybercrime*, and a combination of *routine activity theory* and *cybercrime* and *ransomware*. In order to assist thematic development, I created an application to track references, store annotated bibliographies, and generate thematic mind maps based on keyword density.

The review includes 69 resources, 94% of which were peer-reviewed and verified using Ulrich's Periodicals Directory. Ninety-seven percent had publication dates from 2014 to 2018. I organized the literature review with the routine activity theory framework

first, followed by routine activity theory conceptual constructs, the study of ransomware, ransomware and routine activity theory constructs, theory comparisons, cybersecurity, strategic management and ransomware cybersecurity, ransomware and business, operationalizing routine activity theory constructs, and a summary.

Routine Activity Theory

Routine activity theory existed prior to the notion of cybercrime. Cohen and Felson (1979) developed routine activity theory to analyze crime without relying on offender information. Researchers use this theory to highlight the role of criminal spatial decision making on offender familiarity and ease of access, which in turn serves to increase preferential selection based on proximity and the likelihood of getting caught (Frith, Johnson, & Fry, 2017). The anti-spatial nature of cyberspace is in direct conflict with routine activity theory studies because routine activity theory relies on spatial properties of the physical environment (Leukfeldt & Yar, 2016). The suitability of routine activity theory for examining cybercrime in the antispatial cyberrealm is not immediately evident.

A precedent does exist, however, for using routine activity theory in cyberspace with a major strength of overcoming the challenges inherent in gaining access to offenders in the online environment by removing the requirement of the physical environment. Regardless of the lack of identified spatial features in cyberspace, routine activity theory is suitable for the study of online victimization and high-technology malware-related crimes (Leukfeldt & Yar, 2016). Routine activity theory is flexible enough to accommodate abstract concepts regarding space and time from the physical

world to the virtual. For example, researchers utilize routine activity theory to study victimization in the antispatial realm of cybercrime. Paek and Nalla (2015) used routine activity theory to find a positive relationship with routine online activities and online victimization, and Brady, Randa, and Reyns (2016) used routine activity theory to explore financial cybercrime and found that a significant number of businesses experience cybercrime on a regular basis. Ilievski (2016) conducted a study using routine activity theory to determine that users who spend more time online put themselves at greater risk of becoming a victim of cybercrime. Chen, Beaudoin, and Hong (2017) used routine activity theory to study victimization in the cyberrealm and found careless cybersecurity behavior persists until after victimization occurs.

Researchers also use routine activity theory to overcome challenges inherent with studying cybercrime. Jansen and Leukfeldt (2016) tested the use of routine activity theory and cybercrime to determine awareness and training are the most crucial elements for safely banking online, but no determination of the effectiveness of guardianship occurred. Choi and Lee (2017) concluded that routine activity theory is inadequate for explaining the role of guardianship in cyberinterpersonal violence victimization, and the most effective way to mitigate online threats is to use personal digital guardianship and end-user education on the dangers associated with the Internet. However, Holt, Burruss, and Bossler (2016) found that, despite criticism of the effectiveness of routine activity theory in cybercrime research, the framework is sufficient for exploring cybercrime victimization and for providing target-hardening strategies to combat criminal actors who introduce thousands of new malware variants on a daily basis. Leukfeldt and Yar (2016)

overcame challenges associated with routine activity theory and testing online victimization and high-technology malware-related crimes by using interviews.

Routine activity theory is well suited for the study of victimization and guardianship from malware. However, the study of cybersecurity using routine activity theory extends beyond topics related to malware. Routine activity theory was suitable for developing an understanding of the characteristics of cybervictim targets in phishing scams designed to steal money from victims' bank accounts (Leukfeldt, 2014). One example of a phishing scam involves an attacker sending a fraudulent e-mail to a potential victim to lure the victim to click on a link or to divulge personal information to the attacker (Leukfeldt, 2014). The constructs of routine activity theory encompass a potential victim, a motivated attacker, and a lack of capable guardianship (Cohen & Felson, 1979). In the phishing scam example, the potential victim is the user who might click on the fraudulent link in the e-mail, the motivated attacker is the responsible party sending the offending e-mail, and the lack of capable guardianship could be the lack of protective software or the lack of user knowledge to differentiate between a legitimate link in an e-mail and a fraudulent link in an email. The three constructs of routine activity theory fulfill the prerequisites of crime.

Researchers may not know or have defined the lack of a capable guardian in the context of cybercrime. The capable guardian or protective factor component of routine activity theory, varies based on the type of cybercrime. The protective factor of antivirus software is applicable when the focus is on malware attacks; however, antivirus software fails to provide adequate protection against phishing scams (Leukfeldt, 2014). In cases of

phishing victimization, the capable guardianship or protective element of routine activity theory shifts responsibility to the leadership of financial institutions who coordinate financial transactions on behalf of the consumer (Leukfeldt, 2014). The definition of capable guardianship is flexible enough to define protection elements present in a small business information system.

Small business information systems contain elements exposed to the public Internet. Routine activity theory applied to research involving phishing, hacking, and malware allows researchers to consider the increased potential for victimization based on online activity and target suitability (Reyns, 2015). Offending and victimization related to malware can begin with successful phishing or hacking attacks (Reyns, 2015). Researchers have called for additional research related to identifying correlates for online victimization (Reyns, 2015). Prior research serves as an empirical foundation of the suitability and usefulness of routine activity theory for studying cybercrime (Brady et al., 2016; Chen et al., 2017; Choi & Lee, 2017; Holt et al., 2016; Ilievski, 2016; Jansen & Leukfeldt, 2016; Leukfeldt & Yar, 2016; Paek & Nalla, 2015). Over time, the use of routine activity theory evolved to incorporate and explain routine activity phenomena existing in the online realm rather than as originally intended in the physical realm.

Spatial. Routine activity theory in the spatial context adheres to the original intention of explaining how and why crimes occur in the physical realm. It is possible for potential victims to design the physical environment to deter potential offenders from criminal behavior (Blasdell, 2015). According to researchers, removing a single element of routine activity theory is enough to prevent a crime from occurring (Blasdell, 2015;

Mui & Mailley, 2015). In the absence of capable guardianship or the lack of oversight from management in the physical workplace, perpetration of the crime occurs once a suitable target and a motivated offender make contact (Mui & Mailley, 2015). Researchers use routine activity theory to predict physical and property victimization in the workplace (Kodellas, Fisher, & Wilcox, 2015). The goal of preventing a crime from occurring through the lens of routine activity theory includes the reliance on removing one of the key tenets of the theory.

In the spatial realm, it is possible to define the influencing constructs of routine activity theory in preventing criminal behavior. Lack of surveillance or guardianship, the presence of motivated offenders, and the availability of suitable targets dictate the probability and occurrence of crime (Vries & Gelder, 2015). In routine activity theory the overlap between a motivated offender, susceptible target, and absence of capable guardianship results in victimization (Pratt & Turanovic, 2016). Parental supervision in the form of physical guardianship and the use of antivirus software and other virtual forms of guardianship are effective in reducing cybervictimization (Kalia & Aleem, 2017). Therefore, it is possible to extend routine activity theory to account for victimization in antispatial realms and constructs.

Antispatial. The antispatial context of routine activity theory expands upon the original intentions of explaining how and why crimes occur in the physical realm and includes the immediate or eventual convergence of the offender and victim in a virtual realm. Routine activity theory is an effective framework for studying cybervictimization (Kalia & Aleem, 2017; Näsi, Räsänen, Kaakinen, Keipi, & Oksanen, 2017; Reyns,

Henson, & Fisher, 2016). Perpetual online exposure of potential targets to motivated offenders amplifies the threat of cybervictimization (Brady et al., 2016). A major challenge in routine activity theory and cybervictimization is identifying the parallels between motivated offenders and potential targets (Holt et al., 2016; Leukfeldt & Yar, 2016). The digital nature of cybercrime exceeds the physical precepts initially introduced in routine activity theory and is why some researchers refute the use of routine activity theory in cybercrime research (Holt et al., 2016). Victimization in routine activity theory is a result of criminal opportunity and quantifying criminal opportunity in the antispatial realm is problematic (Brady et al., 2016). Regardless of the difficulties in quantifying criminal opportunity, it is possible to find relationships between opportunity and cybervictimization.

Limitations on accurately reporting cybervictimization reinforce the need for exploring alternative methods to identify victimization correlates. Researchers use routine activity theory to remove the victim from the equation to determine the likelihood of a crime occurring (Wick et al., 2017). Researchers sometimes use routine activity theory in a polemic manner toward victim behavior (Arntfield, 2015). However, it remains unclear if the use of routine activity theory is effective in the study of cybercrime (Leukfeldt & Yar, 2016). Other researchers have found a positive relationship between routine online activities and online victimization (Paek & Nalla, 2015). Fraud and deceit often accompany criminal behavior in cyberspace (Agustina, 2015), and the effective use of routine activity theory in the cyberrealm requires an understanding of how, when, and where guardianship occurs within the context of the study (Reyns et al., 2016).

Identifying the guardianship elements of cybercrime is an alternative method of identifying the victimization correlates and overcoming the reporting limitations.

Study alignment. Routine activity theory depicts the key constructs suitable for studying cybersecurity strategies relevant to the role of small business leadership in protecting business assets from the threat of ransomware. Precedence exists for extending the fundamental principles of routine activity theory into the antispatial realm. Empirical evidence indicates varying levels of the suitability of routine activity theory constructs and its applicability in the study of cybercrime victimization (Leukfeldt & Yar, 2016). Nonetheless, the conceptual constructs facilitate an examination of guardianship, motivated offenders, and target suitability in cybercrime victimization.

Routine Activity Theory Conceptual Constructs

Conceptual constructs are useful in identifying the boundaries of data. Routine activity theory consists of three conceptual constructs: (a) guardianship, (b) suitable targets, and (c) motivated offenders (Leukfeldt & Yar, 2016). In the following sections, I discuss these three conceptual constructs as they apply to routine activity theory and the study of ransomware and cybersecurity.

Guardianship. The effectiveness of applied guardianship differs depending on the environment. The effectiveness of guardianship varies depending on the applicability of guardianship to the phenomenon under study (Wang, Gupta, & Rao, 2015). As technology evolves, researchers continue to explore tools that provide better guardianship to reduce and limit situational crime exposure (Brady et al., 2016). Researchers have determined through using routine activity theory the significant role of guardianship in

target suitability (Näsi, Oksanen, Keipi, & Räsänen, 2015). Guardianship is an evolving and moving target with direct implications for target suitability.

Suitable targets. A suitable target is a prerequisite for cybervictimization to occur. Storing credit card information puts customers at perpetual risk of victimization (Brady et al., 2016). Target suitability includes an assumption of different dimensions based on the type of crime with a direct influence on victimization risk (Reyns & Henson, 2016). A challenge for researchers without economic indicators of target attractiveness is the lack of documented measures to gauge target suitability (Reyns & Henson, 2016). Researchers using routine activity theory rely on valid indicators for unambiguous research (Wolfe, Marcum, Higgins, & Ricketts, 2016). Properly correlating victimization requires the identification of applicable indicators. Researchers select indicators and use suitable target constructs to identify target accessibility.

Researchers identify the qualities of suitable targets to determine accessibility. The acronym VIVA represents value, inertia, visibility, and access to describe accessible targets (Nikitkov, Stone, & Miller, 2014). Motivated offenders' attractions to potential victim characteristics develop from VIVA attributes (Jansen & Leukfeldt, 2016). The elements of VIVA correlate to target suitability, with value as the most prominent predictable attribute (Wang et al., 2015). Properly understanding what makes a target suitable is relevant to understanding what motivates an offender and how victimization occurs.

Value. The value of a target indicates the financial characteristics perceived as desirable by an attacker (Jansen & Leukfeldt, 2016). The original definition of value in

routine activity theory referred to physical goods with an identifiable monetary value (Cohen & Felson, 1979). In the online context, value refers to the monetary value of information assets or the digital representation of physical goods to facilitate exchange in the spatial realm (Wang et al., 2015). The value of regaining access to maliciously encrypted information assets represents the value component of a suitable ransomware target.

Inertia. Researchers commonly attribute inertia to a physical characteristic of an object. The inertia of a target is more difficult to quantify in the digital realm than in the physical (Leukfeldt & Yar, 2016). Jansen and Leukfeldt (2016) omitted inertia from their cybercrime study for lack of correlation. Justifying the measurement of inertia of potential targets in cyberspace is difficult (Nikitkov et al., 2014). Nevertheless, a potential measurement of inertia for a ransomware target is the amount of target data the attacker will maliciously encrypt.

Visibility. Visibility is necessary for target accessibility. The visibility of a target indicates target suitability (Cohen & Felson, 1979; Wang et al., 2015). In an online environment, visibility exists as online activities and behaviors (Jansen & Leukfeldt, 2016; Leukfeldt & Yar, 2016). Visibility depends on knowledge of where the target exists (Wang et al., 2015). The visibility of information assets connected to the Internet indicates potential targets.

Access. Access refers to the accessibility of a target in a physical or virtual realm (Leukfeldt & Yar, 2016). In an online context, digital system weaknesses increase accessibility (Jansen & Leukfeldt, 2016). Ease of access increases target suitability

(Nikitkov et al., 2014; Wang et al., 2015). Therefore, an information asset connected to the Internet features increased accessibility to offenders probing for weaknesses.

Motivated offenders. In the online environment, many motivated offenders exist. The presence of potential offenders in an online environment is enough to satisfy the requirements for motivated offenders in routine activity theory (Näsi et al., 2017). Routine activity theory does not require researchers to understand why motivated offenders choose to offend (Wang et al., 2015). Other frameworks exist to explain why motivated offenders choose to offend beyond just their existence. At the most fundamental level, cybersecurity research involving the Internet meets the existence requirement of the motivated offenders construct.

Competing Theories

Theorists are not bound to routine activity theory to address the multifaceted issues surrounding cybersecurity. Competing victimology theories include a focus on victim behavior to understand how and why crimes occur. In the past, theorists incorporated victim behavior by including routine activity theory with an additional theory or framework.

Examples of competing victimology theories include routine activity theory in combination with another theory. One example included routine activity theory in conjunction with lifestyle theory. In lifestyle theory, researchers take victim behavior into account to build the probability of becoming a victim (Pratt & Turanovic, 2016). Researchers build victim profiles using lifestyle theory to formulate risk (Agustina, 2015). Combining routine activity theory with lifestyle theory extends the ability of the

researcher to consider victim behavior to understand the role of the victim in a criminal event. Cybersecurity theorists can more narrowly define the lifestyle portion of the theory to include behaviors only found in cyberspace.

In the study of victimization occurring in the antispatial realm of cyberspace, victimology theories contain tools researchers can use to account for specific behaviors exhibited by victims that may result in victimization. In cyberroutine activity theory, researchers decide which online behaviors to examine to assist in determining the risk of online victimization in probabilistic terms (Choi & Lee, 2017). An example of an online behavior that increases the likelihood of victimization is remote risky purchasing where the victim conducts an online transaction with a previously unknown online business and becomes a victim of identity theft (Holtfreter, Reisig, Pratt, & Holtfreter, 2015). A commonality among integrated routine activity theories is partial blame attribution to the victim.

Researchers also consider demographics in other competing integrated theories. The measurable variables of gender, race, and social class as a theoretical model in combination with routine activity theory provide researchers with insight into how oppressive factors influence victimization (Blasdell, 2015). Demographic factors are outside the locus of control of participants and provide a measurable variable for research.

Researchers can use an integrated routine activity theory framework to find indicators rather than measurable variables. An integrated routine activity theory using protection motivation theory provides indicators of how victims fail to protect themselves

properly from online victimization (Jansen & Leukfeldt, 2016). In a multiple integrated approach using routine activity theory, negative affectivity, and low self-control theory, lack of victim self-control did not play a role in indicating victimization (Kodellas et al., 2015). Chen et al. (2017) integrated the extended process model, self-control theory, and routine activity theory to determine aspects of individuals who become Internet scam victims and found that individuals who adequately protected themselves mediated the potential of additional online criminological risk. Researchers have demonstrated the use of an integrated self-control and lifestyle-routine activity theory to suggest an effective strategy in preventing cybercrime (Ilievski, 2016). Researchers can combine theoretical frameworks to use different viewpoints, constructs, and indicators to understand cybercrime and suggest preventive measures.

Potential rivals to routine activity theory exist as combined frameworks. Mui and Mailley (2015) were the first researchers to combine routine activity theory with the fraud triangle to research a fraud event. Cressey (1953) developed a primitive version of the fraud triangle to explain the conditions necessary for embezzlement and trust violation to occur. A comprehensive examination of a fraud event is possible when combining the perpetrator-centric focus of the fraud triangle and environment variables of routine activity theory (Mui & Mailley, 2015). Decoupling routine activity theory from the fraud triangle narrows the focus to the perpetrator and diminishes the usefulness of fraud triangle for studying ransomware when access to the perpetrator is limited or nonexistent.

Fraud. Fraud is one component of the broader topic of crime. A perpetrator can commit a crime by force, deceit, or imprudence (Agustina, 2015). In classical criminological research, fraud refers to crime against assets rather than an individual and may require additional thought when investigating the same type of crime in the cyberrealm (Agustina, 2015). It is necessary to understand how the consequences of a crime committed in the cyberrealm intersect with the physical world for classification as fraud (Agustina, 2015). Fraud does not occur only in the physical realm.

