2018

Exploring SME Vulnerabilities to Cyber-criminal Activities Through Employee Behavior and Internet Access

Jerry Allen Twisdale
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Jerry Allen Twisdale

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. Patricia Fusch, Committee Chairperson, Management Faculty
Dr. David Cavazos, Committee Member, Management Faculty
Dr. Craig Barton, University Reviewer, Management Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Small and Medium Enterprise Vulnerabilities to Cybercriminal Activities Through Employee Behavior and Internet Access

by

Jerry Allen Twisdale

MS, Florida Institute of Technology, 2013

BA, University of Alabama-Huntsville, 1984

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

August 2018

Abstract

Cybercriminal activity may be a relatively new concern to small and medium enterprises (SMEs), but it has the potential to create financial and liability issues for SME organizations. The problem is that SMEs are a future growth target for cybercrime activity as larger corporations begin to address security issues to reduce cybercriminal risks and vulnerabilities. The purpose of this study was to explore a small business owner's knowledge about to the principal elements of decision making for SME investment into cybersecurity education for employees with respect to internet access and employee vulnerabilities. The theoretical framework consisted of the psychological studies by Bandura and Jaishankar that might affect individual decision making in terms of employee risks created through internet use. This qualitative case study involved a participant interview and workplace observations to solicit a small rural business owner's knowledge of cybercriminal exploitation of employees through internet activities such as social media and the potential exploitation of workers by social engineers. Word frequency analysis of the collected data concluded that SME owners are ill equipped to combat employee exploitation of their business through social engineering. Qualitative research is consistent with understanding the decision factors for cost, technical support, and security threat prevention that SME organizational leadership and is the focus of this study as emergent themes. The expectation is that this study will aid in the prevention of social engineering tactics against SME employees and provide a platform for future research for SMEs and cybercriminal activity prevention.

Exploring SME Vulnerabilities to Cyber-criminal Activities Through Employee Behavior and Internet Access

by

Jerry Allen Twisdale

MS, Florida Institute of Technology, 2013

BA, University of Alabama-Huntsville, 1984

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

August 2018

Dedication

For my wife Teresa, and my daughters, Jennifer and Katharine. Without their patience and understanding, I would have never made this accomplishment.

Acknowledgments

A very warm and grateful thank you to my mentor and dissertation chair Dr. Patricia Fusch for accepting the role of the academic Captain and who kept this study journey leeward and above the forty-ninth parallel despite my many attempts to steer into the eye of a storm. And many thanks to Dr. David Cavazos, Dr. Sandra Kolberg, and Dr. Craig Bar

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

My study is about the status of the effects of social engineering for cybercrime and the potential impact on small and medium sized enterprises (SMEs) through employee vulnerabilities. For this study, the definition of SME is businesses with fewer than five employees as described by the U.S. International Trade Commission (ITC, 2010). The gap in the literature is related to two theories, where space transition theory (Jaishankar, 2007) represents the actions of the victim and the Bandura theory of selective moral disengagement (Bandura, 2009) that describes the effects of the perpetrator from the psychology aspects of the issue. Jaishankar (2007) illustrated that there is a phenomenon of personality and behavioral change he referred to as space transition theory . Bandura and Donner (2009, 2014), and Marcum, Jennings, Higgins, and Banfield (2014) indirectly addressed the Jaishanker theory from a psychological perspective in the form of moral disengagement and low self-control in the computer environment (Bandura, 2009; Donner et al., 2014).

These articles present the possibility that there is a gap in the literature where the psychology of the behavior and the intersection of the cybercriminal relatively unexplored aspect of the criminal activity. The exploration of this gap may create positive social change through the understanding of how these theoretical interactions between online users create the potential for cybercriminal activity. Exploring the nature of these theories and closing the literary gap might generate an understanding of how their application might serve to create positive social change.

The importance of the study as a contribution to positive social change is implicit in the fact that there appears to be little in the way of a literature connection on the link between Jaishankar's space transition theory, and the Bandura psychological studies behind the human behavior and the anonymity the internet provides. The pursuit of the research is to close the possible gap in the literature and it would be necessary to SME owners to understand the risk associated with on-line employee behavior and cyber-criminal social engineering activity in the form of taking advantage of the psychology behind moral disengagement and space transition theory.

Corporations now seek to create positive social change as an initiative to promote community well-being (Sharma & Good, 2013). My study might perpetuate this effort by alerting SME managers to the risks involved for the community through employee social media activities and online behaviors. Online behavior, social media activity, and social engineering are where the two theories intersect to create a paradox of psychological behavior inherent to internet social behavior in an anonymous virtual reality that potentially establishes the victim/victim environment. The perpetrator is the victim of the ease of the crime, and the victim is the victim of anonymity.

The internet supplies many opportunities for identity theft via internet activity and is a fear factor for e-commerce and customers, (Roberts, Indermaur, & Spiranovic, 2013).

The elements (or variables) of online behavior and anonymity are not addressed, which indicates that there is still confusion about on-line anonymity relative to cyber-criminal activity.

Social engineering is a misuse of influence to gain compliance. Muscanell, Guadagno, and Murphy (2014) submitted that affect is a construct of liking, authority, scarcity, social proof, reciprocity, and commitment. These are weapons in the arsenal of the social engineer to gain access to information. Again, what is missing is the anonymity involved on behalf of the social engineer and the victim. In other words, they do not really know each other because both are operating behind the curtain of anonymity. The victim gives up information with the mindset that the perpetrator has no knowledge of their identity, and, likewise, the offender operates under a condition of anonymity. Two unknown entities exchanging information has no victim (Muscanell et al., 2014).

At the center of the matter is the obtuse reasoning that anonymity breeds malice towards no one. In other words, if one does not know the victim, and one does not know the perpetrator, one would ask what damage could possibly occur. Human behavioral factors include a lack of knowledge of privacy issues with respect to cybercrime (Choras et al., 2015). Again, one can see that the anonymity variable is missing. Simons (2016) asserted that the theory of planned behavior, the theory of self-determination, and control theory might be useful in exploring why people might not be (at least on a conscious level) able to recognize the negative impacts of their actions on society or the community

(Simons, 2016). My study, through the exploration of these theories, might equip SME managers and employees with the knowledge required to assuage the abuses that could possibly occur because of lapses in judgment based on the Simons ideas that, in turn, could bring about positive social change. Further, Natarajan and Edwards (2016) asserted that extended ethical behavior with respect to business economics methodologies apply to everyone and therefore positively or negatively influence positive social change. This postulation includes employee behavioral activity online.

The accompanying literature review, specifically the works of Simons (2016), Natajaran, and Edwards (2016), Sharma, and Good (2013), and Jaishankar (2007) and Bandura (2001) serves to bring the focus of positive social change to Chapters 1 and 2 by marrying the author's (Bandura and Jaishankar) conceptualization of positive social change with the concepts inherent in my study. Weaving these author's theories into the study background and the research literature creates a literary environment where my study has the potential to promote positive social change.

Background of the Study

The study began from my interest in cybercriminal activity and attacks on corporations through breaches in security systems and how those violations occur. Recent media events about corporate cybersecurity breaches created an interest these breaches as well as leading to an interest in conducting this study. I ascertained from the literature review that there is a potential gap in the literature with respect to SME employees and a lack of knowledge about social engineering. This created an evolution of the study towards SMEs and business owner's awareness about employee online behavior. This gap in the literature led me to construct the problem statement, research question, and, subsequently, the significance of the problem.

My review of the literature revealed a tangled understanding of the value of information by business leadership. Shrock, Cole, and Shaffer (2011) conducted a survey of corporate CFOs and asserted that 70% viewed information technology as having adverse effects on the business objectives and 40% revealed that they believe there is an unknown, low, or negative return on information technology investments (Shrock et al., 2011), signifying a general lack of understanding by business leadership about potential loss of information at the corporate leadership level, and it is expected that this trend would continue at the SME ownership level.

The preponderance of the literature for IT governance has been oriented toward managing the physical components (hardware or software) of data management as opposed to the managing the actual data the artifacts contain (Tallon, Ramirez, & Short, 2013) but concerns about SMEs and employee vulnerabilities due to social engineering were not addressed. The purpose of this qualitative case study was to explore SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources.

Employees and users of new technologies might expose companies to cybersecurity breaches (Barbour, 2014) provided information on the security breaches with respect to employee misuse of computer systems but neither addressed the issue as a vulnerability with respect to the psychological elements involved with the SME employee vulnerabilities associated with online activities (Tarafadar et al., 2013). The possible issues with cybersecurity and SMEs are a relatively unexplored area (Tarafadar et al., 2013). This study will possibly open the area for further research once what is known by an SME manager about cyber security can be baselined.

Problem Statement

This study is an exploration into the potential for SME vulnerabilities to cyber-criminal activities through employee behavior and internet access. The general issue is cyber security information breaches are down streaming to small and mid-sized business with losses of 6% of their turnover in the UK (Hayes & Bodhani, 2013). According to a PEW report, there were occurrences of breaches of 7 million U.S. small businesses in 2014 (Raine et al., 2014).

Despite advances in security software, breaches in information systems persist (Steffee, 2014). According to the US Department of Justice, about seven percent of the total population aged sixteen or older, were victims of identity theft in 2014, and identity theft losses totaled $15.4 billion (BJS Bulletin December 2015). According to a study by Steffee based on Kasper-Sky lab’s report in 2014, 94% (based on 3,900 survey responses) of companies had experienced cyber security breaches over the previous year (Steffee, 2014).

In a request for research article, Tarafdar et al. (2013) acknowledged the issue and submitted that fifty to seventy-five percent of information security issues are the result of employee misuse and this misuse is the focus of this study because it is possible, based on the study, that on-line employee behavior may lead to risk to SMEs. While this is a valid assertion, it is the overarching issue of possible poor decisions at the management level with respect to employee education about social engineering that may create an opening for the misuse following with cyberattacks on SMEs to occur.

The problem is that cybersecurity losses among SMEs are growing, and there a lack of consensus as to the elements of a decision model for SME investment in cybersecurity (Chabinsky, 2013; Sangani & Vijayakumar 2012)**.** Sangani and Vijayakumar (2012) provided a comprehensive list of security threats and mitigations for SMEs; however, the study did not include the perspectives of the SME managers. New knowledge about the issue is obtainable through the study of organizational decision-making attributes and activities that might lead to exposure of private and proprietary data to cybercriminal activities. This study is aligning with a two-pronged approach to explore the possibility that the psychology of employee behavior in cyberspace and the cyberattacks relate to respect to internet access and employee vulnerabilities.

Purpose of the Study

The purpose of this qualitative case study was to explore SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources. The first method of data collection was an interview instrument based on 10 open-ended questions that explored the typical small business owners knowledge about internet security and employee access to the web. This study is an exploration into the potential for SME vulnerabilities to cybercriminal activities through employee behavior and internet access by discovering what small business owners feel about the phenomenon. In this qualitative case study approach, I conducted an interview with the proprietor of a small auto parts dealership located in north Alabama; the owner was a study participant and aided in exploring general knowledge of SME owners about cybersecurity.

Observation of the typical business activities and environment to understand potential vulnerabilities of employees and the companies associated with internet access is a secondary method of data collection (Yin, 2014). Through the interview questions and observations (see Appendix A), I established what was known by SME owners about internet access and online employee behavior. The second data collection source I used was journaling and field notes during direct observation of the business activities in an effort to explore SME vulnerabilities to cybersecurity threats as well as direct observation (see Table 1). Direct observation and journaling of the business activities took place over a period of 2 weeks and was used for data analysis. The interview results and the observations of the business activities provided two data points for comparison that may be validated or contradicted by the participant through member checking (see Appendix C) of my interpretations (Yin, 2014).

Research Questions

Research Question: What are the SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources?

Conceptual Framework

My intent in this study was to collect data through participant interview questions to align the study with the problem statement, the study purpose, and the gap in the literature. The statistics demonstrate that data breaches remain on the rise (Steffee, 2014) and the impact on society in terms of victims and costs of identity theft in 2014, identity theft losses totaled $15.4 billion (BJS Bulletin December 2015) and necessitated further research. Further framing support consists of the literature by Barbour who illustrates the employee and user factors and Tarafdar et al. who acknowledged the need for a study (Barbour, 2014; Tarafdar et al., 2013).

The conceptual framework of the study was a two-pronged application of the literature. The first prong is based on the works of Gold et al., Raine et al., Sangani and Vijayakumar, Schrock, Cole, and Shaffer, Steffee, and Tarafdar et al. to illustrate the cyberattack conceptual framework and the inclination for cybercriminals toward SMEs and social engineering attacks. These works demonstrate the nature of cyberattacks, the management perspective on information security investments, and the expected trend toward SME cyberattacks.

The second prong of the study was about the psychology involved in the employee side of vulnerabilities through space transition theory (see Appendix E) and moral disengagement (Bandura, 2009; Jaishankar, 2008). These approaches helped me to explore the psychological aspect of how employees may become victims from the mental side of the issue. Jaishanker (2007) developed space transition theory to explain behavioral changes in the transition from physical space to cyberspace. To extrapolate these behavioral changes to SME employee behavior, and in the online environment, a single case study design may provide a platform to advance the issue for further research. Bandura (2009) and Donner et al. (2014) indirectly addressed the Jaishanker theory from a psychological perspective in the form moral disengagement and low self-control as is applicable to the computer environment. These articles presented the possibility that there is a gap in the literature where the psychology of the behavior and the intersection of the cybercriminal activity may not have received a thorough exploration considering the nature of space transition theory, moral disengagement, and low self-control.

My dissertation study on the SMEs (small and medium enterprises) business owner knowledge about cyber security threats is based on the literature review and the expected theme would be that SME business owners and employees should not have the background and knowledge necessary to adequately protect the business from cyberattacks and threats (Hutchings, 2012; Tarafdar et al., 2013). It is an expectation that SMEs will become more vulnerable to cyber threats with the sealing of the cracks in the large corporation security walls (Hayes & Bodhani, 2013) and should, therefore, prepare for the anticipated new cyberattack approaches.

Cybersecurity concerns appear to be a limitation of cyberattacks from outside of the business with little consideration for cyberattacks and risks (social engineering) from within the firm. There is an inclination to trust employees inside the company according to the literature assertions (Hutchings, 2012; Tarafdar et al., 2013; Willison & Warkentin, 2013; Zhurin, 2015) that there is a general lack of awareness in SME enterprises with respect to the risk from insider cyberattacks through social engineering.

There is an expectation that two established theories will potentially converge into a new theory based on the data collection expected results. Space transition theory (Jaishankar, 2008) explains the vulnerabilities of employees to cybercrime through internet access, and moral disengagement (Bandura, 2009) might explain the cybercriminal ability to dismiss the morality of an action based on internet anonymity properties. From these two theories, a third theory that may emerge from the study is that space transition theory and moral disengagement combine to create a new theory that explains vulnerabilities from both the victim and the criminal's perspectives that create the environment for crime.

Conceptually, it is important to explore what the participant (SME owner) knows and does not know with respect to employee risk and access to the internet. The literature has asserted that SME managers will not realize this danger (Tarafdar et al., 2013). Based on the research assertions, it is necessary to explore an actual randomly selected case to understand what SME owners know about computer security.

The participant that I selected is the proprietor of a small business that services a rural community for mechanical parts and supplies. The chosen site was in north Alabama. The selection of the participant was also based on the Yin (2014) criteria for a Type 1, holistic single-unit of analysis. In this case, the analysis may verify or possibly invalidate the literature assertion that SME owners lack the knowledge necessary to recognize to cybersecurity threats the business (Hutchings, 2012; Tarafdar et al., 2013). Since the SME is a family-owned, rural enterprise, the data analysis could reveal SME cybersecurity knowledge with a unique opportunity to explore a critical test of the literature assertion (Yin, 2014).

Nature of the Study

The nature of the study was a qualitative research method with a case study approach to explore how small business owners feel about potential vulnerabilities due to employee internet access (Eisenhardt, 1989; Yin, 2013). Qualitative research is consistent with understanding the decision factors that SME organizational leadership use that is the focus of this study. A quantitative research design is unavailable because the statistical data required to support the research for SMEs (Threat Stats, NA, 2015) do not exist, and to obtain the data would render the study impossible to complete in a timely manner. However, this study has the potential to launch other research opportunities to get the quantitative data for further study. The study design should assist in consensus building for SME management as to the elements of a decision model for SME investment in cybersecurity education for employees with respect to online behavior.

The other four qualitative approaches are would be incompatible with the study because a historical approach would not adequately capture the dynamics of cybersecurity intrusions, as it would be about an individual story. A stand-alone phenomenological study would not be feasible because the focus would be too narrow for the study. A grounded theory would not be economically or temporally practical because of the extensive amount of time required and a lack existing data to support the research, and an ethnographical study represents cultural differences may or may not manifest itself in cyberattacks and might require a separate study.

The best qualitative approach would be an epistemological instrumental case study approach. An epistemological study is not a recommendation because the study is an attempt to learn the reality of how SME owners and managers make decisions about cybersecurity and protection of information (Andrade, 2009). I chose an instrumental case study approach because the approach is appropriate to answer the research question and aligns with the framework developed by the two theories. Since I made an adjustment to the research question to envelop the theories, I selected a single case study because, in the SME environment, the potential for generalization of a single case study as the instrument to represent the population of SMEs in their entirety is possible.

The second-best approach might be a collective case study approach; however, this method is better suited where multiple case studies might provide different perspectives on the issue. Since the study is about the general treatment of information security in SMEs, I do not expect multiple case studies to provide contradicting or additional data to the study. The research question is as follows: What are the SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources.

The third choice is a grounded theory study. Grounded theory sets the stage for new or emergent theory or theories (Andrade, 2009). In my study, although in their infancy, current approaches frame the phenomenon (Bojanc & Jerman-Blažič, 2013; Jaishankar, 2008).

For this case study, the Yin approach to case study description is the best choice Yin, 2013) with an analytical approach to explanation building (Yin, 2013). Since my expectation is to learn why SMEs may be vulnerable to future cybersecurity breaches, the expectation is also the case study research will offer links to the rationale for the knowledge deficit, if any, and provide insight into the connection between business risk exposure by employee internet access behavior and the threat of cybersecurity breaches.

A single case study using a methodological triangulation approach with multiple sources is necessary to provide validity and reliability to the study (Yin, 2014). Triangulation enhancement is through member checking (see Appendix C) of the analytical results, peer review, and supporting peer-reviewed literature (Carter et al., 2014). Assurance of data validity occurs by triangulation of the data (Carter et al., 2014). Peer review, member checking, and the use of reflective journal verification support content validity (Carter et al., 2014). Attention to ethical concerns for data collection is under the prevue of the Institutional Review Board (IRB) for data gathering and in the ethics section of the dissertation to protect participants. The theory aligns with the qualitative approach because the study design is a meaning-making endeavor (Mariotto, Pinto Zanni & De Moraes, 2014). Both theories could be, but have not been, applied to the study research question. In other words, I attempted to explore the meaning of the research question to the participant so that the theory framework will demonstrate that it applies as expected.

The qualitative approach aligns with the interview method because of the desire to base the study on real world observations for meaning making. The interview process aligns with the research question by asking the participant questions in person and recording the responses while observing the participan**t.** The frame of the case study is in support of the research questions.

Definitions

BCI (*brain computer interface*): A neural feedback loop that could be an interpretation by a computer or the incorporation of human intentions into adaptive software (Huang & Miranda, 2015).

Bot-master: A cyber attacker who uses available technology to infiltrate business and government computers with spam, attack servers and steal information for a price (Décary-Hétu & Dupont, 2013)

Cyber-physical system (*CPS*): A CPS includes sensors, monitoring, and control features embedded in electronics devices to connect cybersystems to the physical world (Ali, Anwar, & Hussain, 2015).

Dark web: The dark or deep web is a layer of the internet considered to be useful for criminal activities. Access to the dark web is by use of TOR (the onion ring) or other anonymity software which conceals the identity of the user (Bradbury, 2014).

Detert moral disengagement scale: A qualitative instrument developed to measure shame and guilt characteristics (Johnson & Connelly, 2016).

Electroencephalography: A measure the human to computer reaction state by EEG (electroencephalography) to understand ways to mimic human to human interactions with a human to computer interactions (Huang & Miranda, 2015).

Honeypot: A website developed to mimic a legitimate website to attract attackers for the purposes of discovering vulnerabilities in the legitimate website (Chang, Venkatasubramanian, West, & Insup 2013).

Moral disengagement: The personal restructuring of self-sanctions to justify inhumane actions through reassignment of blame and excluding personal responsibility, positive restructuring of language, and dehumanization of the victim's dehumanization of the victims (Bandura, 2009).

Man at the end (*MATE*): The attacker (MATE) gains access to a systems hardware or software either by direct contact or remotely which is known as RMATE (Adnan et al., 2015).

Phishing: The gathering of information through deception (Jansson & von Solmes, 2013).

Self -regulation: The concept that from an early age, self-regulation is adoptable through reference values such as goals and social norms (Denissen, Aken, Penke, & Wood, 2013).

Social engineering: The exploitation of weaknesses by the manipulation of the victim into performing actions that benefit that attacker (Flores & Ekstedt, 2016)

Small and medium enterprise (*SME*): An SME is businesses with fewer than five employees as described by the U.S. International Trade Commission (ITC, 2010).

Space transition theory (see Appendix E): Jaishankar's seven conditions under which the phenomenon of space transitions might occur (a) repressed criminal behavior in the physical space may manifest itself in cyber-space should the person be inclined to do so. Personal status and position might otherwise prevent the same individual from committing the crime in the physical world, (b) the choice to commit cybercrime is enabled by dissociative anonymity, lack of deterrence and flexibility of identity in cyberspace, (c) criminal behavior may be imported to physical space and exported to cyber-space, (d) random accessibility to cyber-space and the dynamics of spatial/temporal time allows for a natural escape mechanism, (e) strangers may connect on the internet to commit a crime in physical space and acquaintances in physical space might connect to commit crimes on the web, (f) closed society members are more likely to commit internet crimes than members of an open society, and (g) there can be a conflict of morality, norms, and values in the physical world and cyberspace (Jaishankar, 2007).

The onion ring (*TOR*): Software developed for the purposes of concealing the identity of the users I.P. (internet protocol) address (Bradbury, 2014).

Assumptions

The assumptions for my study are that the participant's knowledge will align with the assertion of the literature that he will not have the experience and knowledge base to recognize cyber-security threats to his business (Hutchings, 2012; Tarafdar et al., 2013).

A further assumption is that the participant will be basing his knowledge on the trust of actual lived experiences (Grant, 2014), in other words, if the participant had not experienced a cyber security breach, he may operate with a lack of knowledge about existing threats like social engineering attacks, and because the member may not be aware that potential cyber-security issues exist within his business, does not mean that they do not currently exist nor have they existed in the past. It only means that the participant is unaware of them. Another assumption is that the typical SME owner is more knowledgeable about cyber-security issues that the literature suggests. It is my expectation that the analysis of the collected data will either confirm or refute the assertion. These assumptions are necessary to the study because the literature authors have asserted them to be true. To either validate or invalidate the assertions in an unbiased way, it is necessary to collect the data and perform the analysis as if the assertions are true to eliminate any potential bias in the data collection and analysis.

Scope and Delimitations

The scope of my study is time bound by the cybersecurity technology available at the time of the study. Future advances in cybersecurity technology may reduce or eliminate some areas of concern with respect to current cybersecurity issues. Another limit to the study was the single case study design methodology, where more case studies may be necessary. In the interest of completing the research as well as limitations in funding, the single case study design supports the literature assertion that SME owners would not have the experience to understand cybersecurity threats to the business (Hutchings, 2012; Tarafdar et al., 2013). Given this assertion, it is evident that further case studies should reveal the same results as the single case study provided herein. The single case study presented here is necessary to capture the extent to which relevant knowledge by SME owners to verify or invalidate the literature assertion and to bound the experience of the SME owners by direct interview and observations (Barratt, Choi, & Li, 2011).

Limitations

The limitations of my study are that my study is outside of a laboratory environment. These limitations result in a lack of experimental control over the research and are an attribute of passive observations in the study environment (Brutus, Aguinis, & Wassmer, 2012). Mitigation to this limitation is the addition of interview questions that serve to reinforce the passive observations. For example, the participant might feel that his business is impervious to cyberattacks based on the lived experience of never encountering such attacks. However, passive observations might reveal that there are physical lapses in the business security environment such as unfettered access to computers that put the company at risk to outside threats. In an informal business environment such as the SME typical environment, security lapses might not be noticeable by those that do not have formal training regarding the potential risks that such an informal business environment might create. This study also has the limitation of a single case study design. Further exploration of SMEs that house customer information might lead to new findings. The study may be generalizable to those SMEs that do not retain a customer information database.

Significance of the Study

A lack of consensus exists in the literature with respect to SMEs about decision-making and resource allocation relative to cybersecurity protection (Chabinsky, 2013). Chabinsky asserted that SMEs are an expected target of cybersecurity breaches and that SMEs will be on the front line for developing cybersecurity solutions (2013). My study will potentially be a contribution to those solutions by including SME owners in those prospective decisions and solutions. Barbour (2014) addressed the problem from the perspective of employees and users of the protected data and the fact they may expose the data to certain risks with respect to new technologies. While this is true, this does not negate the responsibility of management to ensure that decision factors do not allow the problem to occur (Gold, 2014). Ex-hacker Kevin Mitnick pointed out that it only takes one bad business decision by someone in an organization to create an opening for security breaches and illustrated the need for a study to explore the connection between user thinking and cybercriminal attack methods (Gold, 2014). At this point, the literature that addressed the understanding of the value of information and SME owner’s potential perspectives diverged into separate paths for corporate vulnerabilities and SME vulnerabilities for cyberattacks.

To-establish significance of the issue, Hayes and Bodhani (2013) asserted that security breaches of SMEs in the UK accounted for 6% of their financial turnover and is considerable along with Raine et al. (2014) in a Pew Report article, which revealed that 7 million small businesses suffered security breaches in 2014. These statistics present affirmation that Chabinsky's assertion that SMEs are expected targets of cybercrime.

Development of a comprehensive list of threats and mitigations to establish the potential impact of cybercrimes on SMEs for assessment by Sangani and Vijayakumar (2012) creates the need for an SME study. But it is necessary to study SMEs to evaluate the risk to SME vulnerability with respect to cyberattacks through social engineering as well as capture the perspectives of SME owners. An approach to the the gap in the literature in the development of a metric for cybersecurity decision-making processes was provided by Yasasin and Shren (2015) but again, lacked the inclusion of an SME owners perspective. Steffee (2014) provided statistical data on business cybersecurity breaches in 2014 that supported the need for further exploration into the phenomenon There remains the necessity to capture the typical SME owner's knowledge about what cybersecurity threats he thinks he may face and the SME cybersecurity threats that exist. In other words, there has been a literature assessment on what kind of data collection is necessary from SMEs, but the data is evidently not available.

Beyond the research on cyber threats, the literature on the psychology of the victimized employees requires exploration to marry the concepts of cyber threats and employee victimization through social engineering. The importance of my study is implicit in the fact that there appears to be little in the way of a literature connection about the link between Jaishankar’s space transition theory, the psychological studies of human behavior and the anonymity the internet provides when considering social engineering and cybercrime. My study is necessary to close the possible gap in the literature. This study would be relevant to SME owners to understand the risk associated with employee online behavior and cybercriminal social engineering activity in the form of taking advantage of the psychology behind moral disengagement and space transition theory.

Significance to Practice

Corporations seek to create positive social change as an initiative to promote community well-being (Sharma & Good, 2013; Natarajan & Edwards, 2016). My study might perpetuate this effort by alerting SME managers as to the risks involved to the community through employee social media activities and online behaviors. This is where the two theories intersect to create a paradox of psychological behavior inherent to internet social behavior in an anonymous virtual reality that potentially creates the victim/victim environment. The perpetrator is the victim of the ease of the crime, and the victim is the victim of and by anonymity.

Significance to Theory

Since the problem is that cybersecurity losses among SMEs are growing and there is a lack of consensus as to the elements of a decision model for SME investment in cybersecurity (Chabinsky, 2013; Sangani & Vijayakumar 2012)**.** Sangani and Vijayakumar provided a comprehensive list of security threats and mitigations for SMEs; however, the authors of the studies did not include the perspectives of the SME managers. New knowledge about the issue is obtainable through the study of organizational decision-making attributes and activities that might lead to exposure of private and proprietary data to cybercriminal activities. This study is aligning with a two-pronged approach to explore the possibility that the psychology of employee behavior in cyberspace and the cyberattacks relate to respect to internet access and employee vulnerabilities using the Bandura and Jaishankar theories.

Significance to Social Change

My study is about the status of the effects of social engineering for cybercrime and the potential impact on small and medium sized businesses through employee vulnerabilities. A frame for the gap in the literature contains two theories, where space transition theory (Jaishankar, 2007) represents the actions of the victim, and the Bandura theory of selective moral disengagement (Bandura, 2009) that possibly represents the actions of the perpetrator from the psychology aspect of the issue, Jaishankar illustrated that there is a phenomenon of personality and behavioral change he referred to as space transition theory (2007). Bandura and Donner et al. indirectly addressed the Jaishanker theory from a psychological perspective in the form of moral disengagement and low self-control in the computer environment (Bandura, 2009; Donner et al., 2014). These articles presented the possibility that there is a gap in the literature where the psychology of the behavior and the intersection of the cybercriminal activity may require further exploration, and the exploration of this gap may create positive social change through the understanding of how these theoretical interactions between online users create the potential for cybercriminal activity. Exploring the nature of these theories and shuttering the literary gap might generate an understanding of how their application might serve to create positive social change.

The importance of the study as a contribution to positive social change is implicit in the fact that there appears to be little in the way of a literature connection on the link between Jaishankar's space transition theory, and the Bandura psychological studies behind the human behavior and the anonymity the internet provides (see Appendix E). My study attempts to close the possible gap in the literature, and it would be important to SME owners to understand the risk associated with employee online behavior and cybercriminal social engineering activity in the form of taking advantage of the psychology behind moral disengagement and space transition theory. Sharma and Good (2013) asserted that corporations now seek to create positive social change as an initiative to promote community well-being. My study might perpetuate this effort by alerting SME managers as to the risks involved to the community through employee social media activities and online behaviors. This is where the two theories intersect to create a paradox of psychological behavior inherent to internet social behavior in an anonymous virtual reality that potentially creates the victim/victim environment. The perpetrator is the victim of the ease of the crime, and the victim is the victim of anonymity.

Summary and Transition

My study is about the status of the effects of social engineering for cybercrime and the potential impact on small and medium sized businesses through employee vulnerabilities. The gap in the literature is within the envelope of two theories, where space transition theory (Jaishankar, 2007) represents the actions of the victim and the Bandura theory of selective moral disengagement (Bandura, 2009) that represents the actions of the perpetrator from the psychology aspects of the issue. Jaishankar illustrated that there is a phenomenon of personality and behavioral change he referred to as space transition theory (2007). Bandura and Donner et al. indirectly addressed the Jaishanker theory from a psychological perspective in the form of moral disengagement and low self-control in the computer environment (Bandura, 2009; Donner et al., 2014).

The importance of the study as a contribution to positive social change is implicit in the fact that there appears to be little in the way of a literature connection on the link between Jaishankar's space transition theory, and the Bandura psychological studies behind the human behavior and the anonymity the internet provides. The pursuit of my study is to close the possible gap in the literature. It would be important to SME owners to understand the risk associated with employee online behavior and cybercriminal social engineering activity in the form of taking advantage of the psychology behind moral disengagement and space transition theory. Online behavior, social media activity, and social engineering are where the two approaches intersect to create a paradox of psychological behavior inherent to internet social behavior in an anonymous virtual reality that potentially creates the victim/victim environment. The perpetrator is the victim of the ease of the crime, and the victim is the victim of anonymity.

The internet supplies many opportunities for identity theft via internet activity and is a fear factor for e-commerce and customers, (Roberts et al., 2013). The factors (or variables) of online behavior and anonymity are not addressed which indicates that there is still confusion about online anonymity relative to cybercriminal activity. At the center of the matter, is the obtuse reasoning that anonymity breeds malice towards no one. In other words, if one does not know the victim, and one does not know the perpetrator, what damage could possibly occur?

Human behavioral factors only include a lack of knowledge of privacy issues with respect to cybercrime (Choras et al., 2015). Again, we see that the anonymity variable is missing. Simons (2016) noted that the theory of planned behavior, the theory of self-determination and control theory might be useful in exploring why people might not be (at least on a conscious level) able to recognize the negative impacts of their actions on society or the community. My study, through the exploration of these theories, might equip SME managers and employees with the knowledge required to assuage the abuses that could possibly occur because of lapses in judgment based on the Simons ideas that in turn, could bring about positive social change. Further, Natarajan and Edwards (2016) asserted that extended ethical behavior with respect to business economics methodologies apply to everyone and therefore positively or negatively influence positive social change. This postulation includes employee behavioral activity online.

The following literature review, specifically the works of Simons, Natajaran, and Edwards, Sharma and Good, Jaishankar, and Bandura, has served to bring the focus of positive social change to my dissertation chapters one and two by marrying the author's conceptualization of positive social change with the concepts inherent in my study. Weaving the author's theories into the study background and the research literature creates a literary environment where my study has the potential for positive social change.

Chapter 2: Literature Review

The problem is that cybersecurity losses among SMEs are growing and there is a lack of consensus as to the elements of a decision model for SME investment in cybersecurity (Chabinsky, 2013; Sangani & Vijayakumar 2012)**.** Sangani and Vijayakumar (2012) provided a comprehensive list of security threats and mitigations for SMEs; however, the authors of the studies did not include the perspectives of the SME managers. Exploration of new knowledge about the issue through the study of SME organizational decision-making attributes and activities that might lead to exposure of private and proprietary data to cybercriminal activities might provide answers to my research question.

Alignment of this study uses a two-prong approach to explore the possibility that the psychology of employee behavior in cyberspace and the cyberattacks and there is possibly a relationship with respect to internet access and employee vulnerabilities. One limitation to cybersecurity concerns appears to be cyberattacks from outside of the business with little consideration for cyberattacks and risks (social engineering) from within the firm. There is an inclination to trust employees inside the firm according to the literature assertions (Hutchings, 2012, & Tarafdar et al., 2013, Willison & Warkentin, 2013, Zhurin, 2015) that there is a general lack of awareness in SME enterprises with respect to the risk from insider cyberattacks through social engineering.

It is my expectation that two established theories may potentially converge into a new theory based on the data collection expected results. Space transition theory (Jaishankar, 2008) explains the vulnerabilities of employees to cybercrime through internet access, and moral disengagement (Bandura, 2009) might explain the cybercriminal ability to dismiss the morality of an action based on internet anonymity properties. From these two theories, a third theory that may emerge from the study is that space transition theory and moral disengagement combine to create a new theory that explains vulnerabilities from both the victim and the criminal's perspectives that create the environment for crime.

The purpose of this qualitative case study was to explore SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources. This chapter is divided into three major sections: the literature review search strategy, the study conceptual framework, and the literature review. The literature review is divided into eleven sub-sections that explore in detail the literature research that supports the study.

Literature Search Strategy

My research of the literary studies in the Walden Library databases consisted of behavioral and psychological research, the Psych Info and Social Science databases. Search terms were *social cognitive theory, Albert Bandura, moral disengagement, space transition theory, Jaishankar*, *low self-control, risky behavior, internet behavior, and* *self-regulation, personnel psychology, cyber-victimization, moral agency*, *behavior, control theory, psychopath, stress,* and *social networking,* using Boolean word searches.

For the technical peer-reviewed databases searches of the ACM digital library, Information systems and Information Technology Databases, IEEE databases, computer and applied sciences databases using the search terms *cybersecurity, cybersecurity physical systems, cloud computing, social media, social engineering, database security, intrusion, cybercrime losses, SME cybercrime, fraud, malware, information security management, dark web, vulnerabilities, cybercrime, it ,internet, password, login, it policies, computer threats, phishing, risk management, anonymity, insider threat, internet scams, identity theft, deception,* and *security breaches.*

To obtain government supporting documentation, I used Google Scholar searches through the Walden database and at times using Google stand-alone and Academic Search Complete with the search terms *USGOV, Stats, Computer Crimes* as well as Thoreau Multi-database searches. For the technical research design elements of the study, I used the Walden database Academic Search Complete and acquired the necessary textbooks. The search terms used to obtain research methodologies and design applications were *single case study research*, *qualitative research, research methodologies, research ethics,* and *reliability.*

Conceptual Framework

The intent of the research question was to collect data through participant interview questions, observations, reflexive notes and member checking to align the study with the problem statement, the study purpose, and the gap in the literature. The statistics demonstrate that data breaches remain on the rise (Steffee, 2014) and the impact on society in terms of victims and costs of identity theft in 2014, identity theft losses totaled $15.4 billion (BJS Bulletin December 2015), which necessitated further research. Further framing support consists of the literature by Barbour (2014) who illustrates the employee and user factors and Tarafdar et al. (2013) who acknowledged the need for further study.

The conceptual framework of the study is a two-pronged application of the literature. The first prong is based on the works of Gold et al., Raine et al., Sangani and Vijayakumar, Schrock et al., Steffee, and Tarafdar et al. to illustrate the cyberattack conceptual framework and the inclination for cybercriminals toward SMEs and social engineering attacks. These works demonstrate the nature of cyberattacks, the management perspective on information security investments, and the expected trend toward SME cyberattacks.

The second prong of the study is about the psychology involved in the employee side of vulnerabilities through space transition theory and moral disengagement (Bandura, 2009; Jaishankar, 2008). These approaches explore the psychological aspect of how employees may become victims from the mental side of the issue. Jaishanker developed space transition theory to explain behavioral changes in the transition from physical space to cyberspace (2007). To extrapolate these behavioral changes are to SME employee behavior, and the online environment a single case study design may provide a platform to advance the issue. Bandura and Donner et al. indirectly addressed the Jaishanker theory from a psychological perspective in the form moral disengagement and low self-control application to the computer environment (Bandura, 2009; Donner et al., 2014). These articles presented the possibility that there is a gap in the literature where the psychology of the behavior and the intersection of the cybercriminal activity may not have received a thorough exploration considering the nature of space transition theory, moral disengagement, and low self-control.

My dissertation study on the SMEs (small and medium enterprises) business owner knowledge about cybersecurity threats is based on the literature review and the expected theme would be that SME business owners and employees should not have the background and knowledge necessary to adequately protect the business from cyberattacks and threats (Hutchings, 2012; Tarafdar et al., 2013). The expectation is that SMEs will become more vulnerable to cyber threats as the cracks in the large corporation security walls seal (Hayes & Bodhani, 2013) and should, therefore, be ready for the anticipated new cyberattack approaches.

Cybersecurity concerns appear to be about cyberattacks from outside of the business with little consideration for cyberattacks and risks (social engineering) from within the firm. There is an inclination to trust employees inside the company, and there is a general lack of awareness in SME enterprises with respect to the risk from insider cyberattacks through social engineering (Hutchings, 2012; Tarafdar et al., 2013; Willison & Warkentin, 2013 and Zhurin, 2015).

Because of the study theme, it is an expectation that two established theories will potentially converge into a new theory based on the data collection expected results. Space transition theory (Jaishankar, 2008) explains the vulnerabilities of employees to cybercrime through internet access, and moral disengagement (Banduras, 2009) might explain the cybercriminal ability to dismiss the morality of an action based on internet anonymity properties. From these two theories, a third theory that may emerge from the study is that space transition theory and moral disengagement combine to create a new theory that explains vulnerabilities from both the victim and the criminal's perspectives that create the internet environmental argument for criminal activity.

Conceptually, it is important to explore what the participant (SME owner) knows and does not know with respect to employee risk and access to the internet. The literature has asserted that SME managers will not realize that chance (Tarafdar et al., 2013). Based on the research assertions, it is necessary to explore an actual randomly selected case to understand what SME owners know about computer security.

The participant selection is the proprietor of a small business that services a rural community for farm equipment and automobile mechanical parts and supplies. The site location is in North Alabama and selection was due to proximity to my home and the applicability of the study itself. The participant selection is based on the Yin criteria for a type 1, holistic single-unit of analysis (Yin, 2014). In this case, the analysis may verify or possibly invalidate the literature assertion that SME owners lack the knowledge necessary to recognize to cybersecurity threats the business (Hutchings, 2012; Tarafdar et al., 2013). Since the SME is a family owned, rural enterprise, the data analysis could reveal SME cybersecurity knowledge with a unique opportunity to explore a critical test of the literature assertion (Yin, 2014).

Literature Review

Selected articles pertaining to the SME cybersecurity research present a plethora of concerns for cybersecurity in SMEs. The basis that one bad business decision by someone in an organization can create an opening for security breaches (Gold, 2014) illustrated the need for a study to explore the connection between user thinking and cybercriminal attack methods employee's and users of new technologies might expose companies to cybersecurity breaches (Barbour, 2014). SMEs are an expectation with respect to being on the front line of cybersecurity breaches as well as on the front line for solutions and demonstrate the necessity of further research (Chabinsky, 2013).

To establish significance of the issue, security breaches of SMEs in the UK account for 6% of their turnover (Hayes & Bodhani, 2013) is a consideration along with Raine et al. who stated that a Pew Report established that 7 million small businesses suffered security breaches in 2014 (Raine et al., 2014). A comprehensive list of threats and mitigations for SME' to establish the potential impact to SMEs is provided by Sangani, and Vijayakumar (Sangani, and Vijayakumar, 2012) and Shrock et al. provided statistical data on how organizational leadership views information technology investments (Schrock et al., 2011). Steffee provided statistical information on business cybersecurity breaches in 2014 (Steffee, 2014) and again, establishes the need for the study. Tarafadar et al. provided information on the security breaches with respect to employee misuse of computer systems (Tarafdar et al., 2013). Yasasin and Shren provided a decision-making metric for organizations to assist in cybersecurity protection (Yasasin & Schren, 2015). Beyond the literature on cyber threats, research on the psychology of the victimized employees requires exploration to marry the concepts of cyber threats and employee victimization.

From the psychology aspect of the issue, Jaishankar illustrated that there is a phenomenon of personality and behavioral change he referred to as space transition theory .Jaishankar provided the seven space transition theory characteristics that may factor in for online behavioral changes (a) people with repressed criminal inclinations in the physical world might act upon them in cyberspace, (b) Anonymity the cyber world provides freedom from deterrence in cyberspace, (c) freedom to export and import cybercriminal activity between cyber and physical space (identity theft for example), (d) intermittency of cyberspace offers an escape route (the offender controls the access and ingress, (e) stranger unification in cyberspace to commit crimes (as well as in the physical world) communication is exponentially greater over the physical world, (f) closed society access to commit crimes as opposed to an open society access creates the likelihood of cybercriminal activity from the closed society and, g) norms and values conflicts between cyberspace and the physical world creates an environment where those conflicts might manifest themselves.

Bandura and Donner et al. addressed the Jaishanker theory from a psychological perspective in the form moral disengagement and low self-control in the computer environment (Bandura, 2009: Donner et al., 2014). These articles presented the possibility that there is a gap in the literature where exploration of the psychology of the behavior and the intersection of the cybercriminal activity may be lacking depth. Bandura defined moral disengagement as the personal restructuring of self-sanctions to justify inhumane actions through reassignment of blame and excluding personal responsibility, positive restructuring of language, and dehumanization of the victims (Bandura, 2002). Of interest to my study is the dehumanization of the victims and cybercriminal activity (Bandura, 2009; Donner et al., 2014).

The importance of the study is implicit in the fact that there appears to be no literature connection on the link between Jaishankar's space transition theory and the psychological studies of the human behavior and the anonymity the internet provides. This study will pursue this gap in the literature. This would be relevant to SME owners to understand the risk associated with employee online behavior and cybercriminal social engineering activity in the form of taking advantage of the psychology behind moral disengagement and space transition theory.