The fraud triangle. The fraud triangle contains a competitive model while also remaining useful as a complement to routine activity theory. The three perpetrator-focused components of the fraud triangle in forensic accounting are perceived pressure, opportunity, and rationalization (Omidi, Min, & Omidi, 2017; Reinstein & Taylor, 2017; Roden, Cox, & Kim, 2016; Rodgers, Söderbom, & Guiral, 2015). Perceived pressure involves a financial motivation (Roden et al., 2016). In the financial realm, fences serve as a mechanism to limit opportunity (Reinstein & Taylor, 2017). Reducing perpetrators' cognitive dissonance supports rationalization through perceptions, information, judgment, and decisions (Rodgers et al., 2015). The fraud triangle contains the components necessary to investigate a fraud event within a corporate setting.

Studies in which researchers used the fraud triangle to investigate fraud within the corporate setting are different in approach and findings to studies in which researchers used routine activity theory. At the country level, it is possible to predict the incidence of fraud based on increases or decreases in the service, industrial, and manufacturing share of gross domestic product (Omidi et al., 2017). Researchers have found that to reduce the

chance of fraudulent corporate behavior, it is best to avoid having a chief executive officer and chairman of the board serving in a dual-role capacity (Roden et al., 2016). Similarly, incentive-based compensation strategies and the presence of women and outside directors reduce the likelihood of corporate fraud (Roden et al., 2016). Structured fences in the corporate realm protect accounting professionals from committing fraud and engaging in unethical behavior (Reinstein & Taylor, 2017). An embedded ethical process design tree consisting of perception, information, judgment, and decision inside the fraud triangle provides managers a tool set for placing controls to cope with ethical situations effectively (Rodgers et al., 2015). Investigating ransomware from an ethical standpoint may not be the best way to address the issue of fraud and ransomware; however, fraud is a component of cybersecurity.

To perform a scholarly categorization of cyberfraud within the cyberrealm, I will examine how previous researchers defined fraud within the cybercontext. One type of cyberfraud is online auction fraud (Arntfield, 2015). In 2013, online auctions of automobiles garnered one of the most online auction complaints (Brady et al., 2016). Consumer cyberfraud occurs when an attacker fails to fulfill a purchase made online or misrepresents a product or good (Leukfeldt & Yar, 2016). Online auction deception and cyberfraud decreased as auction cyberfraud controls improved (Nikitkov et al., 2014). Online auction cyberfraud controls and accounting fences are similar in protecting unwilling participants from fraud victimization.

Cyberfraud exists and is perpetrated using methods other than through online auctions. Identity theft victimization is another type of cyberfraud perpetrated online

(Holtfreter et al., 2015). Failing to properly protect privacy leads to increased Internet scam victimization that results in fraud (Chen et al., 2017). Identity cyberfraud occurs when attackers either steal or create a fake identity to commit the fraud with or without the use of malware to intercept victim credentials (Leukfeldt & Yar, 2016). Once an attacker is in possession of the potential victim's identity, it becomes easier to convince or lure the victim into clicking malicious links or downloading malicious payloads.

Cyberfraud beyond online auctions includes other potential victims and victimization risks. The interconnected environment of the Internet puts online retailers and online shoppers at risk of becoming targets for cyberfraud (Brady et al., 2016). Cybervictimization and enhanced risks result from identity cyberfraud and consumer cyberfraud from financial crimes perpetrated by attackers communicating with victims using e-mail, Internet auction sites, or a website (Leukfeldt & Yar, 2016). How victims interact with technology can increase the risk of victimization (Nobles, 2018). Routine behavior of using the Internet for checking e-mail, shopping, and browsing the web is enough to become a victim of cyberfraud.

Attackers attempt regular communications to gather intelligence and further perpetrate cybervictimization. Fraudulent e-mails designed to collect and steal information from recipients is one way perpetrators phish for information to perpetrate victimization (Holtfreter et al., 2015). Attackers conduct phishing scams using *phone calls, e-mails, instant messages,* and *text messages* (Paek & Nalla, 2015). Bank fraud phishing victims give security codes, passwords, or remote access to their personal devices to attackers, regardless of protective measures in place, and inadvertently allow

the transfer of money out of the victims' bank account (Jansen & Leukfeldt, 2016). The act of responding to an attacker might lead to a more serious cybervictimization event with factors that might make a potential victim more susceptible to becoming a target for cyberfraud.

Measures exist to calculate the risk of targets becoming victims and to avoid becoming a victim of cyberfraud. Low self-control leads to a higher risk of online consumer cyberfraud (Ilievski, 2016). A correlation exists between low self-control with a higher frequency of online shopping and becoming a victim of cyberfraud (Chen et al., 2017). One way to determine a potential victims' susceptibility to cyberfraud is by measuring self-control. A lack of self-control might be indicated by those willing to make risky investments; high self-control might be indicated by those with an increased awareness and understanding of Internet privacy (Chen et al., 2017). Fraud within the cyberrealm refers to either consumer cyberfraud or identity cyberfraud as a single facet of an interconnected cybercriminal model, which complicates the measurement of calculated risk.

It is possible to reduce the complications of measuring risk using routine activity theory to limit the effects of victim behavior and remove the need to understand the criminal actor. Routine activity theory is flexible and extensible, and it integrates with other theoretical frameworks. The ability to extend routine activity theory into cyberspace allows researchers to study cybercrime without blaming the victim or without having in-depth knowledge of the criminal actor. A narrow focus on ransomware, which is a crime

occurring in cyberspace, is well-suited for a study that includes the routine activity framework as a theoretical lens of investigative inquiry.

Study of Ransomware

The study of ransomware began as a novel thought experiment that included a proposal regarding the potentially destructive nature of two previously unrelated disciplines. Young and Yung (2017) provided a background of over 20 years of research into cryptovirology and cryptovirology ransomware. Young and Yung initially proved that previously scrutinized and mocked research on cryptovirology was factual based on the initial cooperative efforts between a former hacker and cryptographer, circa 1995, as publicity of ransomware infections grew. Those who lack the understanding of the sophistication, formidability, and nature of ransomware have downplayed the reality of the threat of ransomware (Young & Yung, 2017). A lack of regard to the threat of ransomware creates potential victims of the innovator's dilemma by neglecting the proactivity required in staying ahead of the threats and risks associated with ransomware (Young & Yung, 2017). Successful cybersecurity strategies address the factors that explain why one potential target is more likely to suffer harm and become a victim of ransomware than another.

The mystery of how a malicious payload like ransomware presents itself can pose a challenge to end users of technology. A lack of standardization, the increase in Internet use, the popularity of mobile devices, and the monetization of malware help to explain the growth of ransomware (Fanning, 2015). Increased internet usage was found to have a positive influence on the frequency of ransomware infection (Bergmann, Dreißigacker,

Skarczinski, & Wollinger, 2018). Compounding the ransomware problem are curious individuals with minimal experience who have access to freely available and distributable malware (Fanning, 2015). Once a ransomware infection is successful, it becomes more destructive to attempt its removal than to pay the extortion, which leaves the victim at the mercy of the perpetrator (Young & Yung, 2017). A lack of remedial options against ransomware creates a one-sided relationship where a significant benefit exists in preventing the infection and taking a proactive cybersecurity stance.

Opportunities exist to improve a business's security posture against ransomware while also increasing awareness and improving the reactiveness against new and emerging cybersecurity threats. Small business leaders are uniquely able to adapt to new and emerging cybersecurity threats more efficiently than leaders of larger organizations with more complex information systems (Paulsen, 2016). Small business leaders with a proactive cybersecurity posture make themselves more attractive to customers concerned about cybersecurity (Paulsen, 2016). A lack of awareness and an inadequate cybersecurity posture is more detrimental to small businesses' survivability than larger firms' survivability with regard to how a single breach might bankrupt a small business with limited resources (Fanning, 2015). Given the high stakes involved with small business and the permanently destructive potential of ransomware, an argument in favor of a proactive cybersecurity approach, rather than relying on reactive measures and reporting the crime to law enforcement after the occurrence, is the only solution to circumvent initial loss.

One unique characteristic of ransomware compared to other types of infections is that the attacker demands payment for remediation. When an attacker encrypts files and demands payment, the infection is classified as ransomware (Hampton, Baig, & Zeadally, 2018). The preferred method of payment to decrypt files encrypted by ransomware is through the electronic currency Bitcoin (Brown, 2016). The Bitcoin transaction ledger is freely accessible to all Bitcoin users and allows law enforcement to discover the identity of the responsible party (Brown, 2016). The lack of a central authority and the trustless nature of Bitcoin allow a sender to send Bitcoins to a recipient without disclosing the identity of either party (Ortolani, 2016). Law enforcement must triangulate the pseudonyms visible in the public ledger, also known as the blockchain, with other online records to attempt to identify the attacker (Brown, 2016). The success rate of identifying the criminal actor is questionable and does nothing to mitigate or reverse the damages caused by the ransomware infection.

The complex and public nature of reported ransomware incidents emboldens attackers and creates alarm for potential victims. Gareth (2016) opined that news coverage of ransomware attacks, increased reliance on digital records, and increased sophistication in ransomware increase negative effects from infection. Simms (2016) described how ransomware is capable of residing on systems without detection for extended periods to encrypt system backups to limit victim remediation options. Protecting system backups are important for successfully recovering from a ransomware infection without paying the attacker (Thomas & Galligher, 2018). Mature cryptocurrencies such as Bitcoin further complicate ransomware infection and shield the

identity of the attacker (Gareth, 2016). As publicity of ransomware increases and the underlying technology improves, the damage potential of ransomware becomes more severe.

The scope and destruction of ransomware are traceable. Targeted ransomware attacks have higher damage potential with more substantial ransoms (Federal Bureau of Investigation, 2016). Federal law enforcement reported ransomware infection rates are likely a misrepresentation of the number of actual infections because many infections go unreported (Federal Bureau of Investigation, 2016). Researchers at the Internet Crime Complaint Center collect ransomware complaints and disseminates this information to local, state, federal, and international law enforcement agencies (Internet Crime Complaint Center, 2016). An estimated 15% of Internet crime victims in the United States report their crimes to law enforcement (Internet Crime Complaint Center, 2016). The suggestion that ransomware is underreported indicates a challenge in understanding the extent of damage as a result of ransomware attacks.

Damage from ransomware infection varies by ransomware strain and is not limited to a single technology. The most destructive strain of ransomware is the cryptoviral variant that involves encrypting files and folders to prevent the owner from reading them (Choudhary et al., 2016; Richardson & North, 2017). The less destructive version of ransomware is the locker variant where the information system remains unencrypted but perpetrators place the owner behind a locked screen that prevents access to files on the system (Choudhary et al., 2016). Ransomware has evolved beyond computers and is also capable of infecting mobile phones (Brody, Chang, & Schoenberg,

2018; Choudhary et al., 2016). Ransomware infection is a threat to information systems and other devices with embedded operating systems.

Ransomware and Routine Activity Theory Constructs

The three primary routine activity theory constructs are present in the study of ransomware and business. Themes as applied to ransomware include offenders, targets, target value, target protection, and victim behavior. Of these constructs and themes, offenders who obfuscate their identities might be the most difficult to identify and access in a business environment.

Ransomware offenders. Ransomware offenders are the criminal actors who perpetrate attacks against suitable ransomware targets. Without a motivated ransomware offender, routine activity theory indicates there is no crime. Ransomware offenders can either randomly choose targets or selectively choose targets to victimize.

Ransomware offenders attempt to evade discovery by law enforcement with digital cryptocurrencies such as Bitcoin. Digital cryptocurrency transactions are openly exchanged and recorded in a public ledger (Ortolani, 2016). The public ledger, referenced as a blockchain, exists in a peer-to-peer system to bypass conventional financial institution and government regulations (Ortolani, 2016). Attackers use ransomware to infect information systems and hold the data hostage by demanding payment in exchange for a decryption key (Genç et al., 2017; Kharraz et al., 2015; Young & Yung, 2017). Bitcoin supports automated scripting to facilitate electronic payment transactions (Ortolani, 2016). Attackers can take advantage of the scripting features available in cryptocurrencies like Bitcoin to automate the entire ransomware extortion process.

Ransomware targets. Ransomware targets are the data storage systems of potential victims, and ransomware targets are a necessary element for crime. The online behavior of potential ransomware victims may play a role in target suitability. Ransomware targets consist of potential victims willing to pay extortions to criminal actors.

Ransomware target value. Ransomware target value changes based on selectivity factors and perceived value of the data deprived from victims. If data have no value, then victims may not be willing to pay extortions. Depending on the value of the data on the data storage system, potential victims may implement measures to protect the data prior to a ransomware attack.

Ransomware target protection. Ransomware target protection consists of protecting the underlying data storage system where the data reside. If no ransomware target protection exists, it may decrease the difficulty for a criminal actor to comprise the data storage system. Researchers do not know if privacy protection behaviors are effective in mitigating a potential ransomware attack (Chen et al., 2017). Personal capable guardianship and technical capable guardianship are not significant in cybercrime victimization (Leukfeldt & Yar, 2016). Target protection efforts are no longer viable after ransomware compromises an underlying data storage system.

Theory Comparisons

Researchers routinely conduct qualitative metasynthesis studies to explore routine activity theory to understand cybervictimization. Wang et al. (2015) operationalized routine activity theory with survival modeling to determine that victimization risk is

highest from individuals within an organization. Pratt and Turanovic (2016) found an implied nonprobabilistic view of cybervictimization using routine activity theory. Agustina (2015) researched cybervictimization in Spain to explore victim threat mitigation strategies. Agustina operationalized protection efforts in table form to understand that victimization risk and determined risk controls play a significant role in preventing victimization. Leukfeldt and Yar (2016) compared study participants to determine the applicability of the elements of routine activity theory and victimization risk. Leukfeldt and Yar determined visibility is the most prominently observed element with a significant influence on cybercrime victimization. Leukfeldt and Yar also revealed no clear indication of the applicability of accessibility and personal capable guardianship with value. Leukfeldt and Yar found technical capable guardianship was not significant. Blasdell (2015) applied an intersectional approach using a demographic lens to determine higher victimization risk among marginalized populations. Arntfield (2015) conducted a meta-analysis of victimology studies using a lens of cyberbullying and routine activity theory to theorize how the anonymous nature of cyberspace can facilitate deviant and criminal behavior. Ilievski (2016) referenced 57 research articles, drew six main conclusions about lifestyle routine activity theory, and found a significant link did not exist between protective measures and victimization risk. Ilievski noted large samples support the effectiveness of lifestyle routine activity theory over routine activity theory to explain cybercrime and cybervictimization. Qualitative metasynthesis studies involving routine activity theory share a common theme that includes the utility of routine activity theory and victim risk assessment.

Cybercrime victims are not limited to adults aged 18 and over. Wolfe et al. (2016) conducted a telephone survey with random dialing of 800 nationally representative adolescents aged 12 to 17 and their parents. Wolfe et al. reduced the total number of participants to 625 teenagers with cellphones after applying eligibility criteria and found routine activity theory effective for studying and explaining victimization in the cyberrealm. Näsi et al. (2015) studied cybercrime victimization among young people using a four-country sample of 3,506 teenagers and young adults from the ages of 15 to 30 with slander and threat of violence as the most observed cybervictimization. Näsi et al. further delineated the results by demographics and used logistic regression models to test the previous four-country sample of teenagers and young adults to determine exposure to offenders as a significant predictor of cybercrime victimization. Kalia and Aleem (2017) determined the differences between victims and nonvictims of 200 high school students were target suitability and parental supervision using routine activity theory and cybervictimization. Cybercrime researchers delimit studies using demographics as a differentiator outside the control of participants.

Some researchers pool together participants to delimit victim behavior research and interpret findings. Wick et al. (2017) conducted an online survey using 298 university students enrolled in introductory psychology courses in a southwestern state. Wick et al. used an independent sample *t* test, correlations, and hierarchical multiple regression analysis. Choi and Lee (2017) performed a theoretical analysis of cyberinterpersonal violence victimization and offending using cyberroutine activity theory. Choi and Lee determined participating in risky online leisure activity increased

the likelihood of cyberinterpersonal violence. Reyns et al. (2016) performed a dichotomous codification of responses using self-report survey data to determine that offline guardianship was ineffective when compared to online target hardening. Delimiting research makes it possible for researchers to go outside the bounds of routine activity theory and focus on victim behavior.

Researchers collect data from existing surveys to test constructs of routine activity theory. Reyns (2015) focused on Internet victimization as a construct of routine activity theory using survey data. Reyns measured the constructs of the routine activity framework after operationalizing dichotomous survey response data as victims of hacking and malware or victims of phishing to find that online behavior directly correlated with victimization. Reyns and Henson (2016) combined efforts using the same sample data to study *online identity theft victimization with routine activity theory* and found risky online behavior correlated with an increased chance of identity theft victimization. Researchers can use routine activity theory constructs to determine if victim behavior directly relates to online identity theft.

Behavior and personality are testable within routine activity theory. Vries and Gelder (2015) conducted an investigation using routine activity theory to determine personality as a predictor of crime. Nikitkov et al. (2014) compared routine activity triangle with motivated offender as the element connecting routine activity to the fraud triangle of deceptive eBay seller activity. Holtfreter et al. (2015) explored how low self-control contributes to making risky remote-purchase decisions and subsequently contributes to identity theft victimization. Chen et al. (2017) determined that individuals

willing to participate in risky online investments, participate in online shopping, and open e-mails from untrusted parties increased the likelihood of Internet scam victimization. One trend in routine activity theory research in the online realm is examining victim behavior correlates.

Combining routine activity theory with other theoretical constructs is an effective way to study routine activity theory in different environmental contexts. Mui and Mailley (2015) created a theoretical perspective of one perpetrator misappropriating assets mapped to the crime triangle of routine activity theory, with the fraud triangle as an overlay for an environmental perspective. Kodellas et al. (2015) determined low self-control was not significant in predicting physical or property victimization in the workplace using routine activity theory. Jansen and Leukfeldt (2016) studied phishing and malware victims who were online banking customers in the Netherlands and determined that everyone is susceptible to banking fraud victimization, with target suitability having a slight influence on the likelihood of victimization. Not all researchers have attributed victim behavior to victimization risk.

Archived reports of victimization support testing elements of routine activity theory. Holt et al. (2016) used global computer emergency response team reports of malware infections as total reported accounts of malware infection with macrocorrelates of malware infection at the national level and found that countries with a more advanced technological infrastructure were more likely to report malware infection. Brady et al. (2016) redefined household activity ratio to trend financial cybercrime victimization to demonstrate that those completing financial transactions online were at higher risk of

victimization. Paek and Nalla (2015) lacked data points related to guardianship but found a correlation between victims receiving phishing attempts and identity theft and noted that underreporting may exist because victims may not be aware that they are victims. Regardless of the quality of archived victim reports, it is possible that missing data might prevent an accurate representation of the scope of cybervictimization or victims of ransomware.

Cybersecurity

Effective strategies to address ransomware exist within cybersecurity. Cybersecurity is the strategy organizational leaders use to protect digital assets from harm (Haimes, Horowitz, Guo, Andrijcic, & Bogdanor, 2015). Cybersecurity is relevant from national security interests to local businesses in enabling the long-term success of the digital economy (Teoh & Mahmood, 2017). Retail business cybersecurity target risks include people, data, and intellectual property (Densham, 2015). When discussing cybersecurity, it becomes necessary to define who they are protecting, what they are defending, and how to protect the target; targets exist within the confines of personal information, critical infrastructure, e-commerce, military threats, and intellectual property (Carr, 2016). A motivated offender is the last component needed to fulfill the requirements of routine activity theory as an investigative lens in cybersecurity.

The basis of cybersecurity strategy is the threat of the existence of motivated offenders. Motivated criminal actors use fraud to deceive victims and penetrate vulnerable systems (Gartzke & Lindsay, 2015). Critical business and government functions exist online and are susceptible to attack (Gartzke & Lindsay, 2015). The

ability of cybercriminals to pose a threat from a distance complicates cybersecurity strategy and jurisdiction boundaries (Williams & Levi, 2015). Multiple attack vectors further complicate cybersecurity strategy.

Cybersecurity strategy implications affect how companies conduct business. The importance of the private sector in cybersecurity initiatives dominates the cybersecurity initiative discussion, as business leaders' in the private sector maintain and operate 85–90% of cyberinfrastructure (Štitilis, Pakutinskas, Laurinaitis, & Malinauskaitė-van de Castel, 2017). Cybersecurity strategy and application vary between companies due to a lack of standardization in documenting and applying cybersecurity strategy (Štitilis, Pakutinskas, Kinis, & Malinauskaitė, 2016). Employees with personal devices on the corporate network, customer expectations, and poor communication with upper management weaken cybersecurity (Patel, 2015). Effective cybersecurity strategy requires engaging stakeholders to satisfy operational requirements.

Determining the best method to incorporate cybersecurity into business strategy is challenging. Cybersecurity requirements change based on the value and sensitivity of the data (Goutas, Sutanto, & Aldarbesti, 2016). A significant challenge for business leaders is continually aligning business strategy and technology in unstable environments (Hinkelmann et al., 2016). Lacking a proper cybersecurity strategy is a business formula for inevitable failure (Goutas et al., 2016). Available cybersecurity tools and the methods used in organizations to store and retrieve information are incapable of protecting data and resources from criminal actors (German, 2016). Cybercriminals captured over 600 million U.S. customer financial records from the retail sector in 2013 and 2014, and most

breaches have occurred since 2007 (Hemphill & Longstreet, 2016). A lack of cohesion between cybersecurity and business strategy is detrimental to operations and to maintaining a positive public image.

The depth and scope of a cybersecurity strategy contains specific and measureable characteristics and provides accountability for failure. Characteristics of an effective cybersecurity strategy are multiple perspectives, support from senior staff, behavior and awareness training, internal and external information-sharing alliances, and staying up to date with best practices (Esteves, Ramalho, & Haro, 2017). A weak link in cybersecurity is the employee (Manworren, Letwat, & Daily, 2016). Organizations with vulnerability intelligence of attackable targets have an advantage in mitigating cybersecurity threats (Smyth, 2016). Strategic management of cybersecurity strategy requires the identification of capabilities and resources to increase organizational performance by continually improving and adapting the cybersecurity strategy (Azevedo et al., 2015). Measureable characteristics of cybersecurity strategy include the defining terms and common uses of the term cybersecurity, which encompass a range of semantics with risk, asset, and environment as the most common (Schatz, Bashroush, & Wall, 2017). Designing an effective cybersecurity strategy requires a holistic understanding of an organization.

Applying routine activity theory to cybersecurity strategy requires the identification of available constructs. The available constructs exist within prior research and literature on routine activity theory. The following constructs map directly to routine activity theory.

Cybersecurity offenders. Cybersecurity offenders, similar to ransomware offenders, are the criminal actors who perpetrate attacks against cybertargets. Without a cybersecurity offender, there is no crime (Näsi et al., 2017). Cybersecurity offenders can either randomly choose targets or selectively choose targets to victimize.

Cybersecurity targets. Cybersecurity targets are cybertargets consisting of the information systems or technology of potential victims. Cybersecurity targets are a necessary element for cybercrime (Näsi et al., 2017). Behavior of potential cybersecurity victims may play a role in target suitability. Cybersecurity targets consist of potential victims who lack adequate training or protection.

Cybersecurity target value. Cybersecurity target value changes based on selectivity factors and perceived value of the attack. The influence of the perceived target value remains unknown (Näsi et al., 2017). Depending on the value of the information systems or technology, the potential victim may implement measures to safeguard their systems.

Cybersecurity target protection. Cybersecurity target protection consists of protecting or taking adequate precautions to protect owned information systems or technology. If no target protection exists, it may lessen the difficulty for a criminal actor to compromise the system or technology (Näsi et al., 2017). Whether cybersecurity target protection is effective in mitigating a potential attack remains unknown.

Cybersecurity and ransomware. Similarities exist between cybersecurity and ransomware in their application to routine activity theory; however, the relationship between cybersecurity and ransomware is distinct and does not share all qualities equally.

Ransomware is a component of cybersecurity, and researchers expect to observe shared qualities between spatial and antispatial routine activity research (Näsi et al., 2017). In the context of business and effective business strategy, additional implications to adequate protection may exist.

Strategic Management and Ransomware Cybersecurity

The strategic management of information systems and technology has a role in the adequate protection and guardianship constructs of routine activity theory. Companies have a global market of cybersecurity networks to assist in strategically managing cybersecurity (Bailetti & Zijdemans, 2014). Cybersecurity start-up companies offer holistic security solutions, digital identity protection, security automation, distributed security, integration services, password products, security simulation and testing, and training (Bailetti & Zijdemans, 2014). Strategic risk management plans contain provisions for unexpected technology failures (Fraser & Simkins, 2016). Strategically managing costs associated with cybersecurity includes properly classifying costs related to testing versus implementation of cybersecurity tools and strategies (Radziwill & Benton, 2017). Strategically managing cybersecurity requires establishing a budget to protect digital company assets from cybercriminals.

The strategic management of cybersecurity is critical in connected company information systems and technology. Over the past 10 years of strategic management of cybersecurity, cybersecurity failures have cost companies billions of dollars (Hooper & McKissack, 2016). The strategic management of cybersecurity includes electronic information security management systems and proactively monitoring the influence of

cybersecurity programs on the performance and productivity of the workforce (Baronienė & Žirgutis, 2017). The practice of strategic risk management leads to resiliency within company operations (Fraser & Simkins, 2016). In large organizations, a separate position outside the IT department oversees cybersecurity; however, in smaller organizations typically the corporate information officer handles the strategic management of cybersecurity (Hooper & McKissack, 2016). Small business owners use cloud technologies to stay competitive (Forde, 2017). Business leaders responsible for overseeing cybersecurity handle the strategic management of cybersecurity and internal structure with different internal and external controls depending on the size and structure of the organization (Hooper & McKissack, 2016). The tenets of strategic cybersecurity management align with routine activity theory in networked company information systems.

Ransomware and Business

The threat of ransomware is high, with devastating consequences in the event of a successful breach to business information systems. Attackers using cryptovirology are responsible for hundreds of millions of dollars in losses annually, and they continue to evolve ransomware technology to circumvent systems designed to protect information systems while eluding law enforcement with cryptocurrency payouts anonymized in the blockchain (Richardson & North, 2017). The success of the cryptovirology criminal enterprise indicates a failure in preventing successful attacks. The routine activity theory framework as applied to the study appears in Figure 1.

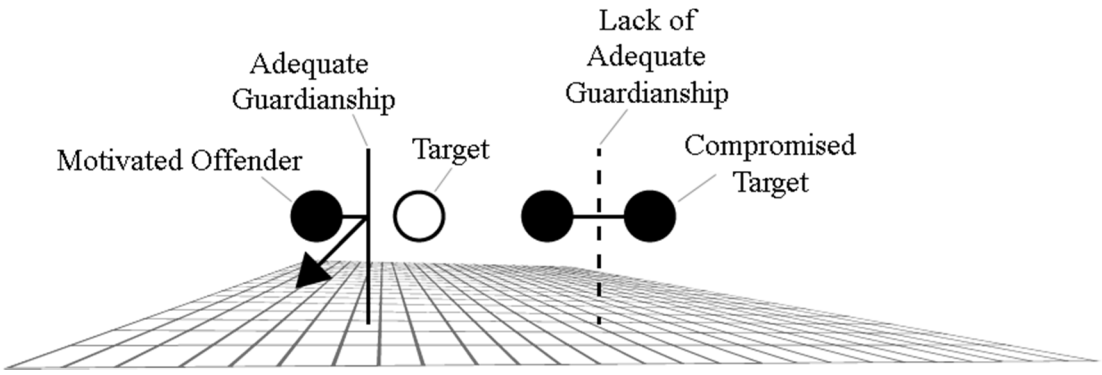

Figure 1. Routine activity theory as applied to the study of ransomware.

Figure 1 depicts the elements necessary for ransomware offenders to circumvent protection, a lack of adequate guardianship, and subsequent compromise of the target information system. The element of adequate guardianship is a primary focus for research involving cybersecurity threats and routine activity theory. A lack of innovation in maintaining adequate protection against ransomware creates opportunity for offenders to extort their victims (Richardson & North, 2017; Young & Yung, 2017). The lack of adequate guardianship or protection against ransomware infection is relevant, within the confines of routine activity theory, if a motivated offender and target exist.

Small business leaders use specific strategies to provide adequate guardianship, limit target visibility, and prevent motivated offenders from compromising the target. Some small business leaders lack strategies to address ransomware and assume adequate cybersecurity protection is in place. The codification of small business leader cybersecurity strategies as active or passive is relevant to the study of cybersecurity strategy. Within the confines of active or passive cybersecurity strategy, unique elements might exist in addressing ransomware infection that apply to other attack vectors outside the scope of ransomware.

Predicting the thematic development and codification of the effective strategies small business leaders use to address ransomware involves bounding relevant data. In case study research, bounding the data and operationalizing conceptual measures improve quality (Yin, 2018). Exploring small business leaders' strategies for effectively addressing ransomware using the routine activity theory construct of adequate guardianship might reveal direct and indirect influential factors that affect the effectiveness of cybersecurity strategy. Identifying how small business leaders influence the organizational cybersecurity posture might lead to a rich understanding of how small business leaders directly and indirectly mitigate the threat of ransomware in small business information systems.

The evolution of ransomware creates a moving target for small business leaders concerned with maintaining adequate protection for their information systems. Adequate protection entails using the latest operating systems, staying up-to-date on operating system patches, maintaining on-site and off-site backups, and actively monitoring vulnerable operating system components with antimalware software (Choudhary et al., 2016; Richardson & North, 2017). The latest Microsoft operating system, Windows 10, was effective in preventing ransomware infection in laboratory tests using variants from the 25 known families of ransomware (Choudhary et al., 2016). The majority of ransomware infections originate from unsuspecting users clicking on infected links or opening infected attachments in e-mail (Richardson & North, 2017). Strategies that may influence the use of e-mail, data backups, using the latest operating systems, and promoting the use of antivirus or antimalware protection in the organization are

potentially significant to studying ransomware infection in small business information systems.

Operationalizing Routine Activity Theory Constructs

Operationalizing the constructs of routine activity theory in the context of small business information systems and ransomware will allow for the clear identification of relevant data and themes encountered during codification of the research data. Proper identification of contextual constructs benefits analysis (Yin, 2018). The contextual constructs of routine activity theory include motivated offenders, targets, and adequate guardianship.

Motivated offenders. Research data might contain information about small business leaders understanding the inherent risks involved in using information systems, the Internet, and the presence of motivated offenders. Knowledge of why motivated offenders choose to behave in a criminal manner is not a prerequisite of routine activity theory (Wang et al., 2015). Information systems exposed to the Internet inherit a precursory qualification of inclusion in the motivated offender construct (Näsi et al., 2017). A lack of a priori knowledge of motivated offenders does not predicate the presence or absence of motivated offenders targeting small business information systems; however, the common utility of small business information systems connected to the Internet justifies the assumption of the existence of motivated offenders threatening the cyberenvironment.

Targets. Understanding the components of a small business information system targeted by motivated offenders allows for proper identification of the prerequisites

required for adequate protection. Unpatched or outdated operating systems are vulnerable targets to ransomware infections (Choudhary et al., 2016; Richardson & North, 2017). The importance of maintaining up-to-date infrastructure is evident in avoiding the transformation of a target into a compromised target. A focus on the types of operating systems in use at a small business will provide data to determine target risk and factors of adequate guardianship for data existing on the small business information system.

Targets exhibit certain behaviors that may increase target viability and subsequently increase victimization risk. The act of having information systems connected to the Internet or the use of information systems in general is enough to satisfy the requirement of a target when using routine activity theory. The original precepts of routine activity theory do not indicate an influence on victimization based on the difference between someone leaving the home, and someone leaving the home and engaging in risky behavior (Pratt & Turanovic, 2016). The ease of establishing a proper definition of a suitable target in cyberspace does not mitigate the problematic antispatial nature of the cyberrealm (Leukfeldt & Yar, 2016). However, operationalizing victim behavior is useful in determining risk for victimization among computer users (Holtfreter et al., 2015). The problematic nature of examining a target in the antispatial realm increases the usefulness of operationalizing victim behavior in determining victimization risk.

VIVA. VIVA contains attributes to categorize target victimization risk. The attributes of the VIVA proposition are value, inertia, visibility, and access relevant in the operationalization of constructs of accessible targets (Nikitkov et al., 2014). If the

primary focus is on adequate guardianship of accessible targets; opportunity exists to explore possible correlates of VIVA with adequate guardianship. An example of potential correlates in a small business environment might consist of company documents indicating value, number of employees indicating inertia, online web presence indicating visibility, and information system security posture combined with system architectures to indicate access.

Relative VIVA attributes are identifiable based on the context of the study environment. Not all data stored on a small business information system share the same amount of value. To calculate value, data must have monetary worth in the spatial realm (Wang et al., 2015). Determining the monetary value of small business information data is not a requirement for establishing target suitability. The number of employees may have an influence on inertia, as a small business with more employees may have fewer employees using computers and generating data; however, a small business with more employees has potentially more human resource data than a small business with fewer employees, which is a possible interesting difference. Difficulty exists in measuring and quantifying inertia in the cybercontext (Jansen & Leukfeldt, 2016; Leukfeldt & Yar, 2016). Visibility, however, is a precursor to understanding target suitability. A potential cyberattacker might discover a suitable target based on evidence of the potential victims' online footprint and location (Jansen & Leukfeldt, 2016; Leukfeldt & Yar, 2016; Wang et al., 2015). Lack of adequate guardianship predisposes visible targets to increased victimization risk (Jansen & Leukfeldt, 2016; Nikitkov et al., 2014; Wang et al., 2015). In the cybercontext, not all VIVA attributes share the same applicability.

Adequate guardianship. Within the context of the study, target protection is analogous to adequate guardianship. Adequate guardianship against Internet-based attacks routinely takes the form of sophisticated firewalls, encryption, installing and updating protection software, and educating users of risks associated with e-mail (Holtfreter et al., 2015). Active target protection must satisfy the requirements necessary to prevent ransomware infection. Continual monitoring for changes in the file system and registry is one prerequisite for adequate active target protection against ransomware infection (Choudhary et al., 2016). The role of passive target protection is similar but identified differently from active target protection. Small business leaders' support for maintaining up-to-date infrastructure, budget allocation to information systems, and cybersecurity concern or lack thereof are examples of possible evidence of passive target protection. Adequate guardianship justification contains both active and passive elements.