While some researchers evaluated threats from a hardware/software concern (Tallon et al., 2013), others addressed the employee and user aspect (Barbour, 2014) and a cross-sectional approach relative to the nature of security threats in the online environment (Sangani & Vijayakumar, 2012). The existing body of knowledge is sparse when it comes to the actual elements of a rational decision model for SME investment in cybersecurity and employee awareness training for social engineering. This disparity in the literature leads to the initiation of the study to explore SME cybersecurity vulnerabilities and employee internet access.

At the center of the matter is the obtuse reasoning that anonymity breeds malice towards no one. In other words, if one does not know the victim, and one does not know the perpetrator, no damage could possibly occur. Choras et al. submitted that human behavioral factors only include a lack of knowledge of privacy issues with respect to cybercrime (Choras et al., 2015). Again, the anonymity variable is missing. Simons asserted that the theory of planned behavior, the theory of self-determination and control theory might be useful in exploring why people might not be (at least on a conscious level) able to recognize the negative impacts of their actions on society or the community (Simons, 2016).

My study, through the exploration of these theories, might equip SME managers and employees with the knowledge required to assuage the abuses that could possibly occur because of lapses in judgment based on the Simons ideas that in turn, could bring about positive social change. Further, Natarajan and Edwards asserted that ethical behavior with respect to business economics methodologies is applicable to everyone. The method could positively or negatively influence positive social change. This postulation may include employee behavioral activity online.

This literature review, specifically the works of Simons et al. and Sharma and Good, Jaishankar, and Bandura, has served to bring the focus of positive social change to my dissertation chapters one and two by marrying the author's conceptualization of positive social change with the concepts inherent in my study as it progresses. Weaving the author's theories into the study background and the research literature creates a literary environment where my study has the potential for positive social change. To answer the research question and because the literature has asserted that SME owners lack the experience to understand the potential exposure to cybersecurity attacks (Hutchings, 2012; Tarafdar et al., 2013), it is necessary to explore the literature for what the expected risks to an SME owner might be. The literature review is divided into nine major sections and twelve sub-sections that detail the obstacles and potential solutions to SME business computer cybersecurity issues.

Space Transition Theory and Anonymity

There are seven postulates based on Jaishankar's space transition theory; (a) repressed criminal behavior in the physical space may manifest itself in cyber-space should the person be inclined to do so. Personal status and position might otherwise prevent the same individual from committing the crime in the physical world, (b) the choice to commit cybercrime is enablable by dissociative anonymity caused by a lack of deterrence and flexibility of identity in cyberspace, (c) criminal behavior may be imported to physical space and exported to cyber-space, (d) random accessibility to cyber-space and the dynamics of spatial/temporal time allows for a natural escape mechanism, (e) strangers may connect on the internet to commit a crime in physical space and acquaintances in physical space might connect to commit crimes on the web, (f) closed society members are more likely to commit internet crimes than members of an open society and, (g) there can be a conflict of morality, norms, and values in the physical world and cyberspace (Jaishankar, 2007). Bradbury addressed the anonymity concern that is of interest to SME cybersecurity.

Among the concerns relevant to cybersecurity is the issue of anonymity on the internet (Bradbury, 2014). The dark or deep web exists on alternate layers of the internet constructed by groups with a desire to maintain anonymity. The use of this aspect of the dark web can be for good such as getting around censorship in dictatorships, and bad activities such as supporting child pornography, hacking and sales of weapons and drugs. Software supports these layers such as TOR (The Onion Ring) that allows anonymous user activity through the advent of onion routing developed by the US Naval Laboratory. This ring process uses several thousand machines to route encrypted information to the destination which makes the origin of the data challenging to trace (Bradbury, 2014). The use of this technology might be to obtain SME owner and/or employee information through e-mail or social media by allowing accurate data to be a one-way exchange. For example, the dark web anonymous user may use phishing techniques (a possible false front) to trick the victim into releasing truthful information such as user IDs and passwords.

Another software platform developed for the purposes of anonymity is the Dissent program. With the realization that the use of software programs such as TOR could be to mask the identity of users that were out to use the anonymity feature of the software for nefarious purposes such as denial of service and Sybil attacks, the Dissent software package sought to alleviate this concern by offering a feature of provability for legitimate users and identifying users with nefarious intentions (Syta et al., 2014).

The DW (dark web) is becoming a catch phrase for cybercriminal activity on the internet (Epiphaniou, French, & Maple, 2014). Epihpaniou et al. explored the application of the DW for P2P clients and explained the properties such as IP address obfuscation that makes detecting these activities difficult. Of particular interest to my cybercriminal, the study is the ability to hide IP addresses for nefarious purposes. The authors could develop a table outlining the risks associated with DW activities from the perspectives of; DW members, (receiver), DW members (senders/receivers), DW victims, Casual visitors, and covert police. Although the study could illustrate the community of the DW atmosphere, the ability to use the information to prevent DW activity was unclear. The methodology was a quantitative analysis using an algorithm to provide a map of the DW activity and how it may operate undetected by law enforcement. The authors suggest further inquiry in the form of government agency involvement to detect extremist activities. One of the reasons employees might access the DW to obtain harmful knowledge could be workplace disaffection.

Workplace disaffection based on internet use is where internet utilization in the workplace can attribute to an explanation of behaviors (Garret & Danziger, 2008). The authors explored the effects of the personal use of the internet at work. The philosophical approach was to understand why employees might use the internet at work for personal reasons. The underlying assumptions were that employees use the internet at work for personal grounds for the same reasons they use the internet elsewhere for personal reasons also known as cyberslacking (Garret & Danziger, 2008). The discovery was that 80% of workers use the internet at work for personal activities. The methodology was a mixed methods qualitative narrative approach to explaining the phenomenon with a quantitative survey analysis of usage designed to inform the reader about the rationale for personal internet use at work (Garret & Danziger, 2008).While the study revealed that high performers were active on the web at work, more research is needed in this area as the study showed that high internet use at work might supplant hostile retaliation and balance might be necessary to achieve productivity and personal internet use balance.

Internet use at work can create an environment that is fertile for cybercrime activity. Employees may become victims of the cybercrime activity due to a knowledge deficit about cybercriminal tactics. In the next section, I explore some of the ways employees may become victimized by cyber criminals.

Behavior and Social Media on the Internet

The depressive effects of Facebook by a historical perspective in 1998 by Kraut et al. was an illustation that Pantic used that asserted that internet use, in general, creates the conditions for depression by the isolation of the user from friends and family creating an environment of loneliness. Pantic uses this illustration to represent that depression from internet use was a concern prior to social media (Facebook having a foundation in 2004). Therefore, it is possible that social media (having increased online activity) will have exacerbated the issue (Pantic, 2014). Pantic suggested a requirement for further research to investigate if the existence of correlation can be causality. For example, does Facebook cause low self-esteem, or are people with low self-esteem more frequent users of

Facebook (Jaishankar, 2008; Pantic, 2014). There is also a necessity to evaluate the potential effects of depression from social media use and the possible correlation to online cybercriminal activity with respect to the Jaishankar space transition theory. For example, does a depressed state from overuse of social media create the potential for retaliation in the form of cybercriminal activity?

Agustina presented an analysis that focused on personality traits of people that might become victimized by their surroundings (information and communication technologies (ICT)), with respect to thoughts desires and actions (Agustina, 2015). Agustina argued that victims elevate their exposure to cybercrimes by engaging in risky cyberspace behaviors (Agustina, 2015). The study has the support of routine activity theory (Cohen & Felson, 1979) and space transition theory (Jaishankar, 2008). Agustina argued that there is an online disinhibition effect where people say and do things in cyberspace that they would not say or do in face-to-face relationships (Agustina, 2015). Agustina concluded that transitioning to the internet could be a comparison to walking down a busy street scantily clad and displaying valuable jewels. This disinhibition can be seen in Jaishankar's postulate that internet anonymity can lead to risky behavior (Jaishankar, 2008). Evidence exists that internet behavioral changes might be a result of a lack of self-control.

Internet use and self-control. Control theory is a model for self-regulation and analyzes human behavior. Carver and Shier asserted that control theory could be implantable to determine person moment-to-moment actions. This would be appropriate for my study since it is necessary to understand why people's behavior may change in the internet environment (space transition theory (Jaishankar, 2008)) that may lead to employee adverse actions involving the internet at work. Carver and Scheier advanced the notion of cybernetics and feedback loops with respect to behavior. In other words, human behavior can be much the same as machine feedbacks loops where specific inputs can result in expected outputs (Carver & Scheier, 2008).

Of interest with respect to control theory is the aspects of self-regulation and social cognition. In these instances, the study examined the two behavioral drivers for both. Self-reward and self-punishment (Carver & Scheier, 2008). In the virtual world, these elements of self-regulation and self-cognition appear to be less of an influence on behavior. For example, self-regulation is possibly in response to some negative external social control where there are consequences for actions that are anti-social whereas, in the virtual world, there are no negative implications in an environment where the actors are anonymous (Carver & Scheier, 2008). Denissen et al. (2013) delivered a study that addressed the psychology behind self-regulation. The concept is that from an early age, the adoption of self-regulation through reference values such as goals and social norms begins. Of interest to my study is the influence of social norms on self-regulation. Behavioral changes on the internet may lack the influences of social norms under the conditions of anonymity that the web may provide to individuals. In this quantitative study, Denissen et al. proposed that adult personalities are functional reactions to environmental effects (Denissen et al., 2013, Jaishankar, 2008). The study concluded that with increases in the reference values (positive and negative inputs) people regulate behavior to match the standards (inputs).

In my study, a proposal is that these positive and negative inputs are absent under the conditions of anonymity. Therefore, there is possibly an erosion of self-regulation. Marken addressed the history of control theory and its origins that that has its roots in a man-machine approach to explaining behavior (Marken, 2002). In my study, it is important to note that the man-machine behavior is not as relevant here as the feedback-loop that is involved in the man-machine behavioral theory. It is potentially the absence of the feedback loop in individual internet activities that may lead to personal vulnerabilities. Marken asserted that man-machine control theory feed control theory in psychology has two main approaches, the grand theory and the man-machine systems theory (Marken, 2002). The grand theory from the 1970s established that control theory is an explanation for all behavior like stimulus/response theory and since grand theory has morphed into self-regulation theory. The man-machine theory has its roots in the concept that analyzing human performance might be tasked in a closed-loop system (Marken, 2002).

Social media and the workplace. An exploration of the time spent on the internet with social networking sites (SNS) and compulsion was the focus of study by De

Cock et al. Gender and age dictate the preponderance of social network activity (5%). The purpose of the study was to explore internet social networking based on age, gender, schooling level, income level, occupation, and leisure activities. The philosophical approach to the study was to explore who is using what sites and the demographics of those individuals based on a study in Belgium conducted by Van Bellegham et al. Some internet users might not be able to control their internet use which has become a concern in the scientific community (De Cock et al., 2014). The methodology employed was a quantitative research method based on random survey results in Belgium (De Cock et al., 2014). The limitations of the study were that it only includes the country of Belgium. It is quite likely that the survey is repeatable in other nations.

The use of social media tools as an opportunity for growth for small and medium businesses with respect to the main factors in management demographics such as innovativeness, company size, managerial age and industry were of interest in a study by Fosso and Carter. The study determined that business size and innovativeness were key elements to the utilization of social media tools (Facebook and Twitter). The purpose of the survey was to investigate the adoption of social media tools by SMEs for the purposes of filling the knowledge gap. The philosophical approach was that a measurement should be of the SME use of social media tools for innovation (Fosso & Carter, 2014). The underlying assumption was that SMEs should take advantage of social media tools to increase commerce. The methodology was a survey-based, quantitative, random sample study of 13,314 B2B small business panel members in Australia, the US, the UK, and India. The respondents were numbered 1,997 (Fosso & Carter, 2014). Limitations of the study are self-report bias (survey-based). The authors suggested that future research might include qualitative data to exclude self-report bias (Fosso & Carter, 2014). The study assumed that there were no risks involved in the use of social media tools by SMEs such as social engineering and security risks.

Social media and group activities. Stranger unification in cyberspace to commit crimes through communication is exponentially greater over the physical world (Jaishankar, 2008). Independent of the influences on individuals of social media is another potential for threats to a business with respect to employee online behavior. An issue with social media is that organizationally, employee use of the internet in terms of social networking and the employers desire to control that use relative to the health of the organization (Lucero, Allen & Elzweig, 2013). The purpose of the study was to develop policies and guidelines for employee personal internet and social media activities with respect to the employer's policies. The underlying assumption is that employees would adhere to company policies and that those policies are enforceable outside of the company's jurisdiction and on employee personal time based on an at-will doctrine (Lucero et al., 2013). The methodology was a qualitative narrative approach designed to inform the reader of the proposed policies. The limitation of the study is the separation of employee personal time and employer's ability to sanction that time.

Behavioral influences might come in the form of groups with agendas to frame the thinking of the participants in media sites (Connelly et al., 2016). Groups that engage in social media such as Facebook and Twitter might use the influence of the social media for the benefit of society, or they might use the same media for nefarious purposes as Connelly et al. suggested. Connelly et al. discussed moral agency in the context of social media as being both a self-regulatory by promoting activities that are right, just and humane, and potentially morally disengaging operations through restructuring thoughts in ways that present the usually reprehensible activity in a manner that make them seem acceptable.

The justification for these morally unacceptable activities is the use of divisive language in terms of creating euphemism or perhaps using of comparisons of worse behaviors to justify behavior that is comparatively less offensive. In other words, creating scenarios where ordinarily offensive behavior is becoming acceptable by comparing them to other atrocities. In their study, Connelly et al. developed a system for identifying and classifying web sites according to violent and non-violent ideologies. The three categories were; extreme ideological, non-violent ideological and non-ideological based on the group's purpose statements.

The findings of Connelly et al. suggested that although the identification of violent ideological groups through watchdog agencies and online media for exposure into the group’s activities and their violent nature, not much a presentation of their psychological manipulation of website participants is necessary (creating euphoria and comparing suggested immoral behavior to more atrocious examples making the action seem less offensive). For my study, the Connelly piece demonstrates another possible facet of how SME employees might become morally disengaged to the point of compromising the protection of the business for what the employee might deem a legitimate but morally reprehensible ideological activity. For example, the employee is anonymously exposing ideologically conflicting business information to the ideological website to gain acceptance within the group. Another concern that is like the group social media interface issue is the computer and human interface problem.

Human to Computer Interface

There is the possibility that people view computers as having unjust behaviors in much the same way that see coercive action as unjust in society. Shank presented the case that people may see computers as vehicles for punishment in the same way humans can be. For example, in situations where a person might deny services such as a bank teller due to a lack of required documentation such as an e-mail account, a computer is programmable to deny access to a site based on the same requirement (Shank, 2012). Shank asserts that computers can have the same attributes as humans when it comes to the human to computer interaction.

Interestingly, Shank suggested that people respond to computer rejection in the same way they would respond to personal rejection. The sample was of 125 participants

(53 men and 68 women (four did not understand the instructions). Shank's study suggested that people do not differentiate between injustice by a machine and injustice by someone else (we have all cursed our cars). Shank recommended that sociologists should further investigate these factors in terms of why people react the same way they would to a machine as they would towards a human being. This is interesting to my study because of Jaishankar's space transition theory. Why exactly do people behave the same towards a machine as they do towards each other? They may sometimes treat a computer the same as if it were a person. As seen in this example, there can be a relationship between the human psychology and the computer state (or program), that may yield frustrations and anxiety that could invoke cybercriminal activity in the form of retaliation (Huang & Miranda, 2015; Pantic, 2014; Shank, 2012). It is possible to lore the human psyche into risky internet behavior. The human computer interface can be a form of feedback loop.

The notion of cybernetics and feedback loops with respect to behavior can be much the same as machine feedbacks loops where specific inputs can result in expected outputs (Carver & Scheier, 2008). Of interest with respect to control, the theory is the aspects of self-regulation and social cognition. In these instances, the authors of the study examined the two behavioral drivers for both. Self-reward and self-punishment (Carver & Scheier, 2008). In the virtual world, these elements of self-regulation and self-cognition appear to be less of influence over behavior. For example, self-regulation is possibly in response to some negative external social influence where there are consequences for actions that are anti-social whereas, in the virtual world, there are no negative implications in an environment where the actors are anonymous (Carver & Scheier, 2008).

Virtual characters can create virtual relationships. The differences in human to computer interactions when the computer is a representation of an agent (device) as opposed to when the computer is an image such as an Avatar (virtual person) and was a focus of a study by Appel von der Pütten, Krämer, and Gratch (2012). The purpose of the survey was to evaluate the potential different perceptions and reactions with respect to social cues evoked from the experimental instruments (virtual character versus text chat exchanges) and the participants (Appel et al., 2012). The philosophical approach was that the interaction between the members, the virtual character and text chat would evoke different social cues in the responses to the two instruments.

The methodology was a quantitative Likert scale measurement to evaluate participant replies to text chat (low agency) as an interface and virtual character (female image). The authors of the study included ninety people (49 females and 41 males). They gathered demographics from the participants as well as consent forms signatures with ages ranging from 19 to 62 are part of the study. The questions used in the experiment were of an intimate and personal nature, so it is an expectation that responses to the virtual image might provoke more socially cued responses. According to the authors, there was no strong support that the virtual image provided any deeper social cues than did the text chat instrument (Appel et al., 2012).

This Appel et al. study is relevant to my study because it explores the human condition with respect to human to computer interaction and provides insight into potential avenues to curb the cybercriminal activity. For example, when a computer becomes more like a human-to-human exchange, the psychology of feelings of a victimless crime might reduce the inclination to engage in cybercriminal activities. The reverse could also be true based on the Huang and Miranda (2015) study.

The ability for human neural inputs for computer systems to feel and understand human input in terms of human intent is the purpose of the Huang and Miranda study. The authors present the results of a systems ability to capture human neural inputs for reaction and commanding actions for computer systems. The philosophical approach was that "smart" systems are the result of the manufacture of complex and dynamic software to capture human neural inputs into the systems (Huang & Miranda, 2015). Huang and Miranda's underlying assumption was that humans have a desire to interact with machines in the same way they wish to interact with each other.

Huang and Miranda used a quantitative methodology as an attempt to measure the human to computer reaction state by EEG (electroencephalography) to understand ways to mimic human to human interactions with a human to computer interactions (Huang & Miranda, 2015). The authors attempted to examine BCI (brain computer interface) as a neural feedback loop that a computer may interpret as the incorporation of human intentions into the adaptive software. For future work, Huang and Miranda suggested that use of P300 systems to control mouse clicks with BCI technology are a possibility. The implication of my study is that there is some evidence that people desire to interface with computers in the same way they interface with other human beings. Denial of a computers emotion might lead to cybercriminal activity (retaliation).

The results of a systems ability to capture human neural inputs for reaction and commanding actions for computer systems were the focus of the study by Huang and Miranda. The philosophical approach was that *smart* systems are the result of the manufacture of complex and dynamic software to capture human neural inputs into the systems. Huang and Miranda attempted to measure the human to computer reaction state by EEG (electroencephalography) to understand ways to mimic human to human interactions with a human to computer interactions.

There is some evidence that people desire to interface with computers in the same way they interface with other people. Denial of a computers emotion (approval, disapproval or denial of access) might lead to cybercriminal activity through retaliation (Huang & Miranda, 2015). The authors of the study indicated that it might be possible for a computer program alone to incite cybercriminal activity and a bot is such a computer program of interest.

Cybercriminal virtual command and control. To understand how bot-masters achieve a high level of success in a cybercriminal market, Décary-Hétu and Dupont explained that Bot-masters use available technology to infiltrate business and government computers with spam, attack servers and steal information for a price (Décary-Hétu & Dupont, 2013). They explored how reputation in the legitimate and black markets on the internet might encourage bot-master activities through notoriety and financial rewards. The purpose of the study was to understand the mechanisms that promote botmaster's cybercriminal activities in cybercriminal markets. The philosophical approach was through a risk/reward bot-masters lens. In other words, what are the factors involved that might lead to bot-master type cybercriminal activity in terms of gains and losses? The underlying assumption was that the possibility that the rewards for cybercriminal activity outweigh the risks.

The methodology employed was a quantitative analysis of a two-part analysis of the variables in a predictive model (static and dynamic). The results were that criminal satisfaction through achievement and reputation are a shared goal for cybercriminals. In other words, the same drivers of fame and accomplishment in the legal world exist in the cybercriminal world. Décary-Hétu and Dupont recommended further studies into identity theft and carding (obtaining stolen credit card information) using the same input variables as for botmasters.

Innocent Users Can Become Deviant Perpetrators

Psychology is beginning to play a significant role in information systems security (Weiderhold, 2014). Weiderhold asserted that the human factor is the weakest link in cybersecurity and as a researcher in the field, I must agree based on the literature (Jaishankar, 2008, and Tarafdar et al., 2013). Wiederhold held that there are five psychological interests in cybercriminal activity; (a) behavioral economics (risk and reward, (b). patterns of criminal behavior, (c) advising on the legislature, (d) public awareness, and (e) impacts to the victims (Weiderhold, 2014). My study is an exploration of five of these activities through the lenses of the researcher and an SME owner to develop an understanding of the application of how these principals may relate to a real-world small business owner and to other developing theories such as space transition theory. Jaishanker developed space transition theory to explain behavioral changes in the transition from physical space to cyberspace (Jaishanker, 2007). These behavioral changes can be attributable to SME employee behavior and the online environment as suggested by the following literature.

An empirical to study to identify what organizational and individual factors contribute to resistance to social engineering by cybercriminals is a concern in this study by Flores and Ekstedt. The purpose of the study was to evaluate possible factors that contribute to individual resistance to social engineering. The philosophical approach was to determine the level of the impact of organizational security cultural on personal behavior relative to social engineering resistance. The underlying assumption was that organizational information security culture was a contributing factor to individual resistance to social engineering cybersecurity threats.

The authors of the study revealed that all factors investigated had an influence on individuals to varying degrees, but individual attitudes were the most profound. The methodology used was a mixed-methods design where qualitative data to develop the research model and survey instrument to quantify factors of resistance to social engineering by both individuals and organizations. 4,296 individuals in Sweden were the recipients of the instrument (Flores & Ekstedt, 2016). A research question designed to discover the organizational factors that influence employees to resist social engineering cyber-threat activity.

The authors asserted that the strongest tie to resistance to social engineering was in individual attitude and the weaker links were in self-efficacy and normative beliefs. Flores and Ekstedt indicated that the data is in support of all the hypotheses, but some indicators were stronger than others for example attitude over self-efficacy (2016). They further revealed that information security culture had a weak correlation to behavioral intention towards social engineering. More research is necessary for determining the effects of attitude towards social engineering. Being aware of threats and education is not enough to prevent the victimization of employees by social engineers. The variances in attitude toward cybersecurity need further research as a predictor of behavioral intentions (Flores & Ekstedt, 2016). Other factors for further exploration are the enterprise's size and industry.

Cybercriminal leveraging of poor judgement. While space transition, self-regulation, and self-control theories offer possible explanations for criminal activity on the internet, there are situations where the vulnerabilities appear to be simply poor judgment on behalf of the user. The use of the same security precautions should apply in cyberspace. Arlitsch and Edelman addressed the use of social engineering (as opposed to hacking) for data breach activities. They asserted that social media is fertile ground for cyber attackers to both obtain user information and relationships with users to gain information. They offered advice on not making it easy for attackers by use of password vaults, strong passwords, data protection, and proper device management (Arlitsch & Edelman, 2014). Arlitsch and Edelman concluded that it is not practical for users to disconnect from the internet, but personal diligence can assuage vulnerabilities (Arlitch & Edleman, 2014, Jaishankar, 2008).

Donner et al. provided an analysis of deviant behavior on computers. The theoretical framework for this survey-instrument-based quantitative convenience analysis is the basis for Gottfredson and Hirschi's general theory of crime (Gottfredson &Hirschi, 1990). The survey conducted was at a large university in the southeast and approval was by the university's institutional review board (Donner et al., 2014). The purpose of the study was to better understand the online behavior of college students and possible resultant deviant behavior in the online environment.

Individuals in the online environment selected the dependent variables as ten deviant behaviors with the independent variables being the measure of low self-control based on the Grasmick scale of low self-control and utilizing the Hirschi & Gottfredson six-element scale (Donner et al., 2012). Donner et al. concluded that there is a link between self-control theory and online deviant behavior (Donner et al., 2012). Deviant behavior on the internet by employees can have an adverse effect on organizations with respect to the organizations brand.

A literature review based, qualitative, narrative study on the effectiveness of a human reliability assessment and improved statistics-based quality control for assurance by Evans, Maglaras, He, and Janicke (2016) asserted that based on the number of high profile security breaches, organizations have begun to focus on brand protection and reputation through assurance protection. To that end, Evans et al. explored the established literature in search of areas of weakness with respect to cybersecurity and provided a brief historical account of cybersecurity breaches in different factions of industry and government (Evans et al., 2016). Evans et al. concluded that half of the cybersecurity breaches involved human error and suggested further research in cybersecurity human factors. Cybersecurity breaches can come from inside or outside of the workplace.

Creating a cybercriminal in the workplace. An approach to moral disengagement and deviant work behavior from the organizational injustice perspective relative to self-reporting is of interest to my study. The Hystad, Mearns, and Eid (2014) study addressed self-reported deviant work behaviors on 11 passenger and freight ships in Norway. In their study, they were interested in moral disengagement with diffusion and displacement of responsibilities as the connection to deviant work behavior. Also, in the study, Hystad et al. was interested in evaluating risk-taking, non-compliance, and lack of participation as results of perceived organizational injustice (Hystad et al., 2014).

With respect to the safety concerns that might arise from corporate injustice, Hystad et al. considered the aspect of an employee's freedom to report near-misses, problems, and concerns without fear of organizational retaliation. Along with the work of D'Arcy et al, Hystad et al. pointed to the Bandura theory of moral disengagement (Bandura, 1990) as evidence that employees may sacrifice internal self-regulatory mechanisms through moral disengagement to justify behavior under the Bandura umbrella of three groups; (a) moral justification, (b) euphemistic labeling and, (c) advantageous comparison. In this study, Hystad et al. considered the mechanisms of displacement of responsibility (individual blame), diffusion of responsibility (organizational blame), and the distortion of the consequences or a victimless infraction (Hystad et al., 2014).

In the Hystad et al. quantitative study, the administration of 340 questionnaires to the crew of 11 Norwegian freight and passenger ships reveal conclusion that there is empirical evidence that moral disengagement influences the sense of organizational injustice and in turn may be causation for deviant behavior. These results are in keeping with my study research question and the D'Arcy et al. proposition that moral disengagement plays a significant role in abnormal work behavior. In the case of my study, this may be retaliation for perceived or real organizational injustice in the form of online deviant behavior. For example, an employee might retaliate against the organization by making negative comments through corporate rating outlets such as *Glassdoor* or social media such as *Facebook* or display other deviant behavior such as online inventory sabotage and release of private customer information. It is an expectation that SME owners would not be cognizant of the potential for employee deviant online behavior based on perceived organizational injustice (Hutchings, 2012).

Work place cybercrime by example. Another aspect of moral disengagement is the perspective that illustrates the effects that management might have on the employees when the leadership engages in unethical behavior. According to Bonner, Greenbaum, and Mayer, employers who demonstrate ethical (moral) disengagement can be a predictor of employee perceptions of ethical leadership (Bonner et al., 2016). Bonner et al. illustrated the construct of how supervisory moral disengagement impacts the perception of employees by demonstrating that there is an intersection of the line from supervisory moral disengagement to employee disengagement that leads to the perceptions of leadership and ultimately affects employee performance. In support of the premise, Bonner et al. employed the use of a seven-point Likert scale from 1 as strongly disagree to 7 as strongly agree. The samples are from a myriad of demographics as well as a diverse cross section of disciplines (from architecture to transportation).

The results of the study survey showed that the relationship of employee disengagement to supervisor disengagement was statistically significant. The author of the study demonstrated that supervisors who rated high on moral disengagement might not be a consideration by employees to be ethical leaders (Bonner et al., 2016). A further finding was that there is a correlation between an employee’s moral disengagement and that of the supervisors. In other words, as predicted by the hypothesis, an employee’s behavior can be a result of the employee’s perception of supervisory moral disengagement.

Of benefit to my study is the potential for SME managers to gain an understanding that their behavior may influence the behavior of employees with respect to online activity both inside and outside of the work environment. It is possible that an employee’s perception of the business owner’s moral disengagement could result in undesirable risk potential when the employee is engaging in online activities either inside or outside of the work environment.

An integrated model of undermining behavior with respect to victims of undermining turning to undermining activity themselves is the focus of the Lee, Kim, Bhave, and Duffy study (2016). Of interest to my research is the prospect of undermining in the work place creating moral disengagement as a form of workplace injustice retaliation. For example, an employee might view gossip about himself and herself as social injustice and might see the sabotage of the perpetrator's computer data as a form of justifiable retaliation. Lee et al. asserted that social undermining behavior could be the result of pressures created by workplace competition. In the study, Lee et al. addressed the employee-to-employee competition as a mechanism that induces employee social undermining (Lee et al., 2016).

The theory presented by Lee et al. suggested that relationships such as undermining in the workplace could negatively influence the moral view of others (employee to employee). According to Lee et al., strategies that attempt to undermine colleagues may result in morally disengaged retaliatory behavior. This means that justification and implementation of the retaliatory undermining actions are acceptable by moral disengagement. In other words, Lee et al. make a connection between undermining and moral disengagement because of unjust treatment that leads to resource depletion in the forms of employee turnover and lost production.

Retaliatory undermining by employees through the constructs of the Bandura moral disengagement theory such as blaming and dehumanizing, changing moral perceptions by personality re-categorization (euphemism labeling) and drawing comparisons that are advantageous to retaliation and last, the retaliate may alter or cloud the retaliatory behavior to make it seem harmless or shifting the responsibility for the conduct (they did it to me first) may justify the action. This creates the victim's perception that retaliating undermining with undermining is justifiable (Lee et al., 2016). The Lee et al. study involved two Korean banks with 25 branches. They conducted Time

1 Surveys that included 208 employees with 92% participation (191 employees). The undermining measurements were the pre-victimization concepts of victimization, moral identity and interpersonal justice with the application of control variables. The time 2 surveys measured for the post-victimization concepts of depletion, moral disengagement, and undermining.

The results of the Lee et al. study demonstrated that there is indeed a connection between undermining, moral disengagement of the victim and retaliatory action by the first casualty. The authors showed in the study that aggression between employees is common in the workplace (Lee et al. 2016). A limiting factor to the study was the inability to link to causes of the undermining. It is possible that these frustrations may manifest themselves through nefarious computer activity in the work place.

Insider cybercrime. The notion that employees may become a liability when accessing customer credit card information is the subject of Cepeda, Gerardo, Perez, and Rivera study. They go through the history of credit cards from oil companies and department stores to diner’s club, to today’s Visa and MasterCard’s. They espouse the excessive number of cards issued in 2013 and the notion that with the use of more cards, the more likely that fraud will occur (Cepeda et al., 2015). They further illustrate the consumer privacy laws that have developed over the years because of the fraudulent activity surrounding the use of credit cards. Cepeda et al. presented the typical credit card transaction process and then proceeded to demonstrate where holes in the process may occur in three ways; employees transferring purchases from the merchant point of sale device to their personal accounts, retaining customer credit card information for personal use and the use of a card skimmer to obtain the card information.

The purpose of the study was to inform business owners of how employees may become a liability in credit card transactions and the use of point of sales tactics to leech credit card information. The philosophical approach was to teach by way of example. The underlying assumption was that employees might take advantage of flaws in a system for personal gain. The methodology was a qualitative narrative approach designed to inform managers of loopholes in the point of sale system. The limitation of the study was the lack of assessment that potential third party (social engineering) collaboration with employees could exist.

Creating cybercriminals 0utside of the workplace. The psychology behind self-regulation is a concept that from an early age is adoptable through reference values such as goals and social norms (Denissen et al., 2013). Of interest to my study is the influence of social norms on self-regulation. Behavioral changes on the internet may lack the influences of social norms under the conditions of anonymity that the web may provide to individuals. In this quantitative study, Denissen et al. proposed that adult personalities are functional reactions to environmental effects (Denissen et al., 2013, Jaishankar, 2008).

Cowan explored the internal mechanisms of the psychopath outside of the generalized phenomena of the serial killer or rapist. Instead, Cowan addresses what is missing at the internal psychological level of the psychopath, which is empathy for other human beings (Cowan, 2014). Cowan turned to Cleckley's work on the psychopath to provide a list 16 of psychopathic personality traits. Some of the attributes from the list that found in the social engineer character are, charm and intelligence, the absence of rational thinking, lack of remorse, untruthfulness, poise, impulsiveness, lack of deep emotions and antisocial behavior (Cowan, 2014). The purpose of the study was to envelop the drivers for psychopathic activity. Cowan's philosophical approach was to illustrate that society has a propensity to reward and revere the successful psychopath to heroic stature despite the knowledge of the ruthlessness that perpetuated the notion through exploitation.

Cowan suggested that we should consider the success of the captains of industry in the context of the American value system that to an extent, encourages the behavior (Cowan, 2014). Of interest to my study, is that these some properties appear to exist among social engineers in their endeavors for revenge and reward. The underlying assumption was that psychologically, society tends to provide an incentive for bad behavior that may lead to anti-social risks. The methodology was a qualitative narrative approach designed to inform the reader using the available literature on the subject. The limitation of the study was the generalization of the psychopathic behavior. More work is necessary on the 16 categories of psychotic behavior on a case study basis.

The psychological literature above contains possible explanations of internet behavioral changes that may influence negative behavior by employees in the work place. Other potential influencing factors may be space transition and the anonymity that the internet provides (Bradbury, 2014, & Jaishankar, 2007). The following sections of the study will address these important aspects of the cybercriminal and victim psychological factors. These factors will serve to grow the knowledge gathered from the data collection about what small business owners understand to be the risks associated with employee internet use.

Cybercrime Victims and Education

A literature review based qualitative study to investigate the factors involved in South African SME's accounting and reporting of cybercriminal activities using a survey-based questionnaire that provided the results of the analysis to determine factors of cybercrime reporting by Bougaardt and Kyobe. Bougaardt and Kyobe identified from the literature review and survey results that there were relationships between recognition of cybercrime and preparation of losses from cybercrime; information system security design, expertise in infosec and risk management, management attitude towards security, awareness of cybercrime and victimization, and knowledge of regulations and compliance (Bougaardt & Kyobe, 2011).

Bougaardt and Kyobe concluded that lack of knowledge and understanding relative to what cyberattacks involve result in further victimization from cybercrimes and further determined that more research in the areas of educating and training SME managers in reporting and compliance as preventive measures for cyberattacks may be necessary (Bougaardt & Kyobe, 2011). Bougaart and Kyobe submitted that their sample size was too small for generalization and further determine different causes of management behavior with respect to cybersecurity (Bougaardt & Kyobe, 2011).

Cybercrime and students. The influences of guilt and shame on ethical decision making may be a concern for cybersecurity according to Johnson and Connelly. In their 5-point Likert scale-based study, guilt and shame are measurements using scenarios developed to test Self-Conscious Effects (TOSCA-3). Johnson and Connelly addressed the emotional contributions of feelings such as fear, anger, and guilt to ethical dilemmas. They differentiate guilt and shame as being inward focused whereas fear and anger might be an outward focus emotionally. Guilt and shame can be attributable to moral disengagement and behavioral tendencies relative to self-regulation. The effects of guilt and shame are that guilt might manifest itself as acceptance of responsibility and behavior intended to make reparations and shame might manifest itself as behavior that reflects as a reduction of self-worth or negative feelings about the self (Johnson & Connelly, 2016).

Johnson and Connelly surveyed a sample of 204 undergraduates (25 had incomplete responses) and measured moral disengagement based on the Detert moral disengagement scale. In the study, based on 12 scenario cases involving ethical decision-making basis, they found that higher levels of guilt affect moral disengagement and ethical decision-making negatively while lower levels do not. In other words, the greater guilt trait the individual exhibited, the closer the connection to realizing the effects of unethical behavior. In the shame measure, the results contrasted with each other in that shame was not a determinate for moral disengagement.

Johnson and Connelly attributed this response to participants showing moderate levels of shame. The study is useable in efforts to identify risk traits in the selection of personnel. The findings suggested that low-level guilt trait moral disengagement creates a reduction in ethical decision-making (negative). In other words, staff with low-levels of guilt trait might increase the moral disengagement properties within the organization.

There is a downward trend of cyberattacks on undergraduate students. Case and King presented that this downward trend is due to improved spam filtration, proactive education and improved student behavior (Case & King, 2013). The study has its roots in a previous 2007 exploratory study by the authors with respect to cybersecurity threats to undergraduate students (Case & King, 2013). The study appears to be a quantitative chi-square analysis of a longitudinal survey design using a questionnaire as the instrument with a convenience sample (from the attendant institution). The convenience sampling approach to the study renders the results ungeneralizable. A requirement for a broader, random institutional sampling would aid in the generalization of the proposed theory. The self-reporting nature of the survey limits the study (Case & King, 2013). The idea of an additional requirement to use qualitative interview data is a possibility. Interview data might produce a richer understanding of the undergraduate’s genuine concerns about cybersecurity as opposed to the current study that has a limitation to a survey questionnaire.

The ease with which cyber criminals can access organizations through phishing is the subject of a study by Ferrillo and Singer. They asserted that it only takes one employee to access a cyberattack link to create large business damage both monetarily and in terms of reputation (Ferrillo & Singer, 2015; Gold, 2014). The purpose of the study was to inform the reader of the risks in inadvertently accessing malicious sites. The philosophical approach was to initiate interest in cybersecurity awareness training. Ferrillo and Singer provide a list of eight rules for best password protection practices as well as protection of company data.

Choras et al. submitted that human behavioral factors only include a lack of knowledge of privacy issues with respect to cybercrime (Choras et al., 2015). The underlying assumption was that rigorous training might prevent malicious cybersecurity intrusions into an organization. The methodology was a qualitative narrative approach designed to inform the reader of potential ways to protect company information from cyberattacks. The limitations of the study were that committing training resources may not be available.

Cyber Criminal Behaviors, Approaches and Forensics

Adnan et al. established the MATE (man-at-the-end) approach to cyberattacks. Under this proposition, the assumption is that the attacker (MATE) has gained access to a system's hardware or software either by direct contact or remotely (RMATE). MATE and RMATE attacks are difficult to detect and resolve due to the possibility that the attacker has an all access capability with respect to the hardware and software. It is only possible to prevent MATE attacks for short periods of time given the unlimited amount of time available to a man-at-the-end to manipulate a system. It is also an assumption that the man-at-the-end has the capabilities to develop compromise and software protection elements (Adnan et al., 2015).

The authors revealed that MATE attacks are comprised of several techniques to compromise a system's hardware and software. Altering the software in ways that the developer had not expected, reverse engineering properties of the software and cloning the software. Under these scenarios, a compromise of the protection software encryption could exist by the fact that the attacker (man-at-the-end) has the capability to inflict harm to the data post-delivery through approaches such as denial of service attacks or by inserting wrong data into the data stream post encryption. In other words, compromise of the encrypted data could result post-encryption.

Adnan et al. illustrated the properties of MATE and RMATE capabilities in a diagram where the attackers tool box contents such as; debugger, emulator, disassembler, tracer de-compiler, slicer, virtual machines and SQL injections with the defensive tool box being comprised of defense-in-depth, digital watermarking, diversity, white-box cryptography, emulator detection, debugger detection obfuscation and tamper-proofing as countermeasures are exposed (Adnan et al., 2015). Germane to my study, Adnan et al. acknowledge that a weakness in the literature is the social cognition factor of the lone attacker. In other words, it is necessary to understand how MATE attackers think to identify the cause of the attacks correctly. To further explore the social cognition factor into the malicious behaviors, it is necessary to determine some of the important psychological studies associated with the response.

A comparison computer forensic analysis and the use of computer investigative analysis (CIA) based on the case of Dennis Rader in a study by Bongardt. Bongardt asserted that if behavior reflects the personality, then, use of CIA in the correct form in a computer to detect network intrusions could be an application (Bongardt, 2010). Bongardt used a qualitative, narrative approach to compare how CIA might apply in much the same way that computer forensics were involved in the capture of serial killer Dennis Rader (Bongardt, 2010).

Bongardt drew parallels to criminal profiling and cybercriminal profiling and explored these attributes at the individual level. Bongardt suggested that cyber criminals could have motivations, objectives, and characteristics that have been a consideration for contributing factors to real world crime. Bongardt issued 14 categories for motives used for profiling cyber attackers (Bongardt, 2010). Bongardt submitted that once the identification of motives, objectives, and characteristics of network intruders occurs, they may make the profiling of the intruders a possibility.

A simulated phishing attack in an effort explore means to train individual users in the secure use of the internet was an exercise by Jansson and von Solmes at the University of South Africa to demonstrate the validity of their study. The purpose of the study was to explore deceptive phishing exercises to understand the individual's susceptibility to phishing attacks. The underlying assumption was that phishing attacks are successful based on the user's lack of awareness of the activity.

The methodology was a quantitative analysis based on simulated phishing attacks and user responses. The evaluation indicated that with proper warnings and training, users became less susceptible to phishing attacks. However, Jansson and von Solmes noted that in the second exercise, users may have received forewarning by word of mouth of the exercise and may have adjusted their behavior accordingly (Jansson & von Solmes, 2013). The authors recommended further research to establish embedded warnings as a training device.

A mixed-methods approach to the Nero, Wardman, Copes, and Warner study to investigate the effectiveness of web-site take-down contractors as a counter measure for e-mail phishing attacks to demonstrate its effectiveness (Nero et al., 2014). For the quantitative analysis, measurements were from analysis of millions of phishing e-mails to determine affected financial institutions. For the qualitative analysis, they conducted interviews with financial fraud investigators from five ranked financial institutions (Nero et al., 2014). The results revealed the participating banks and take down companies, made little use of law enforcement with respect to the attacks. The qualitative results determined that not many financial institutions conduct their own investigations into phishing attacks which support the quantitative data analysis conclusion (Nero et al., 2014). Nero et al. concluded that takedown countermeasures are too late to prevent phishing attacks and that use of phishing attack evidence is rare in the pursuit of perpetrators (Nero et al., 2014). The vulnerability as an SME risk to employees for phishing attacks illustrates the broader concern for employee vulnerabilities about internet cybercrime.

Personnel Risks

Star performers invalidate the belief that the distribution of individual performance is reasonable and that a power law distribution model for individual performance is more appropriate (Aguiness & O'Boyle, 2013). In this qualitative, narrative study, Aguinesss and O'Boyle presented nine propositions in support of their argument backed by relevant statistical data. The article was based on early works in performance assessment where the thinking was that top performers are anomalies and either thrown out of the studies, ignored or forced into normal distribution for performance analysis (Aguiness & O'Boyle, 2013).

The nine propositions that Aguinis and O’Boyle presented were; (a) power law distribution is more practical in 21st-century work model than normal distribution of performance, (b) addition or deletion of star performers will have an extraordinary impact on an organization, (c) performance value will be unbalanced in a star performer group, (d) the closer star performers are to the organization's core competence, the production value increases, (e) competitive advantage can be tied to star performers, (f). the relationship to job searches and turnover will be weaker with star performers, (g) job performance and turnover rates are related (weaker performers have higher turnover), (h) equal distribution of compensation will create a higher turnover for star performers and, (i) there is a relationship between star performers, non-stars, and turnover (Aguiness & O’Boyle, 2013). Of interest to my study is should the star performer competition become unhealthy, there is a potential that organizational injustice can create a retaliatory environment (Hystad, Mearns, & Eid, 2014).

A qualitative narrative study developed to inform the readers of the risks of personal information exposure, cybercriminal techniques to access personal data and offers potential strategies for reducing the risk of identity theft was the product of an Arlitch and Edelman study. The purpose of the article was to inform the reader of the increase in cyberattacks (referencing the 2013 Target and Neiman Marcus attacks by hackers) with an additional warning that 90 percent of businesses fall prey to a security breach (Arlitsch, & Edelman, 2014).

The philosophical approach to the article was a logical, systematic approach from cybercrime statistics to cyberattack techniques and finally to cybercrime prevention methods. The underlying assumption of the article is that the knowledge gained by the readers for the article may help assuage future identity theft. Mostly, the authors promote responsible personal data management by use of strong passwords and encryption (Arlitsch, & Edelman, 2014). The methodology employed was a qualitative narrative study approach designed to inform. A limitation of the study is that the authors appear to have confused social engineering with hacking. A description of hacking could be a code modifying operation to invade systems, and a description of social engineering could be a data collection enterprise to gather personal information to access data.

Cybercriminals accessing employees through social media. A measurement of social status and friend vulnerability in social networking and privacy protection was the product of a study by Gundecha, Barbier, Jiliang, and Huan (2014). They proposed a methodology to reduce one's own vulnerability due to the vulnerability of friends in social network sites (Facebook). In other words, a reduction in vulnerable friends yields a reduction of one's own vulnerability. In the equation, Tang and Huang factor in the social ramification of unfriending socially relevant friends or friends of social utility as they term it (Gundecha et al., 2014).

The purpose and philosophical approach of the article was to produce an algorithm to filter out friends in social networks that increase one's own vulnerabilities to internet cybercrimes by eliminating friends that engage in risky social networking behavior and have no socially redeeming qualities (Gundecha et al., 2014). The underlying assumption was that the reader might be willing to unfriend friends based on a vulnerability risk algorithm. The methodology was a quantitative analysis of data from 2 million social network users and friends and privacy settings. Gundecha et al propose further studies with individual social utility measures in the reduction of user vulnerabilities (Gundecha et al., 2014).

Insider cybercriminal embezzlement. Based on the embezzlement by a Nashville bank manager in the late 1970's, Hayes used the case to explore examples of how fraud may occur and possible prevention techniques. These techniques included detection methods such as unusual account activities, openly questioning the problems, and how fraudsters manage the lies and the fraud (Hayes, 2014). The purpose of the Hayes study was to engage the reader by providing techniques to prevent, detect and expose fraud in an organization. The philosophical approach was to provide evidence to the reader by illustrating how the bank manager used his position of authority to embezzle 6 million dollars from the branch he managed using a lapping scheme (creating fictitious new accounts and servicing them to pay off the pilfered accounts).

It appears that lapping is much like a Ponzi scheme in that the monetary assets are merely numbers on paper and are not actually tangible assets. The underlying assumption was that the ability to commit fraud comes with authority to manage large sums of money (or assets). The methodology was a qualitative narrative approach designed to inform the reader about manipulating accounts for fraudulent activity and the potential for detection of that event. The limitation of the study was that it only involved people in a position of authority and their ability to commit fraud in great amounts. From the literature, and through technology, it is not necessary to hold a position of power to commit massive fraud.

Cybersecurity measures. A qualitative, case study design approach to research the effect of cybercrime on banking and short-term insurance businesses in South Africa and what, if any, legislation might protect them was the subject of a Herselman and Warren study. The study was based on a review of public records for case study evidence, and they asserted that banks, insurance agencies and higher education institutions were the South African based participants of the case study. Data collection was by means of interviews and legal case studies (Herselman & Warren, 2014).

From the study, there was a submission of seven recommendations. Training for clients, international cybercrime treaty, the spread of system rights among proxies, new cyber-laws, reactive and proactive security measures, research and development and security relevance of measures (Herselman & Warren, 2014) The Herselman and Warren conclusion was that further research is a requirement and that the investigation would be in future cases (Herselman & Warren, 2014).

A behavioral model to understand how management may influence the security compliance behavior among company employees was the product of a qualitative literature review-based study by Hu et al. and addressed two research questions for consideration as gaps in the literature; (a) what is the role of organizational culture in developing compliance with security policies and, (b) how does management influence employee's intentions to comply with these policies (Hu et al., 2012). Hu et al. explored various behavioral theories, but for this study, the focus was on the theory of planned behavior or TPB (Hu et al., 2012). The intent of the authors was to define a cultural environment that would support information systems security compliance. Statistical analysis of the survey concluded that there was a good convergent validity.

The study contribution was that it was the only study to factor in top management, organizational culture, and TPB for information security in organizations. The limitation of the survey was the restriction to a unidimensional corporate operation. Since organizational culture is a multidimensional concept; evaluation of other operational habits should be a consideration (Hu et al., 2012). The authors demonstrated the top management influence over information security compliance within an organization.

An evaluation as to why, despite numerous public advisory campaigns for password protection, users still engage in risky behavior with passwords was an initiative of Whitty, Doodson, Creese, and Hodges. In this quantitative, demographic, and questionnaire-based study, they found that eight primary variables might influence the risky behavior of password sharing; age, self-monitoring, cybersecurity knowledge, the locus of control, lack of premeditation, urgency, sensation seeking, and lack of perseverance (Whitty et al., 2015).

A submission of five hypotheses for testing the reasons that may influence password sharing; age (older people are more likely to share passwords) self-monitoring (high self-monitoring people are less liable to engage in password sharing), impulsivity (impulsive people are more likely to share passwords), and locus of control where an individuals believes that they control their environment, internal locus of control where people are more liable to share passwords (Whitty et al., 2015). Whitty et al .concluded that, overall, 51.1% of the participants had shared their passwords in the past. Whitty et al. concluded that three main factors drive potential password sharing; age (youth), perseverance, and self-monitoring (Whitty et al., 2015). While poor judgment is difficult to guard against, there are situations where employee training, hardware, and software protections might avoid exposure to cybercriminal activity.

Equipment and Software

A trust-based approach for cyber systems security is a consideration of Ali et al. They produced a literature based historical study to explore security protection of cyber-physical systems (CPS). A CPS includes sensors, monitoring and control features embedded in electronics devices to connect cyber systems to the physical world (Ali et al., 2015). In the study, Ali et al. presented seven modes that are potential known threats for attacks. Eavesdropping, compromised-key attacks, man-in-the-middle attacks, DOS (denial of service) attacks, resonance attacks, communication jamming attacks and integrity attacks. Ali et al. asserted that internal and external trust in CPS established a boundary for external trust (security software) and internal trust is dependent on interpersonal, structural and dispositional and rely on statistics and probability modeling (Ali et al., 2015). Firewall technology may be another solution to cyberattacks.

Firewall technology is becoming intertwined with hardware and software according to a study by Hunter. In the qualitative, narrative approach, Hunter compared and contrasted firewall technologies and the expected growth of investment and research and development. A graphical representation presented by Hunter illustrated that there is an expectation that commercial firewall sales will grow more than one billion dollars by 2018 (Hunter, 2013). Hunter examined the production of business broadband routers and modems with built-in firewall protection indicating a trend way from firewall protection software initiation from the computing appliance to the routers and modems (Hunter, 2013), in other words, the modems and routers will host the embedded software and updates within the router or modem as opposed to the protection of the computer in commercial enterprises. Hunter compares Juniper and Cisco routers (the top competitors in the business router market), and the conclusion is that the final design features with flexibility will gain the market share.

Employee attitudes and equipment. A study for an analysis that focused on personality traits of people that might become victimized by their surroundings (information and communication technologies (ICT), with respect to thoughts, desires, and actions where Agustina argued that victims elevate their exposure to cybercrimes by engaging in risky cyberspace behaviors (Agustina, 2015). The author of the study had the support of routine activity theory (Cohen & Felson, 1979), and space transition theory (Jaishankar, 2008).

Agustina further argued that there is an online disinhibition effect where people say and do things in cyberspace that they would not say or do in face-to-face relationships Agustina presented four risk reduction preventative activities. Do not introduce targets, identification of risk zones, decontamination and clean up, and, separation of objectives (Agustina, 2015). Agustina concluded that transitioning to the internet is the same as walking down a busy street scantily clad and displaying valuable jewels. The same precautions apply to cyberspace (Agustina, 2015). This disinhibition view can cause lapses in software update judgement as well.

The question of why users do not currently implement security software patches was part of a study by August, August, and Hyoduk (2014). August et al. proposed a fee to system users that forgo implementation of security software patches. Users could opt to pay a premium fee and have the updates automated to eliminate the risk of unsecured systems. In other, words there would be a penalty for not installing security patches or a premium could be to have it done by the software manufacturer (August et al., 2014).

August et al. sought to propose a financial incentive solution for security software implementation by users. The philosophical approach is that users require incentives to keep systems secure with patch updates. The underlying assumption is financial incentives to get users to update security software is logistically feasible. The methodology used was a qualitative narrative study designed to inform the readers of the stakes and potential penalties involved in not maintaining secure systems. The cost of tracking users, updates and billing may not be financially advantageous for SMEs. The scope of the article was to address the advantages and disadvantages of cloud computing for small businesses with respect to security considerations. The significance of the study would be to provide grounds for further research to identify the breakdowns of different business segments (industries) to provide a more comprehensive evaluation of the cloud computing concerns.

The purpose of the study was to examine potential uses of cloud computing for small and medium business enterprises because these companies do not have the resources to acquire the technology that large firms can provide funding for in terms of computer storage space, technology assets, and communications (Badamas, 2012). The philosophical approach was that the study might provide the opportunity for small and medium enterprises to take advantage of cloud computing to leverage these benefits against larger corporations to become more competitive. Badamas identified three security concerns with small and medium business use of cloud computing; infrastructure, data security, and redundancy (Badamas, 2012).

The major underlying assumption of Badamas was that there would need to be adequate protections in the form of security measures, although, it is arguable that small and medium businesses are already operating relatively unprotected with respect to data security (Chabinskey, 2013). Chabinsky asserted that SMEs have exposure to risk without the advantages of cloud computing (Chabinsky, 2013). The methodology used was a quantitative survey, questionnaire, and interview-based analysis anchored to five literature studies. Analysis of the data by using the five-point Likert scale evaluation as the instrument demonstrates that a larger sample size for the study would be necessary to enhance the reliability and validity of the survey (Badamas, 2012). The Alpha, Beta, Gamma and Theta companies surveyed were comprised of two large and two small businesses. Badamas suggested a wider field of investigation would be necessary to capture a finer grain of data for evaluation (Badamas, 2012).

SMEs and Cybersecurity Policies

The issue of how small and medium businesses might cope with assessing their information security through self-assessment and improvements using a model framework is a study provided by Cholez and Gerard. Central to the article was the concern for a business's ability to perform a self –assessment of security maturity and to improve the security process accordingly by using the framework that Cholez and Gerard had developed in this article (Cholez & Gerard, 2014). The data analysis tool used was the ISO 9001 PDCA (Plan, Do, Check, Act) model to measure the best practices employed in the case studies (Cholez & Gerard, 2014).

The underlying assumptions of the article were that small and medium businesses require a road-map type formula to address security issues based on the case study results. The methodological approach was the use of qualitative interview-based case studies in Luxenberg to assimilate the data across SME industries based on the results of six cases. The instrument was an interview questionnaire with 27 open-ended questions with sub-questions to direct the interviewees towards reality-based industry practices (Cholez & Gerard, 2014)

The role of IT governance in small and medium businesses, specifically, IT governance of SMEs in the form of HR resources is an aspect explored by Garbarino. In enterprises where resource usage comes at a premium, it is necessary to develop a lean system of governance. Garbarino noted that SMEs have a simple structure that does not include many specialists to perform the routine IT functions larger corporations might facilitate (Garbarino, 2013). Garbarino asserted that IT (and therefore IT growth) is essential to the success of an organization as an enabler of growth. The purpose of the study was to provide the lessons learned and issues from a case study to implement IT governance into an SME (Garbarino, 2013). The philosophical approach was to identify shortfalls in the human resource management aspect of the implementation of IT governance in SMEs to reach average levels of maturity in IT governance.

The underlying assumption is that SMEs will adapt to the implementation of IT governance tailored to an SME enterprise. Garbarino presented a case study of AAA (a localized pharmaceutical market) and the incorporation of IT governance into the business. The methodology was a single qualitative case study design (for defense, Garbarino cites the Yin definition for a single case study design). The author revealed a positive connection between HR training and IT practices that contribute to the organization's success.

Garbarino suggested a replication of the study in other enterprises. The author indicates a correlation between IT governance and organizational success. The author does not advance the inclusion of security risks and a need for a security training apparatus in the SME IT organization. Giovino addressed the significant growth of occupational crime and fraud and the corresponding increasing need for prevention and detection in the form of internal business audits to protect organizations. Giovino discussed that leadership discussions ethics and integrity should be the routine subject of an open forum (Giovino, 2015).

The purpose of the study was to inform the reader of the importance of open communication on ethics and integrity with respect to organizational cybersecurity. Giovino offered three conditions under which fraud may occur within an organization; (a) incidental pressures (sales or financial goal pressures), (b) opportunities to commit fraud (holes in the security system, unnecessary access privileges) and, (c)motivation for financial gain or disgruntled employee retaliation (Giovino, 2015). Giovino further advised organizations of the processes for reporting cybercriminal activity and the insurance recovery mechanisms that may be available to the victim organizations (Giovino, 2015).

The underlying assumption the author made was that organizational crime and fraud would continue to grow to advance the need for improved protection of organizations. Giovino further asserted that surprise audits, hotlines and training might avert future organizational losses due to fraud. The methodology was a qualitative narrative approach designed to inform the reader on reporting, preventing and recovering from the cybercriminal activity. The limitations of the study were that it did not address SME fraud prevention, detection, and recovery. Unlike larger organizations, SMEs do not typically have the funding required to support internal auditing techniques.

Data Warehousing and SME Cybersecurity

A study to assess the role central data warehousing might play in cybersecurity protection as well as possible correlations between warehouse maintenance and security breaches were the subject of concern in a Bamarara study. Bamarara used a quantitative methodology with a stratified random sampling approach to examine multiple bank types, job types, and work experience and types of threats encountered, in Uttarakhand is the approach. A qualitative data collection includes interview and schedule to support the analysis of the data.

Bamrara concluded from the data that there is a correlation between data warehouse functions and malicious code, identity theft, fishing and credit card fraud Bamrara did not find conclusive evidence of a correlation between denial of service and hacking in the data warehouse operational environment (Bamrara, 2015). Because of the study limitation to banking industries in Uttarakhand, the study population would require a much broader study to be generalizable. It is commendable that Bamrara chose a three-pronged approach (interviews, raw data, and literature review) to support the research. This approach does add to the validity of the study in contrast to the Holm, Holder, Andréasson, Baklien, and Rossow study which had a limitation to a survey only unidimensional based analysis (Holm et al., 2014).

Holm et al. presented a case for the use of expert judgment in situations where direct observation for data collection is not possible and present that credibility might be an issue in the use of expert judgment (Holm et al., 2014). Specifically, Holm et al. explored the use of expert judgment using three variables; consensus, experience, and self-proclamation and concluded that consensus is a good indicator for calibration of expert analysis as applied to cybersecurity analytics).

The methodology employed in the study was a random sampling survey-based quantitative analysis based on two research questions. RQ1 determines the variable (experience, consensus, and self-proclamation) impact on measuring expert judgment and RQ2 would determine potential correlations between the variables (Holm et al., 2014). It is possible that a qualitative case study approach might enhance the research and provide more direct observational data on the effectiveness of expert judgment in a real-life situation. The additional data collection would be an opportunity to support the study with functional data. An additional case study approach would add credibility to the study in terms of validity as well as provide the potential for further generalizability across organizational functions.

The Dark Web, Malware and Security Protection Costs

Web-based malware attacks in terms of the attack model, the root cause, and the enabling vulnerabilities that allow the attacks are a consideration from a study by Chang et al. (2013). They examined latest issues with malware as well as malware defense strategies such as honeypots, code and testing techniques and blacklisting attackers (Chang et al., 2013). In the study, Chang et al. discovered that there were approximately 45,000 URLs out of 18 million URL's detected by a security scanner and exhibited a linkage to spyware.

Of interest to my study is the application of the various malware detection virtual machines (VM's) like *Honeymonkey* and the possibility of capturing malware/spyware infused websites (Chang et al., 2013). The study was a computer survey-based analysis of the categories and approaches to discover, detect, and prevent malware attacks with the intention of the survey to be empirical in nature based on the evaluations of the data collected and the evaluation methods (Chang et al., 2013). Further work in malware detection and prevention in terms of software improvements is necessary. These attacks might occur as an issue of state to state strikes or might trickle down to state to individual (SME) attacks.

In a qualitative, literature based, narrative study, Dunn-Cavelty posited that there are general miss-guided policy issues with cybersecurity in that current practices to prevent cybercrime are not working and in fact are getting worse (Dunn-Cavelty, 2014). The policies, according to Dunn-Cavelty, are for security protection of the state as opposed to the individual citizen that has an adverse effect on the systems (Dunn-Cavelty, 2014). Dunn-Cavelty asserted that a cybersecurity policy oriented toward anti-vulnerability with a proclivity toward protection of individual privacy as well.

It was Dunn-Cavelty's position that the former without the latter is the genesis of cybersecurity vulnerabilities (Dunn-Cavelty, 2014). Dunn-Cavelty enumerated three factors that increase cyber risk. The need for fast software product delivery, the added benefits of the product increases the number of users, and quasi-monopolies all affect the production of secure software negatively (Dunn-Cavelty, 2014). Effective cybersecurity has become the victim of economics. Dunn-Cavelty concluded that a solution might be human-centric protection from vulnerabilities that may require a shift in policies that would voluntary increases in security measures from the corporate sector (Dunn-Cavelty 2014).

Reported primary cybercriminal activities (state-to–state) are questionable, and Filshstinskiy (2013) asserted that sophisticated cyberattacks could still be the work of mere cybercriminals of the DW (Dark Web) as opposed to state-sponsored activities (Epiphaniou et al., 2014). The purpose of the study was to educate the reader to be wary of claims of state sponsored crimes (terrorism) that might be theft. The philosophical approach was an attempt to differentiate between cybercrime and state-sponsored crime.

The underlying assumption was that there is a difference in cybercrimes and state-sponsored cybercrimes. The methodology was a qualitative narrative approach designed to inform the reader. Filshstinskiy listed six cybercriminal activities from e-mail to malware and demonstrated pricing as advertised by cybercriminals. For example, purchase of a denial of service attack software against a website can be between $50 and $500 per day depending on the site and the complexity of the offensive (Filshtinskiy, 2013). Further inquiry into international agreements and laws to prevent cybercriminal activity may be necessary.

Summary and Conclusions

In summary, the exploration of new knowledge about the issue of cybercriminal potential in SMEs through the study of SME organizational decision-making attributes and activities that might lead to exposure of private and proprietary data to cybercriminal activities might provide answers to the research question. Alignment of this study uses a two-prong approach to explore the possibility that the psychology of employee behavior in cyberspace and the cyberattacks and there is possibly a relationship with respect to internet access and employee vulnerabilities. Cybersecurity concerns appear to be a limitation relative to cyberattacks from outside of the business with little consideration for cyberattacks and risks (social engineering) from within the business. There is an inclination to trust employees inside the firm according to the literature assertions (Hutchings, 2012, & Tarafdar et al., 2013, Willison & Warkentin, 2013) that there is a general lack of awareness in SME enterprises with respect to the risk from insider cyberattacks through social engineering.

Due to the study theme, it is an expectation that two established theories will potentially converge into a new theory based on the data collection expected results. Space transition theory (Jaishankar, 2008) explains the vulnerabilities of employees to cybercrime through internet access, and moral disengagement (Bandura, 2009) might explain the cybercriminal ability to dismiss the morality of an action based on internet anonymity properties.

From these two theories, a third theory that may emerge from the study is that space transition theory and moral disengagement combine to create a new theory that explains vulnerabilities from both the victim and the criminal's perspectives that create the environment for crime. The purpose of this qualitative case study is to explore SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources.

This chapter was divided into nine major sections. The chapter includes the literature review search strategy, the study conceptual framework, the literature review introduction, cybercrime and psychology, cybercriminals, space transition theory and anonymity, cybercrime victims and, equipment and software. Chapter three includes the research method and design as well as the potential issues of trustworthiness for my study.

Chapter 3: Research Method

The purpose of this qualitative single case study was to explore what are the SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources. My data collection was an interview instrument based on 14 open-ended questions explored the typical small business owner's knowledge about internet security and employee access to the internet. This study was an exploration into the potential for SME vulnerabilities to cybercriminal activities through employee behavior and internet access by discovering how small business owners feel about the phenomenon. In this qualitative single case study approach, I conducted an interview with the proprietor of a small auto parts dealership located in north Alabama as a study participant to explore general knowledge of SME owners about cybersecurity.

Observation of the typical business activities and environment to understand potential vulnerabilities of employees and the business associated with internet access is a secondary method of data collection. The study participant was the owner of a small auto parts business located in north Alabama. The interview questions established what is known by SME owners about internet access and employee online behavior.

Research Design and Rationale

The dynamics of single case study design is useful for viewing patterns at the individual level (Barton et al., 2016). For my study, it was necessary to explore possible patterns in the knowledge of SME owners to gain an understanding of where insufficient knowledge of cybersecurity threats might present risks to SME owners. The rigor allowed by a single case study design allows the researcher to maximize the two functionalities of a single case study design and provides sufficient and clear documentation.

In my study, this would translate to the literature, and the participant's lens agrees and, (b) the observations and the data points obtained agree. This would mean that the interview responses and the literature agree (Barton et al., 2016). The Barton study gave three examples of single case study design. For my study, it is the first example of a single case study design that is of interest. This model requires that the core intervention (addition of knowledge to the SME owner’s cybersecurity awareness) adds the desired outcome (SME owners have the knowledge and ability to understand and protect themselves from internal and external cybersecurity threats.).

The single case study design has been argued as unscientific and has been rejected as a scientific approach by many researchers (Mariotto et al., 2014). The evidence presented to support this assertion was that there are Few examples of single case study approaches in reputable academic management journals (Mariotto et al., 2014). A major criticism of single case study design has been the lack of any comparison samples (causal relationships/a positivist lens). Although Mariotto et al. (2014) pointed out all the fallacies against a single case study design (internal validity, construct validity, objectivity) comparison samples may drive at the center of the issues. In other words, the real argument is about a lack of comparison and the remaining issues may be merely collateral or fallout to the lack of contrast problem.

Thick description and triangulation of the case a study is necessary to enhance the reliability of the single case study (Mariotto et al., 2014, Yin, 2014). My study involved member checking where the participant reviewed my interpretation of the data to assure I interpreted and captured the meaning (Madill & Sullivan, 2017) as the participant desired it (see Appendix C), as well as provide detailed observations and expert consideration of the study by my dissertation committee to validate the findings.

A single case study using a methodological triangulation approach with multiple sources is necessary to provide validity and reliability to the study (Yin, 2014). Triangulation enhancement occurred through member checking of the analytical results, peer review by my dissertation committee, and supporting peer-reviewed literature (Carter et al., 2014). Assurance of data validity also occurred by triangulation of the data (Carter et al., 2014). Peer review, member checking, and the use of reflective journal verification supported content validity (Carter et al., 2014).

The theory aligns with the qualitative approach because the study design is a meaning-making endeavor (Mariotto et al., 2014). Both theories could be, but have not been, applied to the study research question. In other words, Mariotto et al. (2014) will attempt to examine the meaning of the research question to the participant so that the theory framework will demonstrate that it applies as expected.

The qualitative approach aligns with the interview method because of the desire to base the study on real world observations for meaning making. The interview process aligns with the research question by asking the participant questions in person and recording the responses while observing the participan**t.** The frame of the case study is in support of the research questions

To dispel the assumptions among students that qualitative research is an art and artistic form as opposed to a classification of scientific research (Applebaum, 2012). Applebaum described four assumptions that students make as (a) scientific research is an empirical endeavor, and qualitative research is literary in nature, (b) qualitative research takes the of poetry and aesthetics and does not require the rigor of scientific methodology, (c) objectivity is the providence of natural science and has no place in human science (psychology) and, (d) qualitative research is an interpretation based approach as opposed to a scientific study plan (Applebaum, 2012).

The purpose of the survey was to inform students of the false assumptions relative to qualitative research and its scientific application. The philosophical approach was by way of articulating to the reader the relationship between art and science and that qualitative research may serve to de-alienate or de-mechanize science to provide genuine insight into the phenomenon. Not to oversimplify, but Applebaum is making the philosophical distinction between a creative writing exercise (art) and an actual qualitative research scientific study (science). Applebaum pointed out the risks in going from one extreme to the other. The creative interpretation of a phenomenon on one end of the spectrum to the other end of the spectrum which is strictly a quantitative, mechanical empirical analysis of an event.

Applebaum explored the many philosophical perspectives on qualitative phenomenological approach, particularly from the lens of the quantitative empirical research relative to the construction of theory and the potential disadvantages created by the purest natural science practical side of research, mainly that the purist approach may fallaciously exclude human factors in the natural sciences and render science as mere mechanical procedures (Applebaum, 2012).

The methodology was a qualitative narrative approach based on the literature and designed to inform the reader. Applebaum attempted to create a balance for the audience as to the risks involved in creative writing in research diluting the science required to validate the reasoning. Although it may be outside of the scope of the article, for completeness, mixed methods approach to scientific research might have been appropriate.

The small business survival rate after 4 years is 50% in the United States (Cader & Leatherman, 2011). Cader and Leatherman asserted that omission of relevant data in previous studies on the phenomenon based on only surviving businesses might lead to erroneous conclusions (Cader & Leatherman, 2011). For the purposes of my study, review of future data may reveal the possible impact of cybercriminal activity on SME failures.

Cader and Leatherman explored previous studies where the conclusion was that small business entries and exits could be due to overall industry conditions where the exit rates may have a connection to high entry rates (Cader & Leatherman, 2011). The objective of the study was to determine bias in the sample selection due to the exclusion of data about firms that had failed to survive. The methodology used was a switching model developed by Heckman and Vella where variables of interest observed or industry employment observations (Cader & Leatherman, 2011).

Conditions for failure were reverse engineered to include the variables of interest in the failure causes using a three-step process; ordinary least square, a probit model for Mill's inverse ratio, and then a re-estimation of the ordinary least square model based on the Mill's ratio model (Cader & Leatherman, 2011). It is an assessment of the model against nine variables of interest that may affect three industries. Cader and Leatherman concluded that the previously omitted data may have erroneously inflated the model in previous studies and that technology intensive firms were more likely to fail within five years as opposed to the previous economics-based model (Cader & Leatherman, 2011). There were no recommendations for further study, but I think more variables for inclusion might be lead to an understanding of the potential role that cybercriminal activity might play in SME business failures.

There are two fundamental questions of the reliability of a study. The first question is how faithfully the test reflects the domain (environment) and two, do the tests match the background attributes (Thorndike, 1985). Thorndike approached the reliability of a study as absolute or relative precision. Relative precision asks a question in terms of entity comparisons. Precision reliability measures the variability between entities (Thorndike, 1985). In other words, reliability can be thought of in the two planes of comparison and variability. Thorndike's underlying assumption was that each type of assurance approaches has a particular purpose.

Correlation indices are useful for comparisons, and absolute measurements are helpful for determining variations (Thorndike, 1985). The methodology used in this study was a qualitative, narrative approach to educating on the differences in the matter of reliability strategies. More work might be useful in reliability in terms of ethical factors that might influence a reliability study such as politics, religion or social status. This study has application to my topic because it illustrates the two principle applications of reliability to any study. In my study, it will be necessary to explore relationships between what the participant does know to what the participant should know about cybersecurity in an SME to answer the research question

Role of the Researcher

In my role as the researcher, I am the instrument as an observer and the interviewer. I was not involved in the businesses activities but was observing, journaling and asking questions to understand the activities. This is a best fit role since observation without involvement allowed me to conduct an unbiased study of the business processes as discussed by Yin (2014). If I had been involved in the process, I might affect the behavior of the participant. Yin warned that a participant observer might create bias by manipulating events (Yin, 2014). In a qualitative case study research approach, the researcher is especially susceptible to bias because of the need to understand the issue that I am addressing in the study in advance. This understanding may influence the researcher towards supportive data and away from contrary data (Yin, 2014). Like my approach, Hutchings (2012) and Tarafdar et al. (2013) have asserted that SME owners will not have sufficient knowledge of cybersecurity, so I was able to ascertain if the postulation is true through observation.

I have no personal relationship with the participant. There are only brief, casual professional instances of a proprietor (the participant) to the customer (myself) relationship. There is no power relationship between myself and the participant. The participant has volunteered to participate in the research but at this point only has received very cursory information about my study in a single discussion. Data collection is pending IRB approval. Due to the nature of the study, it was important that the participants answer to the interview questions were with limited exposure to the details of the study to obtain an unfettered view of a randomly selected SME owner and his general knowledge about SME business cybersecurity.

I acted as an individual observer of the case study and, therefore, I provided a clear and unbiased assessment with respect to the research question and the interview results. Based on the literature, it was an expectation that the participant would demonstrate emerging patterns and themes of a complete lack of knowledge about his vulnerabilities when it comes to cybercrime as noted by Hutchings (2012). This same expectation can apply to any SME.

Case study research design differs from other research designs in that there is less control of the environment by the researcher (Yin, 2014). In the laboratory or the survey questionnaire designs, the participants are under the control of the researcher to a larger degree in terms of the data collection methods. In a case study design, the researcher relies on observation and direct interview questioning for data collection (Yin, 2014). As the researcher, I needed to exercise personal discipline in the data collection process to avoid distractions in the observation and interview phases. The participant reviewed the data analysis to ensure the quality and accuracy of the content prior to inclusion into the study as recommended by Yin (2014).

Methodology

For this case study, the application of the Yin approach to case study description using an analytical approach to explanation building is the desired approach (Yin, 2013). Since it is an expectation to learn why SMEs may be vulnerable to future cybersecurity breaches, it is also an expectation that the case study research will offer links to the rationale for the knowledge deficit if any and provide insight into the connection between business risk exposure by employee internet access behavior and the threat of cybersecurity breaches. A case study using a methodological triangulation approach with multiple sources is necessary to provide validity and reliability to the study (Yin, 2014). Implementation of triangulation is through member checking of the study results, peer review and supporting peer-reviewed literature (Carter et al., 2014). Assurance of data validity is by triangulation of the data (Carter et al., 2014). Peer review, member checking of the results (Madill & Sullivan, 2017), and the use of a reflective journal as verification supports content validity (Carter et al., 2014). Assessment of ethical concerns for data collection will be through the IRB (Institutional Review Board) evaluation and in the ethics section of this dissertation to address protection of participants.

Participant Selection Logic

Sampling is a major determiner for the success of a project. Grounded theory aside, qualitative approaches to saturation are less developed (O'Reilly & Parker, 2013). For my study, I have selected a qualitative single case study design based on the criteria provided by the literature. My research involves the security risk that employees of SMEs might create for a business due to internet activity either at work or at home; therefore, a single case study would be necessary to provide insight as to how those activities might avail themselves and how they may manifest into a financial or legal crisis for the business. Yin offered some advice for how a single case study approach might work for a study like mine.

There are four criteria for what constitutes the possibility for a single case study design using a rich explanation of the events (Yin, 2014). The events must be sequential and irreversible. In my case, an employee must pose a potential risk to the business, and that risk cannot be reversible. The catalyst events must always follow other events based on a contingency. In my case study, the data should demonstrate that employee internet access may create a risk to the business. A constraint of events by a time interval is necessary (it must be decisive that event “A” is a cause of event “B”). In my case study, it could be a conclusion that it is possible that employee internet access can lead to risks to the business to validate my research I will be taking a constructivist perspective in the study because, in my study, the truth can be based on the SME owner’s perspective.

Yin stated that a classification time periods of events in a case study could be different from other events. In my case study, a demonstration that employee internet use activities that create risk to the business are not an influence other business activity events are necessary (e.g., in my study, a hardware malfunction does not produce loss of information, but due to the employees exposing the company to risk through online activity. For my single case study design, the potential for risk to a business due to employee internet use is attributable to that activity alone, irreversible and repeatable. Because access to a rural small business that uses the internet for transaction processing is a unique opportunity for the study design, the study results are relevant as noted by Yin (2014) with respect to contributing to the body of knowledge.

I believe from the literature those criteria can apply to my study. This can also translate into a single case study design through the research question because the literature assertion that SME owners have no knowledge of cybersecurity (Hutchings, 2012; Tarafdar et al., 2013) may be either true or false in a single case study. In other words, if the SME owner demonstrates sufficient knowledge about cybersecurity to falsify the assertion, then I have reached data saturation by falsifying the assertion. If the SME owner demonstrates insufficient knowledge about cybersecurity, then the assertion is true, and I have reached saturation. The potential saturation issue being that if the SME owner proves the assertion true, the single case could provide sufficient evidence to uphold the assertion.

If the data is not saturated by expected means (replication, no new data emerging, and when further coding is no longer practical (Fusch & Ness, 2015), I have two options with a case study design; I can attempt to replicate the existing data with additional interviews, observations, case studies as required, or I can end the study with the findings

I have and present the remainder of the study as opportunities for further inquiry if data saturation is going to be too costly and time-consuming.

For example, if my single case study answers the research question in that it is a discovery that employees are a risk to SMEs when online, but the data does not establish the possible occurrences of that phenomenon, further observations or interviews with the participant may be necessary. Yin’s four levels of questioning could provide additional data relative to the study by using the second level of questions (mental line of inquiry that reveals the researchers thinking (Yin, 2014), or potentially would indicate the need for further studies.

For my study, the participant is selection consists of a small business in rural North Alabama. The selection logic is that a small rural business might be most representative sample of the least internet security savvy sample with the least exposure to cybercrime activity and protection. The participant selection is based on proximity to my home and is a random sample because the business location is not under the control of the investigator. In other words, my proximity to the firm is not by design and could be considered as random.

Instrumentation

There were two primary methods of data collection. The first was by observation. As the researcher, I observed the participant’s business for two weeks to understand the operations and functions of the member’s business for an assessment of cybersecurity protection practices. To aide in the exclusion of any researcher bias, it was necessary to observe the business as an outsider so that the observations are a representation of a holistic type 1 single case design (Yin, 2014). The observation of the activities is of importance to the study, and an outsider overview of the business functions would provide an objective perspective without the reflexive influence of involvement in business activities by the researcher (Yin, 2014**).**

I performed unobtrusive observing of the business activities as a casual by-stander. It is an expectation that much knowledge about the typical small and medium business activities from an outsider perspective is available. It is necessary for SMEs to make informed decisions about cybersecurity measures (Ponelis, 2014). A single case study design using observation for data collection contributes to the understanding of a study (Morgan, 2016) and unobtrusive observation served to surface business cybersecurity decisions that may be negatively affecting the business processes. For example, observations that the business owner might leave a computer work station unattended.

There are three types of qualitative interviews (a) the structured interview, (b) the unstructured or semi structured interview, and (c) the group interview (Myers & Newman, 2016) Since my study is a single case study with a single participant, a group interview is inappropriate. According to Myers and Newman, in a structured interview, there is preparation, and a complete script and that script is strictly adhered to. To answer the research question, it is desirable for impromptu participant responses to the interview questions in my study. Therefore, a semi-structured interview process would be the most likely to produce the results that will answer the research. This is also the reason that the interview questions are open-ended and hypothetical. This could probably provide the insightful explanations and personal views of the participant (Yin, 2014).

Caution was necessary on my behalf in the interview because the participant may have a desire to give only the minimum the researcher wants to hear (bias), and create inaccuracies due to poor recall and the possibility of poorly designed questioning, as discussed by Yin (2014). A qualitative interview is a potent data gathering instrument when managed correctly (Myers & Newman, 2007). The interview protocol and the interview questions are researcher designed. A digital recording of the participant interview and a transcription of the recording after the interview will reduce the possibility of bias by the researcher (Gill, Stewart, Treasure, & Chadwick, 2008; Ponelis, 2014). The design of the interview questions is to learn what a typical SME owner knows about computer security that will in turn answer the research question.

Procedures for Recruitment, Participation, and Data Collection

The research question for this study is the following: What is the level of consensus among small business owners as to the key elements of decision making for SME investment into cybersecurity and education for employees with respect to internet access and employee vulnerabilities? The sample size must reach saturation to create validity in a study and to answer the research question. Fusch and Ness asserted that there is neglect in research data saturation because data saturation is a difficult idea to define (Fusch & Ness, 2015). There are four available approaches to assure content validity: (a) construct validity, (b) internal validity, (c) external validity, and (d) reliability (Yin, 2014).

In my study, to answer the research question required a single case study analysis because a single case study would demonstrate or refute the lack of knowledge that the prevailing literature asserts, as found within Hutchings (2012) and Tarafdar et al. (2013). Therefore, in this case, it was better to use a small sample size with rich and thick data from a single source that would provide ample data for the study. Were the research question different, it might be necessary to entertain a larger number of case studies. In my study, a smaller sample size will allow me to go more in-depth with a single case, which will be necessary to understand the participant's perceptions of security threats (or lack thereof).

I (the researcher) collected the data for the study. Data collection frequency occurred over a two-week period with three to four hours of observation per day where I was present at the business for the purposes of collecting the observation data part of the study. I conducted an interview after the completion of the collection of the observation data. An extensive observation period is a requirement because lapses in cybersecurity may occur intermittently, and Yin recommends an intensive observation period (Yin, 2014). Collection of the observation data requires the use of observation sheets to record the observed data and use of digital audio to record the participant interview with a subsequent verbatim transcript that provided data integrity and reduced bias in the data collection. (Rowley, 2012) It is necessary to carefully review and audit transcript data to ensure accuracy (Tuckett, 2005).

The data collection and subsequent analysis may require more case studies to complete the review, a determination by the researcher to finish the study with the available data or request further case studies as a consideration for future researchers as part of the conclusion of this study. After the study, there was a thank you to the participant, and the participant received a copy of the study. The participant had an opportunity to ask any questions about the study. Then I provided the member with details on the protection of his identity.

Baxter and Jack developed a criterion for novice researchers to explore and research through qualitative case study approaches to answer research questions. The purpose of the study was to inform novice researchers as to the advantages and disadvantages of case study research and case study research designs applicability to research questions. The philosophical approach was to define specific elements of case study design to aid novice researchers in selections of the appropriate techniques to answer the research questions with case study designs with the case study being the actual unit of analysis. They proposed there are three questions that to determine the type of data is collection: does one wish to analyze the individual, the organization, the program, or the process (Baxter & Jack, 2008). In my study, my unit of analysis will be the SME process since that would be where the potential cybercriminal activity might manifest itself. In my single case study design, I acted as a non-obtrusive observer in the case study work environment as described by Holmila, Holder, Andréasson, Baklien, and Rossow (2008). For the purposes of the study, it was necessary to observe the business activities on a non-interference basis to discover potential issues with cybersecurity and the interactions between the clients and business employees.

Issues of Trustworthiness

Credibility

Credibility and reliability of a case study are based on the ability to replicate consistent research procedures (Yin, 2014). Reliance is subject to the fundamental norm of sensible guidance (Alonso, 2016). In my single case study design, the sensible guidance will be the standards and procedures the literature provides in the research disciplines. Since the literature has asserted that SME owners should not be aware of cybersecurity threats, my data collection methods are an effort to ascertain the extent of knowledge that a typical SME owner might possess relative to cybersecurity vulnerabilities. A single case study using a methodological triangulation approach with multiple sources is necessary to provide validity and reliability to the study (Yin, 2014). Triangulation enhancement is through member checking of the analytical results, peer review by my dissertation committee and supporting peer-reviewed literature (Carter et al., 2014). Assurance of data validity also will be by triangulation of the data (Carter et al., 2014). Peer review, member checking, and the use of reflective journal verification support content validity (Carter et al., 2014).

Data Analysis Plan

Yin suggested a five-step strategy for case study data analysis. The first step is to put the data into different arrays (Yin, 2014, p, 135). For my study, it will be important to review what data the participant provides from three different perspectives (a) the cybercriminal, (b) the employee, and (c) the business owner (participant). The second step is to matrix the data into the categories from the first step (a, b, and c in my study). The third step in the process is to display the analyzed data as graphically and by charts for examination. For this step, coding of the data using QDA Miner and NVivo software to develop the graphical analysis into charts that provide a meaningful display of the results is necessary (see Appendix G).

The fourth step will be tabulating the data into the frequency of events. In my case study, this may be a comparison of the observations to data from the interview process and what the participant agrees is correct in the data analysis during member checking, as recommended by Yin (2014). The final step involves putting the events (observations and interview results) into a time or order for sense-making of the collected data (Maitlys & Christianson, 2014: Sharma & Good, 2013). Sense-making in information systems has been a complexity as it applies to a user centric model (Olson, 2016). Translation of cybersecurity terminology into language that a participant can relate to or understand carries the same burden of complexity. For example, my participant was unaware of the term social engineering. Dervin developed a sense-making methodology (SMM) for audiences to provide data to inform institutions on policies and procedures for institutions with a public service mandate (Foreman-Wernet., & Dervin, 2017). From their work, they further developed five examples of sense-making applications.

Of interest to my study would be the element of sense-making for a specific cultural product (the SME cybersecurity protection paradigm). This application addresses the use of or engagement with a particular cultural product (in this case, art and music and my case cybersecurity). In the study, Wernet-Foreman and Dervin were able to collect data about art pieces and the viewers perspectives on them; similarly, in my study, I was able to translate between the techno-speak and the participants perspectives on the applications of the technology for his business. In the example above, the participant is able to obtain a clear grasp of what social engineering is and its potential impact to him by explaining the different types of social engineering offenses such as dumpster-diving, or shoulder surfing. It then became clear to the participant the potential risks in leaving work stations unattended (Simms, 2016).

Sense-making between myself and the participant is imperative to the accuracy of the data collected because of the requirement of the participant and I to both understand the collected data on the same terms (making sense of the data) as a part of satisfying member-checking. Commensurate with the observation data collection phase, comprehending of the data was necessary. I used initial or broad coding to uncover and develop the emerging concepts, as described by Houghton, Murphy, Shaw, and Casey (2015).

An assessment of the participant interview responses using QDA Miner and NVivo software for coding produced the necessary graphics and charts the data yields**.** Measurements of the participant responses against what the literature asserts that the participant's concerns for cybersecurity should be and what the participant's interests are were analyzed. Software programs such as QDA Miner and NVivo software use word frequency analysis to explore what the data review reveals between, the observations, the interview results, and the literature (Yin, 2014).

A measurement of the participant's responses against what the literature assertion for what the concerns should be and the observation notes regarding what the processes are, provide a conclusion about the literature assertions. The delta difference in the data analysis and the findings to answer the research question (triangulation) is presented in both chart and narrative forms. A single case study using a methodological triangulation approach using multiple sources was necessary to provide validity and reliability to the study (Yin, 2014). Triangulation enhancement is through member checking of the analytical results, peer review and supporting peer-reviewed literature (Carter et al., 2014).

Assurance of data validity also was by triangulation of the data (Carter et al., 2014). Peer review, member checking, and the use of reflective journal verification support content validity (Carter et al., 2014). Attention to ethical concerns for data collection was under the prevue by the IRB (Institutional Review Board) for the data gathering and in the ethics section of the dissertation to protect participants. The theory aligns with the qualitative approach because the study design is a meaning-making endeavor (Mariotto et al., 2014). Both theories have been, applied to the study research question. In other words, I explored the meaning of the research question to the participant so that the theory framework demonstrates that it applies as expected.