Thematic development. Observed themes in routine activity theory include passive and active components mapped to the theory constructs of motivated offenders, suitable targets, and lack of adequate guardianship. Active component constructs might consist of the presence of publicly identifiable information about the business, public listing of e-mail addresses, internal security software features, and proactive target hardening initiatives. Passive component constructs might consist of data collected during an interview process directly from the interview participant. It is then important to identify and segregate any thematic development from outside bounded research to provide additional context for rival explanations.

Rivals. For rival explanations, researchers can remain within the constructs of routine activity theory to posit that motivated offenders or suitable targets might provide a better explanation of why a target becomes compromised than adequate protection. It is possible an overlap exists between suitable target and adequate protection; discerning between adequate protection with target hardening and the existence of a target is necessary to avoid improper attribution. A possible rival explanation not contained in routine activity theory is that the victim is at fault. Considering the totality of circumstances surrounding ransomware, it is possible to avoid victim blaming and instead choose a victim empowerment perspective using adequate guardianship and remain within the bounds of routine activity theory. The fraud triangle is another possible rival to confirm or refute rival suitability. Identifying and exploring possible rivals is a necessary component of exemplary qualitative case study research (Yin, 2018). The goal of a researcher conducting exemplary qualitative case study research is not to favor the predicted outcome by collecting only the data necessary to confirm predicted outcomes or to consider all possible rivals. The objective of the researcher is to collect and analyze data without bias to achieve quality, rigor, and trustworthy conclusions.

The motivated offender construct is difficult to extrapolate in the context of strategies to address ransomware. An unlimited number of motivated offenders exist on the Internet as people and automated algorithms that participate in random and targeted criminal acts toward individuals or organizations (Brady et al., 2016; Chen et al., 2017; Holtfreter et al., 2015; Näsi et al., 2017). Identifying the presence of a motivated offender

without understanding the inclination toward criminal behavior weakens the rival explanatory position in explaining strategies to address ransomware.

The suitable target construct is likewise difficult to generalize in addressing ransomware. The definition of a suitable target is satisfied after a person or device connects or interacts with the Internet (Jansen & Leukfeldt, 2016; Leukfeldt & Yar, 2016). The only viable strategy in a suitable target perspective is to avoid the online environment. Completely avoiding the online environment is not within the context of realistic expectations for small businesses with a reliance on the Internet infrastructure.

Blaming the victim is unfavorable due to the possibility of double victimization. Researchers consider victim behavior in probabilistic terms when combining routine activity theory and lifestyle theory (Pratt & Turanovic, 2016). Risky behaviors place suitable targets on the Internet at an increased risk of victimization (Holtfreter et al., 2015). Researchers consider and evaluate demographics of suitable targets to determine online victimization risk (Blasdell, 2015). In routine activity theory, it is possible to remove the potential of double victimization with victim blaming because acknowledging victim behavior is not a requirement.

Regardless of behavior or demographic variables, successfully deceived targets become victims. One component of the fraud triangle is opportunity (Omidi et al., 2017; Reinstein & Taylor, 2017; Roden et al., 2016; Rodgers et al., 2015). Deception creates opportunity for criminal actors and is a precursor to fraud (Agustina, 2015). Suitable targets deceived into clicking an infected link or opening an infected attachment from a

phishing scam become victims; however, without access to criminal actors, it is difficult to investigate the remaining components of the fraud triangle.

Adequate guardianship or the lack thereof remains as the final construct in routine activity theory in the cyberrealm. Adequate guardianship as a construct within the cyberrealm defines adequate protection in the form of security hardware, protection software, or end-user knowledge (Holtfreter et al., 2015). A lack of adequate protection and a lack of training and education for end users is a likely candidate for addressing ransomware with capable guardianship from the perspective of small business leaders. The gap in existing literature on adequate or capable guardianship, small business, and ransomware is apparent.

Summary

The routine activity theory may help small business leaders to develop effective strategies to address ransomware. Examples in the literature contain evidence of a lack of end-user training, failure of adequate guardianship, and an increase in target suitability. Overcoming the challenges of preventing a ransomware infection and minimizing damage from ransomware is possible with the proper strategy. End-user training to address ransomware is a potential strategy to strengthen adequate guardianship and reducing target suitability. Routine activity theory contains constructs to investigate effective strategies small business leaders' use to address ransomware.

Transition

In Section 1, I supplied an account of the proposed study, the background of the problem, and a review of the literature associated with the research question. I outlined

the need for small business leaders to stay informed and knowledgeable to counter the escalating and evolving cybersecurity threat of ransomware to small business information systems and supporting technologies. I indicated how I investigated how small business leaders effectively address ransomware and if small business leader strategy aligns with the routine activity theory construct of adequate guardianship. I attempted to frame the research question within the conceptual framework and explored possible rival explanations.

In Section 2, I outline the role of the researcher and justify my research decisions. As an example, I provide the rationale for inclusion criteria for participation. I then include the methodology of my research design prior to the collection of data. I explain how I conduct a multiple-case study to include leaders from multiple small businesses. I also discuss and provide the rationale for ethical research considerations, data organization and analysis, collection techniques, and the way I achieved trustworthiness with dependability, credibility, confirmability, and transferability.

In Section 3, I present my findings, explain the application to professional practice, and offer recommendations. I use my predictions to compare against observed themes and cross-case analysis. The discussion in Section 3 includes the applicability of findings to routine activity theory. I include suggestions for positive social change, application to small business practice, and recommendations for future research. Finally, I provide a summary and reflection regarding effective strategies small business leaders use to address ransomware.

Section 2: The Project

In Section 2, I focus on how I intend to construct a high-quality qualitative case study. I discuss my role as a researcher, the participants, and the research method and design. Section 2 includes ethical research considerations and the methods of data collection, organization, and analysis. This section includes an explanation of how I ensured the reliability and validity of my study.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the cybersecurity strategies some small business leaders use to protect their information systems from ransomware. The targeted population included five small business leaders located in the Knox County region of Tennessee who have successfully implemented cybersecurity strategies to protect their information systems from ransomware. The study's implications for positive social change includes the potential for increasing employment opportunities in the region and supporting the local economy by protecting information systems from ransomware. Furthermore, small business leaders may realize the value of their business as a cybercrime target and consider implementing stronger cybersecurity controls to prevent and mitigate the spread of ransomware to protect confidential and sensitive consumer information.

Role of the Researcher

I served as the primary data collection instrument to provide the depth of inquiry possible in postmodern qualitative case study research. Qualitative inquiry allows researchers to stand in opposition to the scientifically based research movement and go

beyond institutionalized truths (Denzin, 2016). In qualitative case study research, the researcher's responsibility is to collect data from multiple sources to form convergent lines of inquiry through interviews, evidence chains, informant review, and existing records (Yin, 2018). I performed this qualitative case study research of ransomware and small business using skills gained through academia and working in the technology field since 1993. I have experience as a small business owner, employee, and contractor for local business, have worked with more than 20 Fortune 500 companies, local government, and the U.S. Department of Defense during my time working in the technology field. I did not include participants from former or current business clientele. As the primary data collection instrument, I also took into consideration ethical concerns applicable to my study.

I adhered to principles contained in the *Belmont Report* to ensure I maintained acceptable research ethics when working with human subjects. Internal criticisms of ethical models designed from the *Belmont Report* to promote principles of respect, beneficence, and justice in research involving human subjects indicate the common law as most beneficial to biomedical research and discourages artificially risky qualitative research (Denzin, 2016). Researchers use the principals identified in the *Belmont Report* to undertake ethical research and protect study participants (Goss, 2017; Miracle, 2016; National Commission for the Protection of Human Subjects in Biomedical and Behavioral Research, 1979). I did not consider my research inherently risky, nor receive any direct benefit, and I obtained informed consent and followed the *Belmont Report*

protocol to ensure the highest ethical standards of protecting the respect, beneficence, and justice of participants of my study.

A risk for personal bias exists based on my extensive background in information technology and small business, as I may have had a preconceived idea of what small business leaders should be doing to address ransomware in their organization. My personal bias required keeping an open mind and maintaining personal diligence to avoid misinterpreting data from a personally biased position. Identifying researcher bias preserves transparency in qualitative research (Marshall & Rossman, 2016; Yin, 2018). Using multiple sources of data reduces selectivity bias (Marshall & Rossman, 2016; Snow, Richards, & Kinner, 2017; Yin, 2018). Bracketing, member checking, and bounding the case also reduces bias (Marshall & Rossman, 2016; Morse, 2015; Pacho, 2014; Yin, 2018). A successful member checking strategy includes asking for clarification and comparative meaning from previous interviews with the current participant (Yin, 2018). I bracketed my research, used multiple data sources, bound my case study, and distanced mental conclusions during data collection to mitigate bias and to purposefully view the data through the conceptual framework of routine activity theory. I followed an interview protocol (see Appendix). Researchers routinely follow a strict interview protocol to maintain quality in qualitative case study research (Baškarada, 2014; Noble & Smith, 2015; Yin, 2018). I followed a strict interview protocol, obtained consent, performed member checking, and accomplished data saturation during data collection to maintain quality.

Participants

I established eligibility criteria for the participation of small business leaders on those who have successfully implemented cybersecurity strategies to protect their information systems from ransomware to answer my research question. The U.S. Census Bureau (2018) defines businesses with fewer than 500 full-time employees as a small business. The U.S. Small Business Administration in combination with U.S. Census Bureau data classifies over 97% of all businesses in the United States as small businesses (Congressional Research Service, 2018). The Australian Bureau of Statistics (2018) defines a small business as one with fewer than 20 employees and independently owned and operated. I used the Australian Bureau of Statistics criteria to narrow the U.S. Census Bureau definition of small business for participant eligibility to independent owners of small businesses with fewer than 20 employees located in the Knox County region of Tennessee who have successfully implemented cybersecurity strategies to protect their information systems from ransomware.

I located potential candidates through the small business resource directory at the public library. I determined cursory access to the site, small business ownership, and the sine qua non of technology in use at the businesses. Researchers in business and management with flexible research techniques can overcome the challenges inherent with securing access to participants (Lord, Bolton, Fleming, & Anderson, 2016). Researchers use cold calling, e-mail, and letters and share potential benefits of the study to secure access (Fjellström & Guttormsen, 2016). I solicited participation from publicly available sources and explained the purpose of my study with phone calls, via e-mail, or in person

with a courtesy introduction via e-mail or letter, and then met with the potential participants at a time of their choosing.

I established a working relationship with each participant by introducing myself to the business owner, explaining my research study, and describing the data collection process. Relationships between researcher and participant are social and vary based on each participant (Yin, 2016). I explained the potential benefit of my research to small business leader participants. Clear communication of necessary agreements facilitates a healthy working relationship and strengthens data collection efforts (Miles, Huberman, & Saldaña, 2014). After a formal acknowledgment of interest in participating in the study, I confirmed eligibility, collected informed consent, and let the participant choose a physical venue or telephone option at a mutually convenient date and time. Interviewers must maintain a flexible schedule and be willing to meet at participants' chosen place and time (Yin, 2014). In the event that the scheduled time or place was not convenient for me, I adjusted my schedule to accommodate the needs of the participant.

Research Method and Design

I chose a qualitative method after considering quantitative and mixed methods. I selected a multiple case study design within the qualitative method to study effective small business leader strategy for addressing ransomware. The context for my research was multiple small businesses and the unit of analysis was the leader of the respective small businesses. The multiple case study design provided a research design appropriate for interviewing multiple small business owners who have an effective strategy for addressing ransomware.

Research Method

I use a qualitative research method for this study. Qualitative research is the study of a social phenomenon, in context, to gain a rich understanding from participants (Marshall & Rossman, 2016). Holistic, complex, or interpretive research occurring in the natural world is characteristic of the qualitative method (Marshall & Rossman, 2016). Alternatives to the qualitative method include quantitative and mixed-methods. In quantitative research, the researcher collects data in the form of numbers and statistics and tests a hypothesis (McCusker & Gunaydin, 2015). I was not testing a hypothesis; rather, I was exploring what effective strategies small business leaders use and how they overcame related challenges in addressing ransomware.

I did not use the quantitative method, as I did not intend to test a hypothesis. Researchers use mixed-methods design to combine qualitative and quantitative methodologies and to test variables (Halcomb & Hickman, 2015). A mixed-methods approach was inappropriate because I did not intend to collect numbers or statistical data and test a hypothesis in combination with qualitative data to explore the research question and perform variable comparisons.

I used the qualitative method to explore context in the natural world to answer a research question. The vehicle for this exploration was semistructured interviews, which facilitate an in-depth exploration of the topic. Researchers who conduct semistructured interviews go beyond the quantitative resemblance of structured interviewing to overcome the lack of clear direction with unstructured interviewing techniques (Wilson, 2016). Qualitative interviewing techniques allow researchers to obtain rich data from

participants not otherwise available with other methods (Lancaster, 2017; McVey, Lees, & Nolan, 2016). Qualitative methods aligned with my objective to gain a rich understanding of what strategies small business leaders use to address ransomware and provide access to data otherwise unavailable with other methods.

Research Design

I chose a qualitative multiple case study research design after considering case study, phenomenology, and narrative research designs. A qualitative case study research design is appropriate for a deep exploration of a phenomenon in a business context (Achtenhagen, Brunninge, & Melin, 2017; Arasti, Khaleghi, & Noori, 2017; Jarvis & Williams, 2017). Researchers use case study research for flexibility in forming a holistic perspective of what is shared and unique about the case (Hyett, Kenny, & Dickson-Swift, 2014). Researchers use cross-case analysis to explore individual cases holistically within multiple contexts as a way to create a replicable study (Yin, 2018). A case study design is appropriate when the researcher intends to understand the viewpoint of participants (Baškarada, 2014). I used interview questions aligned with my research question to explore the sophisticated phenomenon of effective strategies small business leaders use to address ransomware.

In phenomenology research, researchers attempt to understand cognition and expectations (Fawcett, Fawcett, Cooper, & Daynes, 2014). I was not attempting to explore expectations of participants; therefore, the phenomenology research design was inappropriate. Researchers use narrative research to explore the experience of unique populations (McCann & Brown, 2017). I was not seeking to explore the experience of

small business leaders, but rather, their strategies to address ransomware in their small business.

Researchers have used case study research to indicate the importance of leadership skills in the business sector (Creţu & Iova, 2015). Data gathered from interviews with small business leaders in this multiple case study research may indicate effective strategies small business leaders use to address ransomware. Researchers have also used a qualitative case study research design for investigating ransomware (Ali, 2017; Pascariu, Barbu, & Bacivarov, 2017; Patyal, Sampalli, Qiang, & Rahman, 2017). I conducted semistructured interviews to gain a rich understanding of the phenomenon in a bounded replication multiple case study design. Design replication in case study research occurs during the purposeful selection of cases to include during the design stage (Yin, 2018). I facilitated replication by limiting case selection to the small business sector.

Data saturation in qualitative case study research design indicates quality and rigor. Data, themes, coding, and replication are universal elements in defining data saturation (Fusch & Ness, 2015). Data saturation occurs once shared commonalities among interview participants cease (Constantinou, Georgiou, & Perdikogianni, 2017) and when no gain of new information is possible (Fusch & Ness, 2015; Marshall & Rossman, 2016; Yin, 2018). I analyzed data collected from interview responses and company documents, identified all possible themes, and remained open to expanding my participant pool if needed until I achieved data saturation.

Population and Sampling

The population for this study consisted of five independent small business owners with fewer than 20 employees located in the Knox County region of East Tennessee who use information systems in their organization and have applied strategies to avoid ransomware. I was interested in achieving a depth of understanding only possible with a small number of participants. In-depth qualitative research with information-rich participants justifies a small number of informants (Boddy, 2016; Malterud, Siersma, & Guassora, 2016; Van Rijnsoever, 2017). A purposive sampling method supports selection criteria based on the data collection strategy (Roy, Zvonkovic, Goldberg, Sharp, & LaRossa, 2015). A maximal information strategy is appropriate for purposive sampling when researchers are highly familiar with the field and population (Van Rijnsoever, 2017). Purposive sampling is appropriate when using selection criteria to target a specific population (Asiamah, Mensah, & Oteng-Abayie, 2017; Roy, & Basu, 2015). Establishing trust and using a gatekeeper to coordinate the researcher with a participant is effective in overcoming the challenges inherent with interviewing difficult-to-reach populations (Kasim & Al-Gahuri, 2015). I used purposive sampling to choose independent small business owners within the Knox County region of East Tennessee who use information systems in their businesses.

I achieved data saturation through member checking and triangulation with purposive sampling, maximal information, and bounded case design. Data saturation is possible with only a single informant within in-depth qualitative research (Boddy, 2016). Data saturation is unique to each study, dictated by study design, and possible once no

new themes or explanations for data exist (Fusch & Ness, 2015; Miles et al., 2014; Morse, 2015). I conducted interviews with a minimum of five participants to achieve data saturation.

Ethical Research

I maintained and adhered to ethical standards required by the Institutional Review Board (IRB) at Walden University. Approval by the IRB is essential in scholarly qualitative research, and researchers should disclose values or conflicts of interest (Denzin, 2016). I followed all requirements of IRB and disclosed values and conflict of interest to ensure compliance with ethical research. Ethical research considerations exist at the outset, during, and after the conclusion of research (Drake, 2014). The Walden University IRB approval number for this study is 05-02-19-0612293. I received consent from participants, provided participant withdrawal procedures, and took necessary precautions to protect participants and data before, during, and after the completion of the study.