The qualitative approach aligns with the interview method because of the desire to base the study on real world observations for meaning making. The interview process aligns with the research question by asking the participant questions in person and recording the responses while observing the participan**t.** The frame of the case study is in support of the research questions. Documentation of discrepant cases or discrepant data discovered in the analysis is part of the study findings and conclusions in chapters three and four.

Yin suggested that the fifth component, or criteria for interpreting the study results, is a consideration for statistical analysis. For a case study design, it may be necessary to explore other factors for exploring the data (Yin, 2014). One avenue for consideration is the exploration of rival explanations for the study findings. For example, as opposed to considering one explanation for a lapse in judgement over security protection in the business, there may be alternative explanations to consider. The literature review has served to address many rival explanations for potential cybersecurity issues that SME businesses may encounter. As part of the chapter four data analysis, these rival explanations are a consideration and were subject to evaluation as part of the study findings. The study research question, the study proposal, and the units of analysis (interview results and observation findings) subsequently lead to the interpretation and analysis of the findings (Yin, 2014).

Transferability

For my study, I have selected a qualitative single case study design based on the criteria provided by the literature as found in Yin (2014). Because my study involves the security risk that employees of SMEs (small and medium enterprises) might create for a business due to internet activity either at work or at home, a single case study would be necessary to provide insight as to how those activities might avail themselves and how they may manifest into a financial or legal crisis for the business. Yin offered some advice for how a single case study approach might work for my study.

There are four criteria for what constitutes the possibility for a single case study design using a rich explanation of the events. The events must be sequential and irreversible. In my case, an employee must pose a risk to the business, and that risk must be irreversible. The catalyst events must always follow other events based on a contingency. In my case study, there must be a demonstration that employee internet access may create a risk to the business. The events must be a constraint by a time interval (it must be decisive that event “A” is a cause event “B”). In my case study, it must be a conclusion that it is possible that employee internet access can always lead to risks to the business. Finally, Yin stated that time periods of events in a case study could be a classification of different from other events. In my case study, there must be a demonstration that employee internet use events that create risk to the business is not an influence of other business activity events (e.g., in my study, a hardware malfunction does not produce loss of information, but could create risk due to the employees exposing the company to risk through online activity. For my single case study design, the potential for risk to a business that an employee may create by internet use must be attributable to that activity alone, irreversible and repeatable.

Access to a rural small business that uses the internet for transaction processing is a unique opportunity for the study design; the study results might be relevant (Yin, 2014) with respect to contributing to the body of knowledge. I believe from the literature (Bandura, 2009; Jaishankar, 2008) those criteria area applicable to my study. This can translate into a single case study design through the research question because the literature assertion that SME owners have no knowledge of cybersecurity (Hutchings, 2012; Tarafdar et al., 2013) may be either true or false in a single case study by demonstration. In other words, if the SME owner demonstrates sufficient knowledge about cybersecurity to falsify the assertion, then I have reached data saturation by falsifying the assertion. If the SME owner demonstrates insufficient knowledge about cybersecurity, then the literature assertion is true, and I have reached saturation. The potential saturation issue is that if the SME owner proves the assertion true, a single case may provide sufficient evidence to uphold the assertion.

Dependability

Yin described dependability (or reliability), as the ability to obtain the study results using the same procedures furnished by the study (Yin, 2014). For my study, this task would be an easy accomplishment. In another case study, a researcher need only conduct another case study to either prove or disprove the Hutchings and Tarafdar et al. assertions that SME owners and employees do not have should not have the background and knowledge necessary to adequately protect the business from cyberattacks and threats (Hutchings, 2012, & Tarafdar et al., 2013). Though the findings may be different, the same case study procedure and literature review would either prove or disprove the findings of this case study. In other words, this case study seeks to obtain what knowledge SME owners have about cybersecurity. Another case study using the same procedures would collect the same data (an SME business owner's knowledge about cybersecurity).

Confirmability

Observations of actions may cause participants to proceed differently (Yin, 2014). To negate this possibility, I conducted the observations ahead of the interview Yin referred to this as reflexivity. I felt that the interview may cause the participant to act differently to demonstrate knowledge of cybersecurity based on the knowledge gained about the study because of the interview. I felt that the sequence will be important for me to maintain as much objectivity as possible in my role as the researcher and reduces the possibility of contaminating the participant with pre-observation knowledge about the study. Credibility and reliability of a case study are based on the ability to replicate consistent research procedures (Yin, 2014). Replication of the literature review research can be using the key word search procedure in the chapter two literature review section as well as the collection of data from more small business owner participants.

Ethical Procedures

Research is of importance to developing public policy for solutions to urgent social problems (Graf, 2017). Attention to ethical concerns for data collection was under the guidance of the IRB (Institutional Review Board) of Walden University for the data gathering, recruitment and protection of the participant and is in IRB section to protect the member. Appendix D contains the participant consent form that the participant signed for acceptance to participate in the study. Recruitment of the participant was through personal contact of the business owner and verbal concurrence to take part in the study.

The participation of the study participant was strictly voluntary, and information in writing was available to the participant of his right to withdraw from or desire not to participate in the study at any time with no consequences. The participant does not fall under the category of protected status by the definition of the National Institutes of Health (https://www.nih.gov/). The focus of this study will be on participant well-being during data collection and publication (Kara & Pickering, 2017) The IRB approval number for this study is 11-09-17-0313103, and it expires on November 8th, 2018.

The collected data will be under the protection of myself. No data revealing the identity of the participant will be public. All collected data from the interview and observations will be under the protection of myself and kept in a metal box with a physical lock on the storage device that only I will have access to. The published dissertation data will not contain any identifying properties of the business owner or the business. Destruction of the hardcopy data will occur after the completion of the Universities five-year requirement to retain the data collected for the study.

I am not an employee of the small business and have no relationship with the owner or the other company employees. To my knowledge, there are no conflicts of interest between the researcher (myself) and the study participant.

Summary

In this chapter, I established the methodology, research design and rationale, data collection and data analysis procedures, and addressed the issues of trustworthiness. The purpose of this qualitative single case study is to explore SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources. Data collection will be an interview instrument based on fourteen open-ended questions that will explore the typical small business owner's knowledge about internet security and employee access to the web.

This study is an exploration into the potential for SME vulnerabilities to cybercriminal activities through employee behavior and internet access by discovering how small business owners feel about the phenomenon. In this qualitative single case study approach, an interview with the proprietor of a small auto parts dealership located in North Alabama as a study participant to explore general knowledge of SME owners through the observation and interview process.

Observation of the typical business activities and environment to understand potential vulnerabilities of employees and the business associated with internet access is a secondary method of data collection. Since the study participant is the owner of a small auto parts business located in North Alabama, the interview questions establish what is known by SME owners about internet access and employee online behavior from the perspective of a rural small business owner. Chapter four includes the results for the data collection and analysis.

Chapter 4: Results

The purpose of this qualitative case study was to explore SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources. The research question is RQ- What are the SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources? This chapter is the results part of the study. To satisfy the purpose of the study, I needed to explore an SME organization that has exposure to the potential for loss of commerce through the infiltration of computer systems by cybercriminal social engineering techniques. It is necessary to explore SME owner decision factors such as cost and time impacts to the business to provide security protection from cybercriminal infiltration efforts. Weiderhold asserted that the human factor is the weakest link in cybersecurity and as a researcher in the field, I must agree based on the literature (Jaishankar, 2008; Tarafdar et al., 2013), and the study results. Therefore, the focus will be on potential human factors for SME vulnerabilities.

This chapter contains the research setting description along with detailed figures of where the study has taken place as well as possible organizational features that may expose the business to cybercriminal attempts such as budget issues, personnel changes, and other distractions. The chapter includes data collection techniques, demographics of the site and data analysis of the data collected at the research site. This chapter contains the data in support of the findings. Finally, I address the evidence of trustworthiness for this study. As stated, the research setting begins chapter four.

Research Setting

From my observations, the location of the business in a rural county with only one chain store business within a mile. If any, the chain-store wi-fi router signal strength is insufficient to reach the participants business (see Figure 1). The business isolated from any telecommunications activity except for hardwiring and cell phone activity. Cultivated farmland surrounds the business for about a half mile with a large gravel parking lot connected to a rural two-lane highway. The gravel parking lot has a connecting drive that surrounds the building and is an access for loading and unloading at the three bay doors on the south side of the building. The front entrance faces the parking lot and is on the west side of the building. There is no egress or ingress access elsewhere on the building. Inside the store, walls have product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door). Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair, etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches.

Data collection occurred over a two-week period including four hours a day for four days including November 27th through November 30th and December 5$_{th}$ through

December 8th (a total of 32 hours at the site). These study dates were between the Thanksgiving and Christmas holidays, so the participant and the patronage were in festive spirits during the data collection period. The festive atmosphere served me well for the study since the only distractions during data collection were of a positive nature. There had been no known negative events relative to personnel, policy or procedural changes.

The first day I arrived early (about 7:30 am) with coffee and donuts for the participant and anyone who would care to share them. It was then that the participant informed me that he had diabetes, so we laughed and drank the coffee as he shared the donuts with incoming customers. The participant provided an area with a stool at the counter so that I had a great view of all the activities in the business. From this vantage point, I could log observations about the business layout (see Figure 2) and customer activities. I was particularly interested in the security of the building and that provided insight as to the security concerns of the participant that might benefit my study. Figure 3 is a network schematic that illustrates the layout of the security, phone, and internet provisions for the business.

For the next two weeks, I observed operations and the participant made me very comfortable in the research setting by discussing areas of the business and the clientele. The participant was very helpful and cordial throughout that data collection process and freely answered any questions about the business that I asked him. On the last day, I provided sausage and biscuits (not to repeat the donut error), and coffee and the participant and then I conducted the final interview.

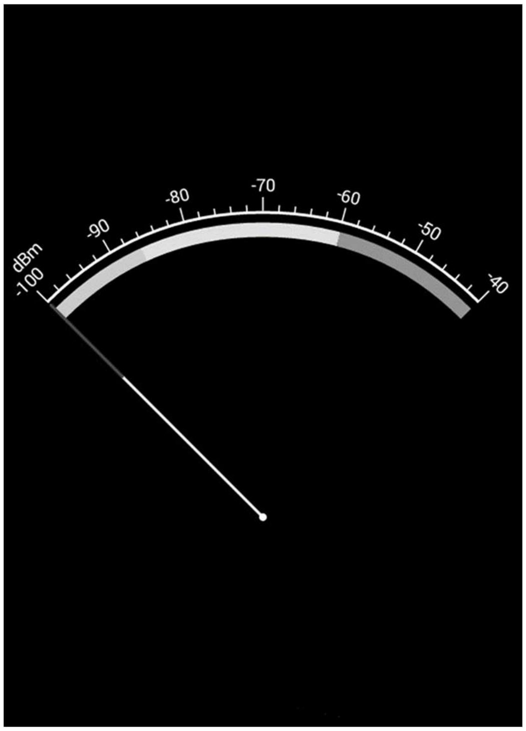


Figure 1. Wi-Fi scan of the premises.

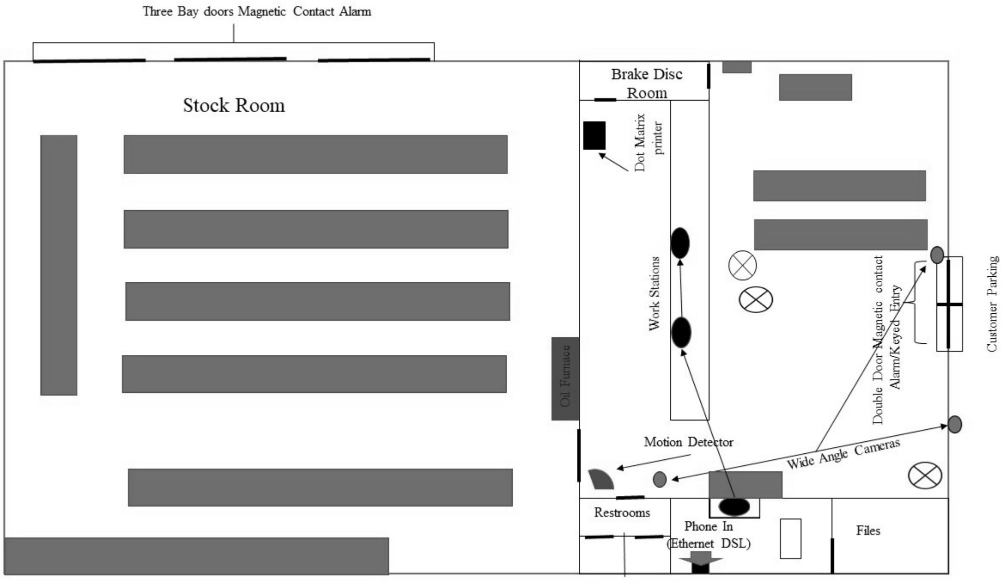


Figure 2. Building layout.

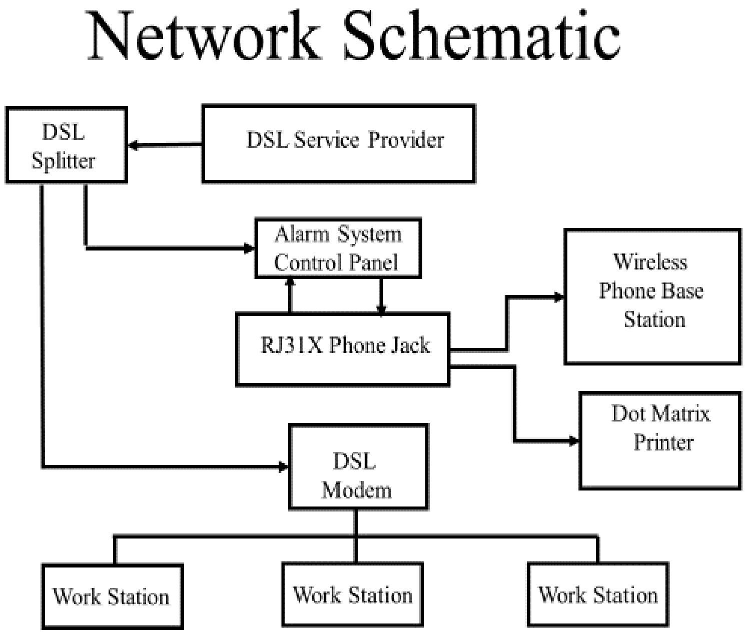


Figure 3. Network schematic.

Demographics

The participant is a middle-aged, Caucasian single male. The business is co-owned by his sister who is responsible for the business accounting and administrative activities. The sister spends the majority of her time at a desk in the office paying bills, doing book keeping, and administration activities. I had very little inter-action with the sister during the data collection process. The brother was the focus on the data collection because he was responsible for the computers and building security functions. Both owners are very polite and friendly and have an easy-going country way about them. The brother and focus of the study, has straight grey hair parted to the left, and grey bearded and wore reading glasses at times. He dresses in blue overalls every day, usually with a blue work shirt. They both act as employees as the need arises.

The participant stated that neither are “particularly tech savvy” in an informal discussion, but from my observations and reflexive notes (see Appendices R and P), the participant knows enough to keep the system functioning and fairly secure with a heavy reliance on third-party tech support. In an informal discussion, the participant did not know the difference between a router and a modem when asked, but did know who to contact should issues arise on the system; “I just call my tech support guy is there is a problem.” According to the participant, the clientele is “about 98% farmers and the other 2% are a regular walk-in trade (meaning they do not represent a demographic). As an observer, I noticed based on conversations that there were also county workers that made transactions at the business on behalf of the county. From discussions, they were largely road construction workers purchasing truck repair items. The business has been in operation since May of 1999. Because of the rural nature of the business, most of the customers were well known to the participant who acts as both employer and employee. The business does hire other seasonal employees at peak farming times during the spring, summer, and fall. Winter (the time of this research period) is slower for the business since farming crops activity slows down during this period. The timing worked to my advantage as the researcher since the participant was not too busy as to accommodate my data collection process and the study length offered opportunities to observe some peak customer traffic hours.

The business has no web-site. Only the internet white pages and a small Facebook area that simply provides minor local advertising and the possibility for customer feedback or reviews but not real substance about the business. The Dell work stations main purpose is to provide access that the national chain warehouse database for ordering merchandise for stock and sales. Most advertising is through local area billboards and signage.

Data Collection

This is a single case study design. The single participant approval on the consent form occurred on November 27th, 2017. All data collection is from a single site and one participant. Data collection occurred over a two-week period of four hours a day for four days including November 27th through November 30th and December 5th through December 8th. During this period, data collection was in the form of observation logs and reflexive journaling. Data collection was between Thanksgiving and Christmas, so the participant and the patronage were in festive spirits during the data collection period. Tese aqctivities served the study well since the only activities during data collection were of a positive nature. There had been no negative events relative to personnel, policy or procedural changes. Other key milestones in the data collection phase are the interview on 12/27/2017, transcript review on 12/14-18/2017 and final member checking (see

Appendix C) approval of the data was on March 3rd, 2018. Polkinhorne asserted that data gathering from participant interviews is the most prominent of the qualitative research tools. Both formal interview and informal discussions were the focus of his study over observation, documents, visual data, and artifacts (Polkinghorne, 2005).

Recording in the observation logs (see Table 1) were daily and throughout the observation period. There were no known variations in the data collection and collection proceeded as planned and on schedule. The observation of the activities is of importance to the study, and an outsider overview of the business functions provided an objective perspective without the reflexive influence of involvement in business activities by the researcher (Yin, 2014**).** A single case study design using observation for data collection contributes to the understanding of a study (Morgan, 2016) and unobtrusive observation might serve to surface business cybersecurity decisions that may be negatively affecting the business processes.

As the study observer, I was particularly interested in how often the work stations are unattended such that there would be an opportunity for social engineers to access the system and do damage or obtain information. The recorded formal interview was approximately 45 minutes. The participant gave relatively short and concise answers to the interview questions. The participant seemed a little nervous and gave some contemplation to each answer. Satisfaction of data saturation occurred on the third day of the second week when observation logs and reflexive notes began to repeat (Fusch & Ness, 2015).

Another angle for data saturation is that the SME owner demonstrated sufficient knowledge of cybersecurity concerns to invalidate the literature that SME owners do not know cybersecurity (Hutchings, 2012; Tarafdar et al., 2013). The owner has concerns that he may be unprotected but is providing the cybercrime defenses (see Appendix J) that he felt were adequate such as a firewall and complex password protection. As the participant stated; “Well I think, you know, that if you make a password that somebody wouldn’t think of you know, I think you would be Okay, but you don’t want to use your uh, uh, address or something like that.”

Table 1

Observation Log Example

Date: 11/28/2017 Time: 07:00-7:30	Observed a wide-angle security camera attached to the drop ceiling on the back-left corner from the entrance of the building. The camera covers the entire store including the counter work stations. Activity on the work stations is not discernable on the video, but a person using the system would be discernable on camera and a determination from a date and time could show when a person is at the workstation. Added to store floor plan.

On December 7th, the last day of data collection, the participant underwent the interview portion of data collection (see Appendix B and Appendix J). To conclude after data analysis, a follow-up interview for clarification based on the collection results that included the analysis of the original interview results, the reflexive journaling, and the observation logs. The only unusual circumstances during data collection were the events surrounding the holiday season such as passing out of calendars (a yearly holiday event for the business with a choice of tractor or barn themes). Other holiday events were bringing in holiday cookies and cakes, preparations for the local Christmas parade the business owner participates in as Santa Claus.

Data Analysis

Story telling in data analysis is important to convey what the data reveals through scenario building (Carbonell, Snache-Esguevillas, & Carro, 2017). In this study, scenario building is crucial because I am attempting to demonstrate the potential risks to SMEs through potential security breaches and the likely scenarios under which those breaches may occur. For example; an angry employee or customer sabotaging internet access for retaliation against the owner might be of concern. As part of the data analysis story-telling process, one uses graphics and charts to aid in the visualization of the data analysis story (Carbonell et al., 2017; Firmin, Bonfils, Luther, Minor, & Salyers, 2017).

Data text analysis by software programs provides information about the types of words used and a platform for organizing those words into categories or themes (Firmin et al., 2017). Using NVivo and QDA Miner, a word frequency test reveals the themes. Using the same software for coding of the themes (see Appendices N through R and Table 2), presentation of the relevance is in the form of, pie, bar and word cloud charts and the tables in this section.

Data coding development was by QDA Miner and NVivo software and word frequency analytics to develop themes (see Appendix G). Global analysis refers to the analytics of the data in its entirety; the carefully, reviewed interview results (Tuckett, 2005), recorded formal, informal and final interviews, the observation logs, and the reflexive notes (see Appendix M and Appendix I). An example of the development of an individual theme from the interview analysis would be that a participant concern is that somebody could intrude into the business computer system. In the data analysis of the observation logs, I found that although this is an infrequent occurrence, an individual familiar with the business could conceivably plan a purchase request such as a hydraulic hose purchase that might keep the business owner at bay leaving the system unattended, as noted by Simms (2016). In this case, the unknown somebody has a connection to the elements of threats as shown in the Appendix K word cloud and is within the percentage value of 10% (security negatives) in Table 2.

As stated in chapter three, Yin suggested a five-step strategy for case study data analysis. The first step is to put the data into different arrays (Yin, 2014, p, 135). Use of graphs and tables is important to a study because they aid in communicating strengths and weaknesses effectively (Leggett, 2017). For my study, it will be important to review what data the participant provides from three different perspectives (a) the cybercriminal, (b) the employee, and (c) the business owner (participant). The second step is to matrix the data into the categories from the first step (a, b, and, c in my study). The third step in the process is to display the analyzed data graphically and by charts for examination. For this step, coding of the data (interviews and direct observations) using QDA Miner and NVivo software to develop the graphical analysis into charts that provide a meaningful display of the results is necessary as recommended by Leggett (2017). The fourth step is coding the data (frequency of events), and the last step is the sequencing or ordering the events. Triangulation of the collected data is important to the study because multiple sources (triangulation) serve to enhance the content validity (Fusch, Fusch, & Ness, 2018; Yin, 2014). In this study, there are three methods of data collection to triangulate; interview questions, informal discussions, observation logs, and reflexive notes. Table 2 is a product of the use of observation logs, interview results and reflexive notes to generate a word frequency table. Appendix H is an example of the NVivo data in bar chart form along with Appendix J in pie chart form, and Appendix M is an example of reflexivity in a word cloud developed from NVivo software as well. Appendix L would be an example of a pie chart created using QDA Miner. Appendices O through R support are a breakdown of the data collected that supports the four emergent themes by data collection method and based on the word frequency analysis of all of the data.

The tables three and four codes are used after the word frequency analysis to delineate security positives and security negatives as well as tech support positives and negatives, that render Table 2. Further analysis reveals that both security and tech support have positive and negative attributes when looked at in the overall application as themes (see Tables 3 and 4 respectively. For example, having a DSL service is both a security positive and a security negative. The lines were buried underground (positive), but the cost to change over to highspeed cable would be prohibitive for enhanced software security (negative).

Table 2

Global Coded Observation Logs, Interview Results, Reflexive Notes, and Member Checking Word Frequency

Coded item	Word phrase count	Percentage frequency
Cost	28	6%
Security	85	25%
Security positives	93	18%
Security negatives	62	10%
Social engineering	72	13%
Tech support positives	26	18%
Tech support negatives	30	5%
Tech support	75	14%

Table 3

Coded Security Concerns

Security positives	Security negatives
Phone cables below ground	No Wi-Fi (Operations)
No Wi-Fi	DSL
DSL	Work Stations may be left unattended
Complex passwords in use	No password time-out on work stations
Banking is off-line	
Software updated monthly	

Table 4

Coded Tech Support Concerns

Tech support positives	Tech support negatives
Fast turnaround	3 services: phone, physical, and internet
Personally know technicians	Social engineering opportunity
Internet security technician is off-site	Antiquated services (DSL)

Table 5

Interview Coded Word Frequency Analysis

Code	Frequency	Word count
Security positives	19%	55
Security	23%	48
Social engineering potentials	16%	38
Security negatives	13%	16
Tech Support negatives	17%	16
Cost	6%	14
Tech support positives	5%	14

Table 6

Observation Log Code Frequency and Word Count

Code	Code frequency	Word count
Security positives	23%	130
Security	20%	180
Social engineering Potentials	16%	95
Security negatives	13%	79
Tech support negatives	17%	40
Cost	6%	41
Tech support positives	5%	130

Table 7

Member Checking Identification of Threats

Identified threat	Percent frequency
Insider (employee)	38.9%
Potential issues	
Hacked system (external)	16.7%
Compromised system	11.1%
Internal/External	
Tech support threats and concerns	33.3%

Table 8

Security Coded Word Distribution (QDA)

Word	Frequency Percent
Security	24%
Security Positives	28.5%
Security Negatives	15.5%
Social Engineering	18.5%

Evidence of Trustworthiness

Credibility

Credibility and reliability of a case study are based on the ability to replicate consistent research procedures (Yin, 2014). Reliance is subject to the fundamental norm of sensible guidance (Alonso, 2016). In my single case study design, the sensible guidance will be the standards and procedures the literature provides in the research disciplines. Since the literature has asserted that SME owners should not be aware of cybersecurity threats, my data collection methods explore the extent of knowledge that a typical SME owner might possess relative to cybersecurity vulnerabilities. A single case study using a methodological triangulation approach with multiple sources is necessary to provide validity and reliability to the study (Yin, 2014). Triangulation enhancement is through member checking of the analytical results (Madill & Sullivan, 2017) that began on January 30th, 2017 and concluded on March 3rd, 2018, and peer reviewed by my dissertation committee who serves as the expert panel review.

The dissertation committee consists of three members. The committee chair, the subject matter expert, and the university reviewer. The panel reviewed the study for alignment, triangulation of the data and applicability of the interview questions. Other supporting triangulation methods are peer-reviewed literature (Carter et al., 2014). Assurance of data validity is by triangulation of the data (Carter et al., 2014). Peer review, member checking, and the use of reflective journal verification support the content validity (Carter et al., 2014).

Transferability

For my study, I have selected a qualitative single case study design based on the criteria provided by the literature found in Yin (2014). My study involves the security risk that employees of SMEs (small and medium enterprises) might create for a business due to internet activity either at work or home. A single case study would be necessary to provide insight as to how those activities might avail themselves and how they may manifest into a financial or legal crisis for the business. Yin offered some advice for how a single case study approach might work for my study.

There are four criteria for what constitutes the possibility for a single case study design using a rich explanation of the events. The events must be sequential and irreversible. In my case, an employee must pose a risk to the business, and that risk must be irreversible. The catalyst events must always follow other events based on a contingency. In my case study, there must be a demonstration that employee internet access may create a risk to the business. The events must be a constraint by a time interval (it must be decisive that event “A” is a cause event “B”). In my case study, it is a conclusion that it is possible that employee internet access can always lead to risks to the business. Finally, Yin stated that time periods of events in a case study could be a classification of different from other events. In my case study, there is a demonstration that employee internet use events that create risk to the business, and is not an influence of other business activity events (e.g. in my study, a hardware malfunction does not produce loss of information, but could create risk due to the employees exposing the company to risk through online activity. For my single case study design, the potential for risk to a business that an employee creates by internet use must be attributable to that activity alone, irreversible and repeatable. My observations of the security measures in place and the fact that employees can create risk by unobserved internet activity, according to space transition theory that asserts how personality changes from reality to cyberspace can create the opportunity for risk on behalf of an employee, as discussed by Jaishankar (2013).

Access to a rural small business that uses the internet for transaction processing is a unique opportunity for the study design; the study results might be relevant (Yin, 2014) concerning contributing to the body of knowledge. I believe from the literature (Bandura, 2009; Jaishankar, 2008) those criteria will be for my study. This criterion can translate into a single case study design through the research question because the literature assertion that SME owners do not know cybersecurity (Hutchings, 2012; Tarafdar et al., 2013) may be either true or false in a single case study by demonstration. I reached saturation in the second week when observation notes and reflexive notes began to repeat. The SME owner did demonstrate sufficient knowledge about cybersecurity to falsify the assertion, and I have reached data saturation again by falsifying the assertion. If the SME owner has insufficient knowledge about cybersecurity, then the literature assertion is true, and I have reached saturation

Dependability

Yin described dependability (or reliability), like the ability to obtain the study results using the same procedures furnished by the study (Yin, 2014). For my study, this task would be an easy accomplishment. In another case study, a researcher need only conduct another case study to either prove or disprove the Hutchings and Tarafdar et al. assertions that SME owners and employees should not have the background and knowledge necessary to adequately protect the business from cyberattacks and threats (Hutchings, 2012; Tarafdar et al., 2013). Though the findings were different from the Tarafdar et al. and Hutchings assertion, the same case study procedure and literature review would either prove or disprove the findings of this case study. In other words, this case study obtains what knowledge SME owners have about cybersecurity. Another case study using the same procedures should collect the same data (an SME business owner's knowledge about cybersecurity).

Confirmability

Observations of actions may cause participants to proceed differently (Yin, 2014). To negate the possibility of influencing the particpant, the observations were conducted before the interview. Yin referred to this as reflexivity. Because the interview was after the observations, I feel that the interview did not cause the participant to act differently to demonstrate knowledge of cybersecurity based on the knowledge gained from the study because of the interview. I feel that the sequence was important for me to maintain as much objectivity as possible in my role as the researcher and reduces the possibility of contaminating the participant with pre-observation knowledge about the study and the strategy was successful. Credibility and reliability of a case study are contingent on the ability to replicate consistent research procedures (Yin, 2014). Replication of the literature review research can be using the key word search procedure in the chapter two literature review section as well as the collection of data from more small business owner participants.

Study Results

From the data review and analysis with the assistance of QDA Miner along with NVivo, four themes emerged when analyzing the data (see Appendix L) with the research question as a key factor for consideration; RQ- What are the SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources? Observations logs, the interview responses, member checking data, and the reflexive notes produce the following themes that emerge as management decision factors to protect information with available resources (see Appendices H and J).

Four Emergent Themes Resulting from the Data Analysis

Emergent Theme One: Cost of Security

The theme of cost relates back to the research question because cost is significant a factor that SME owners must consider when evaluating cyber-secure networks and in chapter one, I presented the conceptual framework for this study. One part of the conceptual framework was also the potential cost element. The conceptual framework of the study was a two-pronged application of the literature. The first prong was based on the works of Gold et al., Raine et al., Sangani and Vijayakumar, Schrock et al., and

Steffee, and Tarafdar et al. to illustrate the cyberattack conceptual framework and the inclination for cybercriminals toward SMEs and social engineering attacks. These works demonstrate the nature of cyberattacks, the management perspective on information security investments, and the expected trend toward SME's cyberattacks. The theme of cost arose as a result of the observations of the business operations, interview results, reflexive notes and member checking verification of the data (see Tables 2, 5, and 6 and Appendix O).

Cost is a significant consideration in answering the research question of the SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources. Based on the anlysis of the data (see Appendix O) for this case study, the participant has opted to use third party tech to maintain the software security system. For this theme, the security risk risk reduction is by the inclusion of experts to manage security. However, there is the added unknown of trust in the third party tech support to consider as a security risk. The technology involved may be beyond some business owners ability and would require the added expense of tech support to maintain a functional system.

Cost also arises as an issue in this case study indirectly where the participant accesses the internet through a DSL (Digital Subscriber Line) which at times creates some disruption to the business services regarding data transfer rates and phone and equipment availability (See figure 3). When asked during member checking what the participant thought the main way cybercriminals access systems illegally he replied, “the Internet connection” (see appendix N). The cost factor also emerged from that fact that I observed on three occasions that customers had to wait for a receipt print out until the participant was off the phone. The system configuration was confirmed by member checking discussions (see Appendix O) and also member checking confirmation of the network design (see Figure 3). This observation rolled over into other cost drivers for SME security (see Appendix O). During observations, I noted that there is a cordless phone service for the business. The printer runs off of the same ethernet line, so that phone use prevents printer operation (see figures 2 & 3). Internet ethernet service should be on a separate line such that there is no interference during transaction processing. The printer is a hole fed dot matrix printer for printing hardcopy receipts and cannot have access in tandem with the phones because of the sequenced wiring of the ethernet.

My observations and interview questions with the participant revealed that the system protection is by a firewall, but the participant is not familiar with the settings required for safe operation of the system. According to the participant, third-party technicians are relied on for maintaining proper software firewall settings, and updates and their services include the monthly cost of the security system. When asked in the interview how often the security software updates as the last question in the formal interview, the participant responded; “Uh, monthly.” He knew that the security system automatically updates monthly for software changes. From member checking, the participant bears a cost for the security software and the associated technical support as discussed by Agustina (2015), but still feels at risk connecting to the internet. As the participant asserted in the formal interview; “I think that if somebody wants in the system they can get in and get what they want if, uh I do not think you are going to be able to just totally stop it. If they want in, they are going to get in.” In member checking, he re-affirmed his position on cost by stating that: “I consider the monthly cost for security as necessary as the cost of electricity.” In my reflexive notes, I have entries that indicate cost as a factor relative to the non-existence of Wi-Fi. By deduction, to upgrade the printer and other peripherals, it may be necessary to use a Wi-Fi router which the participant has elected not to do.

Cost savings is a necessary part of a small businesses survival (Vander Bauwhede, De Meyere, & Van Cauwenberge, (2015). To save cost may mean that SME owners must accept a certain amount of cybersecurity risk and operate with somewhat antiquated equipment. Having observed that there were only ethernet connections to the work stations and no coax cables (the back of the work stations CPU’s face the customer and the connections are easily observable), I deduced that there was no high-speed cable into the facility. Verification of the observation was by inspecting the building interface as well (see figures 2 and 3). To upgrade to cable could mean that the extra cost of pulling new cable and changing providers for high-speed cable would have to be a significant impact and result in an increase in a monthly overhead cable bill. The underground cabling does have the benefit of adding a physical layer of security since access to the underground lines would preclude tampering with the business connections. When asked about converting to high speed cable in informal discussions, the participant agreed that upgrading was too expensive and this was confirmed in member checking (see Appendix O). Small business owners may perceive cybersecurity costs as an unnecessary expense if they are unaffected by the security breaches. In a subsequent informal discussion about highspeed cable, the business owner stated that he has elected to maintain the current network and computer infrastructure on a DSL provider for ethernet connectivity to the internet. According to the participant, the option to upgrade to high speed internet cable could prove cost prohibitive since the current DSL lines are underground. As a follow up to this issue, in member checking I asked if the current system he is using was reliable and how often it failed. The participant stated; "It rarely fails, only if the phone system fails due to a storm or something." He then elaborated; "The last time it failed was about a month ago during a storm." System continuity is likely because it is strictly DSL and as a simple system and has less equipment that is prone to failure (no routers, signal amplifiers, etc.) The simplicity of the data delivery equipment could be considered a security and cost advantage because of the low maintenance.

Although the subject of cost does not directly factor in from a pure word frequency percentile, when identification of cybersecurity elements for cost, has a rating of 6.5% (the averages between observations and interview codes, (see Table 2)) and verified by member checking and my reflexive notes where I wrote; “No Wi-Fi at the facility. Strictly DSL. The Wi-Fi signal was tested five times at random intervals with no signal detected” (see figure 1). I noticed during observations that there were no cable connections to the work station CPU’s. Reflexive notes and member checking confirmed the observations (see Appendix N). In my reflexive notes, I also noted that it would be advantageous to upgrade the system to support extra ethernet ports for separate the printer and phone lines (see Appendix N).The elements for cost become a major factor external to the coding. For example, although DSL appears 69 times in the data collection as a concern (see Appendix N), the cost of converting to high speed cable would be exorbitant. It is an expectation that the issue of the cost for cyber-protection in an SME is to be prevalent (August et al., 2014). These considerations aside, the participant had stated during member checking; “I consider the monthly cost for security as necessary as the cost of electricity.”

Another issue associated with cost is oversight of the system. Being a small business that occasionally employs seasonal help, the network may be at some risk due to the inability to monitor it. When asked about the system oversight the participant stated in the interview; “Uh, now that I don’t know. I don’t know what, you know they would jump in there and try to get that you know, you hadn’t thought about. You know, I don’t know”. From the participant's statement above although at the risk of getting caught, it would be possible for an employee retaliatory type of attack if the proprietor is indisposed for a lengthy period since the employee would need to access the network unsupervised in the performance of their duties.

With the cost impacts of securing the SME local area network and from the observations, interview, informal discussions, member checking and reflexive notes the SME owner has accepted a level of risk because he feels that he has no data worth taking and he also feels as though he is under the umbrella of big corporations that have more furtive data (customer information) to attract cybercrime activity. The acceptance of risk brings about the second emergent theme from the data collection, network security.

Emergent Theme Two: Local Area Network Security

My conceptual framework on the SME business owners knowledge about cybersecurity threats are based on the literature review and the expected theme that SME business owners and employees should not have the background and knowledge necessary to adequately protect the business from cyberattacks and threats (Hutchings, 2012; Tarafdar et al., 2013). It is an expectation that SMEs will become more vulnerable to cyber threats with the sealing of the cracks in the large corporation security walls (Hayes & Bodhani, 2013) and should, therefore, prepare for the anticipated new cyberattack approaches.

The theme of security also arose as a result of the observations of the business operations, interview results, reflexive notes and member checking verification of the data (see Tables 2, 3, 8, and 6 and Appendix P). Small and medium business owners may be complacent because they may feel they are under the umbrella of big companies. As stated by the participant in the interview; *"*Large corporations have got more information on the systems, they've got a lot more credit card activity and stuff than we do so I think that probably that would be a bigger target than a small business.' And as a follow-up question, when asked about what forms of cyberattacks and computer intrusions he was aware of, the "participant responded; Uh, I've just heard of the ones on the big corporations, the small ones, you know, I don't think they have that much trouble with it."

These statements conflict with the studies that indicate that the trend for cybercrime will shift more towards small businesses (Hayes & Bodhani, 2013) and are confirmed in member checking of the data (see Appendix N and Table 2). In the development of these two interview questions, I expected that the SME owner would answer with postulations about what types of attempts to breach his network are used, so it was not an expectation that he deferred to the umbrella protection of large corporations as shown above.

Security concerns were an expectation because the subject of the research is SME internet security, but there is an underlying concern expressed by the participant. In answer to one of the interview questions about breaches into the business systems network, the participant's response was; "I think that if somebody wants in the system they can get in and get what they want if, uh I do not think you are going to be able to just totally stop it. If they want in, they are going to get in." The participant's statement conflicts with the Tarafdar et al. and Hutchings assertion that business owners have no knowledge of cybersecurity (Hutchings, 2012; Tarafdar et al., 2013). From the participant's interview statement, SME owners have knowledge of cybersecurity threats, but they feel helpless to prevent them. My observations and reflexive notes confirm that that participant is concerned about cybersecurity (see figures 2 and 3), he has invested quite a bit in the available technology and pays a monthly fee to a third party security software provider technical support to maintain his internet firewall and connections. I also observed that the participant logged in to the system every morning indicating that the system is not left active over-night. The participant also related the importance of a strong password to protect the system. In response to the question about password strength he said:" Uh, Well I think, you know, that if you make a password that somebody wouldn't think of you know, I think you would be Okay, but you don't want to use your uh, uh, address or something like that" (see Appendix P).

It is arguable that small and medium businesses are already operating relatively unprotected concerning data security (Chabinskey, 2013). The participant statement demonstrated that as an SME owner, he is aware that there are risks and may feel helpless to prevent intrusions into his system even if he feels he has adequate preventative measures in place. From informal discussions and the interview then verified by member checking (see Table 2 and Appendix N, the participant is also aware that people may undergo personality changes when transitioning from reality to cyberspace as in as in Jaishankar's space transition theory). He was aware that people might also do activities on line that they would not ordinarily do including illegal activities as he states; "Well, somebody could walk by that is not an employee and can get into the system and get stuff out of it." From this statement, seemed to hold the belief that cybersecurity breaches would be from the outside and the participant was not cognizant (or at least had not been pre-considered) how an internal security issue might affect his business. Cybersecurity concerns appear to be a limitation of cyberattacks from outside of the business with little consideration for cyberattacks and risks (social engineering) from within the firm. There is an inclination to trust employees inside the company according to the literature assertions (Hutchings, 2012; Tarafdar et al., 2013; Willison & Warkentin, 2013; Zhurin, 2015) that there is a general lack of awareness in SME enterprises with respect to the risk from insider cyberattacks through social engineering.

According to the participant in member checking discussions, there were three attempts to break into the business (see Appendices O and P). Only the first was successful. In that break-in, the perpetrators, escaped with one lap-top that the police later retrieved. The lap-top did have employee information on it such as social security numbers, but the intent was to obtain merchandise and the lap-top for re-sale and personal use. According to the participant, the device had no data taken from it according to the police (See Appendix R). Lap-tops used for business purposes are no longer left-over night. Accounting activities are off-line on a business office managers custom made software program unique to that business. Use of the program is off-line, and all banking activities are off-line.

I noted in the reflexive journals and observations, that if any work stations are left unattended, they are monitored by security video camera at the rear of the store. Activity at the work stations is recorded, but no details of work station would be available except the person at the station and the time of the activity which would be enough to provide any information for an inquiry.

My reflexive notes indicate work stations do not have a password timer or that it is on a long delay and it may need a shorter time out. Sometimes employees may be indisposed for long periods of time and unable to monitor the work stations. I observed that when the participant had to leave the show room to perform a service such as a hydraulic-line repair, the work stations are left unattended and logged in. The logging events were confirmed by member checking when the participant stated that he “logs out and turns off the system at night, and then logs back in again in the morning” (see Appendix R).

In member checking, I asked the participant what security changes they have made since the break-ins, and the participant stated; “If the phone lines are disconnected the police are automatically dispatched” (see Figure 3). Before the break-ins, the audible alarm went off if the magnetic interlocks activated but emergency services were not automatically notified.

The revolving issues of cost and maintaining secure network again indicates a significant reliance on technical support personnel. The research question about management decision factors that positively or negatively influence the organization's influence to protect the capacity for organizations to protect information with available resources is again the reliance on expert technical support to maintain the network. The emergent themes of cost and network security created a link to the technical support emergent theme.

Emergent Theme Three: Technical Support

The conceptual framework provides that the SMEs (small and medium enterprises) business owner knowledge about cybersecurity threats and are based on the literature review. An expected theme would be that SME business owners and employees should not have the background and knowledge necessary to adequately protect the business from cyberattacks and threats (Hutchings, 2012; Tarafdar et al., 2013). Based on the literature review, an SME owner should not have an adequately developed security based network to preclude intrusion into the system. From this case study, relying heavily on outsourcing to a third party tech support was the solution to this issue. From the interview, member checking and observations, the participant counts on his tech support personnel to maintain a secure network. When asked who he calls for internet issues he responded: “My IT support guy.” I observed that some of the technical issues like not being able to use the phone while printing, could be easily overcome by an inexpensive Wi-Fi router so, by deduction, the participant does not possess the technical skill set necessary to make the upgrade himself (see Appendix P). When asked who he would call if he suspected there was a compromise of his network had the participant again responded: “My IT support guy.”

From observations and reflexive notes (see Appendix P and R), I noticed that the back of CPU’s for the work stations was exposed and facing the customers and on middle shelves. The positioning of the CPU’s would make tampering an issue of person chose to do so. For example, partially disengaging an ethernet cable could create intermittent or permanent connection loss with the inability to detect the problem without extensive trouble shooting. From my observations and reflexive notes, this would be an easy target for an unhappy customer with the opportunity to tamper with the system.. A deterrent to the potential tampering would be the camera video security system as indicated in my observations and reflexive notes. Were a person to tamper with the wiring, the action would be caught on video recording. The participant acknowledges that he has considered the possibility that the system is not tamper proof in his statement: Well, somebody could walk by that’s not an employee and can get into the system and get stuff out of it.” Although he meant accessing the system here (as confirmed in member checking) this would also apply to tampering with the system physical configuration.

Another concern that overlaps with the first emergent theme cost is that of the use of an ethernet DSL provider (see Appendix O and R). Although the service provider ethernet connection is by a secure firewall, this configuration may retard the ability to upgrade to a more sophisticated wireless system with the possibility of enhanced performance and security design features (see figure 3). The participant indicated knowledge of the necessity of a firewall in the interview: “Ours has got a firewall on it and uhm, and, I’m not sure about the brand of the uh anti-virus”, (I later verified this by member checking, the anti-virus protection was later determined to be provided by the same service as the firewall protection (see Appendix c)).

Another sign of the system antiquity was the type of printer in use. My observation logs and reflexive notes indicated that the printer was a hole-fed dot matrix type of printer that requires special paper, special software, and special ink ribbons to function. Upgrading to ink jet printer might provide cost savings that could apply to upgrading the remainder of the system. The printer’s only function is to print customer receipts.

Since it is an expectation that SMEs will become more vulnerable to cyber threats with the sealing of the cracks in the large corporation security walls (Hayes & Bodhani, 2013) they should, therefore, prepare for the anticipated new cyberattack approaches. Cyberattack approaches are another decision factor from the research question for SME owners and managers. The selection of trusted technical support services is critical to maintaining the businesses network integrity. Selection off a cost-effective, reliable and trustworthy cybersecurity service as the participant in this study has done is important to SME survival.

Out-sourcing is to a third party IT support in this case study. The IT person assists with connectivity issues and application issues for the supplier data base and is an employee of the wholesale provider. In an informal discussion, the participant asserts that IT support is from three operations. The first is a local business that provides tech support for the building physical security (alarms, motion sensors, and other devices). The second and third forms of tech support are out of town. One is for the phone and ethernet AT&T service (DSL), and the other is with the commercial internet security service (see Table 8). The participant stated that he receives excellent service form his IT support personnel on all three facets of support. When queried about the support, the participant responds favorably that the IT support personnel are who he relies on if he suspects a compromise of the system or the system requires trouble shooting and that the IT personnel respond, “Within the same day and usually within an hour or so.”

The internet security provider provides security IT support for the security software. From my observation logs (see appendices P and R)The only connection to the banking service is via the point of sale credit card scanner through a secure encrypted line for debit and credit cards This is verified through member checking and informal discussions with the participant (see Appendix N). The participant is complimentary of the IT support services with respect to speed and deliverables. As shown in the word cloud in Appendix I, support, internet security, and knowledge are prominent themes that are supported by observations, interviews, reflexive notes and (see Appendix N, P and Table 2).

In my reflexive notes, I noted that in an informal discussion with the participant, the tech support for network security is provided by the security provider for access connectivity issues, maintenance of the system, and software. In member checking, the participant repeated that tech support is from the security software provider but later clarified in an informal discussion that there are three separate tech support personnel; one for the security software, one for the building security management and one from the service provider.

It is possible that a data breach could occur between the point of sale and the bank service, but it is more likely that that breach would occur at the source (the bank) than at the owner's location (Zhurin, 2015). One avenue for phishing might result here. Since there are more than one contact for IT support, a phisher or social engineer might pose as an IT support person to gain access to the system (Simms, 2016). Zhurin addressed the issue of an insider's ability to exploit computer data bases based on intimate familiarity with the system vulnerabilities (see Table 7), thereby being in the position to take advantage of these vulnerabilities (Zhurin, 2015). Zhurin asserted that with the advent of security protection measures information protection systems (IPSs) such as firewalls, hackers have turned to new approaches like social engineering (employees have become the primary source of information to gain access) to obtain credentials and information to access secure systems (Hutchings, 2012; Tarafdar et al., 2013; Willison & Warkentin, 2013; Zhurin, 2015). Tech support can provide much protection from outsider intrusion, but since the SME in this case study does not house any customer or employee personal records such as bank information, social security numbers or credit card data, the threat to these types of SMEs would most likely be retaliatory and possibly by way of social engineering to access and disrupt the business activities.

Emergent Theme Four: Social Engineering, Customer, Employee, and Service Provider Retaliation

From the research question, possibly the most difficult of the SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources is one of the social engineering attacks. The potential inability to protect information is because of the covert nature of this kind of attack and the need to fool the business owner for them to work. In other words, for some small businesses, these types would be planned covert operations designed to stay hidden from discovery.

Once again, from the conceptual framework, the second prong of the study is about the psychology involved in the employee side of vulnerabilities through space transition theory (see Appendix E) and moral disengagement (Bandura, 2009; Jaishankar, 2008). These approaches explore the psychological aspect of how employees may become victims from the mental side of the issue. Jaishanker developed space transition theory to explain behavioral changes in the transition from physical space to cyberspace (2007). To extrapolate these behavioral changes to SME employee behavior, and in the online environment, a single case study design may provide a platform to advance the issue for further research. Bandura and Donner et al. indirectly addressed the Jaishanker theory from a psychological perspective in the form moral disengagement and low self-control as applies to the computer environment (Bandura, 2009; Donner et al., 2014).

These articles presented the possibility that there is a gap in the literature where the psychology of the behavior and the intersection of the cybercriminal activity may not have received a thorough exploration considering the nature of space transition theory, moral disengagement, and low self-control. Part of this studies conceptual framework is that cybersecurity concerns appear to be a limitation of cyberattacks from outside of the business with little consideration for cyberattacks and risks (social engineering) from within the firm. There is an inclination to trust employees inside the company according to the literature assertions that there is a general lack of awareness in SME enterprises with respect to the risk from insider cyberattacks through social engineering and employee retaliation (Hutchings, 2012; Tarafdar et al., 2013; Willison & Warkentin, 2013; Zhurin, 2015). The theme of social engineering arose as a result of observations of business operations, interview results, reflexive notes, and member checking verification of the data (see Tables 2, 4, 6, 7 and Appendix R).

There is an expectation that two established theories will potentially converge into a new theory based on the data collection expected results. Space transition theory (Jaishankar, 2008) explains the vulnerabilities of employees to cybercrime through internet access, and moral disengagement (Banduras, 2009) might explain the cybercriminal ability to dismiss the morality of an action based on internet anonymity properties. From these two theories, a third theory that may emerge from the study is that space transition theory and moral disengagement combine to create a new theory that explains vulnerabilities from both the victim and the criminal's perspectives that create the environment for crime.

SME owners may have a knowledge deficit relative to social engineering. As stated by the participant; "If somebody wants to get in, they can get in." There is an awareness on behalf of the participant for the potential for a cybersecurity breach, but there is a lack of understanding as to exactly how those breaches might occur. The participant was unaware of the difference in hacking and social engineering and, to him, there is probably no reason to make the distinction, and perhaps there is no need to as stated in chapter one. As the participant relates; "Well, like our business there's not that much I don't think that anybody would use, you know, we don't have that much information actually on our system, but you know, there's always the chance." The participant is aware of the possibility, but from the above statement. He feels the content of his network has no information of value in the form of customer personal information. From informal discussions, member checking, notes, and observations (see Table 2) the participant has not taken into account the possibility of customer or employee retaliation (Huang & Miranda, 2015; Pantic, 2014; Shank, 2012).

In an informal discussion, the participant was aware of social engineering, though not by that name, and that people can undergo personality changes when online (Jaishankar, 2013). In informal discussions, the participant was also aware of phishing for information via e-mails. The participant was aware of these cybersecurity issues but not by the technical terminology and not to what extent they may affect him. In another informal discussion, the participant was not sure what the methods were for hackers to access business systems via the internet. In other words, the participant knew what preventative measures (firewalls and limited internet access) were necessary to limit potential cybercriminal attacks, but he was not sure about the means attackers use to gain access (social engineering and hacking).In an informal discussion, after explaining to the participant what social engineering and space transition theory was by definition, he acknowledged that he was aware of the concepts but did not know them by name. This discussion led to a better platform for communication between the participant and I for the study topic.

Social engineering is a misuse of influence to gain compliance (Muscanell et al., 2014). There are three types of social engineering processes that may be used to gain access to a network. One is a face-to-face approach. This ploy to gain information may be by impersonation; for example, someone pretending to be a tech support person that needs to access the network. The second way is a telephone call approach by gaining information by fooling the person on the other end that one needs information to solve a problem (See table 7). The third is computer based on delivering corruption software through e-mail, posting ransomware, or posting requests for information (Simmons, 2016). These social engineering attempts to gain information or disrupt services can be of use to employees, tech support, or customers as forms of retaliation.

There can be a relationship between the human psychology and the computer state (or program), that may yield frustrations and anxiety that could invoke cybercriminal activity in the form of retaliation (Huang & Miranda, 2015; Pantic, 2014; Shank, 2012) SME owners would benefit from knowledge on why and how employees and customers might resort to cybersecurity breaches by social engineering (Hutchings, 2012; Tarafdar et al., 2013). Because the business does not house any customer credit card, bank, or personal information on the system most likely, SME cyberattacks would come because of customer, employee, or tech support retaliation in the form of a DOS (denial of service) attack (Ali et al., 2015; Chang et al., 2013). In other words, by deduction the from the business owners statement, he has not considered that cyberattacks could come from the perspective of retaliation as opposed to financial gains.

The participant did not show any forethought about employee or customer retaliatory events when queried about the possibility and confirmed by member checking; “Uh, That I don’t know, I don’t know what, you know, they would jump in there and try to get that you know, you hadn’t thought about. You know, I don’t know.” In one respect, this answer agrees with the literature that asserts that SME owners would not know about cybersecurity issues, (Hutchings, 2012; Tarafdar et al., 2013) but this was an exception to what the data demonstrates that the owner does know about cybersecurity issues. The expectation when developing the question was that there would have been some reasoning as to why that should not be an issue from the participant’s perspective. For example; we only hire people we know and trust, or we keep a close eye on the temporary employees, however, from the answer, there is a degree of uncertainty by the participant as to why the insider threat might be a concern for him.

The results of the Lee et al. study demonstrated that there is indeed a connection between undermining, moral disengagement of the victim and retaliatory action by the first casualty. The authors showed in the study that aggression between employees is common in the workplace (Lee et al., 2016). This undermining action can also occur between a business owner and an employee. For example, a business may undermine an employee to humiliate or disgrace him or her or perhaps use undermining to create an uncomfortable environment for an employee the owner desires to get rid of an employee.

High performers were active on the web at work; more research is needed in this area as the study showed that high internet use at work might supplant hostile retaliation and balance might be necessary to achieve productivity and personal internet use balance (Garret & Danziger, 2008). Pantic uses this illustration to represent that depression from internet use was a concern before social media (Facebook having a foundation in 2004). Therefore, it is possible that social media (having increased online activity) will have exacerbated the issue (Pantic, 2014). Pantic suggested a requirement for further research to investigate if the existence of correlation can be causality. For example, does Facebook cause low self-esteem, or are people with low self-esteem more frequent users of Facebook (Jaishankar, 2008; Pantic, 2014). There is also a necessity to evaluate the potential effects of depression from social media use and the possible correlation to online cybercriminal activity concerning the Jaishankar space transition theory. For example, does a depressed state from overuse of social media create the potential for retaliation in the form of cybercriminal activity? There is some evidence that people desire to interface with computers in the same way they interface with other people. Denial of a computers emotion (approval, disapproval or denial of access) might lead to cybercriminal activity through retaliation (Huang & Miranda, 2015).

The only feasible way to obtain credit card or bank information from the participants business would be using a credit card scanner at the point of sale (Hutchings & Holt, 2016). Using a credit card scanner would be an unlikely method because it would be difficult to install it unseen and the owner would likely notice any modification to the current scanner because of the high frequency of use by the owner. The technology notwithstanding, phishing to access the system is still a major concern for SMEs (Goel, Williams, & Dincelli, 2017).

An empirical to study to identify what organizational and individual factors contribute to resistance to social engineering by cybercriminals is a concern in this study by Flores and Ekstedt. The purpose of the Flores and Ekstedt study was to evaluate possible factors that contribute to an individual's resistance to social engineering. The philosophical approach was to determine the level of the impact of organizational security cultural on personal behavior relative to social engineering resistance. The underlying assumption was that organizational information security culture was a contributing factor to an individual's resistance to social engineering cybersecurity threats.

The authors of the study revealed that all factors investigated had an influence on individuals to varying degrees, but individual attitudes were the most profound. The methodology used was a mixed-methods design where qualitative data to develop the research model and survey instrument to quantify factors of resistance to social engineering by both individuals and organizations. 4,296 individuals in Sweden were the recipients of the instrument (Flores & Ekstedt, 2016). A research question designed to discover the organizational factors that influence employees to resist social engineering cyber-threat activity.

The authors asserted that the strongest tie to resistance to social engineering was in the individual's attitude and the weaker links were in self-efficacy and normative beliefs. Flores and Ekstedt indicated that the data is in support of all the hypotheses, but some indicators were stronger than others for example attitude over self-efficacy (2016). They further revealed that information security culture had a weak correlation to behavioral intention towards social engineering. More research is necessary for determining the effects of attitude towards social engineering. Being aware of threats and education is not enough to prevent the victimization of employees by social engineers. The variances in attitude toward cybersecurity need further research as a predictor of behavioral intentions (Flores & Ekstedt, 2016). Other factors for further exploration are the enterprise's size and industry.

While space transition, self-regulation, and self-control theories offer possible explanations for criminal activity on the internet, there are situations where the vulnerabilities appear to be simply poor judgment on behalf of the user. The use of the same security precautions should apply in cyberspace. Arlitsch and Edelman addressed the use of social engineering (as opposed to hacking) for data breach activities. They asserted that social media is fertile ground for cyber attackers to both obtain user information and relationships with users to gain information. They offered advice on not making it easy for attackers by use of password vaults, strong passwords, data protection, and proper device management (Arlitsch & Edelman, 2014). Arlitsch and Edelman concluded that it is not practical for users to disconnect from the internet, but personal diligence can assuage vulnerabilities (Arlitch & Edleman, 2014, Jaishankar, 2008).

Summary

The interviews, observations notes, reflexive notes, and member checking notes were combined and analyzed using word frequency analysis and coding of the data with NVivo and QDA Miner software to produce the four emergent themes that in turn were used to develop the answers to the research question which is: What are the SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources?

Emergent theme one, cost, does not appear as an emergent theme on a stand-alone basis and is not granular in the data as compared to the other themes (see Appendix O). One must take a step back and view the data holistically to understand how cost effects SME security. Because some business owners may have become acclamated to the revolving cost of security as a necessity of doing business, it may become lost in the myriad of expense requirements SME owners routinely have.

Emergent theme two is an attribute of the tewchnical concerns with the hardware and software parts of security. Figures one, two and three provide an overview of the system design and Appendix P observations, notes, and interivews create the basis for both the software and hardware concerns the data analysis has revealed.

Emergent theme three regards technical support features that some SME enterprises might employ. Tech support can become a detriment because it allows an outside resource to be familiar with the security features (passwords, access, user names, etc.). Emergent theme four addresses the main concern for SME potential security issues, social engineering. Social engineering may use to glean access data from business owners and employees.

Based on the participant responses to the interview questions and supported by the researcher observations, member checking data, and reflexive notes at the site, the findings of Hutchings (2012) and Tarafdar et al. (2013), that SME owners would not know about cybersecurity threats, are not entirely accurate. Based on the data analysis, the participant demonstrated rudimentary knowledge of cybersecurity threats and preventative measures (See Appendices I and M) . Some examples from the interview are that the participant knew the importance of a complex password and the risks associated with non-employee access to work stations. The participant was also aware of the vulnerabilities that internet access creates for SMEs and on the SME network that has a connection to the internet (see Tables 2 through 8).

An area of concern that the participant was not cognizant of was the general issue that cybersecurity information breaches are down streaming to small and mid-sized business with losses of 6% of their turnover in the UK (Hayes & Bodhani, 2013). Since SMEs are just becoming the targets of cyberattacks according to the report, this is not at all surprising, especially from a rural business (which is one reason a rural business was the selection for the research). The participant felt that the risk of attacks on large corporations is still greater than the risk to SMEs; When asked in the interview about small business computer intrusions, the participant responded; "I've just heard of the ones on the big corporations, the small ones, you know, I don't think they have that much trouble with it"

The SME business owner often serves as her employee, meaning, due to operational cost constraints, it may be necessary for the owner to perform employee functions. As ex-hacker Kevin Mitnick pointed out, it only takes one bad business decision by someone in an organization to create an opening for security breaches and illustrated the need for a study to explore the connection between user thinking and cybercriminal attack methods (Gold, 2014).

Based on the collected data, there are four findings from this study, the analysis and emergent themes that could affect the SMEs owner decisions to protect the business network. First the element of cost, second, the element of security, third, the element technical support and fourth, the element social engineering. These factors are included in the following chapter as the findings.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this qualitative case study was to explore SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources. The nature of the study is a qualitative research method with a case study approach to explore how small business owners feel about potential vulnerabilities due to employee internet access (Eisenhardt, 1989; Yin, 2013). The study began as an interest of this researcher in cybercriminal activity and attacks on corporations through breaches in security systems and how those violations occur. I ascertained from the literature review that there is a potential gap in the literature concerning SME employees and a lack of knowledge about social engineering.

As the study progressed, the data indicated that customer retaliation is an additional factor of concern for cyber-retaliation against an SME business. Customer retaliation created an evolution of the study towards SMEs and business owner's knowledge about employee and customer online behavior. This gap in the literature led me to construct the problem statement, research question, and subsequently the significance of the problem. This exploration of the literature and the site research led to the discovery that an SME may be more of a target for insider amd customer reatliation type threats rather than external hacking threats and that tech support personnel (see Appendix N) are potentially an insider threat (Simmons, 2016) These concerns are within in the following chapter for the findings and results of the study.

Interpretation of Findings

The study resulted in four findings from the emergent themes. The first finding is that cost can be a barrier to SME cybersecurity. The security equipment purchased and maintained to protect the businesses physical property, by default protects the businesses physical security apparatus (work stations and network equipment). The second finding is that the SME owner contradicted the literature (Hutchings, 2012; Tarafdar et al., 2013; Willison & Warkentin, 2013), by having some knowledge and concerns about cybersecurity. The third finding is that in some cases, there may be the third party IT support provided by an external entity, and the fourth finding is that a lack of knowledge about social engineering does exist in the SME environment. An examination of the Appendix K word cloud illustrates the SME owner's considerable lack of understanding of how cybercriminals might attempt to gain access to their system that resulted in the fourth finding and the concerns the lack of knowledge about social engineering among some small business owners.

Finding One: The Cost of Securing a Small and Medium Enterprise Network

Based on the analysis of the data (see Appendix O), for this case study, the participant has opted to use third party tech support to maintain the physical and software security system. Cost savings is a necessary part of a small businesses survival (Vander Bauwhede, De Meyere, & Van Cauwenberge, 2015). August et al. sought to propose a financial incentive solution for security software implementation by users. The philosophical approach is that users require incentives to keep systems secure with patch updates. The underlying assumption is financial incentives to get users to update security software is logistically feasible. The methodology August et al. used was a qualitative narrative study designed to inform the readers of the stakes and potential penalties involved in not maintaining secure systems. The cost of tracking users, updates and billing may not be financially advantageous for SMEs. The scope of the article was to address the advantages and disadvantages of cloud computing for small businesses concerning security considerations. Security cost for businesses is not understood and how to distribute that cost among the stakeholders of businesses, but regardless of who pays for it, the software bugs will need to be repaired (Anderson, 2018).

From chapter two, a trust-based approach for cyber systems security is a consideration of Ali et al. They produced a literature based historical study to explore security protection of cyber-physical systems (CPS). A CPS includes sensors, monitoring and control features embedded in electronics devices to connect cyber systems to the physical world (Ali et al., 2015). In the study, Ali et al. presented seven modes that are potential known threats for attacks. Eavesdropping, compromised-key attacks, man-in-the-middle attacks, DOS (denial of service) attacks, resonance attacks, communication jamming attacks and integrity attacks. Ali et al. asserted that internal and external trust in CPS established a boundary for external trust (security software) and internal trust is dependent on interpersonal, structural and dispositional and rely on statistics and probability modeling (Ali et al., 2015). From this study, employee, customer and tech support trust are important factors for an SME. Sophisticated monitoring systems like are not fiscally feasible for SMEs. It is, therefore, necessary to include a trust-based relationship with employees, customers, and tech support to have some assurance of network integrity. Firewall technology may be another solution to cyberattacks.

Firewall technology is becoming intertwined with hardware and software according to a study by Hunter. In the qualitative, narrative approach, Hunter compared and contrasted firewall technologies and the expected growth of investment and research and development. A graphical representation presented by Hunter illustrated that there is an expectation that commercial firewall sales will grow more than one billion dollars by 2018 (Hunter, 2013). Hunter examined the production of business broadband routers and modems with built-in firewall protection indicating a trend way from firewall protection software initiation from the computing appliance to the routers and modems (Hunter, 2013), in other words, the modems and routers will host the embedded software and updates within the router or modem as opposed to the protection of the computer in commercial enterprises. Hunter compares Juniper and Cisco routers (the top competitors in the business router market), and the conclusion is that the final design features with flexibility will gain the market share. Use of an embedded firewall is the case with some small businesses and is true of this study in particular (see Figure 3). The participant uses a different firewall manufacturer than Cisco, but the firewall is embedded in the security supplied modem as Hunter suggests. This configuration has the added advantage of automatic software updates. Firewalls and software provide a measure of security for small and medium enterprises, the aspect of the security threats should is addressed in the next subsection.

Finding Two: Security and Threats to a Small and Medium Business

Employee (as well as tech support) and customer retaliation should be of considerable concern. As discussed in chapter two, small and medium businesses require a road-map type formula to address security issues based on the case study results of Choles and Gerard (2014). According to the findings of this case study, SME owners may rely in part on the assessment of third party tech support for the application of security appliances and software. Again, the two conflicting statements appear as a factor of uncertainty in SME owner's concerns that supported the Hutchings and Tarafdar et al. assertions that SME owners know nothing about cybersecurity (Hutchings, 2012; Tarafdar et al., 2013). However, some small business owners are aware of those risks which are a contradiction to the Hutchings and Tarafdar et al. assertion. There are two possible perspectives here. One, the participant is aware of the risks associated with cybersecurity breaches and two, he is not certain what measures he can to minimize risk take beyond what he has in place. The literature and this case study suggest that the biggest threat to some SME owners may be in retaliation by employees, customers or tech support personnel.

Donner et al. provided an analysis of deviant behavior on computers. The purpose of the study was to better understand the online behavior of college students and possible resultant deviant behavior in the online environment. Individuals in the online environment selected the dependent variables as ten deviant behaviors with the independent variables being the measure of low self-control based on the Grasmick scale of low self-control and utilizing the Hirschi and Gottfredson six-element scale (Donner et al., 2012). Donner et al. concluded that there is a link between self-control theory and online deviant behavior (Donner et al., 2012). Deviant behavior on the internet by employees can hurt organizations concerning the organizations brand. Deviant behavior may be a factor for SME owners hiring and retention practices. For example, an employee that spends an inordinate amount of time in cyber-space at work may be exposing the business to cybercriminal risks.

A literature review based qualitative, narrative study on the effectiveness of a human reliability assessment and improved statistics-based quality control for assurance by Evans et al. asserted that based on the number of high profile security breaches, organizations have begun to focus on brand protection and reputation through assurance protection. To that end, Evans et al. explored the established literature in search of areas of weakness concerning cybersecurity and provided a brief historical account of cybersecurity breaches in different factions of industry and government (Evans et al., 2016). Evans et al. concluded that half of the cybersecurity breaches involved human error and suggested further research in cybersecurity human factors. Cybersecurity breaches can come from inside or outside of the workplace. Some small business owners may not perceive insiders (employee and tech support) as a security threat. Some small and medium business owners may be complacent because they may feel they are under the umbrella of big companies for cyber-threat conditions. From my study, some business owners may not be aware of the threat posed to them by employees. Another finding from my study is the potential for tech support retaliation.

Finding Three: Technical Support for a Small and Medium Enterprise

The third finding is that in some cases, there may be third-party IT support provided by an external entity. Another prevalent theme from the data was the use of tech support for security. Tech support was not an expectation as an issue because it was an assumption before the study that SME owners would not be able to afford the on-going costs of tech support. This this turned out not to be that case for some SMEs, and the nature of outsourcing to a third party for security became a theme and a finding. Simms submitted that tech support may be a cause for concern when it comes to protecting a system from cybersecurity. A perpetrator may infiltrate a system disguising as tech support (Simms, 2016).

The role of IT governance in small and medium businesses, specifically, IT governance of SMEs in the form of HR resources is an aspect explored by Garbarino. In enterprises where resource usage comes at a premium, it is necessary to develop a lean system of governance. Garbarino noted that SMEs have a simple structure that does not include many specialists to perform the routine IT functions larger corporations might facilitate (Garbarino, 2013). Garbarino asserted that IT (and therefore IT growth) is essential to the success of an organization as an enabler of growth. The purpose of the study was to provide the lessons learned and issues from a case study to implement IT governance into an SME (Garbarino, 2013). The philosophical approach was to identify shortfalls in the human resource management aspect of the implementation of IT governance in SMEs to reach average levels of maturity in IT governance.

The underlying assumption is that SMEs will adapt to the implementation of IT governance tailored to an SME enterprise. Garbarino presented a case study of AAA (a localized pharmaceutical market) and the incorporation of IT governance into the business. The methodology was a single qualitative case study design (for defense, Garbarino cited the Yin definition for a single case study design). The author revealed a positive connection between HR training and IT practices that contribute to the organization's success. In my study, some SMEs have no formal independent departments such as H.R. to carry out the training function IT governance. Instead, the owners themselves train and support the temporary staff of the business and rely on third party tech support to maintain functionality of the system.

Garbarino suggested a replication of the study in other enterprises. The author indicates a correlation between IT governance and organizational success. The author does not advance the inclusion of security risks and a need for a security training apparatus in the SME IT organization. Giovino addressed the significant growth of occupational crime and fraud and the corresponding increasing need for prevention and detection in the form of internal business audits to protect organizations. Giovino discussed that leadership discussions ethics and integrity should be the routine subject of an open forum (Giovino, 2015). From my study results, internal audits may be institutionalized but it is doubtful that they would be stringent enough based on my observations and interviews of the environment owner and the heavy reliance on the third party IT support for the business.

The purpose of Giovino study was to inform the reader of the importance of open communication on ethics and integrity concerning organizational cybersecurity. Giovino offered three conditions under which fraud may occur within an organization; (a) incidental pressures (sales or financial goal pressures), (b) opportunities to commit fraud (holes in the security system, unnecessary access privileges), and (c)motivation for financial gain or disgruntled employee retaliation (Giovino, 2015). Giovino further advised organizations of the processes for reporting cybercriminal activity and the insurance recovery mechanisms that may be available to the victim organizations (Giovino, 2015).

The underlying assumption the author made was that organizational crime and fraud would continue to grow to advance the need for improved protection of organizations. Giovino further asserted that surprise audits, hotlines and training might avert future organizational losses due to fraud. The methodology was a qualitative narrative approach designed to inform the reader on reporting, preventing and recovering from the cybercriminal activity. The limitations of the study were that it did not address SME fraud prevention, detection, and recovery. Unlike larger organizations, SMEs do not typically have the funding required to support internal auditing techniques. From my case study, it would not be feasible for an SME owner to conduct possible time-consuming enterprises such as surprise audits, hotlines and training. Some SMEs only have single digit employees making surprise audits and hot lines impractical. Since IT might be outsourced to a third party vendor as is the case in this case study, the audits and hotlines might be a deferral to that vendor.

A study to assess the role central data warehousing might play in cybersecurity protection as well as possible correlations between warehouse maintenance and security breaches were the subject of concern in a Bamarara study. Bamarara used a quantitative methodology with a stratified random sampling approach to examine multiple bank types, job types, and work experience and types of threats encountered.

Bamrara concluded from the data that there is a correlation between data warehouse functions and malicious code, identity theft, fishing and credit card fraud. Bamrara did not find conclusive evidence of a correlation between denial of service and hacking in the data warehouse operational environment (Bamrara, 2015). Because of the study limitation to banking industries in Uttarakhand, the study population would require a much broader study to be generalizable. It is commendable that Bamrara chose a three-pronged approach (interviews, raw data, and literature review) to support the research. This approach does add to the validity of the study in contrast to the Holm, Holder, Andréasson, Baklien, and Rossow study which had a limitation to a survey only unidimensional based analysis (Holm et al., 2014). As applied to my study, some SME owners do not warehouse any data. Instead, they may rely on the supplier to provide access to a warehouse of data and supplies that they access to order merchandise.

Holm et al. presented a case for the use of expert judgment in situations where direct observation for data collection is not possible and present that credibility might be an issue in the use of expert judgment (Holm et al., 2014). Specifically, Holm et al. explored the use of expert judgment using three variables; consensus, experience, and self-proclamation and concluded that consensus is a good indicator for calibration of expert analysis as applied to cybersecurity analytics).

The methodology employed in the study was a random sampling survey-based quantitative analysis based on two research questions. RQ1 determines the variable (experience, consensus, and self-proclamation) impact on measuring expert judgment and RQ2 would determine potential correlations between the variables (Holm et al., 2014). It is possible that a qualitative case study approach might enhance the research and provide more direct observational data on the effectiveness of expert judgment in a real-life situation. My study accomplished that in providing a much needed perspective of a small business owner. An unexpected outcome of my study would be that some SME owners may defer expert judgement to a third party tech support function. The additional data collection would be an opportunity to support the study with functional data. An additional case study approach would add credibility to the study regarding validity as well as provide the potential for further generalizability across organizational functions. As Holm et al. indicated, some SME owners might opt to take advantage of a third party tech support provider for expert judgement.

Web-based malware attacks in terms of the attack model, the root cause, and the enabling vulnerabilities that allow the attacks are a consideration from a study by Chang et al. (2013). They examined latest issues with malware as well as malware defense strategies such as honeypots, code and testing techniques and blacklisting attackers (Chang et al., 2013). In the study, Chang et al. discovered that there were approximately 45,000 URLs out of 18 million URL's detected by a security scanner and exhibited a linkage to spyware. My study indicates that there is the possibility of the introduction of malware and spyware into some SMEs because the network does have the capability to connect to the internet. However, the system is protected by a firewall with associated tech support.

Of interest to my study is the application of the various malware detection virtual machines (VM's) like *Honeymonkey* and the possibility of capturing malware/spyware infused websites (Chang et al., 2013). The study was a computer survey-based analysis of the categories and approaches to discover, detect, and prevent malware attacks with the intention of the survey to be empirical based on the evaluations of the data collected and the evaluation methods (Chang et al., 2013). Further work in malware detection and prevention regarding software improvements is necessary. These attacks might occur as an issue of state to state strikes or might trickle down to state to individual (SME) attacks. My study reveals that since some SMEs harbor no warehouse data, malware detection, and prevention should be incorporated at a level above the SME local area network (the vendor or supplier). Another aspect of preventative measures might be the institution of policies for cybersecurity.

Dunn-Cavelty posited that there are general miss-guided policy issues with cybersecurity in that current practices to prevent cybercrime are not working and in fact are getting worse (Dunn-Cavelty, 2014). The policies, according to Dunn-Cavelty, are for security protection of the state as opposed to the individual citizen that hurts the systems (Dunn-Cavelty, 2014). Dunn-Cavelty asserted that a cybersecurity policy oriented toward anti-vulnerability with a proclivity toward protection of individual privacy as well. From my study results, some small businesses do not retain employees long enough to establish extensive cybersecurity. The solution might be to limit employee access to the internet.

It was Dunn-Cavelty’s position that the former without the latter is the genesis of cybersecurity vulnerabilities (Dunn-Cavelty, 2014). Dunn-Cavelty enumerated three factors that increase cyber risk. The need for fast software product delivery, the added benefits of the product increases the number of users, and quasi-monopolies all affect the production of secure software negatively (Dunn-Cavelty, 2014). Effective cybersecurity has become the victim of economics. Dunn-Cavelty concluded that a solution might be human-centric protection from vulnerabilities that may require a shift in policies that would voluntary increases in security measures from the corporate sector (Dunn-Cavelty 2014).This issue could be a transfer to the Tech Support and security software outsourced by the SMEs. In other words, this issue would be under the auspices of the cybersecurity product delivery that is routinely updated (see emergent theme three).

Reported primary cybercriminal activities (state-to–state) are questionable, and Filshstinskiy (2013) asserted that sophisticated cyberattacks could still be the work of mere cybercriminals of the DW (Dark Web) as opposed to state-sponsored activities (Epiphaniou et al., 2014). The purpose of the study was to educate the reader to be wary of claims of state sponsored crimes (terrorism) that might be theft. The philosophical approach was an attempt to differentiate between cybercrime and state-sponsored crime.. Filshstinskiy listed six cybercriminal activities from e-mail to malware and demonstrated pricing as advertised by cybercriminals. For example, purchase of a denial of service attack software against a website can be between $50 and $500 per day depending on the site and the complexity of the offensive (Filshtinskiy, 2013). Further inquiry into international agreements and laws to prevent cybercriminal activity may be necessary.

Per my study, cybersecurity invasion by another state would be unlikely since some SME owners do not provide ware housing for customer data. It would be more likely an insider threat than an external threat to contend with in the form of deviant employee behavior.

An approach to moral disengagement and deviant work behavior from the organizational injustice perspective relative to self-reporting is of interest to my study. The Hystad, Mearns, and Eid (2014) study addressed self-reported deviant work behaviors on 11 passenger and freight ships in Norway. In their study, they were interested in moral disengagement with diffusion and displacement of responsibilities as the connection to deviant work behavior. Also, in the study, Hystad et al. were interested in evaluating risk-taking, non-compliance, and lack of participation as results of perceived organizational injustice (Hystad et al., 2014). Concerning the safety concerns that might arise from corporate injustice, Hystad et al. considered the aspect of an employee's freedom to report near-misses, problems, and concerns without fear of organizational retaliation. Along with the work of D'Arcy et al., Hystad et al. pointed to the Bandura theory of moral disengagement (Bandura, 1990) as evidence that employees may sacrifice internal self-regulatory mechanisms through moral disengagement to justify behavior under the Bandura umbrella of three groups; (a) moral justification, (b) euphemistic labeling and, (c) advantageous comparison. In this study, Hystad et al. considered the mechanisms of displacement of responsibility (individual blame), diffusion of responsibility (organizational blame), and the distortion of the consequences or a victimless infraction (Hystad et al., 2014). In my study, there are not the politics present that may be a nemesis to larger organizations. Some SMEs may not have but one or two employees at a given time, making the Hystad et al. and D’Arcy et al. provisions for work place displacement and diffusion of responsibilities less prevalent. From my study, the case would more likely be employee retaliation against the organization for vengeance.

In the Hystad et al. quantitative study, the administration of 340 questionnaires to the crew of 11 Norwegian freight and passenger ships reveal conclusion that there is empirical evidence that moral disengagement influences the sense of organizational injustice and in turn may be causation for deviant behavior. These results are in keeping with my study research question and the D’Arcy et al proposition that moral disengagement plays a significant role in abnormal work behavior. In the case of my study, this may be retaliation for perceived or real organizational injustice in the form of online deviant behavior. For example, an employee might retaliate against the organization by making negative comments through corporate rating outlets such as *Glassdoor* or social media such as *Facebook* or display other deviant behavior such as online inventory sabotage and release of private customer information. It is an expectation that SME owners would not be cognizant of the potential for employee deviant online behavior based on perceived organizational injustice (Hutchings, 2012).

Finding Four: Lack of Knowledge About Social Engineering Among Small and Medium Business Owners

As stated in chapter four, out-sourcing is to the third party IT support in this case study. The IT personnel assist with connectivity issues and application issues for the supplier data base and are employees of the wholesale provider. In an informal discussion, the participant asserts that IT support is from three operations. The issue that the literature does not address, is the lack of knowledge and education from some small business owners about social engineering and cybercriminal behavior. According to Goel et al., the main issue with breaches to systems is our vulnerability and our predisposition to susceptibility to fraud. The technology notwithstanding, phishing to access the system is still a major concern for SMEs (Goel, Williams, & Dincelli, 2017).

An empirical to study to identify what organizational and individual factors contribute to resistance to social engineering by cybercriminals is a concern in the study by Flores and Ekstedt. The purpose of the study was to evaluate possible factors that contribute to an individual’s resistance to social engineering. The philosophical approach was to determine the level of the impact of organizational security culture on personal behavior relative to social engineering resistance. The underlying assumption was that organizational information security culture was a contributing factor to an individual’s resistance to social engineering cybersecurity threats.

The authors of the study revealed that all factors investigated had an influence on individuals to varying degrees, but individual attitudes were the most profound. The methodology used was a mixed-methods design where qualitative data to develop the research model and survey instrument to quantify factors of resistance to social engineering by both individuals and organizations. 4,296 individuals in Sweden were the recipients of the instrument (Flores & Ekstedt, 2016). A research question designed to discover the organizational factors that influence employees to resist social engineering cyber-threat activity. For my study, it would be important for SME owners to understand the construct social engineering and how it might be used in a retaliatory way to create disfunction or in the organizational activities

Bongardt drew parallels to criminal profiling and cybercriminal profiling and explored these attributes at the individual level. Bongardt suggested that cyber criminals could have motivations, objectives, and characteristics that have been a consideration for contributing factors to real world crime. Bongardt issued 14 categories for motives used for profiling cyber attackers (Bongardt, 2010). Bongardt submitted that once the identification of motives, objectives, and characteristics of network intruders occurs, they may make the profiling of the intruders a possibility. In my case study, some SME owners work closely with the staff and may be able to detect cybercriminal activity as it occurs.

A simulated phishing attack in an effort explore means to train individual users in the secure use of the internet was an exercise by Jansson and von Solmes at the University of South Africa to demonstrate the validity of their study. The purpose of the study was to explore deceptive phishing exercises to understand the individual’s susceptibility to phishing attacks. The underlying assumption was that phishing attacks are successful based on the user’s lack of awareness of the activity.

The methodology was a quantitative analysis based on simulated phishing attacks and user responses. The evaluation indicated that with proper warnings and training, users became less susceptible to phishing attacks. However, Jansson and von Solmes noted that in the second exercise, users may have received forewarning by word of mouth of the exercise and may have adjusted their behavior accordingly (Jansson & von Solmes, 2013). The authors recommended further research to establish embedded warnings as a training device. In the case of some SMEs, it might be necessary for the business owner to offer tips and training to alert the employees to the nature of phishing attacks.

A mixed-methods approach to the Nero, Wardman, Copes, and Warner study to investigate the effectiveness of web-site take-down contractors as a counter measure for e-mail phishing attacks to demonstrate its effectiveness (Nero et al., 2014). For the quantitative analysis, measurements were from analysis of millions of phishing e-mails to determine affected financial institutions. For the qualitative analysis, they conducted interviews with financial fraud investigators from five ranked financial institutions (Nero et al., 2014). The results revealed the participating banks and take down companies, made little use of law enforcement concerning the attacks. The qualitative results determined that not many financial institutions conduct their investigations into phishing attacks which support the quantitative data analysis conclusion (Nero et al., 2014). Nero et al. concluded that takedown countermeasures are too late to prevent phishing attacks and that use of phishing attack evidence is rare in the pursuit of perpetrators (Nero et al., 2014). The vulnerability as an SME risk to employees for phishing attacks illustrates the broader concern for employee vulnerabilities about internet cybercrime. Take down operations being too late would be the case for some SMEs. Any take down operations would likely be after the damage was done. An SME owner would have little chance of discovering who committed a phishing attack. In this case, the outsourced tech support personnel may be required to assess the damage and recover the system.

Limitations of the Study

The limitations of my study are that my study is outside of a laboratory environment. These limitations result in a lack of experimental control over the research and are an attribute of passive observations in the study environment (Brutus, Aguinis, & Wassmer, 2012). Mitigation for this limitation is by the addition of interview questions that serve to reinforce the passive observations. For example, the participant might feel that his business is impervious to cyberattacks based on the lived experience of never encountering such attacks. However, passive observations reveal that there are physical lapses in the business security environment such as unfettered access to computers at times that put the company at risk to inside and outside threats. In an informal business environment such as the SME typical environment, security lapses might not be noticeable by those that do not have formal training regarding the potential risks that such an informal business environment might create. This study also has the limitation of a single case study design. Further exploration of SMEs that house customer information might lead to new findings. The study may be generalizable to those SMEs that do not retain a customer information database.

More research is also required for the possible connections between Jaishankar's space transition theory and the Bandura's moral disengagement theory. The understanding is that further exploration of these two theories may hold some promise to for detecting early warning signs of a potential cybersecurity due to employee, tech support, or customer retaliatory cybercriminal activity. The exploration of these two theories would be especially beneficial to enterprises required to protect customer online personal data.

Recommendations

Further case study analysis might add to the confirmation of the findings of this study. Although this case study is generalizable about other SMEs security practices and procedures, it has a limitation to a case study of an SME that does not store personal information on the LAN (local area network.). Further case studies that apply to businesses that sore online customer personal data would be advantageous to business owners that require that level of network protection. Since the study was outside of a laboratory, the data collection was not under the restrictions of a laboratory environment. These limitations result in a lack of experimental control over the research and are also an attribute of passive observations in the study environment (Brutus, Aguinis, & Wassmer, 2012).

The exploration of new knowledge about the issue of cybercriminal potential in SMEs through the study of SME organizational decision-making attributes and activities that might lead to exposure of private and proprietary data to cybercriminal activities might provide answers to the research question. Alignment of this study uses a two-prong approach to explore the possibility that the psychology of employee behavior in cyberspace and the cyberattacks and there is possibly a relationship concerning internet access and employee vulnerabilities. From these two theories, a third theory that emerged from the study is that space transition theory and moral disengagement combine to create a new theory that explains vulnerabilities from both the victim and the criminal’s perspectives that create the environment for crime. The purpose of this qualitative case study is to explore SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources. Further study is requiered to explore the connection between space transition theory and moral disengement as an expalination for cybercriminal activity. From the literature review, there were nine aspects of SME concerns; The literature review revealed two theories and nine attributes that may enable those theories application in the SME work place: space transition theory and anonymity (Jaishankar, 2008), and moral disengagement and (Bandura, 2009).

For behavior and social media concerns, Pantic uses social media, as an illustration, to represent that depression from internet use was a concern before social media (Facebook having a foundation in 2004). Therefore, it is possible that social media (having increased online activity) will have exacerbated the issue (Pantic, 2014). Pantic suggested a requirement for further research to investigate if the existence of correlation can be causality. For example, does Facebook cause low self-esteem, or are people with low self-esteem more frequent users of Facebook (Jaishankar, 2008; Pantic, 2014).

The human to computer interface suggests the possibility that people view computers as having unjust behaviors in much the same way that see coercive action as unjust in society. Shank presented the case that people may see computers as vehicles for punishment in the same way humans can be. For example, in situations where a person might deny services such as a bank teller due to a lack of required documentation such as an e-mail account, a computer is programmable to deny access to a site based on the same requirement (Shank, 2012). Shank asserts that computers can have the same attributes as humans when it comes to the human to computer interaction. Shank's study suggested that people do not differentiate between injustice by a machine and injustice by someone else (we have all cursed our cars). Psychology is beginning to play a significant role in information systems security. In the light of Shank's study, employees or Tech Support may become frustrated with a computer and retaliate against the business owner as a result.

Psychology is beginning to play a significant role in information systems security (Weiderhold, 2014). Weiderhold asserted that the human factor is the weakest link in cybersecurity and as a researcher in the field, I must agree based on the literature (Jaishankar, 2008; Tarafdar et al., 2013). Wiederhold held that there are five psychological interests in cybercriminal activity; (a) behavioral economics (risk and reward, (b). Patterns of criminal behavior, (c) advising on the legislature, (d) public awareness, and (e) impacts to the victims (Weiderhold, 2014). My study is an exploration of five of these activities through the lenses of the researcher and an SME owner to develop an understanding of the application of how these principals may relate to a real-world small business owner and other developing theories such as space transition theory. Jaishanker developed space transition theory to explain behavioral changes in the transition from physical space to cyberspace (Jaishanker, 2007). These behavioral changes can be attributable to SME employee behavior and the online environment as suggested by the following literature.