Informed consent is part of a process to allow participants to understand a study before deciding whether to take part. Participants received adequate time to review, understand, and sign an emailed, mailed, or hand delivered informed consent letter prior to inclusion in the study. Informed consent protects the participant, researcher, and institution from potential harm arising from participation in research (Byerley et al., 2017; Petrovic, 2017). Complex certificates of confidentiality lower participant trust, while simple and accurate language increases trust and participation (Beskow, Check, & Ammarell, 2014). A significant risk in research is that participants will not dedicate

enough time to reading consent forms to ensure proper understanding and instead will perform only a cursory read before signing (Knepp, 2014). An IRB may work with researchers to customize consent form language appropriate to a study (Check, Wolf, Dame, & Beskow, 2014). I ensured participants were aware of what they were consenting to and that consent was for the entire scope and duration of the study.

Participants could withdraw from the study at any time. I allowed participants to make their request to withdraw from the study at any time before or during the study by phone call, by text message, in person, or by e-mail. An informed consent form containing clear instructions of what happens if a participant withdraws supports a researcher's action and decision to use partial data (Thorpe, 2014). Participants did not suffer any penalties for withdrawing at any time before or during the study, and I discarded any research from participants who withdrew from the study.

I used pseudonyms with the naming convention of P1, P2, P3, P4, and P5 to protect the identity of participants and stored all research data on an encrypted and password-protected USB storage device. I outlined my responsibilities in protecting the collected research data while seeking informed consent. The researcher's responsibility is to avoid divulging demographics or other identifying characteristics that may violate participant confidentiality (Morse & Coulehan, 2015). I did not consider demographic constructs and did not disclose demographic markers of participants beyond the general region of the location of the study. Data stored on encrypted and password-protected USB storage will be stored for 5 years in a biometric safe located in my home office. I

use pseudonyms and will destroy all research data after 5 years to protect participant confidentiality.

Data Collection Instruments

I was the data collection instrument for the study. I conducted semistructured interviews, examined company documents, followed an interview protocol (see Appendix), and performed member checking. I used open-ended semistructured interviews to gather data on effective strategies to address ransomware in small business. Interviews are one way to gather a large amount of data from participants on problems that are technical in nature (Marshall & Rossman, 2016). Some researchers use an interview protocol to conduct semistructured interviews (Cohen & Kassan, 2018; Mao & Bottorff, 2017; Sollie, Kop, & Euwema, 2017). In a semistructured interview, the interviewer has the flexibility to prompt for additional information as interesting information emerges from questions contained in the interview protocol (Baškarada, 2014). Member checking enhances the interview protocol to determine if what the interviewer understands and what the participant means is correct (Yin, 2018). I attempted to enhance the reliability and validity of the study using an interview protocol and member checking process. Member checking occurs during the initial interview and after data analysis is complete (Yin, 2018). I conducted interviews and performed immediate member checking during the initial interview with the participant and executed a later member check by contacting participants by telephone or email after data analysis.

I requested copies of company documents showing the types of information systems in use at the small business, information security training programs, and information security software and hardware. Company documents contain contextual information used for validating and triangulating data (Marshall & Rossman, 2016). Company documents for this case included purchase receipts, training documentation, and an inventory of operating systems, security software, and security devices. Security in the form of antivirus software might contain provisions to prevent a ransomware infection (Patyal et al., 2017). Beyond antivirus software, end-user behavior also has a significant role in preventing ransomware infection (Ali, 2017). Documents that might reveal company choice of operating systems, antivirus software, and training that affects end user behavior are important to understanding effective strategies used to address ransomware. I collected documents necessary to form a holistic view of the state of the information systems in use at the companies and to corroborate interview findings.

Data Collection Technique

I explored effective strategies to address ransomware by conducting interviews, reviewing archival records, and gathering company documents. A sense of trust between the interviewee and the interviewer, facilitated when the interviewer receives a referral to the interviewee from someone else, improves the sharing of data in semistructured interviews (Nguyen, 2015). To achieve an intimate understanding of a phenomenon and to capture interviewees' viewpoint requires a balance of neutral and embodied inquiry (Alby & Fatigante, 2014). In a semistructured interview, the interviewer can expand the inquiry as information emerges to develop a better understanding of the interviewees'

viewpoint (Baškarada, 2014). Disadvantages of using interviews as a data collection technique include the possibility of misunderstanding interviewees' responses and the influence of bias from interviewer or interviewee in interpreting responses or providing responses to interview questions (Baškarada, 2014). However, I mitigated these disadvantages by identifying my biases, verifying interviewee responses, and conducting as many follow-up member checking sessions as necessary to ensure I captured the interviewees' viewpoint.

I conducted member checking to enhance the reliability and validity of data collection. Member checking occurs when the researcher builds trust in the results by reviewing analyzed interview data from a participant interview with the participant to verify, modify, and confirm the analysis (Birt, Scott, Cavers, Campbell, & Walter, 2016). Member checking can increase the rigor of information systems research involving participants and in deriving if participant meanings from interview questions align with researcher interpretations (Iivari, 2018). A researcher can confirm and validate with member checking by providing a summary of the interview to the interviewee (Marshall & Rossman, 2016). I engaged in member checking during and after each interview with the participant to increase my depth of understanding of participant meaning to the interview question responses.

I digitally recorded the interviews. Researchers can digitally record interviews and transcribe interviews verbatim (Fernandez, Sheppard-Law, Curtis, Bancroft, & Smith, 2018; Kohn, Belza, Petrescu-Prahova, & Miyawaki, 2016; Porteous & Machin,

2018). After digitally recording the interview, I transferred the digital recording to a computer with an encrypted hard drive and transcribed the interview verbatim.

I kept a reflective journal during the study. Researchers can use reflective journaling during the data collection phase of research to increase awareness and improve research quality (Digby, Lee, & Williams, 2016; Perlman et al., 2018; Zulfikar & Mujibur, 2018). I used a composition book to handwrite reflective journal entries during and after the interview. I digitized my reflective journal and stored it with the transcribed interview on an encrypted hard drive.

I requested company documents and archival records. Researchers can use semistructured interviews and company documents to corroborate and triangulate data (Jussani, Wright, & Ibusuki, 2017; Kaminska & Borzillo, 2017; Ye & Lau, 2018). One disadvantage to archival records is they can be challenging to search and may be incomplete (Jones & O'Neill, 2014). However, diligently searching through data from archival research can lead to new meaning and hidden truths (Norquay, 2017). I requested copies of company documents and archival records showing the types of information systems in use at the small business, information security training programs, and information security software and hardware.

Data Organization Technique

I used a purposeful and methodical approach to organize my data. I temporarily stored all collected data on an encrypted hard drive in a research folder with separate codified folders for each participant. I maintained a backup copy of the research folder on an encrypted and password-protected USB drive. I used a digital recorder to record the

interviews and then transfer the recordings to a computer with a password protected and encrypted hard drive. I transcribed the interviews into a Microsoft Word document for data analysis and to back up the original audio files; I transcribed my reflective journal into multiple Word documents and stored the file inside the respective coded participant folder. Next, I organized and digitally stored the company documents that I collected inside the coded participant folder. I used Microsoft Excel, Microsoft Access, QSR NVivo, and Microsoft Azure SQL to organize the collected data for further analysis. Researchers have used QSR NVivo, spreadsheets, and databases to collect, store, codify, and analyze research data (Cook, LaVan, & Zilic, 2018; Hunt & Bakker, 2018; Woods, Paulus, Atkins, & Macklin, 2016). After I completed the data analysis, I made a final backup of the contents of the research folder onto two encrypted and password-protected USB drives. I stored the USB drives in a biometric-protected safe, to which only I had access, in my home office for at least 5 years. I will have erased the contents of the USB drives after the mandatory 5-year retention period.

Data Analysis

I followed a reiterative process of analyzing collected data. Qualitative researchers can analyze data using a reiterative process of reviewing data, organizing data, coding data, and developing themes (Miles et al., 2014; Yin, 2014, 2018). Yin (2016) noted a five-cycle approach to this reiterative process would include (a) compiling, (b) disassembling, (c) reassembling, (d) interpreting, and (e) concluding. I used these reiterative approaches to guide my data analysis process decisions.

The process of reviewing and compiling data included source material from interview transcripts, member checking, reflective journal entries, and company documents. I carefully organized my data into a meaningful database to prepare the initial codification, disassembling, and reassembling. I used methodological triangulation to perform my data analysis. Case study triangulation consists of methodological, investigator, theory, and data source triangulation (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014; Renz, Carrington, & Badger, 2018). Triangulation involves converging multiple sources of data (Marshall & Rossman, 2016). Data in methodological triangulation can come from sources such as interviews and company documents (Abdalla, Oliveira, Azevedo, & Gonzalez, 2018), and a researcher can use these data sources to provide a rich understanding of the studied phenomenon (Varpio, Ajjawi, Monrouxe, O'Brien, & Rees, 2017). I performed data analysis to identify themes using methodological triangulation with interviews and company documents, which included information system specifications and training documents.

I engaged in an iterative and methodological process of analyzing collected data from each case. I analyzed the collected data using different techniques. One technique of case study data analysis is using pattern matching logic (Yin, 2018). I codified the data and looked for patterns. Another technique is cross-case synthesis, where the researcher compares case conclusions to answer the research question (Yin, 2018). I went beyond treating each case as an independent topic and explored the combined cases from a holistic perspective to identify themes and phenomena of effective strategies to address ransomware.

Researchers can use computer-assisted qualitative data analysis software to iteratively explore their data and identify patterns (Yin, 2018). I used QSR International (QSR) NVivo to assist in identifying patterns and analyzing the data. Cook et al. (2018) used QSR NVivo to analyze almost 10 million words from reports using categories developed from a conceptual framework. Hunt and Bakker (2018) performed a similar analysis using audio-recorded data and QSR NVivo. Woods et al. (2016) reported most researchers from 763 empirical studies used NVivo for data management and analysis. I repeated the process of disassembling and reassembling until substantive themes emerged. I interpreted the data against the literature, conceptual framework, and rival explanations to conclude and report my research findings.

I initially based my interpretation on themes identified in the literature review. The themes included (a) adequate guardianship, (b) suitable targets and VIVA constructs, (c) motivated offenders, (d) within framework rivalry, (e) victim behavior rival, and (f) fraud triangle deception rival. Adhering to the themes identified in the literature review allowed for a thorough examination using the conceptual framework and a comparison against rival explanations.

Reliability and Validity

A qualitative case study research approach using routine activity theory goes beyond quantitative hypothesis testing. Reliability and validity are predominant in quantitative research (Cypress, 2017); however, creating and following a strict case study protocol in qualitative research achieves the same rigor (Denzin, 2016; Yin, 2018). Qualitative methods are beneficial in cybersecurity strategy research (Štitilis et al., 2017).

Following a case study protocol supports theory development through a rich understanding of the case study (Baškarada, 2014). I followed a qualitative case study protocol to develop a rich understanding of the phenomenon.

Reliability

Researchers interpret reliability through a qualitative lens to determine dependability. The dependability of a study is the extent to which the study is repeatable with similar results (Grossoehme, 2014; Yin, 2018). Following a strict case study protocol increases repeatability (Noble & Smith, 2015; Yin, 2018). Member checking, data interpretation, bracketing, and methodological triangulation increases the dependability and replicability of case study research (Morse, 2015; Pacho, 2014; Yin, 2018). I followed a strict case study protocol, used bracketing, included multiple sources of data for methodological triangulation, and conducted member checking to achieve study dependability and replicability.

Validity

Quality in qualitative case study research consists of identifiable factors. Critical factors of quality in qualitative case study research include credibility, transferability, confirmability, and data saturation (Yin, 2018). The critical factors of quality as applied to this study are discussed below.

Validate. Validation is a critical factor of quality. Validating participant responses with member checking is one method to establish credibility (Cope, 2014; Noble & Smith, 2015; Taylor & Thomas-Gregory, 2015). Qualitative credibility also involves identifying bias and keeping detailed research logs (Noble & Smith, 2015;

Taylor & Thomas-Gregory, 2015). I validated participant responses with member checking, identified my biases, and maintained a research log to ensure credibility.

Transfer. Transferability is another critical factor of quality. Transferability is a decision best made by other researchers based on the robustness of the research and is dependent upon providing sufficient detail on the development of themes, participant selection, and context of the case study (Cope, 2014; Elo et al., 2014; Smith & Noble, 2014; Taylor & Thomas-Gregory, 2015). I provided a rich description of thematic development, described how I chose participants, and provided a clear distinction between case and context of the study to improve transferability.

Confirm. The next critical factor of quality is confirmation. Confirmability exists when external examination corroborates distinct research conclusions beyond the culmination of data gathered from participants (Cope, 2014; Elo et al., 2014; Noble & Smith, 2015). I did not treat each case as a single data set but rather as a composite to identify complex themes and phenomena to aid in confirming research conclusions.

Saturate. An additional critical factor of quality is saturation. Data saturation occurs once no new information is observed (Boddy, 2016; Cleary, Horsfall, & Hayter, 2014; Cronin, 2014; Fusch & Ness, 2015; Gross, Blue-Banning, Turnbull, & Francis, 2015; Smith & Noble, 2014). I conducted member checking during and after the interview process, kept detailed research logs, identified researcher bias, detailed the codification process, engaged in purposive participant selection, differentiated findings from participant-provided information, and used replication logic until data saturation to establish quality and rigor.

Transition and Summary

In Section 2, I restated the purpose statement, outlined the role of the researcher, and described participants. Participants included small business owners in the Knox County region of Tennessee. I continued in Section 2 with identifying the research method, research design, population and sampling, and information about ethical research. I described how I conducted my research according to ethical standards as set forth by the Walden IRB. I also discussed my role as the data collection instrument, as well as the data collection technique, data organization, data analysis, and the way I addressed reliability and validity. Further, I discussed how I used methodological triangulation to perform data analysis and support research rigor.

In Section 3, I present my findings and provide recommendations for possible future research. I continue in Section 3 by comparing my predictions with observed themes and rival explanations. Section 3 also includes a discussion of the benefits to business practice and society. After sharing my recommendations possible future research, I provide my reflections of the research process and my concluding thoughts.

Section 3: Application to Professional Practice and Implications for Change

In Section 2, I addressed the bias in my data collection, participant selection, the research method and design, ethical considerations, and data collection technique. In Section 3, I present the findings from data collection, discuss the application to professional practice, social change implications, and provide recommendations for action and further research. I close with my reflections on the doctoral journey and conclusion of the research.

Introduction

The purpose of this qualitative multiple case study was to explore the cybersecurity strategies some small business leaders use to protect their information systems from ransomware. Findings from this study may aid small business leaders in developing effective strategies to address ransomware. The findings came from data I collected by interviewing five small business leaders located in the southeast region of the United States, from reviewing company documents, and from examining peer-reviewed literature. In the following sections, I explore themes developed from the data. I identified three emergent themes from the interviews and document review. The emergent themes were (a) ransomware strategy, (b) support structure, and (c) cybersecurity awareness. The findings support the conclusions and answer the research question about effective strategies small business leaders use to address ransomware.

Presentation of the Findings

The research question for this study was as follows: What cybersecurity strategies do some small business leaders use to protect their information systems from

ransomware? After data analysis I found three emergent themes. The three emergent themes were (a) ransomware strategy, (b) support structure, and (c) cybersecurity awareness. The emergent themes from participant comments appear in Table 1 with percentage of contribution to emergent theme.

Table 1

Emergent Study Themes

Theme	Total contributing participants	Percentage of contribution to emergent theme
Theme 1: Ransomware strategy	5	100
Theme 2: Support structure	5	100
Theme 3: Cybersecurity awareness	5	100

All five participants contributed to each emergent theme. Themes were developed by comparing manually and auto-coded themes from QSR NVivo using data collected from interview transcripts, member checking, reflective journal entries, and company documents.

Theme 1: Ransomware Strategy

Each participant expressed "[using] antivirus" as a strategy for effectively addressing ransomware. Bergmann et al. (2018) identified protective factors to avoid becoming a victim of cybercrime include using antivirus software, keeping software updated, using strong passwords, verifying the safety of websites, and deleting suspicious emails. Participant P2 and participant P4 lacked confidence in older versions of antivirus and thought to upgrade to the latest versions of software as just as important for effectively addressing ransomware. Participant P2 stated, "we use the [factory installed] virus protection." Participant P4 stated, "we use [antivirus software] as our protection

[and recently] upgraded [to stay safe].” Participant P1, participant P3, and participant P5 rely heavily on antivirus and the alerts presented on screen to gauge the effectiveness of their strategy to effectively address ransomware. Participant P1 stated, “we basically use an antivirus protection program and it sends out alerts.” Participant P3 was especially confident in the ability of antivirus to keep their systems safe from ransomware and stated “[antivirus] works very well and [alerts when the antivirus] cleans everything up.” Participant P5 stated, “usually they [the antivirus program] will give you a message or something will appear on your computer telling you that you need to double check or run a report.” Participant P2 and participant P4 gauged effectiveness by stating that their information systems had not yet been held for ransom as evidence of effectiveness. Participant P2 stated, “well, in a very simple manner that we’ve not been infected or not had to pay a ransom. That is probably the best answer I can give you. I have not been held ransom yet or had to send anybody a check.” Participant P4 stated, “I haven’t had any issues and I haven’t had any problems at all.” Three participants rely on alerts, while two participants gauge effectiveness based on not being held for ransom. The distribution of how participants gauge the effectiveness of their strategy to address ransomware using antivirus appear in Table 2 with percentage values.