The topic of cybercrime and education produced a study by Bougaardt and Kyobe that concluded that a lack of knowledge and understanding relative to what cyberattacks involve, result in further victimization from cybercrimes and further determined that more research in the areas of educating and training SME managers in reporting and compliance as preventive measures for cyberattacks may be necessary (Bougaardt & Kyobe, 2011). Bougaart and Kyobe submitted that their sample size was too small for generalization and further determine different causes of management behavior concerning a cybersecurity (Bougaardt & Kyobe, 2011).

The research for behaviors during a cybercriminal attack produces the study by Adnan al illustrated the properties of MATE and RMATE capabilities in a diagram where the attackers tool box contents such as; debugger, emulator, disassembler, tracer de-compiler, slicer, virtual machines and SQL injections with the defensive tool box being comprised of defense-in-depth, digital watermarking, diversity, white-box cryptography, emulator detection, debugger detection obfuscation and tamper-proofing as countermeasures are exposed (Adnan et al. 2015). Germane to my study, Adnan et al. acknowledge that a weakness in the literature is the social cognition factor of the lone attacker. In other words, it is necessary to understand how MATE attackers think to identify the cause of the attacks correctly. To further explore the social cognition factor into the malicious behaviors, it is necessary to determine some of the important psychological studies associated with the response.

A comparison computer forensic analysis and the use of computer investigative analysis (CIA) based on the case of Dennis Rader in a study by Bongardt. Bongardt asserted that if behavior reflects the personality, then, use of CIA in the correct form in a computer to detect network intrusions could be an application (Bongardt, 2010). Bongardt used a qualitative, narrative approach to compare how CIA might apply in much the same way that computer forensics were involved in the capture of serial killer Dennis Rader (Bongardt, 2010). Interestingly, a MATE attack would be an avenue for a tech support retaliation attack.

Personnel risks associated with insider threats for SMEs produced the perspectives of employees under competitive stress that applies to the SME environment and assume the form of employee retaliation. Star performers invalidate the belief that the distribution of individual performance is reasonable and that a power law distribution model for individual performance is more appropriate (Aguiness & O'Boyle, 2013). In this qualitative, narrative study, Aguinis and O'Boyle presented nine propositions in support of their argument backed by relevant statistical data. The article is based on early works in performance assessment where the thinking was that top performers are anomalies and either thrown out of the studies, ignored or forced into normal distribution for performance analysis (Aguiness & O'Boyle, 2013)

Equipment and software pose an additional concern for SMEs because as my study reveals, SMEs suffer great difficulty in maintaining current appliances and up-to-date software technology. Cyber systems security is a consideration of Ali et al. They produced a literature based historical study to explore security protection of cyber-physical systems (CPS). A CPS includes sensors, monitoring and control features embedded in electronics devices to connect cyber systems to the physical world (Ali et al., 2015). In the study, Ali et al. presented seven modes that are potential known threats for attacks. Eavesdropping, compromised-key attacks, man-in-the-middle attacks, DOS (denial of service) attacks, resonance attacks, communication jamming attacks and integrity attacks. Ali et al. asserted that internal and external trust in CPS established a boundary for external trust (security software), and internal trust is dependent on interpersonal, structural and dispositional and rely on statistics and probability modeling (Ali et al., 2015) These are forms of attacks that might be perpetrated on an SME as a retaliatory attack by employee's, Tech Support, or customers. Firewall technology may be another solution to some of these cyberattacks.

According to the participant, firewall technology is a major source of protection for his business. When asked how he might protect his network his response was; "Uh, probably like use a firewall and kind of limit the access to the internet." Firewall technology is becoming intertwined with hardware and software according to a study by Hunter. In the qualitative, narrative approach, Hunter compared and contrasted firewall technologies and the expected growth of investment and research and development. A graphical representation presented by Hunter illustrated that there is an expectation that commercial firewall sales will grow more than one billion dollars by 2018 (Hunter, 2013). Hunter examined the production of business broadband routers and modems with built-in firewall protection indicating a trend way from firewall protection software initiation from the computing appliance to the routers and modems (Hunter, 2013), in other words, the modems and routers will host the embedded software and updates within the router or modem as opposed to the protection of the computer in commercial enterprises. Hunter compares Juniper and Cisco routers (the top competitors in the business router market), and the conclusion is that the final design features with flexibility will gain the market share.

The issue of how small and medium businesses might cope with assessing their information security through self-assessment and improvements using a model framework is a study provided by Cholez and Gerard (2014). Central to the article was the concern for business ability to perform a self –assessment of security maturity and to improve the security process accordingly by using the framework that Cholez and Gerard had developed in this article. The data analysis tool used was the ISO 9001 PDCA (Plan, Do, Check, Act) model to measure the best practices employed in the case studies (Cholez & Gerard, 2014). From my study, the participant was uncertain as to his system status relative to internet threats: " I think that if somebody wants in the system they can get in and get what they want if, uh I don't think you're going to be able to just totally stop it. If they want in, they're going to get in." This statement also indicates that the participant may need guidance as to policies and procedures to follow for network security. As seen again in chapter two, the role of IT governance in small and medium businesses, specifically, IT governance of SMEs in the form of HR resources is an aspect explored by Garbarino. In enterprises where resource usage comes at a premium, it is necessary to develop a lean system of governance. Garbarino noted that SMEs have a simple structure that does not include many specialists to perform the routine IT functions larger corporations might facilitate (Garbarino, 2013). Garbarino asserted that IT (and therefore IT growth) is essential to the success of an organization as an enabler of growth. The purpose of the study was to provide the lessons learned and issues from a case study to implement IT governance into an SME (Garbarino, 2013). The philosophical approach was to identify shortfalls in the human resource management aspect of the implementation of IT governance in SMEs to reach average levels of maturity in IT governance.

The underlying assumption is that SMEs will adapt to the implementation of IT governance tailored to an SME enterprise. Garbarino presented a case study of AAA (a localized pharmaceutical market) and the incorporation of IT governance into the business. The methodology was a single qualitative case study design (for defense, Garbarino cited the Yin definition for a single case study design). The author revealed a positive connection between HR training and IT practices that contribute to the organization's success.

Garbarino suggested a replication of the study in other enterprises. The author indicates a correlation between IT governance and organizational success. The author does not advance the inclusion of security risks and a need for a security training apparatus in the SME IT organization. Giovino addressed the significant growth of occupational crime and fraud and the corresponding increasing need for prevention and detection in the form of internal business audits to protect organizations. Giovino discussed that leadership discussions ethics and integrity should be the routine subject of an open forum (Giovino, 2015).

The purpose of the study was to inform the reader of the importance of open communication on ethics and integrity concerning organizational cybersecurity. Giovino offered three conditions under which fraud may occur within an organization; (a) incidental pressures (sales or financial goal pressures), (b) opportunities to commit fraud (holes in the security system, unnecessary access privileges) and, (c)motivation for financial gain or disgruntled retaliation (Giovino, 2015). Giovino further advised organizations of the processes for reporting cybercriminal activity and the insurance recovery mechanisms that may be available to the victim organizations (Giovino, 2015).

The underlying assumption the author made was that organizational crime and fraud would continue to grow to advance the need for improved protection of organizations. Giovino further asserted that surprise audits, hotlines and training might avert future organizational losses due to fraud. The methodology was a qualitative narrative approach designed to inform the reader on reporting, preventing and recovering from the cybercriminal activity. The limitations of the study were that it did not address

SME fraud prevention, detection, and recovery. Unlike larger organizations, SMEs do not typically have the funding required to support internal auditing techniques. For SMEs, the policies and procedures may have to be kept to a minimum as there is no human resources or governance staff to maintain and enforce them. Perhaps a simple small rule book for new hires could be developed to maintain a standard of expected behavior when using online company resources.

Implications

Corporations seek to create positive social change as an initiative to promote community well-being (Natarajan & Edwards, 2016; Sharma & Good, 2013). My study might perpetuate this effort by alerting SME managers as to the risks involved to the community through employee social media activities and online behaviors. These risks are where the two theories intersect to create a paradox of psychological behavior inherent to internet social behavior in an anonymous virtual reality that potentially creates the victim/victim environment. The perpetrator is the victim of the ease of the crime, and the victim is the victim of and by anonymity.

Since the problem is that cybersecurity losses among SMEs are growing and there is a lack of consensus as to the elements of a decision model for SME investment in cybersecurity (Chabinsky, 2013; Sangani & Vijayakumar 2012)**.** Sangani and Vijayakumar provided a comprehensive list of security threats and mitigations for SMEs; however, the authors of the studies did not include the perspectives of the SME managers. New knowledge about the issue by studying organizational decision-making attributes and activities might lead to exposure of private and proprietary data to cybercriminal activities. This study is in alignment with a two-pronged approach to explore the possibility that the psychology of employee behavior in cyberspace and the cyberattacks relate to respect to internet access and employee vulnerabilities using the Bandura and Jaishankar theories.

The possible impact of the positive social change would be an improvement in the understanding of SME owners as to why SME cybersecurity networks systems breaches may occur. For example, and understanding by SME owners about social engineering and employee, tech support or customer retaliation and that cyberattacks against a network are not a necessarily a product of greed (Hutchings, 2012; Tarafdar et al., 2013; Willison & Warkentin, 2013; Zhurin, 2015). An attack on an SME that does not house any customer data or bank information would most likely be one of retaliation or for a cybercriminal simply to brag about the adventure

Significance to Social Change

My study is about the status of the effects of social engineering for cybercrime and the potential impact to small and medium sized businesses through employee vulnerabilities using a small business for a case study to explore the vulnerability to social engineering. A frame for the gap in the literature contains two theories, where space transition theory (Jaishankar, 2007) represents the actions of the victim, and the

Bandura theory of selective moral disengagement (Bandura, 2009) that possibly represents the actions of the perpetrator from the psychology aspect of the issue, Jaishankar illustrated that there is a phenomenon of personality and behavioral change he referred to as space transition theory (2007). Bandura and Donner et al. indirectly addressed the Jaishanker theory from a psychological perspective in the form of moral disengagement and low self-control in the computer environment (Bandura, 2009; Donner et al., 2014). These articles presented the possibility that there is a gap in the literature where the psychology of the behavior and the intersection of the cybercriminal activity may require further exploration, and the exploration of this gap may create positive social change through the understanding of how these theoretical interactions between online users create the potential for cybercriminal activity (see Appendix F). Exploring the nature of these theories and shuttering the literary gap might generate an understanding of how their application might serve to create positive social change. From the study results based on the observations, interview questions, and reflexive notes, a cybersecurity intrusion into an SME would most likely occur as a form of retaliation from a customer, an employee, or tech support personnel (Hutchings, 2012; Tarafdar et al., 2013; Willison & Warkentin, 2013; Zhurin, 2015). Zhurin identified tech support impersonation as a means to gain access to the system, in the light of this study, tech support could also be a retaliatory concern the same as a customer and employee retaliation is a concern.

The importance of the study as a contribution to positive social change is implicit in the fact that there appears to be little in the way of a literature connection on the link between Jaishankar's space transition theory, and the Bandura psychological studies behind the human behavior and the anonymity the internet provides. My study attempts to close the possible gap in the literature, and it would be important to SME owners to understand the risk associated with online employee behavior and cybercriminal social engineering activity in the form of taking advantage of the psychology behind moral disengagement and space transition theory. Sharma and Good (2013) asserted that corporations now seek to create positive social change as an initiative to promote community well-being. My study might perpetuate this effort by alerting SME managers as to the risks involved to the community through employee social media activities and online behaviors. Employee online behavior is where the two theories intersect to create a paradox of psychological behavior inherent to internet social behavior in an anonymous virtual reality that potentially creates the victim/victim environment. The perpetrator is the victim of the ease of the crime, and the victim is the victim of anonymity.

Conclusions

In his article on perspectives of knowledge, Jianwei qouted Socrates as having said:"As for me, all I know is that I know nothing." (Jianwei, 2012). In this case study, the evidence suggests that SME managers and owners may not posess the skills and expertise to protect themselves from cybercriminal attacks, but as is the case with this study, business owners may accept the wisdom of Socrates and defer to the experts for the skills necessary to protect themselves. There are things that the business owners can do to protect themselves from cybersecurity breaches. Since some SMEs do not provide data storage of customer information or bank data on the local area network, it is unlikely that cyber attacks would come from an entity disassociated with the business so the potential for cyberattacks due to the employee, customer or tech support retaliation comes to the forefront of the concerns.

The purpose of this qualitative case study was to answer the research question by exploring SME management decision factors that may positively or negatively influence the capacity for organizations to protect information with available resources. Some business owners rely heavily on third party tech support for network security. Some business owners may not consider that there are other reasons besides obtaining information or financial gains that may cause cyberattacks such as employee, customer or Tech Support retaliation (Huang & Miranda, 2015; Pantic, 2014; Shank, 2012).

Moral disengagement is the theoretical mechanism and Space transition is the theoretical vehicle that enables retaliatory behavior online. During space transition from the reality environment to cyber-space environment and operating on moral disengagement (Bandura, 2009; Jaishankar, 2008), an employee, customer, or tech support personnel might take advantage of their knowledge of the system to retaliate against the organization by making negative comments through company rating outlets such as *Glassdoor* or social media such as *Facebook,* or display more severe deviant behavior such as online inventory sabotage by accessing the ethernet IP address to inflict a denial of service attack using an obtained password from a social engineering process (shoulder surfing or dumpster diving) as discussed by Simms (2016). It is an expectation that SME owners would not be cognizant of the potential for employee, tech support or customer deviant online behavior based on perceived organizational injustice (Hutchings, 2012). SME owner education relative to the causes of insider cyberattacks might serve as a preventative measure to an insider (employee) and external (customer and third party tech support) retaliatory cyberattacks.

There is also a necessity to evaluate the potential effects of depression from social media use and the possible correlation to online cybercriminal activity concerning the Jaishankar space transition theory. For example, does a depressed state from overuse of social media create the potential for retaliation in the form of cybercriminal activity? Zhurin identified tech support impersonation as a means to gain access to the system, in the light of this study, tech support could also be a retaliatory concern the same as customer and employee retaliation is a concern.

Ultimately, small and medium business cyber -security is a matter of understanding the motives behind cyber- security intrusions. Because some small businesses, from this case study, may not house customer personal or financial information on the business network, the motives are more likely to be about a customer, employee, or technical support retaliatory attacks on the system rather than for the financial gain that is normally the motive for cybercriminal activity. The real issue that is not in the literature is the lack of knowledge and education from some small business owners about social engineering and cybercriminal behavior. The literature seems to propose a scaled down version of the corporate cybercrime prevention methods. For example, Giovino’s recommendation for an HR IT function and surprise audits may not be practical to an SME organization with two or three employees. Levying these kind of requirements on SME employees would be like to trying to scale down aircraft carrier operational instructions for use as canoe operational instructions. The two endeavors are too dissimilar for cross pollination of requirements in some cases. The corporate top down institution of requirements may not be applicable in some SME cases; a bottoms-up approach would be more fitting because of the relatively short chain of command in some SMEs. For some SMEs as is the situation in this case study, understanding how to maintain a secure network may be a matter of understanding people and motives rather than the application institutional technology and policies.

References

Adnan, A., Sookhak , M., Badrul, N., Anuar, A., Gani, E., Ahmed, M., & Khurram K. (2015). Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications 48* (2015)44-57. doi:10.1016/j.jnca.2014.10.

Aguinis, H., & O'Boyle, E. (2014). Star performers in twenty-first century organizations. *Personnel Psychology, 67*, 313-350. doi:10.1111/peps.1205

Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the Disinhibition effect. *International Journal of Cyber Criminology, 9*(1), 35-54. Retrieved from http://www.cybercrimejournal.com/

Ali, S., Anwar, R. W., & Hussain, O. K. (2015). Cyber security for cyber physical systems: a trust-based approach. *Journal of Theoretical & Applied Information Technology, 71*(2), 144-152. Retrieved from http://www.jatit.orgd/

Alonso, F. M. (2016). Reasons for reliance. *Ethics*, (2),311.-328 doi:10.1086/683536

Anderson, R. (2018). Making security sustainable. *Communications of the ACM, 61*(3), 24-26. doi:10.1145/3180485

Appel, J., von der Pütten, A., Krämer, N. C., & Gratch, J. (2012). Does humanity matter? Analyzing the importance of social cues and perceived agency of a computer system for the emergence of social reactions during human-computer interaction.

Advances in Human-Computer Interaction (10 pages), Article ID 324694, Volume 2012 (2012*).* doi:10.1155/2012/324694

Applebaum, M. (2012). Phenomenological psychological research as science. *Journal of Phenomenological Psychology, 43*(1), 36-72. doi:10.1163/156916212x632952

Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration, 54*(1), 46-56. doi:10.1080/01930826.2014.893116

Arquilla, J., & Guzdial, M. (2017). Crafting a national cyberdefense, and preparing to support computational literacy. *Communications of the ACM*, *60*(4), 10-11. doi:10.1145/3048379

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

Badamas, M. A. (2012). Cyber security considerations when moving to public cloud computing. *Communications of the IIMA, 12*(3), 1-18. Retrieved from http://www.iima.org/index.php?option=com_phocadownload&view=section&id=10&Itemid=68

Bamrara, A. (2015). Evaluating database security and cyber-attacks: A relational approach. *Journal of Internet Banking & Commerce, 20*(2), 1-8. doi:10.4172/12045357.1000115ethods

Bandura, A. (1990). Selective activation and disengagement of moral control. *Journal of Social Issues, 46*(1), 27-46. doi:10.1111/j.1540-4560.1990.tb00270.x

Bandura, A. (2009). Selective moral disengagement in the exercise of moral agency. *Journal of Moral Education*, *31* (2) 101-119 doi:10.1080/0305724022014322

Barbour, T. (2014). Cyber security. *Alaska Business Monthly*, *30*(10), 138-140. Retrieved from https://issuu.com/alaska_business_monthly/docs/abm_oct_2014_4_web/140

Barratt, M., Choi, T. Y., & Li, M. (2011). Qualitative case studies in operations management: Trends, research outcomes, and future research implications. *Journal of Operations Management*, *29*, 329-342. doi:10.1016/j.jom.2010.06.002

Barton, E., Ledford, J., Lane, D., Germansky, S., Hemmeter, M., & Kaiser, A. (2016) The iterative use of single case research designs to advance the science of EI/ECSE. *Topics in Early Childhood Special Education, 36*, 4-14. doi:10.1177/0271121416630011

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report, 13*, 544-559. Retrieved from http://www.nova.edu/ssss/QR/QR13-4/baxter

Bojanc, R., & Jerman-Blažič, B. (2013). A quantitative model for information-security risk management. *Engineering Management Journal, 25*(2)25-37. Retrieved from http://www.scimagojr.com/journalsearch.php?q=29088&tip=sid&clean=0

Bongardt, S. A. (2010). An introduction to the behavior profiling of computer network intrusions. *The Forensic Examiner, 19*(3), 20-25. Retrieved from http://www.theforensicexaminer.com/

Bonner, J., Greenbaum, R., & Mayer, D., (2016). My boss is morally disengaged: The role of ethical leadership in explaining the interactive effect of supervisor and employee moral disengagement on employee behaviors. *Journal of Business Ethics, 137*, 731-742. doi:10.1007/s10551-014-2366-6

Bougaardt, G., & Kyobe, M. (2011). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cybercrime in South Africa. *Electronic Journal of Information Systems Evaluation, 14*(2), 167-178. Retrieved from http://ejise.com/main.html

Bradbury, D. (2014). Feature: Unveiling the dark web. *Network Security, 20,* 1414-1417. doi:10.1016/S1353-4858(14)70042-X

Brutus, S., Aguinis, H., & Wassmer, U. (2012). Self-reported limitations and future directions in scholarly reports analysis and recommendations. *Journal of Management, 39*(1) 48-75. doi:10.1177/0149206312455245

Cader, H. A., & Leatherman, J. C. (2011). Small business survival and sample selection bias. *Small Business Economics, 37*, 155-165. doi:10.1007/s11187-009-9240-4.

Carbonell, J., Sánchez-Esguevillas, A., & Carro, B. (2017). From data analysis to storytelling in scenario building. A semiotic approach to purpose-dependent writing of stories. *Futures,* 8815-29. doi:10.1016/j.futures.2017.03.002

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

Carver, C. S., & Scheier, M. F. (1982). Control theory: A useful conceptual framework for personality–social, clinical, and health psychology. *Psychological Bulletin, 92*(1), 111-135. doi:10.1037/0033-2909.92.1.11

Case, C. J., & King, D. L. (2013). Cyber security: a longitudinal examination of undergraduate behavior and perceptions. *ASBBS Ejournal, 9*(1), 21-29. Retrieved from http://asbbs.org/ejournal.html

Cepeda, T. P., Gerardo, K. R., Perez, K. T., & Rivera, J. J. (2015). Credit card fraud: when employees move from being an employer's biggest asset to their biggest liability. *Journal of the International Academy for Case Studies, 21*(4), 23-30. Retrieved from http://www.alliedacademies.org/the-international-academy-for-case-studies/

Chang, J., C., Venkatasubramanian, K. K., West, A. G., & Insup, L. (2013). Analyzing and defending against web-based malware. *ACM Computing Surveys, 45*(4), 49. doi:10.1145/2501654.2501663

Cholez, H., & Girard, F. (2014). Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of Software: Evolution & Process, 26*, 496-503. doi:10.1002/smr.1609

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review, 44*, 588- 608. doi:10.2307/2094589

Connelly, S., Dunbar, N. E., Jensen, M. L., Griffith, J., Taylor, W. D., Johnson, G., & Mumford, M. D. (2016). Social categorization, moral disengagement, and credibility of ideological group websites. *Journal of Media Psychology: Theories, Methods, and Applications, 28*(1), 16-31. doi:10.1027/1864-1105/a000138

Chabinsky, S. (2013). Cyber security for SMEs: Prioritize, isolate and protect. *Security, 50*(7), 30. Retrieved from http://www.securitymagazine.com/articles/84479-cyber-security-for-smes-prioritize-isolate-and-protect

Choras, M., Kozik, R., Torres Bruna,. P., Yautsiukhin, A., Churchill, A., Maciejewska, I., & Jomni, A. (2015, August). Comprehensive approach to increase cyber security and resilience. *In Proceedings of ARES (International Conference on Availability, Reliability and Security*, *Touluse)* 686-692. Retrieved from https://www.ares-conference.eu/

Cowan, L. (2014). The psychopath: What's love got to do with it? *Psychological Perspectives, 57*, 291-311. doi:10.1080/00332925.2014.936241

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*, 285-318. doi:10.2753/MIS0742-1222310210

De Cock, R., Vangeel, J., Klein, A., Minotte, P., Rosas, O., & Meerkerk, G. (2014). Compulsive use of social networking sites in Belgium: Prevalence, profile, and the role of attitude toward work and school. *Cyberpsychology, Behavior, and Social Networking, 17*(3), 166-171. doi:10.1089/cyber.2013.0029

Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global Crime, 14*(2/3), 175-196. doi:10.1080/17440572.2013.801015

Denissen, J. J., Aken, M. A., Penke, L., & Wood, D. (2013). Self-regulation underlies temperament and personality: An integrative developmental framework. *Child Development Perspectives, 7*, 255-260. doi:10.1111/cdep.12050

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

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

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*, 532-550. doi:10.5465/AMR.1989.4308385

Epiphaniou, G., French, T., & Maple, C. (2014). The darkweb: Cyber-security intelligence gathering opportunities, risks and rewards. *Journal of Computing & Information Technology,* 21-30. doi:10.2498/cit.1002282

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). *Human behaviour as an aspect of cyber security assurance.* 9 (17) 4667-4679 Retrieved from http://arxiv.org/ftp/arxiv/papers/1601/1601.03921.pdf

Ferrillo, P., & Singer, R. (2015). Is employee awareness and training the holy grail of cybersecurity? *Corporate Governance Advisor, 23*(3), 10-13. Retrieved from http://www.wklawbusiness.com

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

Firmin, R., Bonfils, K., Luther, L., Minor, K., & Salyers, M., (2017). Using text-analysis computer software and thematic analysis on the same qualitative data: A case example. *Qualitative Psychology, 4*(3), 201-210. doi:10.1037/qup0000050

Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness.

Department of Industrial Information and Control Systems, Royal Institute of Technology, Stockholm, Sweden 59, 26-44. doi:10.1016/j.cose.2016.01.004

Foreman-Wernet., L. & Dervin, B. (2017) Hidden depths and everyday secrets: How audience sense- making can inform arts policy and practice, *The Journal of Arts Management, Law, and Society, 47*(1), 47-63. doi:10.1080/10632921.2016.1229642

Fosso Wamba, S., & Carter, L. (2014). Social media tools adoption and use by SME's: An empirical study, *Journal of End User and Organizational Computing* (26), 1-16. Retrieved from http://www.igi-global.com/journal/journal-organizational-end-user- computing/1071

Fusch, P., & Ness, R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*, 1408-1416. Retrieved from http://tqr.nova.edu/wp-content/uploads/2015/09/fusch

Fusch, P., Fusch, G., & Ness, L., (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change 10* (01), 19-32. doi:10.5590/JOSC.2018.10.1.02

Garbarino-Alberti, H. (2013). IT governance and human resources management: A framework for SME's. *International Journal of Human Capital and Information Technology Professionals 4*(3), 40-57. doi:10.4018/jhcitp.2013070104

Garrett, R. K., & Danziger, J. N. (2008). Disaffection or expected outcomes: Understanding personal Internet use during work. *Journal of Computer-Mediated Communication, 13*, 937-958. doi:10.1111/j.1083-6101.2008. 00425.x

Gill, P., Stewart, K. Treasure, E., & Chadwick, B. (2008) Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal, 204(6)* 291-295. Retrieved from https://www.nature.com/bdj/journal/v204/n6/full/bdj.2008.192.html

Giovino, C. J. (2015). The fraud response. *Internal Auditor, 72*(1), 43-47. Retrieved from https://na.theiia.org/periodicals/pages/internal-auditor-magazine.aspx

Gold, S. (2014). Get your head around hacker psychology. *Engineering & Technology (17509637)*, *9*(1), 76-80. Retrieved from http://eandt.theiet.org/

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of The Association for Information Systems, 18*(1), 22-44. Retrieved from aisel.aisnet.org/jais/

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

Graf, C. (2017). The pillars of publication ethics and research integrity: Spread the word. *Chinese Medical Journal, 130*(12). doi:10.4103/0366-6999.207483

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

Gundecha, P., Barbier, G., Jiliang, T., & Huan, L. (2014). User vulnerability and its reduction on a social networking site. *ACM Transactions on Knowledge Discovery from Data, 9*(2), 12:1-12:25. doi:10.1145/2630421

Hayes, A. A. Jr. (2014). Other lessons from the six million dollar man. *Journal of Government Financial Management, 63*(1), 62-63. Retrieved from https://www.agacgfm.org/Resources/Journal-of-Government-Financial-Management.aspx

Hayes, J., & Bodhani, A. (2013). Cyber Security: Small firms under fire. *Engineering & Technology 8* (6),80-83. Retrieved from https://eandt.theiet.org/content/articles/2013/06/cyber-security-small-firms-now-in-the-firing-line/

Herselman, M., & Warren, M. (2004). Cyber-crime influencing businesses in South Africa. *Issues in Informing Science & Information Technology, 1* 253-266. Retrieved from http://www.informingscience.org/Journals/IISIT/Overview

Holm, H., Sommestad, T., Ekstedt, M., & Honeth, N. (2014). Indicators of expert judgement and their significance: an empirical investigation in the area of cyber security. *Expert Systems, 31*, 299-318. doi:10.1111/exsy.12039

Holmila, M., Holder, H., Andréasson, S., Baklien, B., & Rossow, I. (2008). Roles for researchers in community action projects to prevent alcohol and other drug problems: Methodological choices. *Drugs: Education, Prevention & Policy, 15*, 410-423. doi:10.1080/09687630701839149

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

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*, 615-660. doi:10.1111/j.1540-5915.2012.00361.x

Huang, S., & Miranda, P. (2015, May). Incorporating human intention into self-adaptive systems. In *Proceedings of the 37th International Conference on Software Engineering-Volume 2,* 571-574. IEEE Press. doi:10.1109/ICSE.2015.196

Hunter, P. (2013). Cyber security's new hard line. *Engineering & Technology (17509637), 8*(8), 68-71. doi:10.1049/et.2013.0809

Hutchings, A. (2012). Computer security threats faced by small businesses in Australia. *Trends & Issues in Crime & Criminal Justice,* (433), 1-6. Retrieved from http://www.aic.gov.au/publications/current%20series/tandi.html

Hutchings, A. & Holt, T. (2016) The online stolen data market: disruption and intervention approaches, *Global Crime, 18*:1, 11-30, DOI: 10.1080/17440572.2016.1197123

Hystad, S., Mearns, K., Eid, J., (2014), Moral disengagement as a medium between perceptions of organizational justice and deviant work behaviors. *Safety Science. 68*,138-145. doi:10.1016/j.ssci.2014.03.012

Jaishankar, K. (2007) Establishing a theory of cyber-crimes. *International Journal of Cyber Criminology, 1*(2), 7-9. Retrieved from http://www.cybercrimejournal.com/

Jaishankar K. (2008). *Space transition theory of cybercrimes*: *Crimes of the internet*. Upper Saddle River, NJ: Pearson.

Jianwei, Z. (2012). Different images of knowledge and perspectives of pedagogy in Confucius and Socrates. *Complicity: An International Journal Of Complexity & Education*, *9*(1), 75. Retrieved from https://gfbertini.wordpress.com/2014/04/01/different-images-of-knowledge-and-perspectives-of-pedagogy-in-confucius-and-socrates/

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology, 32*, 584-593. doi:10.1080/0144929X.2011.632650

Johnson, J. F., & Connelly, S. (2016). Moral disengagement and ethical decision-making: The moderating role of trait guilt and shame. *Journal of Personnel Psychology 15*(4), 184-189. doi:10.1027/1866-5888/a000166

Kara. H., & Pickering, L. (2017) New directions in qualitative research ethics. *International Journal of Social Research Methodology, 20*, 239-241. doi:10.1080/13645579.2017.1287869

Lee, K., Kim, E., Bhave, D. P., & Duffy, M. K. (2016). Why victims of undermining at work become perpetrators of undermining: An integrative model. *Journal of Applied Psychology, 101*, 915-924. doi:10.1037/apl0000092

Leggett, T. (2017). A picture is worth a thousand words: Visualization in data analysis. *Radiologic Technology, 89*(1), 79-82. Retrieved from http://www.radiologictechnology.org/

Lucero, M., Allen, R., & Elzweig, B. (2013). Managing employee social networking: evolving views from the national labor relations board. *Employee Responsibilities & Rights Journal, 25*(3), 143-158. doi:10.1007/s10672-012-9211-9

Madill, A., & Sullivan, P. (2017). Mirrors, portraits, and member checking: Managing difficult moments of knowledge exchange in the social sciences. *Qualitative* = *Psychology*, doi:10.1037/qup0000089

Maitlys, S., & Christianson, M. (2014). Sense-making in organizations: Taking stock and moving forward. *The Academy of Management Annals, 8*(1), 57-125. doi:10.1080/19416520.2014.873177

Mariotto, F. L., Pinto Zanni, P., & De Moraes, G. M. (2014). What is the use of a single-case study in management research? *RAE: Revista De Administração De Empresas, 54*, 358-369. doi:10.1590/S0034-759020140402

Marken, R. S. (2002). Looking at behavior through control theory glasses. *Review of General Psychology, 6*, 260-270. doi:10.1037/1089-2680.6.3.260

Morgan, S., Pullon, S., Macdonald, L., McKinlay, E., & Gray, B., (2016). Case study observational research a framework for conducting case study research where observation data are the focus. *Qualitative Health Research* 27 (7) 1060 - 1068. doi:10.1177/1049732316649160

Muscanell, N., Guadagno, R., & Murphy, S. (2014). Weapons of influence misused: A social influence analysis of why people fall prey to internet scams. *Social and Personality Psychology Compass, 8*, 388-396. doi:10.1111/spc3.12115

Myers, M., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization, 17*(1) 2-26. doi:10.1016/j.infoandorg.2006.11.001

Natarajan, T., & Edwards, W. (2016). Institutions and values: A methodological inquiry. *Journal of Economic Issues (M.E. Sharpe Inc.), 50*, 575-583. doi:10.1080/00213624.2016.1179067

Nero, P. J., Wardman, B., Copes, H., & Warner, G. (2011, November). Phishing: Crime that pays. *In eCrime researchers summit (eCrime)*, 2011 1-10. IEEE. Retrieved from http://ecrimeresearch.org/events/eCrime2013

Olsson, M. R. (2016). Re-thinking our concept of users. *Australian Academic & Research Libraries*, *47*, 286. doi:10.1080/00048623.2016.1253426

O'Reilly, M., & Parker, N. (2013). Unsatisfactory saturation: A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research, 13* (2), 190-197 doi:10.1177/1468794112446106

Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. *Journal of counseling and Psyshology,52*(2),137. doi:10.1037/0022-0167.52.2.137

Ponelis, S., (2015). Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of information systems research in small and medium enterprises. *International Journal of Doctoral Studies, 10*. Retrieved from http://ijds.org/

Pantic, I. (2014). Online social networking and mental health. *Cyberpsychology, Behavior, and Social Networking, 17*, 652-657. doi:10.1089/cyber.2014.0070

Raine, L., Anderson, J., & Connolly, J. (2014, October.). Cyber-attacks likely to increase. *Pew Report.* Retrieved from http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law, 20*, 315-328. doi:10.1080/13218719.2012.672275

Rowley, J., (2012). Conducting research interviews. *Management Research Review, 35* (3/4). doi:10.1108/01409171211210154

Sangani, N. K., & Vijayakumar, B. (2012). Cyber security scenarios and control for small and medium enterprises. *Informatica Economica, 16*(2), 58-71. Retrieved from http://revistaie.ase.ro/

Schrock, D., Cole, J., & Shaffer, J., (2011), Getting IT right: How to plan, manage and deliver on technologies promise. *Industry Week*, 6-37. Retrieved from http://www.industryweek.com/

Shank, D. B. (2012). Perceived justice and reactions to coercive computers. *Sociological Forum, 27*, 372-391. doi:10.1111/j.1573-7861.2012.01322.x

Sharma, G., & Good, D. (2013). The work of middle managers: Sensemaking and sensegiving for creating positive social change. *Journal of Applied Behavioral Science, 49*(1), 95-122. doi:10.1177/0021886312471375

Simms, C. (2016). Is social engineering the easy way in? *Itnow*, *58*(2), 24-25. Retrieved from http://itnow.oxfordjournals.org/

Simons, J. J. (2016). Psychological frameworks for persuasive information and communications technologies. *IEEE Pervasive Computing, 15*(3), 68-76. doi:10.1109/MPRV.2016.52

Steffee, S. (2014). Security breaches widespread. *Internal Auditor, 71*(5), 13. Retrieved from https://na.theiia.org/Pages/IIAHome.aspx

Syta, E., Corrigan-Gibbs, H., Weng, S., Wolinsky, D., Ford, B., & Johnson, A. (2014). Security analysis of accountable anonymity in dissent. *ACM Transactions on Information & System Security (TISSEC), 17*(1), 1-35. doi:10.1145/2629621

Tallon, P. P., Ramirez, R. V., & Short, J. E. (2013). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems, 30*(3), 141-178. doi:10.2753/MIS0742-1222300306

Tarafdar, M., Gupta, A., & Turel, O. (2013). The dark side of information technology use. *Information Systems Journal*, *23*, 269-275. doi:10.1111/isj.12015

Thorndike, R. (1985). Reliability. *Journal of Counseling & Development, 63*, 527-530. doi:10.1002/j.1556-6676. 1985.tb 02754.x

Tóth, A., & Kovács, T. (2017). Qualification system of the private security sector. Acta technica corvininesis - *Bulletin of Engineering, 10*(4), 131-135. Retrieved from http://acta.fih.upt.ro/bibliographic-info.html

Tuckett, A. (2005). Part II. Rigour in qualitative research: complexities and solutions *Nurse Researcher, 13*(1) 29-42. Retrieved from http://journals.rcni.com/loi/nr

United States International Trade Commission. (2010). *Small and medium-sized enterprises: U.S and EU export activities, and barriers and opportunities* *experienced by U.S. firms.* Retrieved from https://www.usitc.gov/publications/332/pub4169.pdf

Vander Bauwhede, H., De Meyere, M., & Van Cauwenberge, P. (2015). Financial reporting quality and the cost of debt of SMEs. *Small Business Economics, 45*(1), 149-164. doi:10.1007/s11187-015-9645-1

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cybersecurity behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior & Social Networking*, *18*(1), 3-7. doi:10.1089/cyber.2014.0179

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking, 17*(3), 131-132. doi:10.1089/cyber.2014.1502

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20. Retrieved from http://www.misq.org/

Yin, R. K. (2013). Validity and generalization in future case study evaluations *Evaluation, 19*, 321-332. Retrieved from http://www.eval.org/

Yin, R. K. (2014). *Case study research: Design and methods*. Thousand Oaks, CA: Sage Publications.

Yu, A. (2014). Let's get physical: Loss of use of tangible property as coverage in cyber insurance. *Rutgers Computer & Technology Law Journal, 40*, 229-255. Retrieved from http://www.rctlj.org/

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

Appendix A: Observation Protocol Example

Schedule	**Monday-Saturday for two weeks**
Date:	**TBD**
Background; **Physical layout of the location**	**The Background will describe the physical environment where the observations are taking place. Since this is a single case study design, there will be only one detailed entry for this section. A detailed illustration of the physical layout of the setting will be included.**
People: **Customers and Proprietors**	**A detailed description of each observed person will be provided.**
The Action: **What is occurring**	**The activities of the customers and proprietors will be included in detail to provide insight to the study research question.**

Time:	**Observation:**

Appendix B: Interview Protocol Example

The interview will be an informal open-ended question style,

RQ- What is the level of consensus among small business owners as to the key elements of decision making for SME investment into cybersecurity and education for employees with respect to internet access and employee vulnerabilities?

To begin the interview;

1. I will introduce myself and provide the participant with a short informal background on the University, my study and how his contribution to the study as a participant will provide data that will contribute to positive social change by potentially reducing cyber-security attacks on small businesses.
2. I will request permission to record the interview and explain that the recording is necessary to produce a transcript for later verification of the accuracy of the collected data and the transcript synopsis.
3. Next, I will begin the interview questions.
    a. During the interview questioning, I will be watching and recording non-verbal cues such as gesturing or hesitation.
    b. I will keep the questions at a non-technical level.
    c. I will ask follow-up probing questions to get more details and in-depth answers.

4. The interview questions;

1. How long has your business been in operation?

2. Who are your businesses main clientele**?**

3. What measures do feel that small businesses might use to protect from outside computer attacks to protect the business information?

4.What might be your concerns about protecting small and medium business information from cybercrime?

5. Why do you feel that large corporation computer systems are a target of cybercrime more often than small and medium businesses?

6. What forms of cybercriminal small and medium business computer systems intrusions are you aware of if any?

7. In terms of protection of customer personal information, why might credit card corporation security measures not be enough to protect small and medium business customers from computer system breaches?

8. What oversight might be involved in employee access to the small and medium businesses information to insure information integrity?

9. Why do you feel large corporations might be more susceptible to computer systems breaches than small and medium sized businesses?

10. Why do you think it might be necessary for small and medium business employees to log out of computer systems when not in use?

11**.** How do you feel about user passwords and login IDs being adequate protection for small and medium business computer systems access?

12. How do you feel about small and medium business computer systems relative to adequate protection from computer systems intrusions?

13. What type of anti-virus software and firewall protection does your computer system currently use?

14. How is your computer security software updated?

1. After the last question, the participant will be asked if they would like to add any additional information.
2. The interviewee will be thanked for their participation and a follow-up member checking interview will be requested and scheduled at this time.

Appendix C: Member Checking Protocol

1. After Interviewing participant taking notes and recording interview (See Appendix B)

2. Transcription from recording for the member checking meeting.

3. Critically analyze transcript and interview notes.

4. Synthesize my interpretation for participant answer by question

5. Introduce follow-up interview and set the stage;

a. Thank the participant for his continued support to the study. Remind the participant of the importance of the study and his contribution to positive social change.

6. Next, I will begin a review of the transcript synthesis.

7. Member check my interpretation by sharing a paper version of the question and my synthesis.

8. Note and record any additional in-depth data from the participant.

9. For transcript review;

a. Share a copy of the succinct synthesis for each individual question

b. Inform the participant of the reason and importance of the transcript synthesis review (to verify the accuracy of the synthesis with the participant to ensure that it is true to what he meant.

c. Bring in probing questions related to other information that you may have found—note the information must be related so that you are probing and adhering to the IRB approval. Walk through each question, read the interpretation and ask: Did I miss anything? Or, what would you like to add?

10. For member checking of the collected data;

a. To verify that the participant agrees with the collected data results.

11. For a third interview (if required) repeat 2 through 6 if needed for more in-depth data collection

12. Interview question synthesis for member checking with the participant;

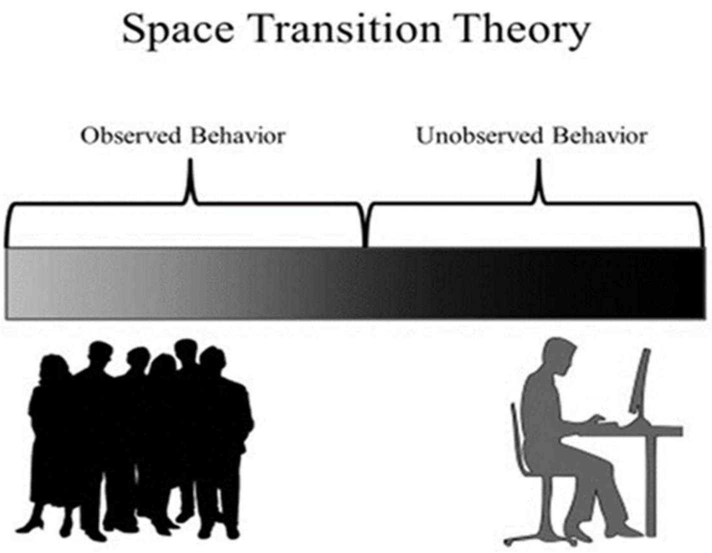
Question and succinct synthesis of the interpretation—

1. How long have you been in business? No changes to transcript or synthesis.
2. Who are your businesses main clientele, who are your main customers**?** No changes to transcript or synthesis
3. What measures do feel that small businesses might use to protect from outside? No Changes to transcript or synthesis.
4. What might be your concerns about protecting small and medium business information from cybercrime? No changes from synthesized transcript review.
5. Why do you feel that large corporation computer systems are a target of cybercrime more often than small and medium businesses? No changes from synthesized transcript review
6. What forms of cybercriminal small and medium business computer systems intrusions are you aware of if any? No changes from synthesized transcript review
7. In terms of protection of customer personal information, why might credit card corporation security measures not be enough to protect small and medium business customers from computer system attacks?

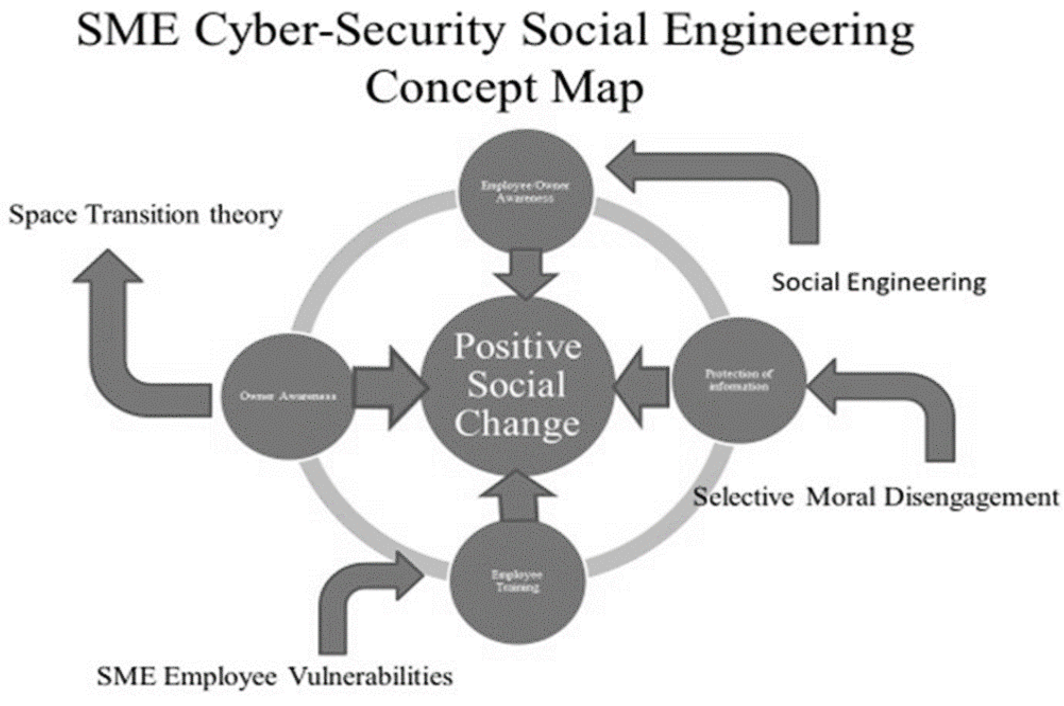
	No changes from synthesized transcript review.
8.	What oversight might be involved in employee access to the small and medium businesses information to insure information integrity? No changes from synthesized transcript review.
9.	Why do you feel large corporations might be more susceptible to computer systems breaches than small and medium sized businesses? I know it’s the same question? No changes from synthesized transcript review.
10.	Why do you think it might be necessary for small and medium business employees to log out of computer systems, uh when not in use? No changes from synthesized transcript review.
11.	How do you feel about user passwords and login IDs being adequate protection for small and medium enterprise businesses systems and access? No changes from synthesized transcript review.
12	How do you feel about small and medium business computer systems relative to adequate protection from computer systems intrusions? No changes from synthesized transcript review.
13	What type of anti-virus software and firewall protection does your computer system currently use? No changes from synthesized transcript review.
14	How often is your computer security software updated? No changes from synthesized transcript review.
Interview follow-up questions;	
1	What is the difference between social engineering and hacking? “Now that I do not know.”

2 What do you think is the main way internet criminals access systems illegally? “Through the internet connection.” 3 Who do you call if you suspect your system has been compromised? “My IT support guy.”
4 Does he do all the IT support services like trouble shooting? “Yes, we just e-mail him”
5 Does he respond right away? “Yes, that same day, usually within an hour or so.”
6 Who provides the tech support? “The security software provider, it all comes under one package.” This was clarified to mean 3 tech support personnel. One for service provider, one for physical security and one for internet/software security.

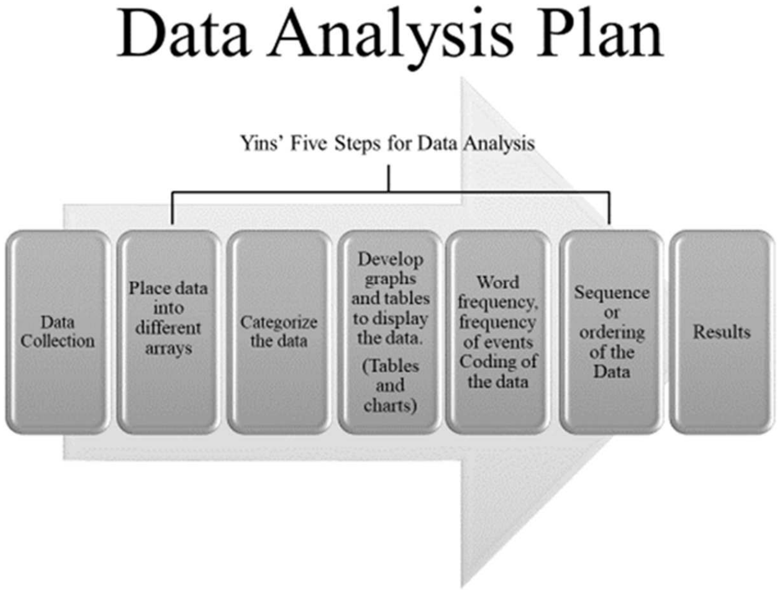
Appendix D: Space Transition Theory



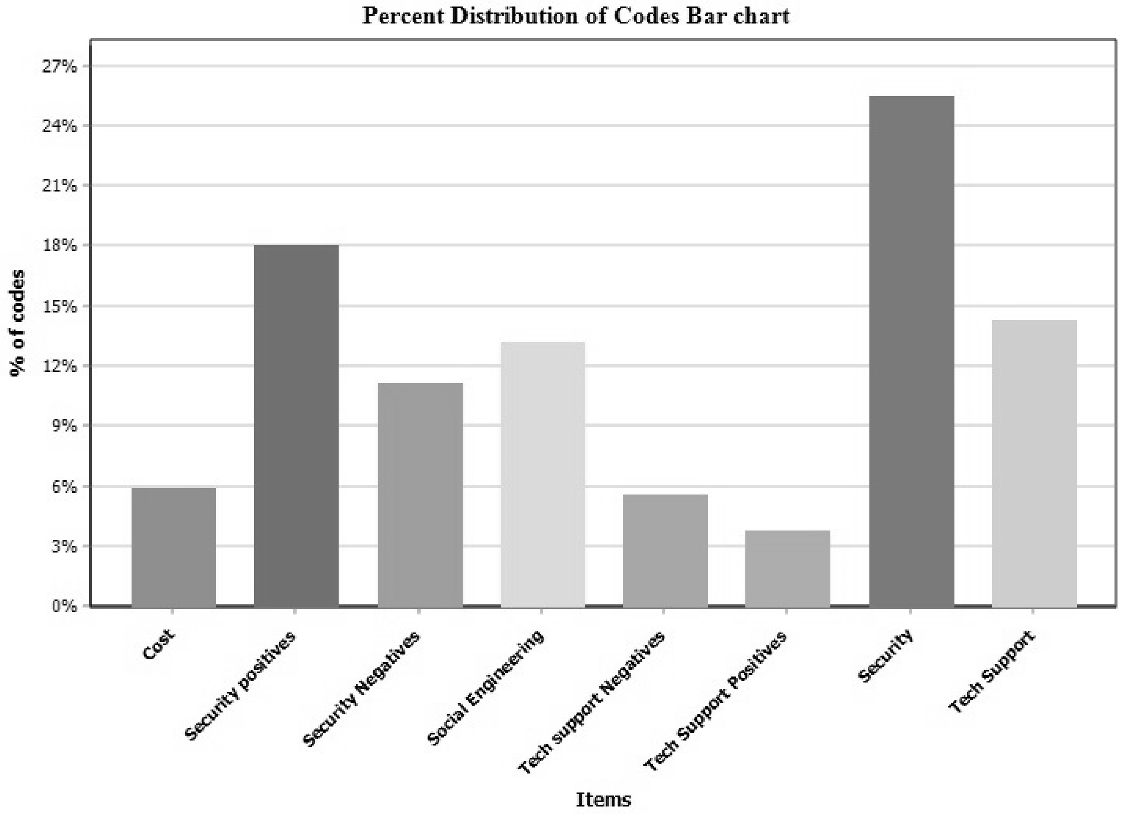
Appendix E: SME Cyber Security Concept Map


SME Cyber-Security Social Engineering Concept Map
Space Transition theory
Employee/Owner Awareness
Social Engineering
Owner Awareness
Positive Social Change
Protection of information
Selective Moral Disengagement
Employee Training
SME Employee Vulnerabilities

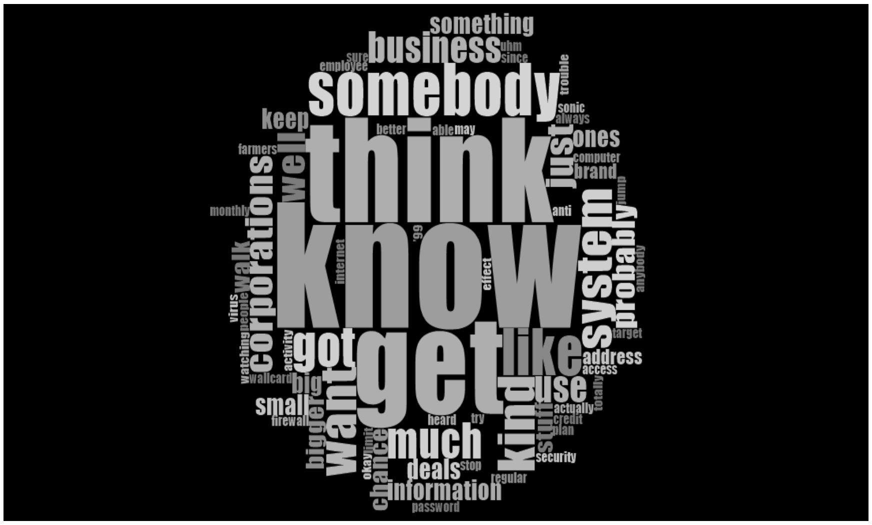
Appendix F: Data Analysis Plan


Data Analysis Plan
Yins' Five Steps for Data Analysis
Data Collection
Place data into different arrays
Categorize the data
Develop graphs and tables to display the data. (Tables and charts)
Word frequency, frequency of events Coding of the data
Sequence or ordering of the Data
Results

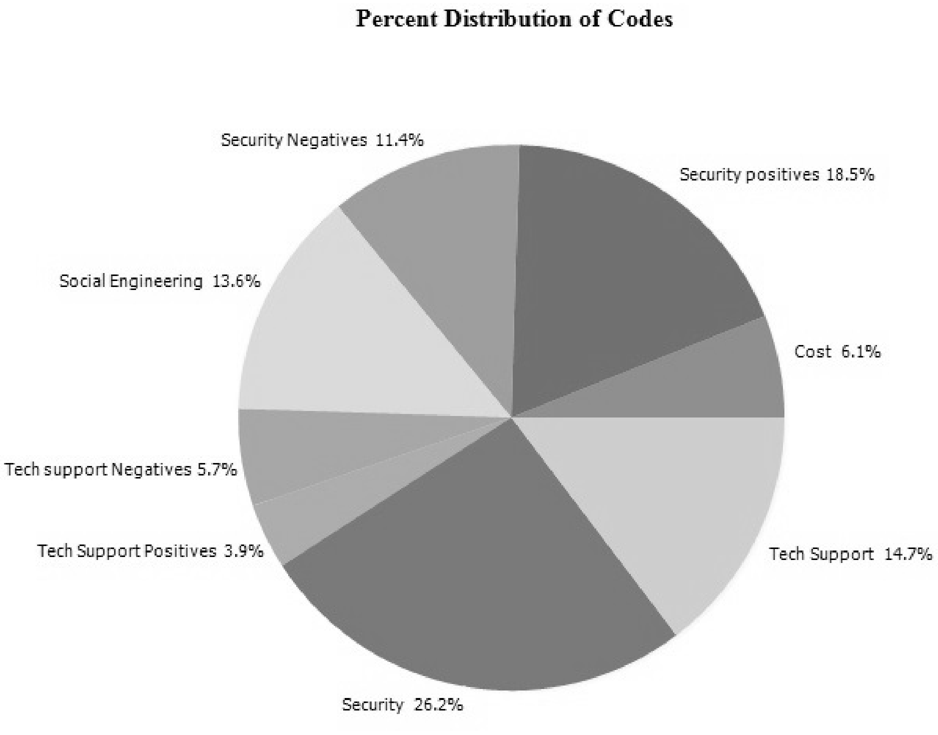
Appendix G: Emergent Themes from Coding



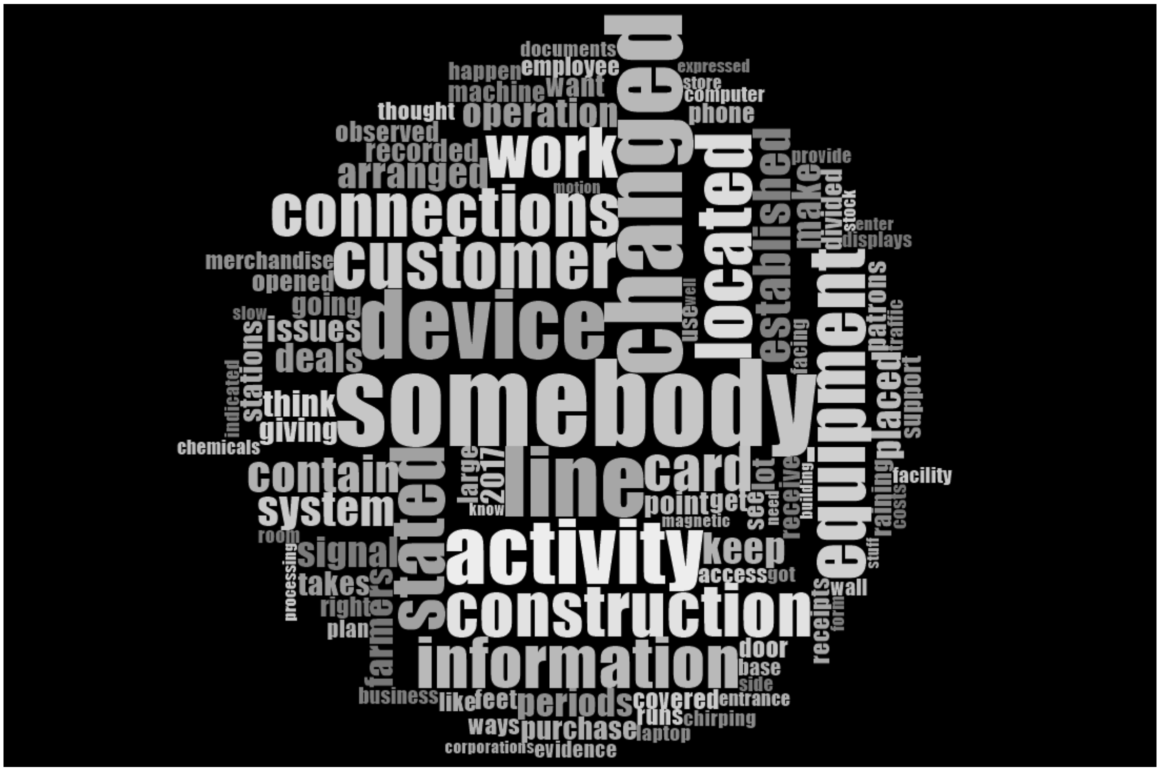
Appendix H: Observation Logs Word Cloud



Appendix I: Interview Word Frequency Coded Results

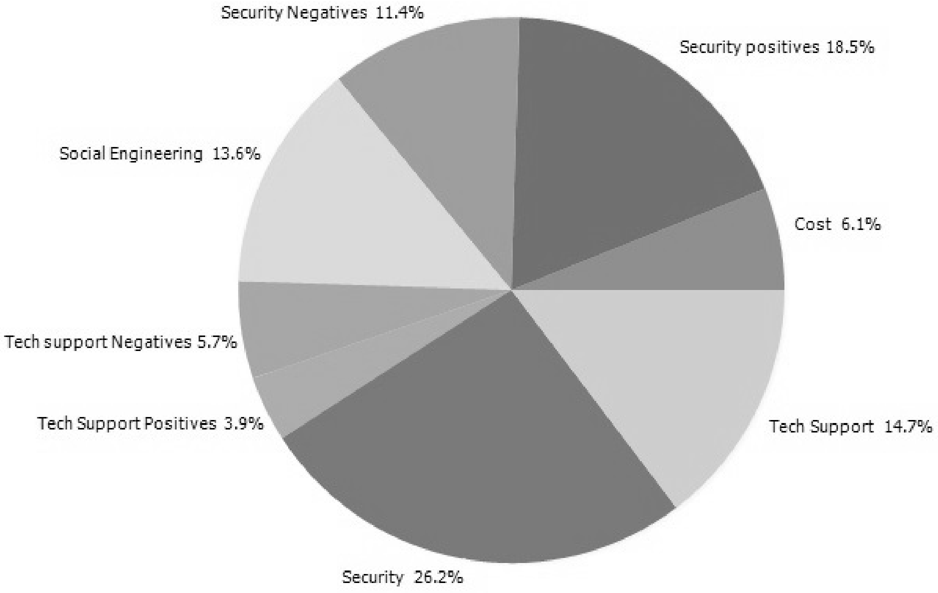


Appendix J: Word Cloud Results (Interviews and Observation logs)

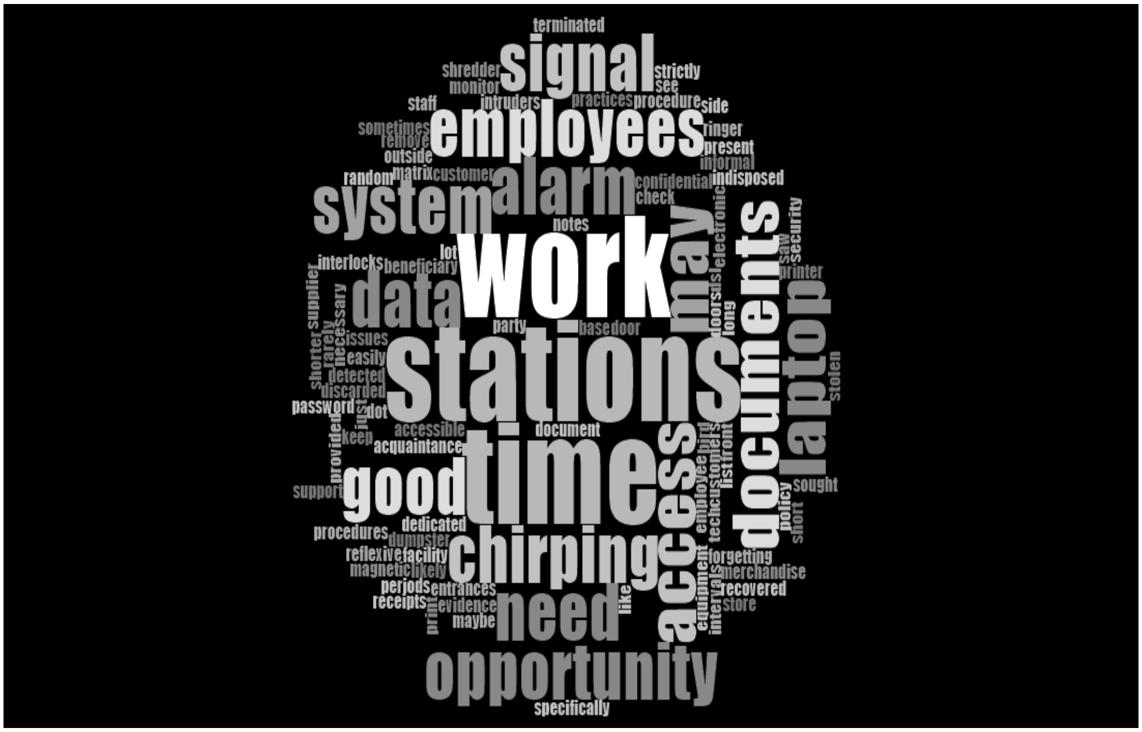


Appendix K: Distribution of Codes Pie Chart

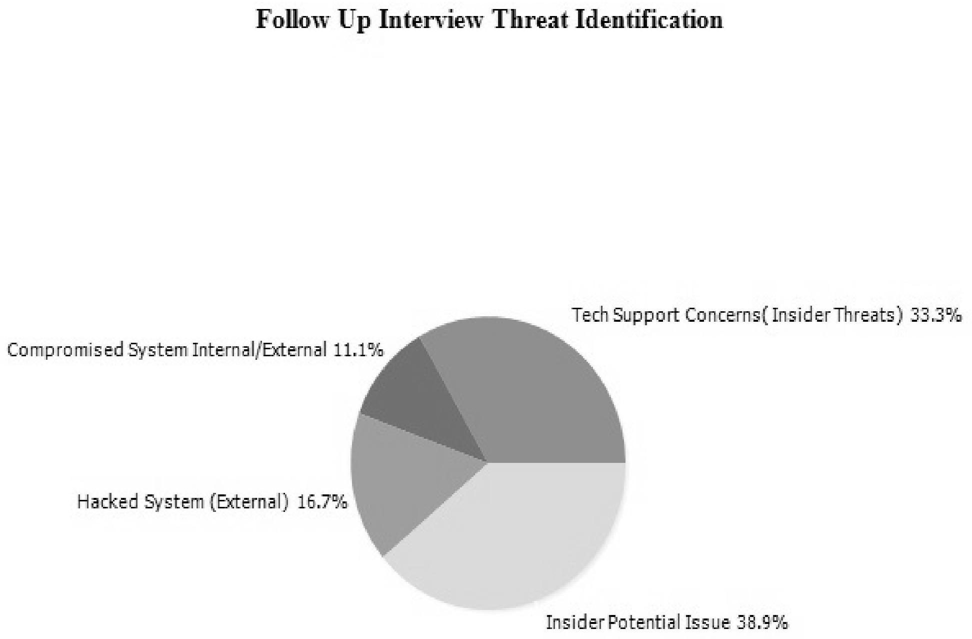
Distribution of Codes from Emergent Themes



Appendix L: Word Cloud from Reflexive Notes



Appendix M: Member Checking Follow-Up Interview Threat Identification



Appendix N: Coded Data

Code	Method(s)	Text	Date	Words	%Words
Security positives	Observation Logs Only	Smart phone Wi-fi scan produced no results	2/26/2018	8	0.6%
Tech Support Negatives	Observation Logs Only	Smart phone Wi-fi scan produced no results (no wi-fi signals within range	3/1/2018	14	1.0%
Cost	Observation Logs Only	Wi-fi scan produced no results	2/26/2018	6	0.4%
Social Engineering	Observation Logs Only	The CPUs placed under the counter with the connections facing outward (customer facing)	2/26/2018	15	1.1%
Security Negatives	Observation Logs Only	he CPUs placed under the counter with the connections facing outward (customer facing	2/26/2018	15	1.1%
Security positives	Observation Logs Only	Cpu connections prevented by product displays.	2/26/2018	7	0.5%
Security Negatives	Observation Logs Only	At &T cordless phone service for the business	2/26/2018	8	0.6%
Social Engineering	Observation Logs Only	At &T cordless phone service for the business	2/26/2018	8	0.6%
Tech Support Negatives	Observation Logs Only	At &T cordless phone service for the business. The printer runs off of the same AT&t ethernet line. Phone operation prevents printer operation. Internet ethernet internet service by separate line such that there is no interference during transaction processing. Printer is a hole fed dot matrix printer for printing hardcopy receipts	3/1/2018	52	3.8%
Cost	Observation Logs Only	The printer runs off of the same AT&t ethernet line	2/26/2018	11	0.8%
Cost	Observation Logs Only	Phone operation prevents printer operation	2/26/2018	5	0.4%
Security Negatives	Observation Logs Only	Phone operation prevents printer operation.	2/26/2018	5	0.4%
Security positives	Observation Logs Only	Internet ethernet internet service by separate line	2/26/2018	7	0.5%
Cost	Observation Logs Only	. Printer is a hole fed dot matrix printer for printing hardcopy receipts	2/26/2018	12	0.9%
Security positives	Observation Logs Only	Magnetic security devices on three bay doors as well as the front entry doors	2/26/2018	14	1.0%
Security positives	Observation Logs Only	There is an audible chirping thru out the facility when the front door opened to alert staff of an entry	2/26/2018	21	1.5%
Security positives	Observation Logs Only	Observed a wide-angle security camera attached to the drop ceiling on the back-left corner from the entrance of the building	2/26/2018	22	1.6%
Security positives	Observation Logs Only	The camera covers the entire store including the counter work stations	2/26/2018	11	0.8%
Security Negatives	Observation Logs Only	Activity on the work stations not observed,	2/26/2018	8	0.6%
Tech Support Negatives	Observation Logs Only	Activity on the work stations not observed	3/1/2018	8	0.6%
Social Engineering	Observation Logs Only	activity on the work stations not observed	2/26/2018	8	0.6%
Tech Support Positives	Observation Logs Only	a person using the system can be and a date and time established as to when a person is at the workstation	3/1/2018	24	1.8%
Security positives	Observation Logs Only	a person using the system can be and a date and time established as to when a person is at the workstation	2/26/2018	24	1.8%
Social Engineering	Observation Logs Only	Heavy customer traffic	2/26/2018	3	0.2%
Security Negatives	Observation Logs Only	Discussed power supply. Cable and phone. AT&T provides the DSL service and phone	2/26/2018	14	1.0%

Cost	Observation Logs Only	. AT&T provides the DSL service and phone	2/26/2018	8	0.6%
Tech Support Negatives	Observation Logs Only	AT&T provides the DSL service and phone	3/1/2018	8	0.6%
Security positives	Observation Logs Only	Alarm system connected to a motion and magnetic interlock system that activates an alarm.	2/26/2018	15	1.1%
Tech Support Positives	Observation Logs Only	Alarm system connected to a motion and magnetic interlock system that activates an alarm. All service connections are inside the building.	3/1/2018	22	1.6%
Security positives	Observation Logs Only	All service connections are inside the building	2/26/2018	7	0.5%
Social Engineering	Observation Logs Only	All service connections are inside the building	2/26/2018	7	0.5%
Security Negatives	Observation Logs Only	they have had three break-ins in the 19 years that have been in business.	2/26/2018	15	1.1%
Social Engineering	Observation Logs Only	they have had three break-ins in the 19 years that have been in business	2/26/2018	15	1.1%
Security Negatives	Observation Logs Only	One instance a lap-top with employee personal information taken	2/26/2018	11	0.8%
Social Engineering	Observation Logs Only	One instance a lap-top with employee personal information taken	2/26/2018	11	0.8%
Security positives	Observation Logs Only	Procedure changed to not leave lap-top overnight	2/26/2018	8	0.6%
Security Negatives	Observation Logs Only	expressed that tech support is a third-party IT rep from the supplier	2/26/2018	13	1.0%
Social Engineering	Observation Logs Only	expressed that tech support is a third-party IT rep from the supplier.	2/26/2018	13	1.0%
Tech Support Negatives	Observation Logs Only	expressed that tech support is a third-party IT rep from the supplier. For on-line issues. The rep is located off site and offers help desk type support but will come in as required	3/1/2018	35	2.6%
Security positives	Observation Logs Only	tech support is a third-party IT rep	2/26/2018	8	0.6%
Security Negatives	Observation Logs Only	The rep is located off site and offers help desk type support	2/26/2018	12	0.9%
Social Engineering	Observation Logs Only	The rep is located off site and offers help desk type support but will come in as required	2/26/2018	18	1.3%
Social Engineering	Observation Logs Only	There are customer store credits	2/26/2018	5	0.4%
Security Negatives	Observation Logs Only	customer store credits but only the purchase receipts stored for records	2/26/2018	12	0.9%
Security positives	Observation Logs Only	No billing, customer or payment information kept in-house	2/26/2018	10	0.7%
Social Engineering	Observation Logs Only	receipts discarded in waste receptacle upon payment.	2/26/2018	8	0.6%
Security Negatives	Observation Logs Only	discarded in waste receptacle upon payment	2/26/2018	6	0.4%
Security Negatives	Observation Logs Only	work stations unattended	2/26/2018	3	0.2%
Social Engineering	Observation Logs Only	work stations unattended	2/26/2018	3	0.2%
Social Engineering	Observation Logs Only	The participant is on a first name basis with all of the patrons with the exception of a scant few.	2/26/2018	20	1.5%
Security positives	Observation Logs Only	participant is on a first name basis with all of the patrons with the exception of a scant few	2/26/2018	19	1.4%
Security positives	Observation Logs Only	monitored by security video camera at the rear of the store	2/26/2018	13	1.0%
Security positives	Observation Logs Only	Activity at the work station recorded	2/26/2018	8	0.6%
Security Negatives	Observation Logs Only	but no details of work station would be available	2/26/2018	9	0.7%

Social Engineering	Observation Logs Only	no details of work station would be available with the exception of the person at the station	2/26/2018	17	1.3%
Security positives	Observation Logs Only	the person at the station and the time of the activity which would be enough to provide any information for an inquiry.	2/26/2018	22	1.6%
Security positives	Observation Logs Only	security video recording device is located out of sight and disguised covered by an empty cardboard container	2/26/2018	20	1.5%
Security Negatives	Observation Logs Only	Store walls lined with product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door). Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches	2/26/2018	80	5.9%
Social Engineering	Observation Logs Only	Store walls lined with product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door). Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches	2/26/2018	80	5.9%
Social Engineering	Observation Logs Only	The main floor of the store divided three shelves about six feet high and double sided with the circular displays arranged around the perimeter.	2/26/2018	25	1.8%
Social Engineering	Observation Logs Only	customer traffic and phone calls are heaviest early in the morning	2/26/2018	11	0.8%
Security positives	Observation Logs Only	Door alert goes off when customers enter and leave (chirping & tweeting sounds)	2/26/2018	12	0.9%
Cost	Observation Logs Only	I noticed that the cannot print when talking on the phone (DSL)	2/26/2018	13	1.0%
Security Negatives	Observation Logs Only	I noticed that the cannot print when talking on the phone (DSL).	2/26/2018	13	1.0%
Social Engineering	Observation Logs Only	I noticed that the cannot print when talking on the phone (DSL). No wi-fi.	2/26/2018	16	1.2%
Tech Support Negatives	Observation Logs Only	noticed that the cannot print when talking on the phone (DSL). No wi-fi. Dot matrix printer.	3/1/2018	18	1.3%
Cost	Observation Logs Only	No wi-fi	2/26/2018	3	0.2%
Security positives	Observation Logs Only	No wi-fi.	2/26/2018	3	0.2%
Cost	Observation Logs Only	Dot matrix printer	2/26/2018	3	0.2%
Social Engineering	Observation Logs Only	Small talk with farmers swapping stories and gossip about each other	2/26/2018	11	0.8%
Security positives	Observation Logs Only	Cameras and motion detector well placed	2/26/2018	6	0.4%
Security positives	Observation Logs Only	phone and electrical egress to the building is under ground with no exterior access	2/26/2018	14	1.0%
Cost	Observation Logs Only	phone and electrical egress to the building is under ground with no exterior access	2/26/2018	14	1.0%
Security Negatives	Observation Logs Only	store inventory accessed on-line	2/26/2018	7	0.5%
Cost	Observation Logs Only	No scanning system point and click system for receipt print out	2/26/2018	11	0.8%

Security positives	Observation Logs Only	No scanning system point and click system for receipt print out.	2/26/2018	11	0.8%
Security Negatives	Observation Logs Only	No scanning system point and click system for receipt print out.	2/26/2018	11	0.8%
Tech Support Negatives	Observation Logs Only	No scanning system point and click system for receipt print out	3/1/2018	11	0.8%
Tech Support Negatives	Observation Logs Only	The absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall.	3/1/2018	23	1.7%
Cost	Observation Logs Only	The absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall	2/26/2018	23	1.7%
Security positives	Observation Logs Only	he absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall.	2/26/2018	23	1.7%
Social Engineering	Observation Logs Only	So, access to the system requires a password and user name	2/26/2018	11	0.8%
Tech Support Positives	Observation Logs Only	o access to the system requires a password and user name. The has indicated that he is aware of the necessity of a strong password.	3/1/2018	25	1.8%
Security positives	Observation Logs Only	access to the system requires a password and user name	2/26/2018	10	0.7%
Security positives	Observation Logs Only	he is aware of the necessity of a strong password.	2/26/2018	10	0.7%
Social Engineering	Observation Logs Only	the potential still exists for retaliation from disgruntled customers over money or merchandise dissatisfaction. Some merchandise can be very expensive. For a fuel dispenser costs almost $500.00.	2/26/2018	28	2.1%
Security Negatives	Observation Logs Only	retaliation from disgruntled customers over money or merchandise dissatisfaction	2/26/2018	9	0.7%
Security positives	Observation Logs Only	The building is metal construction on a concrete slab	2/26/2018	9	0.7%
Security positives	Observation Logs Only	Adequate fluorescent lighting	2/26/2018	3	0.2%
Security positives	Observation Logs Only	standard emergency lighting and exit signs that activated by an emergency generator.	2/26/2018	14	1.0%
Social Engineering	Observation Logs Only	9:00-10:00- Work stations (three) are Dell computers with a firewall with anti-virus protection that updated monthly and maintained by third party tech support. relies mostly on the third party (out-sourced) tech support for computer security and protection	2/26/2018	43	3.2%
Cost	Observation Logs Only	Work stations (three) are Dell computers	2/26/2018	6	0.4%
Tech Support Positives	Observation Logs Only	Work stations (three) are Dell computers with a firewall with anti-virus protection that updated monthly and maintained by third party tech support. relies mostly on the third party (out-sourced) tech support for computer security and protection	3/1/2018	39	2.9%
Security positives	Observation Logs Only	a firewall with anti-virus protection that is updates monthly and maintained by third party tech support.	2/26/2018	17	1.3%
Security Negatives	Observation Logs Only	third party tech support. relies mostly on the third party (out-sourced) tech support for computer security and protection.	2/26/2018	19	1.4%
Tech Support Negatives	Observation Logs Only	relies mostly on the third party (out-sourced) tech support for computer security and protection.	3/1/2018	15	1.1%
Security positives	Observation Logs Only	The building surrounded on three sides by a soy bean field	2/26/2018	12	0.9%

Security positives	Observation Logs Only	but the business internet and phone activity is through the DSL carrier only	2/26/2018	13	1.0%
Social Engineering	Observation Logs Only	but the business internet and phone activity is through the DSL carrier only.	2/26/2018	13	1.0%
Security	Observation Logs Only	Lot of activity from uniform service. Changing out uniforms and replacing carpets.	3/3/2018	12	0.9%
Security positives	Observation Logs Only	Smart phone Wi-fi scan produced no results	2/26/2018	8	0.6%
Tech Support Negatives	Observation Logs Only	Smart phone Wi-fi scan produced no results (no wi-fi signals within range	3/1/2018	14	1.0%
Security	Observation Logs Only	Smart phone Wi-fi scan produced no results	3/3/2018	8	0.6%
Tech Support	Observation Logs Only	Smart phone Wi-fi scan produced no results	3/3/2018	8	0.6%
Cost	Observation Logs Only	Wi-fi scan produced no results	2/26/2018	6	0.4%
Security	Observation Logs Only	(no wi-fi signals within range)	3/3/2018	6	0.4%
Security	Observation Logs Only	Observed two work station CRTS with keyboards on customer service counter	3/3/2018	11	0.8%
Tech Support	Observation Logs Only	Observed two work station CRTS with keyboards on customer service counter	3/3/2018	11	0.8%
Social Engineering	Observation Logs Only	The CPUs placed under the counter with the connections facing outward (customer facing)	2/26/2018	15	1.1%
Security	Observation Logs Only	The CPUs placed under the counter with the connections facing outward (customer facing	3/3/2018	15	1.1%
Tech Support	Observation Logs Only	The CPUs placed under the counter with the connections facing outward (customer facing	3/3/2018	15	1.1%
Security Negatives	Observation Logs Only	The CPUs placed under the counter with the connections facing outward (customer facing	2/26/2018	15	1.1%
Tech Support Negatives	Observation Logs Only	he CPUs placed under the counter with the connections facing outward (customer facing)	3/1/2018	15	1.1%
Security	Observation Logs Only	Full access to cpu connections prevented by product displays.	3/3/2018	10	0.7%
Tech Support	Observation Logs Only	Full access to cpu connections prevented by product displays.	3/3/2018	10	0.7%
Security positives	Observation Logs Only	cpu connections prevented by product displays.	2/26/2018	7	0.5%
Tech Support	Observation Logs Only	2 At &T cordless phone service for the business	3/3/2018	9	0.7%
Security Negatives	Observation Logs Only	At &T cordless phone service for the business	2/26/2018	8	0.6%
Social Engineering	Observation Logs Only	At &T cordless phone service for the business	2/26/2018	8	0.6%
Tech Support Negatives	Observation Logs Only	At &T cordless phone service for the business. The printer runs off of the same AT&t ethernet line. Phone operation prevents printer operation. Internet ethernet internet service by separate line such that there is no interference during transaction processing. Printer is a hole fed dot matrix printer for printing hardcopy receipts	3/1/2018	52	3.8%
Security	Observation Logs Only	At &T cordless phone service for the business	3/3/2018	8	0.6%
Cost	Observation Logs Only	The printer runs off of the same AT&t ethernet line	2/26/2018	11	0.8%
Tech Support	Observation Logs Only	The printer runs off of the same AT&t ethernet line	3/3/2018	11	0.8%
Security	Observation Logs Only	e printer runs off of the same AT&t ethernet line	3/3/2018	11	0.8%
Cost	Observation Logs Only	Phone operation prevents printer operation	2/26/2018	5	0.4%
Security Negatives	Observation Logs Only	Phone operation prevents printer operation.	2/26/2018	5	0.4%
Security	Observation Logs Only	Phone operation prevents printer operation	3/3/2018	5	0.4%
Tech Support	Observation Logs Only	Phone operation prevents printer operation	3/3/2018	5	0.4%

Tech Support	Observation Logs Only	Internet ethernet internet service by separate line such that there is no interference during transaction processing	3/3/2018	16	1.2%
Security positives	Observation Logs Only	Internet ethernet internet service by separate line	2/26/2018	7	0.5%
Security	Observation Logs Only	Internet ethernet internet service by separate line such that there is no interference during transaction processing	3/3/2018	16	1.2%
Cost	Observation Logs Only	. Printer is a hole fed dot matrix printer for printing hardcopy receipts	2/26/2018	12	0.9%
Security	Observation Logs Only	Printer is a hole fed dot matrix printer for printing hardcopy receipts.	3/3/2018	12	0.9%
Tech Support	Observation Logs Only	Printer is a hole fed dot matrix printer for printing hardcopy receipts.	3/3/2018	12	0.9%
Security	Observation Logs Only	I also learned that some farmers are very superstitious and will not perform some farm activities if the signs are not right. (Full moon etc.)	3/3/2018	25	1.8%
Security	Observation Logs Only	. Magnetic security devices on three bay doors as well as the front entry doors	3/3/2018	14	1.0%
Security positives	Observation Logs Only	Magnetic security devices on three bay doors as well as the front entry doors	2/26/2018	14	1.0%
Tech Support	Observation Logs Only	Magnetic security devices on three bay doors as well as the front entry doors.	3/3/2018	14	1.0%
Security positives	Observation Logs Only	There is an audible chirping thru out the facility when the front door opened to alert staff of an entry	2/26/2018	21	1.5%
Security	Observation Logs Only	There is an audible chirping thru out the facility when the front door opened to alert staff of an entry	3/3/2018	21	1.5%
Tech Support	Observation Logs Only	There is an audible chirping thru out the facility when the front door opened to alert staff of an entry.	3/3/2018	21	1.5%
Security positives	Observation Logs Only	Observed a wide-angle security camera attached to the drop ceiling on the back-left corner from the entrance of the building	2/26/2018	22	1.6%
Security	Observation Logs Only	Observed a wide-angle security camera attached to the drop ceiling on the back-left corner from the entrance of the building.	3/3/2018	22	1.6%
Tech Support	Observation Logs Only	Observed a wide-angle security camera attached to the drop ceiling on the back-left corner from the entrance of the building.	3/3/2018	22	1.6%
Tech Support	Observation Logs Only	The camera covers the entire store including the counter work stations. Activity on the work stations are not observable	3/3/2018	19	1.4%
Security positives	Observation Logs Only	The camera covers the entire store including the counter work stations	2/26/2018	11	0.8%
Security	Observation Logs Only	The camera covers the entire store including the counter work stations. Activity on the work stations are not observable, but a person using the system can be and a date and time established as to when a person is at the workstation.	3/3/2018	44	3.2%
Security Negatives	Observation Logs Only	Activity on the work stations not observable.	2/26/2018	8	0.6%
Tech Support Negatives	Observation Logs Only	Activity on the work stations not observable.	3/1/2018	8	0.6%
Social Engineering	Observation Logs Only	Activity on the work stations not observable	2/26/2018	8	0.6%

Tech Support	Observation Logs Only	but a person using the system can be and a date and time established as to when a person is at the workstation	3/3/2018	25	1.8%
Tech Support Positives	Observation Logs Only	a person using the system can be and a date and time established as to when a person is at the workstation	3/1/2018	24	1.8%
Security positives	Observation Logs Only	a person using the system can be and a date and time established as to when a person is at the workstation	2/26/2018	24	1.8%
Social Engineering	Observation Logs Only	Heavy customer traffic	2/26/2018	3	0.2%
Security Negatives	Observation Logs Only	Discussed power supply. Cable and phone. AT&T provides the DSL service and phone	2/26/2018	14	1.0%
Tech Support	Observation Logs Only	Discussed power supply	3/3/2018	3	0.2%
Security	Observation Logs Only	power supply	3/3/2018	2	0.1%
Security	Observation Logs Only	Cable and phone	3/3/2018	3	0.2%
Tech Support	Observation Logs Only	Cable and phone	3/3/2018	3	0.2%
Cost	Observation Logs Only	. AT&T provides the DSL service and phone	2/26/2018	8	0.6%
Tech Support Negatives	Observation Logs Only	AT&T provides the DSL service and phone	3/1/2018	8	0.6%
Security	Observation Logs Only	AT&T provides the DSL service and phone. Line service	3/3/2018	10	0.7%
Tech Support	Observation Logs Only	AT&T provides the DSL service and phone	3/3/2018	8	0.6%
Tech Support	Observation Logs Only	Line service.	3/3/2018	2	0.1%
Security positives	Observation Logs Only	Alarm system connected to a motion and magnetic interlock system that activates an alarm.	2/26/2018	15	1.1%
Tech Support Positives	Observation Logs Only	Alarm system connected to a motion and magnetic interlock system that activates an alarm. All service connections are inside the building.	3/1/2018	22	1.6%
Security	Observation Logs Only	Alarm system connected to a motion and magnetic interlock system that activates an alarm. All service connections are inside the building	3/3/2018	22	1.6%
Tech Support	Observation Logs Only	alarm system connected to a motion and magnetic interlock system that activates an alarm	3/3/2018	15	1.1%
Security positives	Observation Logs Only	All service connections are inside the building	2/26/2018	7	0.5%
Social Engineering	Observation Logs Only	All service connections are inside the building	2/26/2018	7	0.5%
Tech Support	Observation Logs Only	All service connections are inside the building	3/3/2018	7	0.5%
Security Negatives	Observation Logs Only	they have had three break-ins in the 19 years that have been in business.	2/26/2018	15	1.1%
Social Engineering	Observation Logs Only	they have had three break-ins in the 19 years that have been in business	2/26/2018	15	1.1%
Security	Observation Logs Only	they have had three break-ins in the 19 years that have been in business	3/3/2018	15	1.1%
Security Negatives	Observation Logs Only	One instance a lap-top with employee personal information taken	2/26/2018	11	0.8%
Social Engineering	Observation Logs Only	One instance a lap-top with employee personal information taken	2/26/2018	11	0.8%
Security	Observation Logs Only	One instance a lap-top with employee personal information taken	3/3/2018	11	0.8%
Security positives	Observation Logs Only	Procedure changed to not leave lap-top overnight	2/26/2018	8	0.6%
Security	Observation Logs Only	Procedure changed to not leave lap-top overnight. The laptop recovered.	3/3/2018	12	0.9%
Security	Observation Logs Only	expected that the laptop was stolen for use and not data because of the nature of the recovery	3/3/2018	19	1.4%