Table 2

Gauging Effectiveness of Using Antivirus

Response	Total contributing participants	Percentage of contribution to response
Alerts	3	60
Not being held for ransom	2	40

Antivirus emerged as the dominant ransomware strategy small business leaders use to address ransomware. The majority of small business leaders stated their reliance on a feedback mechanism in the form of alerts, as a function of the antivirus software, to aid in gauging the effectiveness of using antivirus. Hampton et al. (2018) observed legacy cryptographic functions, abnormal file activity, abnormal internet connection attempts, the creation of start-up items, and obfuscated code execution attempts during ransomware infection analysis and determined detection was possible at the operating system level. Small business leaders use antivirus protection to mitigate risks, threats, and attacks at the operating system level to prevent a ransomware infection.

Antivirus, as the dominant participant response, manifested as evidence for an effective strategy for mitigating the threat of ransomware and malware to small business information systems. It is possible that antivirus software is capable of providing protection even if a user unintentionally performs an adverse action that might inadvertently infect a previously uninfected information system. Risks, threats, and attacks from ransomware and malware are addressed using antivirus as protection. However, the current function of antivirus does not fully address data and network security concerns for these small business leaders. In compiling interview data, it was apparent other concerns surfaced. These concerns led to a sub-theme of securing data and the network.

The sub-theme of securing data and the network emerged from the additional actions these small business leaders were performing to secure their systems from ransomware. Data security consisted of the small business leader securing their data and

the network from ransomware. Information security responsibility and threat targets included data stored on the computer and data traversing the network. The small business leaders used similar strategies to secure small business data and the network.

The small business leaders were most concerned with protecting their local data, and the threat from ransomware was not singled out among any specific cybersecurity threat as more or less dangerous from the small business leader perspective. Participant P3 and participant P5 have a formal procedure in place for backing up their data regularly, and both use antivirus software with the capability of only allowing approved or known good applications to run or make changes to data. Thomas and Galligher (2018) suggested having data backups available for restoring company data to a date that would have preceded the occurrence of a ransomware infection. Thomas and Galligher also suggested, as an additional precaution, using data backups that are at least 14 to 21 days older than the ransomware infection date to prevent an inadvertent reintroduction of ransomware. The most recent data backup might contain the malicious code responsible for infecting the information system with ransomware. In two instances, participant P3 and participant P5 were using USB thumb drives to back up their data. The USB drives were also disconnected from the information system and stored in a safe place to protect from environmental threats such as fire or unauthorized access as an additional safety precaution.

Threats to data traversing the network and general connectivity beyond the local information system are exterior to local storage of protected small business data. All participants were most concerned with protecting the local information system rather than

any data stored outside of their local information system. Participants assumed their antivirus software provided protection regardless of the threat vector or target. However, ransomware is not limited to infecting information systems used to support business processes but rather any system capable of storing data (Brody et al., 2018). The threat posed by ransomware has the potential to affect other systems that are not locally attached or directly used to support business processes and requires additional network protection to limit threat exposure.

One method of protecting the network and limiting exposure is through the use of a firewall for devices connected over a network. In all instances, the participants were unaware of the function of the firewall. However, all participants were using a physical firewall integrated with their modem provided by their Internet service provider (ISP) or using a second physical firewall in conjunction with the firewall provided by their ISP as an added layer of security. Additionally, all participants had software-based firewalls enabled at the operating systems level and benefited from the network protections provided by their antivirus solution.

Theme 2: Support Structure

An additional theme discovered from the data analysis was the emergence of support structures to address ransomware. Ransomware victims experience four stages of an attack that includes infection, encryption, demand, and outcome (Hampton et al., 2018). Pre-planning is required to prevent initial infection and subsequent encryption of protected data. The demand and eventual outcome would occur after the infection and encryption stage with the outcome need for post-incident support. All participants work

with either customer support or their peer-network for pre-planning or post-incident support. Participant P1 and participant P3 rely on vendor-supplied customer support for pre-planning and post-incident support. Participant P1 relies on support from the antivirus vendor noting, "we would probably contact the virus people; we don't have a tech guy." Participant P3 stated, "[they] would call for customer support." Participant P2, participant P4, and participant P5 were more confident in reaching out through their peer-network to find support based on a peer recommendation either during pre-planning or post-incident. Participant P2 stated,

> Probably like many would, I would have to hire it out, I would have to get with one of our people that help us and assist us with all of that. I would just let them walk us through it or get us pointed in the right direction.

Participant P4 stated, "I would reach out to one of my friends and say – hey this popped up what do I need to do?" Participant P5 stated, "[they] have a go to person and they can usually get some information from them." All participants indicated that they relied upon support structures, as evident in the initial preparation phase against a potential threat such as ransomware and the strategy to recover post-incident.

All five participants were prepared to address ransomware through their preferred method of support before and after a potential ransomware incident. Brody et al. (2018) suggested companies either outsource their information security or implement a dedicated information security department to manage cybersecurity and proactively prevent harm against the growing threat of malware. It may be challenging for some small business leaders to justify the expense of implementing a dedicated information security

department to address information security concerns. These small business leaders outsourced their information security needs, involved their peer network, or worked directly with a security provider. Implementing a dedicated department for information security was unnecessary for these small business leaders.

Theme 3: Cybersecurity Awareness

Cybersecurity awareness stems from a user-centric view of cybersecurity strategy, involving multiple pathways of learning and information gathering. Small business leaders are self-taught, reach out and ask questions from those in their peer network, and rely on antivirus vendors to provide educational information. Cybersecurity strategies that do not include user training fail to address behavioral-based errors that lead to successful ransomware attacks (Nobles, 2018). These self-taught small business leaders were knowledgeable in their strategies to address ransomware. The participants were comfortable reaching out to those in their peer network for guidance and education before an incident or in the event of an infection as a post-incident reactionary response. Participant P1, participant P3, and participant P5 take advantage of antivirus vendor supplied educational information. The vendor of participant P1 offered a service named "security awareness training" and sent out regular communication via email that reinforces knowledge of the threat of ransomware. Participant P3 and participant P5 have access to what was listed as "free cyber security training" from their chosen vendor and received monthly email newsletters that include the latest information and trends related to ransomware infection. Participant P2 and participant P4 thought that simplified instruction was best and expressed interest in learning more about cybersecurity. All

participants were aware of the threats posed by informal cyber activities such as reckless cyber behavior in opening emails from unknown senders, and visiting unfamiliar websites, and were inclined to follow advice from trusted sources rather than pursuing formal education in cybersecurity training.

Participants understood the importance of using caution when operating their information systems and staying up to date. Participant P2 stated, "as simple as this sounds, we try to be careful of what files or [junk mail] that we open [through email]" and participant P5 stated, "[they] try to stay up to date with what is going on and that [they] receive regular updates and keep [their] computers updated as often as possible." Participant P1 stated, "[they] stay informed [of the latest protection against ransomware] by reading [about the topic] and take [appropriate] action and uses the latest operating systems to stay up to date [with the latest trends]." Proactively using caution with opening files and keeping information systems software updated provided these small business leaders with one strategy to effectively address ransomware. An instinctive approach appeared to be effective; however, a proactive approach based on cybersecurity awareness of staying informed and up to date and end-user education was also evident.

Participant P2 and participant P4 used their knowledge to effectively address ransomware. Participant P2 stated, "shoots from the hip" as one way to describe how they respond to threats such as ransomware. Participant P4 lacked confidence in knowledge and understanding of outdated software to protect their information systems from ransomware. Participant P4 reacted by switching to a perceived more secure platform to conduct daily business while limiting use on the system viewed as more vulnerable to

threats. Participant P4 stated, “I don’t do as much work on the [older system] anymore as I used to, I have got a [newer system] and use it because I think it is safer and use it more.” Cybersecurity awareness culminates in a user-centric view of small business leader strategy in responding to the threat posed to their information systems from ransomware.

Findings Related to Routine Activity Theory

Findings from the data analysis revealed adherence to routine activity theory as all participants were adamant on using antivirus as part of their ransomware strategy for effectively addressing ransomware. Antivirus as a ransomware strategy indicates participants use antivirus as a tool to provide adequate protection or guardianship over their information systems. A lack of adequate protection or guardianship allows a ransomware offender to compromise the target information system. While antivirus may provide adequate protection or guardianship over the target information system other factors such as support structure and cybersecurity awareness also influence adequate guardianship.

All participants used, “antivirus” as a ransomware strategy, had support structures in place ranging from formal to informal, and had a user-centric view of cybersecurity. Based on the findings from the small business leaders, it was possible to protect small business information systems against ransomware with effective strategies and support structures. I selected routine activity as the conceptual framework for my study. Referencing Jansen and Leukfeldt’s (2016) recommendation, I focused on guardianship as a way to explain effective strategies to address a single threat of ransomware to small

business information systems. Bergmann et al. (2018) used a routine activity approach and recommended studying cybercrime offenses separately to gain a rich understanding of how potential victim risk factors and protective strategies influence outcomes. Through the lens of effective guardianship, the role of antivirus in ransomware strategy was significant with unanimous agreement between participant responses. The connection between the emergent themes and routine activity theory construct guardianship was apparent.

Other factors discovered during data collection may influence the effectiveness of an aspect of the conceptual framework, adequate guardianship. These other factors as identified during the data collection process as emergent themes included (a) ransomware strategy, (b) support structure, and (c) cybersecurity awareness. A lack of adequate guardianship may result in victimization and reinforces the need for protection in the cyber realm (Choi, Cho, & Lee, 2019; Choi, Earl, Lee, & Cho, 2019; Vakhitova, Alston-Knox, Reynald, Townsley, & Webster, 2019). Proactive protection may support adequate guardianship, while, reactive protection in the form of a support structure and rudimentary knowledge and understanding may also contribute to adequate guardianship. Combining proactive and reactive security measures is effective in combating cybercrime (Donegan, 2019; Ogunlana, 2019). Having an adequate support arrangement with either a peer network or vendor-supplied support prior to a ransomware attack may support adequate guardianship. Cybersecurity awareness includes educating oneself against the threat of ransomware and how best to protect target information systems from infection. While Whitty (2019) indicated the act of being cautious because of an awareness of a

cybersecurity threat is not enough to prevent victimization, Williams, Levi, Burnap, and Gundur, (2019) found repeated exposure to information on how to protect oneself online decreased victimization risk. Cybersecurity awareness supports adequate guardianship. Data and network security includes maintaining adequate backups and protecting the network (Thomas & Galligher, 2018). Data and network security supports adequate guardianship, while, failing to properly keep adequate backups of data or securing the network with firewalls contribute to a lack of adequate guardianship. These contributing factors were evidence of the strategic value the respondents placed on their joint application to achieve guardianship to prevent a compromised target by ransomware.

Guardianship emerged as a critical factor in technology and routine activity theory studies in preventing victimization. Jansen and Leukfeldt (2016) and Ilievski (2016) both discussed the importance of guardianship as technological protection such as antivirus in their research involving routine activity theory. Routine activity theory provides constructs of guardianship, motivated offender, and victim. The emergent themes from this study aligned with guardianship. Figure 2 depicts specific routine activity theory studies from the literature review. The intersecting studies in Figure 2 reinforce the value of guardianship in a cyber context.

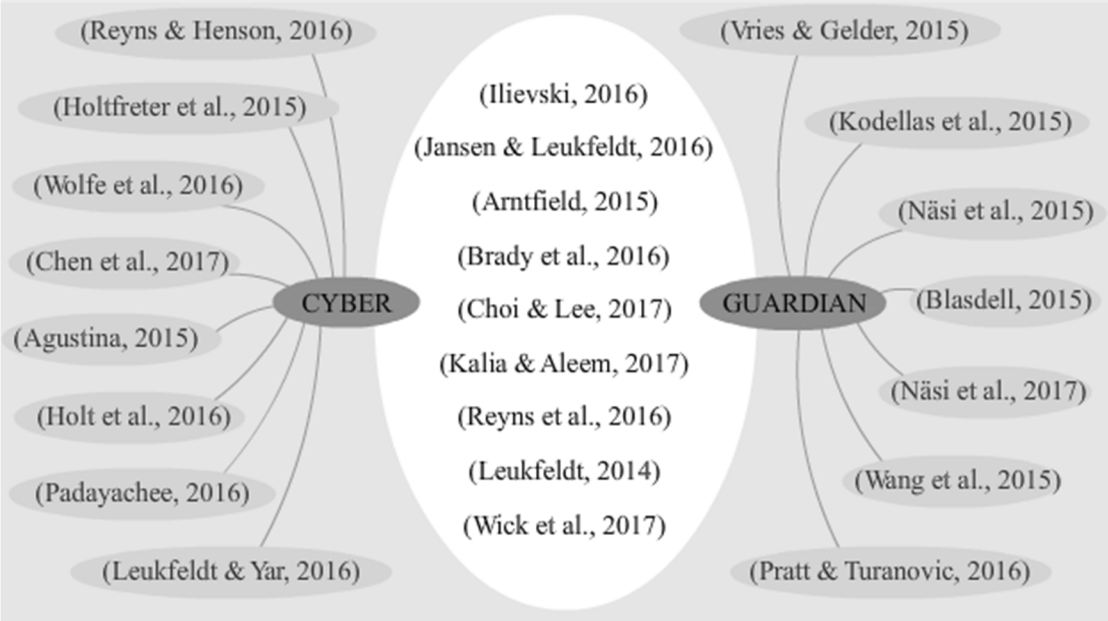

Figure 2. Intersection of cyber and guardian in routine activity studies.

Figure 2 depicts the studies, highlighted in white, discussed in the literature review, that contain the routine activity theory conceptual construct guardianship within the context of the cyber realm. This study on effective strategies small business leaders used to address ransomware might fit within the same categorization of the studies highlighted in white. Categorization justification is based on findings linking cyber guardianship and the emergent themes. Ransomware strategy, support structure, and cybersecurity awareness fit within the context of routine activity theory guardianship. Findings from this study echo the importance of the guardianship conceptual construct of routine activity theory and may have real-world applications that contribute to professional practice.

Application to Professional Practice

The findings of this study are relevant to improve strategies small business leaders use to address ransomware before victimization occurs. Small business leaders can use the results from this study to confirm if implemented strategies in their organization fall short, match, or exceed what other leaders of small businesses are doing in their organizations to address security against ransomware. Organizations whose leaders fail to measure and address their internal cybersecurity posture create an opportunity for victimization to occur (Williams et al., 2019). The growing threat of ransomware to small business information systems is capable of denying access to information system resources required for daily business operations and specific strategies exist to mitigate the threat.

Small business leaders can adapt their strategies to address ransomware by examining their management approach of data and the network, support structure, and cybersecurity awareness. Reducing the likelihood of victimization requires going beyond the act of examining cybersecurity strategies with implementation (Whitty, 2019). Based on the findings of the study, small business leaders may consider evaluating how they are backing up critical information system assets. Increasing the retention period may improve the chances of recovery in case of a successful ransomware attack (Thomas & Galligher, 2018). Users should carefully scrutinize email messages before opening, keep operating systems updated (Bergmann et al., 2018), and consider incorporating a strategy to keep important small business data backed up (Thomas & Galligher, 2018). The small business leaders of this study had adequate support structures, access to trusted sources of

information on cybersecurity, and were confident in their ability to address the evolving threat of ransomware.

Implications for Social Change

One positive implication for social change is providing research results that may help mitigate the existing threat of motivated offenders who commit cybercrimes, specifically ransomware. Some of the prerequisites of routine activity theory are satisfied when studying cybercrime and users on the Internet, as cybercriminals are prevalent on the Internet and Internet users fulfill the role of suitable targets (Bergmann et al., 2018). Individuals accountable for securing information systems similar to what is in use at a small business may use the research results to help identify effective strategies used to mitigate the specific threat of ransomware.

Mitigating the threat of ransomware may benefit communities and other organizations. Communities and other organizations may benefit when small business leaders ensure continuity of operations and maintain customer expectations. Small business leaders might use the study results to implement strategies to address ransomware and prevent data loss, prevent delays, and mitigate damage arising from a successful ransomware attack.

Small business leaders may use study results to increase awareness and improve the security culture of their local organization and beyond. Increasing awareness of strategies to effectively address ransomware may help promote security at a societal level. Society as a whole may benefit as small business leaders might reach beyond their local peer network and influence others who may be responsible for implementing

strategies to address ransomware, reduce uncertainty, and promote a healthy cybersecurity culture beyond the local communities they serve.

Recommendations for Action

The recommendations I am providing are based on the research findings and could possibly serve as a starting point for future publications targeted to small business leaders responsible for strategies to address ransomware in their organization. Based on the research findings, I would recommend installing adequate antivirus protection, keeping software updated, using caution when opening files, and incorporating a data backup strategy to safeguard important small business information system files. Additionally, small business leaders having a peer-network with access to technical expert contacts or who use paid customer support channels were more confident in their strategy to address ransomware.

I plan to disseminate the results of this study publicly as a keynote speaker at a Nutanix .NEXT conference or as a Cisco Live! panelist. The general content and specific findings from this study may be a useful resource for future work and career endeavors. I will use the research findings to justify solicited advice I might give during client discussions, while professionally consulting, and through my chain of command.

Recommendations for Further Research

One limitation of the findings is ransomware is an evolving threat, and successful strategies for addressing ransomware may continue to change. Known best practices may need adjustment to counter the evolving threat of ransomware. Future researchers may

need to consider ransomware evolution and how threat vectors may change over time to gauge strategy effectiveness to address ransomware.

Future researchers may consider expanding the sample size, studying a different population, or modifying the research design. The sample size for this study was sufficient to reach saturation; however, future researchers may include a larger sample to verify results. Future researchers may focus on a specific sector of small business that may be known as more of a target for ransomware attacks, such as the financial or health sector. A quantitative or mixed-method design might allow future researchers to add to the discussion by incorporating additional data points and broadening the scope of inquiry. Additionally, future researchers might choose to investigate the inverse of this study and evaluate successful ransomware infections to understand failure and recovery.

Reflections

I began my scholarly journey as a degree-seeking student in March of 2008. I started by taking online classes, and as an information technology expert, the online environment was a natural fit for my existing skillsets. The culmination of effort, dedication, and focus on achieving high academic goals and following in the footsteps of giants has been a gratifying experience. I am better prepared to take on the challenges of working in a competitive environment where I can use what I have learned to improve performance and discover new information. The doctor of business administration process has taught me how to investigate the world using new tools and techniques to create meaningful change, sustainability, and positively influence those around me. Ultimately, it is my goal to share information and be the change in the world I want to

see. Sharing knowledge and improving the local community is one way to improve the world around me. I will continue to set a positive example by pursuing excellence and leading by example through servant leadership. Achieving the high academic standards of a doctorate is a challenging and difficult journey, but so are the rewards for those with the perseverance, determination, and tenacity to undertake and complete the challenge.

Conclusion

The findings of this multiple case study contain effective strategies to address ransomware, revealed the multifaceted strategy of support structures, and contains evidence of the cybersecurity awareness required to effectively address the threat of ransomware from the perspective of a small business leader. Additionally, the findings contribute to the literature on effective strategies small business leaders use to address ransomware in the context of routine activity theory. The small business leaders interviewed during this study were aware of the importance of protecting their information systems and implemented formal and instinctive strategies. The small business leaders who were successfully addressing ransomware: (a) relied on antivirus and firewalls to protect their data and network, (b) kept their information systems updated, (c) scrutinized files before opening, (d) had a support structure for assistance in the event of an adverse event affecting their information systems, and (e) used their cybersecurity awareness of threats as a strategy to effectively address ransomware.

Some of the small business leaders were unimpressed with free software purporting to protect their information systems and instead preferred to pay for antivirus protection from reputable vendors. The small business leaders were cognizant of the

threats posed by fraudulent emails and were cautious about opening suspicious email attachments. The small business leaders who lacked confidence in the ability of their existing information systems switched to newer systems as alternatives they perceived as superior to conduct daily business operations.

References

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

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

Achtenhagen, L., Brunninge, O., & Melin, L. (2017). Patterns of dynamic growth in medium-sized companies: Beyond the dichotomy of organic versus acquired growth. *Long Range Planning*, *50*, 457-471. doi:10.1016/j.lrp.2016.08.003 0024-6301

Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, *9*, 35-54. doi:10.5281/zenodo.22239

Alby, F., & Fatigante, M. (2014). Preserving the respondent's standpoint in a research interview: Different strategies of 'doing' the interviewer. *Human Studies*, *37*, 239-256. doi:1007/s10746-013-9292-y

Ali, A. (2017). Ransomware: A research and personal case study of dealing with this nasty malware. *Issues in Informing Science and Information Technology Education*, *14*, 87-99. doi:10.28945/3707

Arasti, M., Khaleghi, M., & Noori, J. (2017). Corporate-level technology strategy and its

linkage with corporate strategy in multi-business companies: IKCO case study. *Technological Forecasting & Social Change*, *122*, 243-252. doi:10.1016/j.techfore.2016.02.013 0040-1625

Arntfield, M. (2015). Toward a cybervictimology: Cyberbullying, routine activities theory, and the anti-sociality of social media. *Canadian Journal of Communication*, *40*, 371-388. doi:10.22230/cjc.2015v40n3a2863

Asiamah, N., Mensah, H. K., & Oteng-Abayie, E. (2017). General, target, and accessible population: Demystifying the concepts for effective sampling. *The Qualitative Report*, *22*, 1607-1621. Retrieved from http://nsuworks.nova.edu

Australian Bureau of Statistics. (2018). *Australian industry, 2016-17* (ABS Issue No. 8155.0) [Issue Summary]. Retrieved from http://www.abs.gov.au

Azevedo, C. B., Iacob, M., Almeida, J. A., Sinderen, M., Pires, L. F., & Guizzardi, G. (2015). Modeling resources and capabilities in enterprise architecture: A well-founded ontology-based proposal for ArchiMate. *Information Systems*, *54*, 235-262. doi:10.1016/j.is.2015.04.008

Bailetti, T., & Zijdemans, E. (2014). Cybersecurity startups: The importance of early and rapid globalization. *Technology Innovation Management Review*, *4*(11), 14-21. Retrieved from http://www.timreview.ca/

Baronienė, L., & Žirgutis, V. (2017). Cybersecurity facets: Counterfactual impact evaluation of measure “procesas lt” in enterprises of the it sector. *Journal of Security and Sustainability Issues*, *6*, 445-456. doi:10.9770/jssi.2017.6.3(10)

Baškarada, S. (2014). Qualitative case study guidelines. *The Qualitative Report*, *19*(40),

1-18. Retrieved from http://nsuworks.nova.edu/tqr

Bergmann, M. C., Dreißigacker, A., Skarczinski, B., & Wollinger, G. R. (2018). Cyber-dependent crime victimization: The same risk for everyone? *Cyberpsychology, Behavior, and Social Networking*, *21*, 84-90. doi:10.1089/cyber.2016.0727

Beskow, L. M., Check, D. K., & Ammarell, N. (2014). Research participants' understanding of and reactions to certificates of confidentiality. *AJOB Primary Research*, *5*(1), 12-22. doi:10.1080/21507716.2013.813596

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

Blasdell, R. (2015). The intersection of race, gender, and class in routine activities: A proposed criminological model of victimization and offending. *Race, Gender & Class; New Orleans*, *22*, 260-273. Retrieved from http://rgc.uno.edu/

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

Brady, P. Q., Randa, R., & Reyns, B. W. (2016). From WWII to the world wide web: A research note on social changes, online "places," and a new online activity ratio for routine activity theory. *Journal of Contemporary Criminal Justice*, *32*, 129-147. doi:10.1177/1043986215621377

Bridget, J. (2016). Ransomware recovery. *ITNow*, *58*(4), 32-33. doi:10.1093/itnow/bww103

Brody, R. G., Chang, H. U., & Schoenberg, E. S. (2018). Malware at its worst: Death and

destruction. *International Journal of Accounting & Information Management*, *26*, 527-540. doi:doi.org/10.1108/IJAIM-04-2018-0046

Brown, S. D. (2016). Cryptocurrency and criminality: The bitcoin opportunity. *The Police Journal: Theory, Practice and Principles*, *89*, 327-339. doi:10.1177/0032258XI6658927

Byerley, L., Lane, H., Ludy, M., Vitolins, M. Z., Anderson, E., Niedert, K., . . . Abram, J. (2017). Ethical considerations for successfully navigating the research process. *Journal of the Academy of Nutrition and Dietetics*, *117*, 1302-1307. doi:10.1016/j.jand.2017.02.011

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*, 43-62. doi:10.1111/1468-2346.12504

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

Check, D. K., Wolf, L. E., Dame, L. A., & Beskow, L. M. (2014). Certificates of confidentiality and informed consent: Perspectives of IRB chairs and institutional legal counsel. *IRB: Ethics and Human Research*, *36*(1), 1-8. doi:10.1038/gim.2014.102

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291-302. doi:10.1016/j.chb.2017.01.003

Choi, K., Cho, S., & Lee, J. R. (2019). Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. *Computers in Human Behavior*, *100*, 1-10. doi:10.1016/j.chb.2019.06.007

Choi, K., Earl, K., Lee, J. R., & Cho, S. (2019). Diagnosis of cyber and non-physical bullying victimization: A lifestyle and routine activities theory approach to constructing effective preventative measures. *Computers in Human Behavior*, *92*, 11-19. doi:10.1016/j.chb.2018.10.014

Choi, K., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394-402. doi:10.1016/j.chb.2017.03.061

Choudhary, M., Zavarsky, P., & Lindskog, D. (2016). Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, *94*, 465-472. doi:10.1016/j.procs.2016.08.072

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

Cohen, J. A., & Kassan, A. (2018). Being in-between: A model of cultural identity negotiation for emerging adult immigrants. *Journal of Counseling Psychology*, *65*, 133-154. doi:10.1037/cou0000265

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

Congressional Research Service. (2018, April 17). Small business size standards: A historical analysis of contemporary issues. Retrieved from https://www.everycrsreport.com/reports/R40860.html

Constantinou, C. S., Georgiou, M., & Perdikogianni, M. (2017). A comparative method for themes saturation (CoMeTS) in qualitative interviews. *Qualitative Research*, *17*, 571-588. doi:10.1177/1468794116686650

Cook, L., LaVan, H., & Zilic, I. (2018). An exploratory analysis of corporate social responsibility reporting in US pharmaceutical companies. *Journal of Communication Management*, *22*, 197-211. doi:10.1108/JCOM-02-2017-0020

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

Cressey, D. (1953). *Other people's money*. Glencoe, IL: The Free Press.

Creţu, D., & Iova, R. A. (2015). Identification of leadership skills and behaviours, in the business sector. Case study. *Procedia - Social and Behavioral Sciences*, *186*, 526-534. doi:10.1016/j.sbspro.2015.04.057

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher*, *21*, 19-27. Retrieved from http://www.rcnpublishing.com/journal/nr

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. *Dimensions*

of Critical Care Nursing, *36*, 253-263. doi:10.1097/DCC.0000000000000253

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

Denzin, N. K. (2016). *Qualitative inquiry under fire: Toward a new paradigm dialogue*. New York, NY: Routledge.

Digby, R., Lee, S., & Williams, A. (2016). Interviewing people with dementia in hospital: Recommendations for researchers. *Journal of Clinical Nursing*, *25*, 1156-1165. doi:10.1111/jocn.13141

Donegan, M. (2019). Crime script for mandate fraud. *Journal of Money Laundering*, *22*, 770-781. doi:10.1108/JMLC-03-2019-0025

Drake, G. (2014). The ethical and methodological challenges of social work research with participants who fear retribution: To 'do no harm'. *Qualitative Social Work*, *13*, 304-319. doi:10.1177/1473325012473499

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

Esteves, J., Ramalho, E., & Haro, G. (2017). To improve cybersecurity, think like a hacker. *MIT Sloan Management Review*, *58*, 70-77. Retrieved from http://sloanreview.mit.edu

Fanning, K. (2015). Minimizing the cost of malware. *Journal of Corporate Accounting & Finance*, *26*(3), 7-14. doi:10.1002/jcaf.22029

Fawcett, A. M., Fawcett, S. E., Cooper, M. B., & Daynes, K. S. (2014). Moments of

angst: A critical incident approach to designing customer-experience value systems. *Benchmarking: An International Journal*, *3*, 450-480. doi:10.1108/BIJ-09-2012-0059

Federal Bureau of Investigation. (2016). *Ransomware victims urged to report infections to federal law enforcement* [Public Service Announcement]. Retrieved from https://www.ic3.gov/media/2016/160915.aspx

Fernandez, R., Sheppard-Law, S., Curtis, S., Bancroft, J., & Smith, W. (2018). Exploring the experiences of neophyte nurse mentors: A qualitative study. *Nurse Education in Practice*, *29*, 76-81. doi:10.1016/j.nepr.2017.11.011

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

Forde, E. S. (2017). *Security strategies for hosting sensitive information in the commercial cloud* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 10278501)

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

Frith, M., Johnson, S., & Fry, H. (2017). Role of the street network in burglars' spatial decision-making. *Criminology*, *55*, 344-376. doi:10.1111/1745-9125.12133

Fusch, P., & Ness, L. (2015). Are we there yet? Data saturation in qualitative

research. *Qualitative Report*, *20*, 1408-1416. Retrieved from http://tqr.nova.edu/

Gareth, N. (2016). Ransom ware. *ITNow*, *58*(4), 21. doi:10.1093/itnow/bww097

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*, 316-348. doi:10.1080/09636412.2015.1038188

Gelling, L. (2014). Complexities of ethnography. *Nurse Researcher*, *22*(1), 6-7. doi:10.7748/nr.22.1.6.s2

Genç, Z. A., Lenzini, G., & Ryan, P. Y. (2017). Cipher, the random and the ransom: A survey on current and future ransomware. In I. Bernik, B. Markelj, & S. Vrhovec (Eds.), *Advances in Cybersecurity 2017* (pp. 89-102). doi:10.18690/978-961-286-114-8.8

German, P. (2016). A new month, a new data breach. *Network Security*, *2016*(3), 18-20. doi:10.1016/S1353-4858(16)30029-0

Goldberg, A. E., & Allen, K. R. (2015). Communicating qualitative research: Some practical guideposts for scholars. *Journal of Marriage and Family*, *77*, 3-22. doi:10.1111/jomf.12153

Goss, B. (2017). The Nuremberg veil: Le voil de Nuremberg. *Ethics, Medicine and Public Health*, *3*, 452-459. doi:10.1016/j.jemep.2017.09.011

Goutas, L., Sutanto, J., & Aldarbesti, H. (2016). The building blocks of a cloud strategy: Evidence from three SaaS providers. *Communications of the ACM*, *50*, 90-97. doi:10.1145/2756545

Gross, J. M. S., Blue-Banning, M., Turnbull, H. R., III., & Francis, G. L. (2015).

Identifying and defining the activities of participant direction programs: A document analysis. *Journal of Disability Policy Studies*, *25*, 220-232. doi:10.1177/1044207313502538

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

Haimes, Y. Y., Horowitz, B. M., Guo, Z., Andrijcic, E., & Bogdanor, J. (2015). Assessing systemic risk to cloud-computing technology as complex interconnected systems of systems. *Systems Engineering*, *18*, 284-299. doi:10.1002/sys.21303

Halcomb, E., & Hickman, L. (2015). Mixed methods research. *Nursing Standard*, *29*(32), 41-47. doi:10.7748/ns.29.32.41.e8858

Hampton, N., Baig, Z., & Zeadally, S. (2018). Ransomware behavioural analysis on windows platforms. *Journal of Information Security and Applications*, *40*, 44-51. doi:10.1016/j.jisa.2018.02.008

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

Hernández-Flores, M. D., Otazo-Sánchez, E. M., Galeana-Pizaña, M., Roldán-Cruz, E. I., Razo-Zárate, R., González-Ramírez, C. A., . . . Gordillo-Martínez, A. J. (2017). Urban driving forces and megacity expansion threats: Study case in the Mexico City periphery. *Habitat International*, *64*, 109-122. doi:10.1016/j.habitatint.2017.04.004

Hinkelmann, K., Gerber, A., Karagiannis, D., Thoenssen, B., Merwe, A., & Woitsch, R. (2016). A new paradigm for the continuous alignment of business and IT: Combining enterprise architecture modelling and enterprise ontology. *Computers in Industry*, *79*, 77-86. doi:10.1016/j.compind.2015.07.009

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2016). Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology*, 1-22. Advance online publication. doi:10.1177/0306624X16679162

Holtfreter, K., Reisig, M. D., Pratt, T. C., & Holtfreter, R. E. (2015). Risky remote purchasing and identity theft victimization among older Internet users. *Psychology, Crime & Law*, *21*, 681-698. doi:10.1080/1068316X.2015.1028545

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

Hunt, S. L., & Bakker, C. J. (2018). A qualitative analysis of the information science needs of public health researchers in an academic setting. *Journal of the Medical Library Association*, *106*, 184-197. doi:10.5195/jmla.2018.316

Hyett, N., Kenny, A., & Dickson-Swift, V. (2014). Methodology or method? A critical review of qualitative case study reports. *International Journal of Qualitative Studies on Health and Well-being*, *9*, 1-12. doi:10.3402/qhw.v9.23606

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

realities. *Information Technology & People*, *31*, 111-133. doi:10.1108/ITP-07-2016-0168

Ilievski, A. (2016). An explanation of the cybercrime victimisation: Self-control and lifestile/routine activity theory. *Innovative Issues and Approaches in Social Sciences*, *9*, 30-47. doi:10.12959/issn.1855-0541.IIASS-2016-no1-art02

Internet Crime Complaint Center. (2016). *2016 Internet Crime Report*. [Data file]. Retrieved from https://www.pdf.ic3.gov/2016_IC3Report.pdf

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*, 79-91. doi:10.5281/zenodo.58523

Jarvis, J. E., & Williams, I. A. (2017). A case study exploration of strategies to improve first-line supervisor problem-solving abilities in the retail supermarket industry. *International Journal of Applied Management and Technology*, *16*(1), 86-110. doi:10.5590/IJAMT.2017.16.1.06

Jones, M., & O'Neill, C. (2014). Identity, records and archival evidence: Exploring the needs of forgotten Australians and former child migrants. *Archives & Records*, *35*, 110-125. doi:10.1080/23257962.2014.951032

Joyce, M. (2015). Using narrative in nursing research. *Nursing Standard*, *29*(38), 36-41. doi:10.7748/ns.29.38.36.e9008

Jussani, A. C., Wright, J. C., & Ibusuki, U. (2017). Battery global value chain and its technological challenges for electric vehicle mobility. *Innovation & Management*

Review, *14*, 333-338. doi:10.1016/j.rai.2017.07.001

Kalia, D., & Aleem, S. (2017). Cyber victimization among adolescents: Examining the role of routine activity theory. *Journal of Psychosocial Research*, *12*, 223-232. Retrieved from http://printspublications.com

Kaminska, R., & Borzillo, S. (2017). Challenges to the learning organization in the context of generational diversity and social networks. *The Learning Organization*, *25*, 92-101. doi:10.1108/TLO-03-2017-0033

Kasim, A., & Al-Gahuri, H. A. (2015). Overcoming challenges in qualitative inquiry within a conservative society. *Tourism Management*, *50*, 124-129. doi:10.1016/j.tourman.2014.01.004

Kharraz, A., Robertson, W. K., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian knot: A look under the hood of ransomware attacks [Monograph]. *Lecture Notes in Computer Science*, 9148, 2-20. doi:10.1007/978-3-319-20550-2_1

Knepp, M. M. (2014). Personality, sex of participant, and face-to-face interaction affect reading of informed consent forms. *Psychological Reports*, *114*, 297-313. doi:10.2466/17.07.PR0.114k13w1

Kodellas, S., Fisher, B. S., & Wilcox, P. (2015). Situational and dispositional determinants of workplace victimization: The effects of routine activities, negative affectivity, and low self-control. *International Review of Victimology*, *21*, 321-342. doi:10.1177/0269758015591930

Kohn, M., Belza, B., Petrescu-Prahova, M., & Miyawaki, C. E. (2016). Beyond strength:

Participant perspectives on the benefits of an older adult exercise program. *Health Education & Behavior*, *43*, 305-312. doi:10.1177/1090198115599985

Lancaster, K. (2017). Confidentiality, anonymity and power relations in elite interviewing: Conducting qualitative policy research in a politicised domain. *International Journal of Social Research Methodology*, *20*, 93-103. doi:10.1080/13645579.2015.1123555

Leukfeldt, E. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *CyberPsychology & Behavior, and Social Networking*, *17*, 551-555. doi:10.1089/cyber.2014.0008

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

Levy, J., Fabian, M., & Peters, J. (2015). Meta-analytic approaches for multistressor dos-response function development: Strengths, limitations, and case studies. *Risk Analysis*, *35*, 1040-1049. doi:10.1111/risa.12208

Lord, R., Bolton, N., Fleming, S., & Anderson, M. (2016). Researching a segmented market: Reflections on telephone interviewing. *Management Research Review*, *39*, 786-802. doi:10.1108/MRR-01-2015-0020

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

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target

data breach. *Business Horizons*, *59*, 257-266. doi:10.1016/j.bushor.2016.01.002

Mao, A., & Bottorff, J. L. (2017). A qualitative study on unassisted smoking cessation among Chinese Canadian immigrants. *American Journal of Men's Health*, *11*, 1703-1712. doi:10.1177/1557988315627140

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

McCann, E., & Brown, M. (2017). Discrimination and resilience and the needs of people who identify as Transgender: A narrative review of quantitative research studies. *Journal of Clinical Nursing*, *26*, 4080-4093. doi:10.1111/jocn.13913

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

McVey, L., Lees, J., & Nolan, G. (2016). Reflective-verbal language and reverie in qualitative interview. *Counselling & Psychotherapy Research*, *16*, 132-140. doi:10.1002/capr.12059

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). In H. Salmon et al. (Eds.) *Qualitative data analysis: A methods sourcebook* (3rd ed.). Thousand Oaks, CA: Sage.

Miracle, V. A. (2016). The Belmont Report: The triple crown of research ethics. *Dimensions of Critical Care Nursing*, *35*, 223-228. doi:10.1097/DCC.0000000000000186

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative

inquiry. *Qualitative Health Research*, *25*, 1212-1222. doi:10.1177/1049732315588501

Morse, J. M., & Coulehan, J. (2015). Maintaining confidentiality in qualitative publications. *Qualitative Health Research*, *25*, 151-152. doi:10.1177/1049732314563489

Mui, G., & Mailley, J. (2015). A tale of two triangles: Comparing the fraud triangle with criminology's crime triangle. *Accounting Research Journal*, *28*, 45-58. doi:10.1108/ARJ-10-2014-0092

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

Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2017). Do routine activities help predict young adults' online harassment: A multi-nation study. *Criminology & Criminal Justice*, *17*, 418-432. doi:10.1177/1748895816679866

National Commission for the Protection of Human Subjects in Biomedical and Behavioral Research. (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subject's research*. [Supplemental material]. Washington, DC: National Institutes of Health. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Nguyen, T. Q. (2015). Conducting semi-structured interviews with the

Vietnamese. *Qualitative Research Journal*, *15*, 35-46. doi:10.1108/QRJ-04-2014-0012

Nikitkov, A. N., Stone, D. N., & Miller, T. C. (2014). Internal controls, routine activity theory (RAT), and sustained online auction deception: A longitudinal analysis. *Journal of Information Systems*, *28*, 311-337. doi:10.2308/isys-50708

Niven, K., & Boorman, L. (2016). Assumptions beyond the science: Encouraging cautious conclusions about functional magnetic resonance imaging research on organizational behavior. *Journal of Organizational Behavior*, *37*, 1150-1177. doi:10.1002/job.2097

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence Based Nursing*, *18*(2), 34-35. doi:10.1136/eb-2015-102054

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *Holistica*, *9*, 71-88. doi:10.2478/hjbpa-2018-0024

Norquay, N. (2017). Extensions and applications: Bringing a silenced community to life: Animating the archival record. *Vitae Scholasticae*, *34*, 86-89. Retrieved from http://www.isebio.com

Ogunlana, S. O. (2019). Halting Boko Haram / Islamic State's West Africa Province propaganda in cyberspace with cyberspace technologies. *Journal of Strategic Security*, *12*(1), 72-106. doi:10.5038/1944-0472.12.1.1707

Omidi, M., Min, Q., & Omidi, M. (2017). Combined effect of economic variables on fraud, a survey of developing countries. *Economics & Sociology*, *10*, 267-278. doi:10.14254/2071-789X.2017/10-2/20

Ortolani, P. (2016). Self-enforcing online dispute resolution: Lessons from Bitcoin. *Oxford Journal of Legal Studies*, *36*, 595-629. doi:10.1093/ojls/gqv036

Pacho, T. O. (2014). Exploring participants' experiences using case study. *International Journal of Humanities and Social Science*, *5*(4), 44-53. Retrieved from www.ijhssnet.com

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, *43*, 626-642. doi:10.1016/j.ijlcj.2015.02.003

Pascariu, C., Barbu, I., & Bacivarov, I. C. (2017). Investigative analysis and technical overview of ransomware based attacks. Case study: WannaCry. *International Journal of Information Security & Cybercrime*, *6*(1), 26-27. doi:10.19107/IJISC.2017.01.06

Patel, A. (2015). Network performance without compromising security. *Network Security*, *2015*(1), 9-12. doi:10.1016/S1353-4858(15)70008-5

Patyal, M., Sampalli, S., Qiang, Y., & Rahman, M. (2017). Multi-layered defense architecture against ransomware. *International Journal of Business & Cyber Security*, *1*(2), 52-64. Retrieved from http://www.ijbcs.abrmr.com

Paulsen, C. (2016). Cybersecuring small businesses. *Computer (New York)*, *49*(8), 92-97. doi:10.1109/MC.2016.223

Perlman, D., Taylor, E., Moxham, L., Sumskis, S., Patterson, C., Brighton, R., & Heffernan, T. (2018). Examination of a therapeutic-recreation based clinical placement for undergraduate nursing students: A self-determined

perspective. *Nurse Education in Practice*, *29*, 15-20. doi:10.1016/j.nepr.2017.11.006

Petrovic, R. (2017). Ethical credibility of scientists in social research. *Research in Pedagogy*, *7*, 98-105. doi:10.17810/2015.52

Porteous, D. J., & Machin, A. (2018). The lived experience of first year undergraduate student nurses: A hermeneutic phenomenological study. *Nurse Education Today*, *60*, 56-61. doi:10.1016/j.nedt.2017.09.017

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders*, *11*, 335-354. doi:10.1080/15564886.2015.1057351

Radziwill, N., & Benton, M. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. *Software Quality Professional*, *19*(4), 25-36. Retrieved from http://www.asq.org

Reinstein, A., & Taylor, E. Z. (2017). Fences as controls to reduce accountants' rationalization. *Journal of Business Ethics*, *141*, 477-488. doi:10.1007/s10551-015-2701-6

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

Reyns, B. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*, *22*, 396-411. doi:10.1108/JFC-06-2014-0030

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with

none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*, 1119-1139. doi:10.1177/0306624X15572861

Reyns, B. W., Henson, B., & Fisher, B. S. (2016). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice*, *32*, 148-168. doi:10.1177/1043986215621378

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10-21. Retrieved from http://www.scholarspress.us

Roden, D. M., Cox, S. R., & Kim, J. Y. (2016). The fraud triangle as a predictor of corporate fraud. *Academy of Accounting and Financial Studies Journal*, *20*, 80-92. Retrieved from http://www.abacademies.org/

Rodgers, W., Söderbom, A., & Guiral, A. (2015). Corporate social responsibility enhanced control systems reducing the likelihood of a fraud. *Journal of Business Ethics*, *131*, 871-882. doi:10.1007/s10551-014-2152-5

Roy, K., Zvonkovic, A., Goldberg, A., Sharp, E., & LaRossa, R. (2015). Sampling richness and qualitative integrity: Challenges for research with families. *Journal of Marriage and Family*, *77*, 243-260. doi:10.1111/jomf.12147

Roy, S., & Basu, R. (2015). Industrial sickness and its impact on the economy: A case study of Haora district, West Bengal. *Economic Affairs: A Quarterly Journal of Economics*, *60*(1), 57-62. doi:10.5958/0976-4666.2015.00006.6

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security & Law*, *12*(2), 53-74. Retrieved from http://www.jdfsl.org

Simms, C. (2016). A matter of survival. *ITNow*, *58*(4), 30-31. doi:10.1093/itnow/bww102

Smith, J., & Noble, H. (2014). Bias in research. *Evidence Based Nursing*, *17*(4), 100-101. doi:10.1136/eb-2014-101946

Smyth, V. (2016). Vulnerability intelligence. *ITNow*, *58*(4), 26-27. doi:10.1093/itnow/bww100

Snow, K. J., Richards, A. H., & Kinner, S. A. (2017). Use of multiple data sources to estimate hepatitis C seroprevalence among prisoners: A retrospective cohort study. *Plos ONE*, *12*(7), 1-9. doi:10.1371/journal.pone.0180646

Sollie, H., Kop, N., & Euwema, M. C. (2017). Mental resilience of crime scene investigators: How police officers perceive and cope with the impact of demanding work situations. *Criminal Justice and Behavior*, *44*, 1580-1603. doi:10.1177/0093854817716959

Štitilis, D., Pakutinskas, P., Kinis, U., & Malinauskaitė, I. (2016). Concepts and principles of cyber security strategies. *Journal of Security and Sustainability Issues*, *6*, 197-210. doi:10.9770/jssi.2016.6.2(1)

Štitilis, D., Pakutinskas, P., Laurinaitis, M., & Malinauskaitė-van de Castel, I. (2017). A model for the national cyber security strategy: The Lithuanian case. *Journal of Security and Sustainability Issues*, *6*, 357-372. doi:10.9770/jssi.2017.6.3(3)

Taylor, R., & Thomas-Gregory, A. (2015). Case study research. *Nursing Standard*, *29*,

36-40. doi:10.7748/ns.29.41.36.e8856

Teoh, C. S., & Mahmood, A. K. (2017). National cyber security strategies for digital economy. *Journal of Theoretical and Applied Information Technology*, *95*, 6510-6522. Retrieved from http://www.jatit.org/

Thomas, J. E., & Galligher, G. C. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. *Computer and Information Science*, *11*, 14-25. doi:10.5539/cis.v11n1p14

Thorpe, A. S. (2014). Doing the right thing or doing the thing right: Implications of participant withdrawal. *Organizational Research Methods*, *17*, 255-277. doi:10.1177/1094428114524828

Turner, J., & Danks, S. (2014). Case study research: A valuable learning tool for performance improvement professionals. *Performance Improvement*, *53*(4), 24-31. doi:10.1002/pfi.21406

U.S. Census Bureau. (2018). 2015 SUSB annual data tables by establishment industry. Retrieved from https://www.census.gov/data/tables/2015/econ/susb/2015-susb-annual.html

Vakhitova, Z. I., Alston-Knox, C. L., Reynald, D. M., Townsley, M. K., & Webster, J. L. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse?. *Computers in Human Behavior*, *101*, 225-237. doi:10.1016/j.chb.2019.07.012

Van Rijnsoever, F. J. (2017). (I can't get no) saturation: A simulation and guidelines for sample sizes in qualitative research. *PLoS ONE*, *12*(7), 1-17.

doi:10.1371/journal.pone.0181689

Varpio, L., Ajjawi, R., Monrouxe, L. V., O'Brien, B. C., & Rees, C. E. (2017). Shedding the cobra effect: Problematising thematic emergence, triangulation, saturation and member checking. *Medical Education*, *51*, 40-50. doi:10.1111/medu.13124

Vries, R. E., & Gelder, J. (2015). Explaining workplace delinquency: The role of honesty-humility, ethical culture, and employee surveillance. *Personality and Individual Differences*, *86*, 112-116. doi:10.1016/j.paid.2015.06.008

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

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*, 277-292. doi:10.1108/JFC-10-2017-0095

Wick, S. E., Nagoshi, C., Basham, R., Jordan, C., Kim, Y. K., Nguyen, A. P., & Lehmann, P. (2017). Patterns of cyber harassment and perpetration among college students in the United States: A test of routine activities theory. *International Journal of Cyber Criminology*, *11*, 24-38. doi:10.5281/zenodo.495770

Williams, M., & Levi, M. (2015). Perceptions of the ecrime controllers: Modelling the influence of cooperation and data source factors. *Security Journal*, *28*, 252-271. doi:10.1057/sj.2012.47

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior*, *40*, 1119-1131.

doi:10.1080/01639625.2018.1461786

Wilson, A. (2015). A guide to phenomenological research. *Nursing Standard*, *29*(34), 38-43. doi:10.7748/ns.29.34.38.e8821

Wilson, V. (2016). Research methods: Interviews. *Evidence Based Library and Information Practice*, *11*(1S), 47-49. Retrieved from https://journals.library.ualberta.ca/

Wolfe, S. E., Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2016). Routine cell phone activity and exposure to sext messages: Extending the generality of routine activity theory and exploring the etiology of a risky teenage behavior. *Crime & Delinquency*, *62*, 614-644. doi:10.1177/0011128714541192

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

Ye, Y., & Lau, K. H. (2018). Designing a demand chain management framework under dynamic uncertainty: An exploratory study of the Chinese fashion apparel industry. *Asia Pacific Journal of Marketing and Logistics*, *30*, 198-234. doi:10.1108/APJML-03-2017-0042

Yeoh, P. (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance*, *25*, 196-208. doi:10.1108/JFRC-08-2016-0068

Yin, R. K. (2014). In V. Knight et al. (Eds.) *Case study research: Design and*

methods (5th ed.). Thousand Oaks, CA: Sage.

Yin, R. K. (2016). *Qualitative research from start to finish* (2nd ed.). New York, NY: Guilford.

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

Young, A., & Yung, M. (2017). Cryptovirology: The birth, neglect, and explosion of ransomware. *Communications of the ACM*, *60*(7), 24-26. doi:10.1145/3097347

Zulfikar, T., & Mujibur, R. (2018). Understanding own teaching: Becoming reflective teachers through reflective journals. *Reflective Practice*, *19*, 1-13. doi:10.1080/14623943.2012.1295933

Appendix: Interview Protocol

Participant Information:

Date: _____

Participant Identifier: _____

Introduction:

1. I will introduce myself to the participant and ensure I have a signed informed consent from the participant.
2. I will begin the interview with: Thank you for participating in this interview to explore effective strategies small business leaders use to address ransomware. I will audio record the interview for transcription purposes and take notes as the interview progresses. I will keep your identity and responses confidential, you can skip any of the interview questions, or stop the interview at any time. Do you have any questions for me before we start?
3. I will begin the audio recording now.
4. I will stay cognizant of any non-verbal cues, ask follow-up probing questions when appropriate, and conduct member checking during and post-interview.

Interview Questions

1. What strategies do you use to protect your information systems from ransomware?
2. How did you assess the effectiveness of your strategies for protecting your information systems from ransomware?
3. What were the key barriers to implementing the strategies for protecting your company from ransomware?
4. How did you address the key barriers to implementing the strategies for improving your protection against ransomware?
5. What other information could you add that might be applicable to the strategies that small business owners use to protect their information systems from ransomware?

Conclusion:

I will conclude the interview by thanking the participant for their participation and arrange for a convenient time for me to contact them to conduct a member checking interview.

Member Checking:

1. I will contact the participant by telephone and confirm if the participant agrees with the meanings I derived from the interview responses.
2. I will repeat the process of member checking until we agree with the meanings I derive from their responses.