Security Negatives	Observation Logs Only	expressed that tech support is a third-party IT rep from the supplier	2/26/2018	13	0.9%
Social Engineering	Interview	expressed that tech support is a third-party IT rep from the supplier.	2/26/2018	13	0.9%
Tech Support Negatives	Interview	expressed that tech support is a third-party IT rep from the supplier. For on-line issues. The rep is located off site and offers help desk type support but will come in as required	3/1/2018	35	2.6%
Tech Support	Interview	expressed that tech support is a third-party IT rep from the supplier	3/3/2018	13	0.9%
Security positives	Interview	tech support is a third-party IT rep	2/26/2018	8	0.6%
Tech Support	Interview	For on-line issues	3/3/2018	4	0.3%
Tech Support	Interview	The rep is located off site and offers help desk type support but will come in as required.	3/3/2018	18	1.3%
Security Negatives	Interview	The rep is located off site and offers help desk type support	2/26/2018	12	0.9%
Social Engineering	Interview	The rep is located off site and offers help desk type support but will come in as required	2/26/2018	18	1.3%
Security	Observation logs only	There are customer store credits but only the purchase receipts stored for records. No billing, customer or payment information kept in-house	3/3/2018	24	1.8%
Social Engineering	Observation logs only	There are customer store credits	2/26/2018	5	0.4%
Security Negatives	Observation logs only	customer store credits but only the purchase receipts stored for records	2/26/2018	12	0.9%
Security positives	Observation logs only	No billing, customer or payment information kept in-house	2/26/2018	10	0.7%
Security	Observation logs only	in other words, no useful information or any information of value). R	3/3/2018	12	0.9%
Security	Observation logs only	Receipts discarded in waste receptacle upon payment	3/3/2018	8	0.6%
Social Engineering	Observation logs only	receipts discarded in waste receptacle upon payment.	2/26/2018	8	0.6%
Security Negatives	Observation logs only	discarded in waste receptacle upon payment	2/26/2018	6	0.4%
Security	Observation logs only	makes custom hydraulic hoses which takes some time with work stations unattended	3/3/2018	12	0.9%
Security Negatives	Observation logs only	work stations unattended	2/26/2018	3	0.2%
Social Engineering	Observation logs only	work stations unattended	2/26/2018	3	0.2%
Social Engineering	Observation logs only	The participant is on a first name basis with all of the patrons with the exception of a scant few.	2/26/2018	20	1.5%
Security	Observation logs only	he participant is on a first name basis with all of the patrons with the exception of a scant few.	3/3/2018	20	1.5%
Security positives	Observation logs only	participant is on a first name basis with all of the patrons with the exception of a scant few	2/26/2018	19	1.4%
Security	Observation logs only	I noted that if any work stations left unattended	3/3/2018	10	0.7%
Tech Support	Observation logs only	I noted that if any work station left unattended	3/3/2018	10	0.7%
Security positives	Observation logs only	monitored by security video camera at the rear of the store	2/26/2018	13	0.9%
Security	Observation logs only	monitored by security video camera at the rear of the store.	3/3/2018	13	0.9%
Tech Support	Observation logs only	monitored by security video camera at the rear of the store	3/3/2018	13	0.9%
Security positives	Observation logs only	Activity at the work stations recorded	2/26/2018	8	0.6%
Security	Observation logs only	Activity at the work stations recorded	3/3/2018	8	0.6%

Tech Support	Observation logs only	Activity at the work stations recorded	3/3/2018	8	0.6%
Security Negatives	Observation logs only	but no details of work station would be available	2/26/2018	9	0.7%
Security	Observation logs only	but no details of work station would be available with the exception of the person at the station	3/3/2018	18	1.3%
Tech Support	Observation logs only	but no details of work station would be available with the exception of the person at the station and the time of the activity which would be enough to provide any information for an inquiry.	3/3/2018	35	2.6%
Social Engineering	Observation logs only	no details of work station would be available with the exception of the person at the station	2/26/2018	17	1.2%
Security positives	Observation logs only	the person at the station and the time of the activity which would be enough to provide any information for an inquiry.	2/26/2018	22	1.6%
Security	Observation logs only	and the time of the activity which would be enough to provide any information for an inquiry.	3/3/2018	17	1.2%
Security	Observation logs only	The security video recording device is located out of sight and disguised by covering by an empty cardboard container giving it the appearance of regular store merchandise.	3/3/2018	29	2.1%
Tech Support	Observation logs only	he security video recording device is located out of sight and disguised by covering by an empty cardboard container giving it the appearance of regular store merchandise	3/3/2018	29	2.1%
Security positives	Observation logs only	security video recording device is located out of sight and disguised covering by an empty cardboard container	2/26/2018	20	1.5%
Security	Observation logs only	security layout	3/3/2018	2	0.1%
Security Negatives	Observation logs only	Store walls are lined with product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door). Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches	2/26/2018	80	5.8%
Social Engineering	Observation logs only	Store walls lined with product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door). Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches	2/26/2018	80	5.8%
Security	Observation logs only	Store walls lined with product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door	3/3/2018	23	1.7%
Security	Observation logs only	Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the	3/3/2018	57	4.2%

		counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches.			
Social Engineering	Observation logs only	The main floor of the store divided three shelves about six feet high and double sided with the circular displays arranged around the perimeter.	2/26/2018	25	1.8%
Security	Observation logs only	The main floor of the store divided three shelves about six feet high and double sided with the circular displays arranged around the perimeter	3/3/2018	25	1.8%
Security	Observation logs only	The shelves dividing the main floor contain plumbing, electrical painting, body repair brackets and assorted brackets and fluids and chemicals, safety equipment, light bulbs, etc.	3/3/2018	25	1.8%
Security	Observation logs only	(customer traffic and phone calls are heaviest early in the morning).	3/3/2018	11	0.8%
Social Engineering	Observation logs only	customer traffic and phone calls are heaviest early in the morning	2/26/2018	11	0.8%
Security	Observation logs only	. Door alert goes off when customers enter and leave (chirping & tweeting sounds).	3/3/2018	12	0.9%
Security positives	Observation logs only	Door alert goes off when customers enter and leave (chirping & tweeting sounds)	2/26/2018	12	0.9%
Tech Support	Observation logs only	Door alert goes off when customers enter and leave (chirping & tweeting sounds).	3/3/2018	12	0.9%
Cost	Observation logs only	I noticed that the can not print when talking on the phone (DSL)	2/26/2018	13	0.9%
Tech Support	Observation logs only	I noticed that the can not print when talking on the phone (DSL	3/3/2018	13	0.9%
Security Negatives	Observation logs only	I noticed that the can not print when talking on the phone (DSL).	2/26/2018	13	0.9%
Social Engineering	Observation logs only	I noticed that the can not print when talking on the phone (DSL). No wi-fi.	2/26/2018	16	1.2%
Tech Support Negatives	Observation logs only	noticed that the can not print when talking on the phone (DSL). No wi-fi. Dot matrix printer.	3/1/2018	18	1.3%
Security	Observation logs only	noticed that the can not print when talking on the phone (DSL	3/3/2018	12	0.9%
Cost	Observation logs only	No wi-fi	2/26/2018	3	0.2%
Security positives	Observation logs only	No wi-fi.	2/26/2018	3	0.2%
Security	Observation logs only	No wi-fi. Dot matrix printer.	3/3/2018	6	0.4%
Tech Support	Observation logs only	No wi-fi. Dot matrix printer.	3/3/2018	6	0.4%
Cost	Observation logs only	Dot matrix printer	2/26/2018	3	0.2%
Social Engineering	Observation logs only	Small talk with farmers swapping stories and gossip about each other	2/26/2018	11	0.8%
Security	Observation logs only	farmers swapping stories and gossip about each other	3/3/2018	8	0.6%
Security	Observation logs only	We worked in back putting away stock	3/3/2018	7	0.5%
Security positives	Observation logs only	Cameras and motion detector well placed	2/26/2018	6	0.4%
Security	Observation logs only	Cameras and motion detector well placed (see security map	3/3/2018	9	0.7%
Tech Support	Observation logs only	Cameras and motion detector well placed (see security map).	3/3/2018	9	0.7%
Security	Observation logs only	. Customer can access most of the merchandise in the front of the store for shopping.	3/3/2018	15	1.1%
Security	Observation logs only	The exterior of the building is corrugated steel construction with about a 20-degree pitch roof with plumbing and heating vents only	3/3/2018	22	1.6%
Security	Observation logs only	. Plumbing, phone and electrical egress to the building is under ground with no exterior access.	3/3/2018	15	1.1%

Security positives	Observation logs only	phone and electrical egress to the building is under ground with no exterior access	2/26/2018	14	1.0%
Cost	Observation logs only	phone and electrical egress to the building is under ground with no exterior access	2/26/2018	14	1.0%
Tech Support	Observation logs only	phone and electrical egress to the building is under ground with no exterior access.	3/3/2018	14	1.0%
Security	Observation logs only	states that 98% are farmers.	3/3/2018	5	0.4%
Security	Observation logs only	. I noted that there are a lot of county employees making purchases on store credit. There are two possible charges- to the truck or to the shop.	3/3/2018	27	2.0%
Security Negatives	Observation logs only	store inventory accessible on-line	2/26/2018	7	0.5%
Security	Observation logs only	store inventory accessible on-line. No scanning system point and click system for receipt print out	3/3/2018	18	1.3%
Tech Support	Observation logs only	store inventory accessible on-line	3/3/2018	7	0.5%
Cost	Observation logs only	No scanning system point and click system for receipt print out	2/26/2018	11	0.8%
Security positives	Observation logs only	No scanning system point and click system for receipt print out.	2/26/2018	11	0.8%
Security Negatives	Observation logs only	No scanning system point and click system for receipt print out.	2/26/2018	11	0.8%
Tech Support Negatives	Observation logs only	No scanning system point and click system for receipt print out	3/1/2018	11	0.8%
Tech Support	Observation logs only	No scanning system point and click system for receipt print out.	3/3/2018	11	0.8%
Tech Support Negatives	Observation logs only	The absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall.	3/1/2018	23	1.7%
Cost	Observation logs only	The absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall	2/26/2018	23	1.7%
Tech Support	Observation logs only	The absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall	3/3/2018	23	1.7%
Security positives	Observation logs only	he absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall.	2/26/2018	23	1.7%
Security	Observation logs only	he absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall.	3/3/2018	23	1.7%
Social Engineering	Observation logs only	access to the system requires a password and user name	2/26/2018	11	0.8%
Security	Observation logs only	access to the system requires a password and user name	3/3/2018	11	0.8%
Tech Support Positives	Observation logs only	o access to the system requires a password and user name. The has indicated that he is aware of the necessity of a strong password.	3/1/2018	25	1.8%
Security positives	Observation logs only	access to the system requires a password and user name	2/26/2018	10	0.7%
Tech Support	Observation logs only	access to the system requires a password and user name. The has indicated that he is aware of the necessity of a strong password	3/3/2018	24	1.8%
Security	Observation logs only	The has indicated that he is aware of the necessity of a strong password.	3/3/2018	14	1.0%
Security positives	Observation logs only	he is aware of the necessity of a strong password.	2/26/2018	10	0.7%
Security	Observation logs only	on a first name basis with the owner,	3/3/2018	8	0.6%
Social Engineering	Observation logs only	the potential still exists for retaliation from disgruntled customers over money or	2/26/2018	28	2.0%

		merchandise dissatisfaction. Some merchandise can be very expensive. For a fuel dispenser costs almost $500.00.			
Security	Observation logs only	the potential still exists for retaliation from disgruntled customers over money or merchandise dissatisfaction	3/3/2018	14	1.0%
Security Negatives	Observation logs only	retaliation from disgruntled customers over money or merchandise dissatisfaction	2/26/2018	9	0.7%
Security	Observation logs only	Some merchandise can be very expensive	3/3/2018	6	0.4%
Security	Observation logs only	For a fuel dispenser costs almost $500.00.	3/3/2018	8	0.6%
Security	Observation logs only	The building is metal construction on a concrete slab.	3/3/2018	9	0.7%
Security positives	Observation logs only	The building is metal construction on a concrete slab	2/26/2018	9	0.7%
Security positives	Observation logs only	Adequate fluorescent lighting	2/26/2018	3	0.2%
Security	Observation logs only	Adequate fluorescent lighting	3/3/2018	3	0.2%
Security	Observation logs only	There is standard emergency lighting and exit signs that can activated by an emergency generator.	3/3/2018	16	1.2%
Security positives	Observation logs only	standard emergency lighting and exit signs activated by an emergency generator.	2/26/2018	14	1.0%
Social Engineering	Observation logs only	9:00-10:00- Work stations (three) are Dell computers with a firewall with anti-virus protection updated monthly and maintained by third party tech support. relies mostly on the third party (out-sourced) tech support for computer security and protection	2/26/2018	43	3.1%
Tech Support	Observation logs only	Work stations (three) are Dell computers with a firewall with anti-virus protection updated monthly and maintained by third party tech support	3/3/2018	24	1.8%
Cost	Observation logs only	Work stations (three) are Dell computers	2/26/2018	6	0.4%
Tech Support Positives	Observation logs only	Work stations (three) are Dell computers with a firewall with anti-virus protection updated monthly and maintained by third party tech support. relies mostly on the third party (out-sourced) tech support for computer security and protection	3/1/2018	39	2.8%
Security	Observation logs only	Work stations (three) are Dell computers with a firewall	3/3/2018	9	0.7%
Security positives	Observation logs only	a firewall with anti-virus protection updated monthly and maintained by third party tech support.	2/26/2018	17	1.2%
Security	Observation logs only	anti-virus protection updated monthly and maintained by third party tech support.	3/3/2018	14	1.0%
Security Negatives	Observation logs only	third party tech support. relies mostly on the third party (out-sourced) tech support for computer security and protection.	2/26/2018	19	1.4%
Tech Support	Observation logs only	relies mostly on the third party (out-sourced) tech support for computer security and protection.	3/3/2018	15	1.1%
Tech Support Negatives	Observation logs only	relies mostly on the third party (out-sourced) tech support for computer security and protection.	3/1/2018	15	1.1%
Security	Observation logs only	relies mostly on the third party (out-sourced) tech support for computer security and protection.	3/3/2018	15	1.1%
Security	Observation logs only	Building stands approximately 200 feet from the two-lane main county thoroughfare	3/3/2018	12	0.9%
Security positives	Observation logs only	The building surrounded on three sides by a soy bean field	2/26/2018	12	0.9%

Security	Observation logs only	The building surrounded on three sides by a soy bean field.	3/3/2018	12	0.9%
Security	Observation logs only	The nearest cell tower is less than a half mile away	3/3/2018	11	0.8%
Security positives	Observation logs only	but the business internet and phone activity is through the DSL carrier only	2/26/2018	13	0.9%
Social Engineering	Observation logs only	but the business internet and phone activity is through the DSL carrier only.	2/26/2018	13	0.9%
Security	Observation logs only	t the business internet and phone activity is through the DSL carrier only.	3/3/2018	13	0.9%
Tech Support	Observation logs only	business internet and phone activity is through the DSL carrier only.	3/3/2018	11	0.8%
Insider Potential Issue	Interview follow up questions raw data	08:30 am What is the difference between social engineering and hacking? Now that I do not know	3/1/2018	18	13.4%
Hacked System (External)	Interview follow up questions raw data	What is the difference between social engineering and hacking?	3/1/2018	9	6.7%
Hacked System (External)	Interview follow up questions raw data	What is the difference between social engineering and hacking? Now that I do not know	3/1/2018	15	11.2%
Compromised System Internal/External	Interview follow up questions raw data	What do you think is the main way internet criminals access systems illegally? Through the internet connection	3/1/2018	17	12.7%
Hacked System (External)	Interview follow up questions raw data	What do you think is the main way internet criminals access systems illegally? Through the internet connection (the participant is very uncertain on this)	3/1/2018	24	17.9%
Insider Potential Issue	Interview follow up questions raw data	What do you think is the main way internet criminals access systems illegally? Through the internet connection (the participant is very uncertain on this)	3/1/2018	24	17.9%
Insider Potential Issue	Interview follow up questions raw data	Who do you call if you suspect your system compromised? My IT support guy	3/1/2018	16	11.9%
Compromised System Internal/External	Interview follow up questions raw data	Who do you call if you suspect your system compromised? My IT support guy	3/1/2018	16	11.9%
Insider Potential Issue	Interview follow up questions raw data	Who do you call if you suspect your system compromised? My IT support guy	3/1/2018	16	11.9%
Tech Support Concerns (Insider Threats)	Interview follow up questions raw data	Who do you call if you suspect your system compromised? My IT support guy	3/1/2018	16	11.9%
Tech Support Concerns (Insider Threats)	Interview follow up questions raw data	Who do you call if you suspect your system compromised? My IT support guy	3/1/2018	8	6.0%
Insider Potential Issue	Interview follow up questions raw data	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/1/2018	17	12.7%
Tech Support Concerns (Insider Threats)	Interview follow up questions raw data	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/1/2018	17	12.7%
Tech Support Concerns (Insider Threats)	Interview follow up questions raw data	Does he respond right away? Yes, that same day, usually within an hour or so	3/1/2018	15	11.2%
Tech Support Concerns (Insider Threats)	Interview follow up questions raw data	Does he respond right away? Yes, that same day, usually within an hour or so	3/1/2018	15	11.2%
Insider Potential Issue	Interview follow up questions raw data	Who provides the tech support? The security software provider, it all comes under one package.	3/1/2018	15	11.2%
Insider Potential Issue	Interview follow up questions raw data	Who provides the tech support? The security software provider, it all comes under one package. (he gave me the name of the	3/1/2018	38	28.4%

		company, but I didn't bother to write it down since I cannot use it anyway)			
Tech Support Concerns (Insider Threats)	Interview follow up questions raw data	Who provides the tech support? The security software provider, it all comes under one package.	3/1/2018	15	11.2%
Security	Observation logs interview reflexive with participant removed	Lot of activity from uniform service. Changing out uniforms and replacing carpets.	3/3/2018	12	0.5%
Security positives	Observation logs interview reflexive with participant removed	Smart phone Wi-fi scan produced no results	2/26/2018	8	0.4%
Tech Support Negatives	Observation logs interview reflexive with participant removed	Smart phone Wi-fi scan produced no results (no wi-fi signals within range	3/1/2018	14	0.6%
Security	Observation logs interview reflexive with participant removed	Smart phone Wi-fi scan produced no results	3/3/2018	8	0.4%
Tech Support	Observation logs interview reflexive with participant removed	Smart phone Wi-fi scan produced no results	3/3/2018	8	0.4%
Cost	Observation logs interview reflexive with participant removed	Wi-fi scan produced no results	2/26/2018	6	0.3%
Security	Observation logs interview reflexive with participant removed	(no wi-fi signals within range)	3/3/2018	6	0.3%
Security	Observation logs interview reflexive with participant removed	Observed two work station CRTS with keyboards on customer service counter	3/3/2018	11	0.5%
Tech Support	Observation logs interview reflexive with participant removed	Observed two work station CRTS with keyboards on customer service counter	3/3/2018	11	0.5%
Social Engineering	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	2/26/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	3/3/2018	15	0.7%
Tech Support	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	3/3/2018	15	0.7%
Security Negatives	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	2/26/2018	15	0.7%
Tech Support Negatives	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	3/1/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	3/3/2018	10	0.5%
Tech Support	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	3/3/2018	10	0.5%
Security positives	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	2/26/2018	7	0.3%
Tech Support	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	3/3/2018	9	0.4%

Security Negatives	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	2/26/2018	8	0.4%
Social Engineering	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	2/26/2018	8	0.4%
Tech Support Negatives	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	3/1/2018	52	2.4%
Security	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	3/3/2018	8	0.4%
Cost	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	2/26/2018	11	0.5%
Tech Support	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	3/3/2018	11	0.5%
Security	Observation logs interview reflexive with participant removed	Observation logs interview reflexive with participant removed	3/3/2018	11	0.5%
Cost	Observation logs interview reflexive with participant removed	Phone operation prevents printer operation	2/26/2018	5	0.2%
Security Negatives	Observation logs interview reflexive with participant removed	Phone operation prevents printer operation.	2/26/2018	5	0.2%
Security	Observation logs interview reflexive with participant removed	Phone operation prevents printer operation	3/3/2018	5	0.2%
Tech Support	Observation logs interview reflexive with participant removed	Phone operation prevents printer operation	3/3/2018	5	0.2%
Tech Support	Observation logs interview reflexive with participant removed	Internet ethernet internet service by separate line such that there is no interference during transaction processing	3/3/2018	16	0.7%
Security positives	Observation logs interview reflexive with participant removed	Internet ethernet internet service by separate line	2/26/2018	7	0.3%
Security	Observation logs interview reflexive with participant removed	Internet ethernet internet service by separate line such that there is no interference during transaction processing	3/3/2018	16	0.7%
Cost	Observation logs interview reflexive with participant removed	. Printer is a hole fed dot matrix printer for printing hardcopy receipts	2/26/2018	12	0.5%
Security	Observation logs interview reflexive with participant removed	Printer is a hole fed dot matrix printer for printing hardcopy receipts.	3/3/2018	12	0.5%
Tech Support	Observation logs interview reflexive with participant removed	Printer is a hole fed dot matrix printer for printing hardcopy receipts.	3/3/2018	12	0.5%
Security	Observation logs interview reflexive with participant removed	I also learned that some farmers are very superstitious and will not perform some farm activities if the signs are not right. (Full moon etc.)	3/3/2018	25	1.1%
Security	Observation logs interview reflexive with participant removed	. Magnetic security devices on three bay doors as well as the front entry doors	3/3/2018	14	0.6%
Security positives	Observation logs interview reflexive with participant removed	Magnetic security devices on three bay doors as well as the front entry doors	2/26/2018	14	0.6%

Tech Support	Observation logs interview reflexive with participant removed	Magnetic security devices on three bay doors as well as the front entry doors.	3/3/2018	14	0.6%
Security positives	Observation logs interview reflexive with participant removed	There is an audible chirping thru out the facility when the front door is opened to alert staff of an entry	2/26/2018	21	1.0%
Security	Observation logs interview reflexive with participant removed	There is an audible chirping thru out the facility when the front door is opened to alert staff of an entry	3/3/2018	21	1.0%
Tech Support	Observation logs interview reflexive with participant removed	There is an audible chirping thru out the facility when the front door opened to alert staff of an entry.	3/3/2018	21	1.0%
Security positives	Observation logs interview reflexive with participant removed	Observed a wide-angle security camera attached to the drop ceiling on the back-left corner from the entrance of the building	2/26/2018	22	1.0%
Security	Observation logs interview reflexive with participant removed	Observed a wide-angle security camera attached to the drop ceiling on the back-left corner from the entrance of the building.	3/3/2018	22	1.0%
Tech Support	Observation logs interview reflexive with participant removed	Observed a wide-angle security camera attached to the drop ceiling on the back-left corner from the entrance of the building.	3/3/2018	22	1.0%
Tech Support	Observation logs interview reflexive with participant removed	The camera covers the entire store including the counter work stations. Activity on the work stations not observed	3/3/2018	19	0.9%
Security positives	Observation logs interview reflexive with participant removed	The camera covers the entire store including the counter work stations	2/26/2018	11	0.5%
Security	Observation logs interview reflexive with participant removed	The camera covers the entire store including the counter work stations. Activity on the work stations not observed, but a person using the system can be and a date and time established as to when a person is at the workstation.	3/3/2018	44	2.0%
Security Negatives	Observation logs interview reflexive with participant removed	Activity on the work stations not observed,	2/26/2018	8	0.4%
Tech Support Negatives	Observation logs interview reflexive with participant removed	Activity on the work stations not observed	3/1/2018	8	0.4%
Social Engineering	Observation logs interview reflexive with participant removed	Activity on the work stations not observed	2/26/2018	8	0.4%
Tech Support	Observation logs interview reflexive with participant removed	but a person using the system can be and a date and time established as to when a person is at the workstation	3/3/2018	25	1.1%
Tech Support Positives	Observation logs interview reflexive with participant removed	a person using the system can be and a date and time established as to when a person is at the workstation	3/1/2018	24	1.1%
Security positives	Observation logs interview reflexive with participant removed	a person using the system can be and a date and time established as to when a person is at the workstation	2/26/2018	24	1.1%
Social Engineering	Observation logs interview reflexive with participant removed	Heavy customer traffic	2/26/2018	3	0.1%
Security Negatives	Observation logs interview reflexive with participant removed	Discussed power supply. Cable and phone. AT&T provides the DSL service and phone	2/26/2018	14	0.6%
Tech Support	Observation logs interview reflexive with participant removed	Discussed power supply	3/3/2018	3	0.1%

Security	Observation logs interview reflexive with participant removed	power supply	3/3/2018	2	0.1%
Security	Observation logs interview reflexive with participant removed	Cable and phone	3/3/2018	3	0.1%
Tech Support	Observation logs interview reflexive with participant removed	Cable and phone	3/3/2018	3	0.1%
Cost	Observation logs interview reflexive with participant removed	. AT&T provides the DSL service and phone	2/26/2018	8	0.4%
Tech Support Negatives	Observation logs interview reflexive with participant removed	AT&T provides the DSL service and phone	3/1/2018	8	0.4%
Security	Observation logs interview reflexive with participant removed	AT&T provides the DSL service and phone. Line service	3/3/2018	10	0.5%
Tech Support	Observation logs interview reflexive with participant removed	AT&T provides the DSL service and phone	3/3/2018	8	0.4%
Tech Support	Observation logs interview reflexive with participant removed	Line service.	3/3/2018	2	0.1%
Security positives	Observation logs interview reflexive with participant removed	Alarm system connected to a motion and magnetic interlock system that activates an alarm.	2/26/2018	15	0.7%
Tech Support Positives	Observation logs interview reflexive with participant removed	Alarm system connected to a motion and magnetic interlock system that activates an alarm. All service connections are inside the building.	3/1/2018	22	1.0%
Security	Observation logs interview reflexive with participant removed	Alarm system connected to a motion and magnetic interlock system that activates an alarm. All service connections are inside the building	3/3/2018	22	1.0%
Tech Support	Observation logs interview reflexive with participant removed	Alarm system connected to a motion and magnetic interlock system that activates an alarm	3/3/2018	15	0.7%
Security positives	Observation logs interview reflexive with participant removed	All service connections are inside the building	2/26/2018	7	0.3%
Social Engineering	Observation logs interview reflexive with participant removed	All service connections are inside the building	2/26/2018	7	0.3%
Tech Support	Observation logs interview reflexive with participant removed	All service connections are inside the building	3/3/2018	7	0.3%
Security Negatives	Observation logs interview reflexive with participant removed	they have had three break-ins in the 19 years that have been in business.	2/26/2018	15	0.7%
Social Engineering	Observation logs interview reflexive with participant removed	they have had three break-ins in the 19 years that have been in business	2/26/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	they have had three break-ins in the 19 years that have been in business	3/3/2018	15	0.7%
Security Negatives	Observation logs interview reflexive with participant removed	One instance a lap-top with employee personal information taken	2/26/2018	11	0.5%

Social Engineering	Observation logs interview reflexive with participant removed	One instance a lap-top with employee personal information taken	2/26/2018	11	0.5%
Security	Observation logs interview reflexive with participant removed	One instance a lap-top with employee personal information taken	3/3/2018	11	0.5%
Security positives	Observation logs interview reflexive with participant removed	Procedure changed to not leave lap-top over-nigh	2/26/2018	8	0.4%
Security	Observation logs interview reflexive with participant removed	Procedure changed to not leave lap-top overnight. The laptop recovered.	3/3/2018	12	0.5%
Security	Observation logs interview reflexive with participant removed	It is an expectation that the laptop stolen for use and not data because of the nature of the recovery	3/3/2018	19	0.9%
Security Negatives	Observation logs interview reflexive with participant removed	expressed that tech support is a third-party IT rep from the supplier	2/26/2018	13	0.6%
Social Engineering	Observation logs interview reflexive with participant removed	expressed that tech support is a third-party IT rep from the supplier.	2/26/2018	13	0.6%
Tech Support Negatives	Observation logs interview reflexive with participant removed	expressed that tech support is a third-party IT rep from the supplier. For on-line issues. The rep is located off site and offers help desk type support but will come in as required	3/1/2018	35	1.6%
Tech Support	Observation logs interview reflexive with participant removed	expressed that tech support is a third-party IT rep from the supplier	3/3/2018	13	0.6%
Security positives	Observation logs interview reflexive with participant removed	tech support is a third-party IT rep	2/26/2018	8	0.4%
Tech Support	Observation logs interview reflexive with participant removed	For on-line issues	3/3/2018	4	0.2%
Tech Support	Observation logs interview reflexive with participant removed	The rep is located off site and offers help desk type support but will come in as required.	3/3/2018	18	0.8%
Security Negatives	Observation logs interview reflexive with participant removed	The rep is located off site and offers help desk type support	2/26/2018	12	0.5%
Social Engineering	Observation logs interview reflexive with participant removed	The rep is located off site and offers help desk type support but will come in as required	2/26/2018	18	0.8%
Security	Observation logs interview reflexive with participant removed	There are customer store credits but only the purchase receipts stored for records. No billing, customer or payment information kept in-house	3/3/2018	24	1.1%
Social Engineering	Observation logs interview reflexive with participant removed	There are customer store credits	2/26/2018	5	0.2%
Security Negatives	Observation logs interview reflexive with participant removed	customer store credits but only the purchase receipts stored for records	2/26/2018	12	0.5%
Security positives	Observation logs interview reflexive with participant removed	No billing, customer or payment information is kept in-house	2/26/2018	10	0.5%
Security	Observation logs interview reflexive with participant removed	in other words, no useful information or any information of value). R	3/3/2018	12	0.5%

Security	Observation logs interview reflexive with participant removed	Receipts discarded in waste receptacle upon payment	3/3/2018	8	0.4%
Social Engineering	Observation logs interview reflexive with participant removed	receipts discarded in waste receptacle upon payment.	2/26/2018	8	0.4%
Security Negatives	Observation logs interview reflexive with participant removed	discarded in waste receptacle upon payment	2/26/2018	6	0.3%
Security	Observation logs interview reflexive with participant removed	makes custom hydraulic hoses which takes some time with work stations unattended	3/3/2018	12	0.5%
Security Negatives	Observation logs interview reflexive with participant removed	work stations unattended	2/26/2018	3	0.1%
Social Engineering	Observation logs interview reflexive with participant removed	work stations unattended	2/26/2018	3	0.1%
Social Engineering	Observation logs interview reflexive with participant removed	The participant is on a first name basis with all of the patrons with the exception of a scant few.	2/26/2018	20	0.9%
Security	Observation logs interview reflexive with participant removed	he participant is on a first name basis with all of the patrons with the exception of a scant few.	3/3/2018	20	0.9%
Security positives	Observation logs interview reflexive with participant removed	participant is on a first name basis with all of the patrons with the exception of a scant few	2/26/2018	19	0.9%
Security	Observation logs interview reflexive with participant removed	I noted that if any work stations are left unattended	3/3/2018	10	0.5%
Tech Support	Observation logs interview reflexive with participant removed	I noted that if any work stations are left unattended	3/3/2018	10	0.5%
Security positives	Observation logs interview reflexive with participant removed	monitored by security video camera at the rear of the store	2/26/2018	13	0.6%
Security	Observation logs interview reflexive with participant removed	monitored by security video camera at the rear of the store.	3/3/2018	13	0.6%
Tech Support	Observation logs interview reflexive with participant removed	monitored by security video camera at the rear of the store	3/3/2018	13	0.6%
Security positives	Observation logs interview reflexive with participant removed	Activity at the work stations recorded	2/26/2018	8	0.4%
Security	Observation logs interview reflexive with participant removed	Activity at the work stations recorded	3/3/2018	8	0.4%
Tech Support	Observation logs interview reflexive with participant removed	Activity at the work stations recorded	3/3/2018	8	0.4%
Security Negatives	Observation logs interview reflexive with participant removed	but no details of work station would be available	2/26/2018	9	0.4%
Security	Observation logs interview reflexive with participant removed	but no details of work station would be available with the exception of the person at the station	3/3/2018	18	0.8%
Tech Support	Observation logs interview reflexive with participant removed	but no details of work station would be available with the exception of the person at the station and the time of the activity which	3/3/2018	35	1.6%

		would be enough to provide any information for an inquiry.			
Social Engineering	Observation logs interview reflexive with participant removed	no details of work station would be available with the exception of the person at the station	2/26/2018	17	0.8%
Security positives	Observation logs interview reflexive with participant removed	the person at the station and the time of the activity which would be enough to provide any information for an inquiry.	2/26/2018	22	1.0%
Security	Observation logs interview reflexive with participant removed	and the time of the activity which would be enough to provide any information for an inquiry.	3/3/2018	17	0.8%
Security	Observation logs interview reflexive with participant removed	The security video recording device is located out of sight and disguised by covered by an empty cardboard container giving it the appearance of regular store merchandise.	3/3/2018	29	1.3%
Tech Support	Observation logs interview reflexive with participant removed	he security video recording device is located out of sight and disguised by covered by an empty cardboard container giving it the appearance of regular store merchandise	3/3/2018	29	1.3%
Security positives	Observation logs interview reflexive with participant removed	security video recording device is located out of sight and disguised by covered by an empty cardboard container	2/26/2018	20	0.9%
Security	Observation logs interview reflexive with participant removed	security layout	3/3/2018	2	0.1%
Security Negatives	Observation logs interview reflexive with participant removed	Store walls lined with product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door). Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches	2/26/2018	80	3.6%
Social Engineering	Observation logs interview reflexive with participant removed	Store walls lined with product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door). Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches	2/26/2018	80	3.6%
Security	Observation logs interview reflexive with participant removed	Store walls lined with product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door	3/3/2018	23	1.0%
Security	Observation logs interview reflexive with participant removed	Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches.	3/3/2018	57	2.6%
Social Engineering	Observation logs interview reflexive with participant removed	The main floor of the store divided three shelves about six feet high and double sided	2/26/2018	25	1.1%

		with the circular displays arranged around the perimeter.			
Security	Observation logs interview reflexive with participant removed	The main floor of the store divided three shelves about six feet high and double sided with the circular displays arranged around the perimeter	3/3/2018	25	1.1%
Security	Observation logs interview reflexive with participant removed	The shelves dividing the main floor contain plumbing, electrical painting, body repair brackets and assorted brackets and fluids and chemicals, safety equipment, light bulbs, etc.	3/3/2018	25	1.1%
Security	Observation logs interview reflexive with participant removed	(customer traffic and phone calls are heaviest early in the morning).	3/3/2018	11	0.5%
Social Engineering	Observation logs interview reflexive with participant removed	customer traffic and phone calls are heaviest early in the morning	2/26/2018	11	0.5%
Security	Observation logs interview reflexive with participant removed	. Door alert goes off when customers enter and leave (chirping & tweeting sounds).	3/3/2018	12	0.5%
Security positives	Observation logs interview reflexive with participant removed	Door alert goes off when customers enter and leave (chirping & tweeting sounds)	2/26/2018	12	0.5%
Tech Support	Observation logs interview reflexive with participant removed	Door alert goes off when customers enter and leave (chirping & tweeting sounds).	3/3/2018	12	0.5%
Cost	Observation logs interview reflexive with participant removed	I noticed that the can not print when talking on the phone (DSL)	2/26/2018	13	0.6%
Tech Support	Observation logs interview reflexive with participant removed	I noticed that the can not print when talking on the phone (DSL	3/3/2018	13	0.6%
Security Negatives	Observation logs interview reflexive with participant removed	I noticed that the can not print when talking on the phone (DSL).	2/26/2018	13	0.6%
Social Engineering	Observation logs interview reflexive with participant removed	I noticed that the can not print when talking on the phone (DSL). No wi-fi.	2/26/2018	16	0.7%
Tech Support Negatives	Observation logs interview reflexive with participant removed	noticed that the can not print when talking on the phone (DSL). No wi-fi. Dot matrix printer.	3/1/2018	18	0.8%
Security	Observation logs interview reflexive with participant removed	noticed that the can not print when talking on the phone (DSL	3/3/2018	12	0.5%
Cost	Observation logs interview reflexive with participant removed	No wi-fi	2/26/2018	3	0.1%
Security positives	Observation logs interview reflexive with participant removed	No wi-fi.	2/26/2018	3	0.1%
Security	Observation logs interview reflexive with participant removed	No wi-fi. Dot matrix printer.	3/3/2018	6	0.3%
Tech Support	Observation logs interview reflexive with participant removed	No wi-fi. Dot matrix printer.	3/3/2018	6	0.3%
Cost	Observation logs interview reflexive with participant removed	Dot matrix printer	2/26/2018	3	0.1%
Social Engineering	Observation logs interview reflexive with participant removed	Small talk with farmers swapping stories and gossip about each other	2/26/2018	11	0.5%

Security	Observation logs interview reflexive with participant removed	farmers swapping stories and gossip about each other	3/3/2018	8	0.4%
Security	Observation logs interview reflexive with participant removed	We worked in back putting away stock	3/3/2018	7	0.3%
Security positives	Observation logs interview reflexive with participant removed	Cameras and motion detector well placed	2/26/2018	6	0.3%
Security	Observation logs interview reflexive with participant removed	Cameras and motion detector well placed (see security map	3/3/2018	9	0.4%
Tech Support	Observation logs interview reflexive with participant removed	Cameras and motion detector well placed (see security map).	3/3/2018	9	0.4%
Security	Observation logs interview reflexive with participant removed	. Customer can access most of the merchandise in the front of the store for shopping.	3/3/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	The exterior of the building is corrugated steel construction with about a 20-degree pitch roof with plumbing and heating vents only	3/3/2018	22	1.0%
Security	Observation logs interview reflexive with participant removed	. Plumbing, phone and electrical egress to the building is under ground with no exterior access.	3/3/2018	15	0.7%
Security positives	Observation logs interview reflexive with participant removed	phone and electrical egress to the building is under ground with no exterior access	2/26/2018	14	0.6%
Cost	Observation logs interview reflexive with participant removed	phone and electrical egress to the building is under ground with no exterior access	2/26/2018	14	0.6%
Tech Support	Observation logs interview reflexive with participant removed	phone and electrical egress to the building is under ground with no exterior access.	3/3/2018	14	0.6%
Security	Observation logs interview reflexive with participant removed	states that 98% are farmers.	3/3/2018	5	0.2%
Security	Observation logs interview reflexive with participant removed	. I noted that there are a lot of county employees making purchases on store credit. There are two possible charges- to the truck or to the shop.	3/3/2018	27	1.2%
Security Negatives	Observation logs interview reflexive with participant removed	store inventory can be accessed on-line	2/26/2018	7	0.3%
Security	Observation logs interview reflexive with participant removed	store inventory can be accessed on-line. No scanning system point and click system for receipt print out	3/3/2018	18	0.8%
Tech Support	Observation logs interview reflexive with participant removed	store inventory can be accessed on-line	3/3/2018	7	0.3%
Cost	Observation logs interview reflexive with participant removed	No scanning system point and click system for receipt print out	2/26/2018	11	0.5%
Security positives	Observation logs interview reflexive with participant removed	No scanning system point and click system for receipt print out.	2/26/2018	11	0.5%
Security Negatives	Observation logs interview reflexive with participant removed	No scanning system point and click system for receipt print out.	2/26/2018	11	0.5%
Tech Support Negatives	Observation logs interview reflexive with participant removed	No scanning system point and click system for receipt print out	3/1/2018	11	0.5%

Tech Support	Observation logs interview reflexive with participant removed	No scanning system point and click system for receipt print out.	3/3/2018	11	0.5%
Tech Support Negatives	Observation logs interview reflexive with participant removed	The absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall.	3/1/2018	23	1.0%
Cost	Observation logs interview reflexive with participant removed	The absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall	2/26/2018	23	1.0%
Tech Support	Observation logs interview reflexive with participant removed	The absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall	3/3/2018	23	1.0%
Security positives	Observation logs interview reflexive with participant removed	he absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall.	2/26/2018	23	1.0%
Security	Observation logs interview reflexive with participant removed	he absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall.	3/3/2018	23	1.0%
Social Engineering	Observation logs interview reflexive with participant removed	access to the system requires a password and user name	2/26/2018	11	0.5%
Security	Observation logs interview reflexive with participant removed	access to the system requires a password and user name	3/3/2018	11	0.5%
Tech Support Positives	Observation logs interview reflexive with participant removed	o access to the system requires a password and user name. The has indicated that he is aware of the necessity of a strong password.	3/1/2018	25	1.1%
Security positives	Observation logs interview reflexive with participant removed	access to the system requires a password and user name	2/26/2018	10	0.5%
Tech Support	Observation logs interview reflexive with participant removed	access to the system requires a password and user name. The has indicated that he is aware of the necessity of a strong password	3/3/2018	24	1.1%
Security	Observation logs interview reflexive with participant removed	The has indicated that he is aware of the necessity of a strong password.	3/3/2018	14	0.6%
Security positives	Observation logs interview reflexive with participant removed	e is aware of the necessity of a strong password.	2/26/2018	10	0.5%
Security	Observation logs interview reflexive with participant removed	on a first name basis with the owner,	3/3/2018	8	0.4%
Social Engineering	Observation logs interview reflexive with participant removed	the potential still exists for retaliation from disgruntled customers over money or merchandise dissatisfaction. Some merchandise can be very expensive. For a fuel dispenser costs almost $500.00.	2/26/2018	28	1.3%
Security	Observation logs interview reflexive with participant removed	the potential still exists for retaliation from disgruntled customers over money or merchandise dissatisfaction	3/3/2018	14	0.6%
Security Negatives	Observation logs interview reflexive with participant removed	retaliation from disgruntled customers over money or merchandise dissatisfaction	2/26/2018	9	0.4%
Security	Observation logs interview reflexive with participant removed	Some merchandise can be very expensive	3/3/2018	6	0.3%
Security	Observation logs interview reflexive with participant removed	For a fuel dispenser costs almost $500.00.	3/3/2018	8	0.4%

Security	Observation logs interview reflexive with participant removed	The building is metal construction on a concrete slab.	3/3/2018	9	0.4%
Security positives	Observation logs interview reflexive with participant removed	The building is metal construction on a concrete slab	2/26/2018	9	0.4%
Security positives	Observation logs interview reflexive with participant removed	Adequate fluorescent lighting	2/26/2018	3	0.1%
Security	Observation logs interview reflexive with participant removed	Adequate fluorescent lighting	3/3/2018	3	0.1%
Security	Observation logs interview reflexive with participant removed	There is standard emergency lighting and exit signs t activated by an emergency generator.	3/3/2018	16	0.7%
Security positives	Observation logs interview reflexive with participant removed	standard emergency lighting and exit signs by an emergency generator.	2/26/2018	14	0.6%
Social Engineering	Observation logs interview reflexive with participant removed	9:00-10:00- Work stations (three) are Dell computers with a firewall with anti-virus protection updated monthly and maintained by third party tech support. relies mostly on the third party (out-sourced) tech support for computer security and protection	2/26/2018	43	2.0%
Tech Support	Observation logs interview reflexive with participant removed	Work stations (three) are Dell computers with a firewall with anti-virus protection updated monthly and maintained by third party tech support	3/3/2018	24	1.1%
Cost	Observation logs interview reflexive with participant removed	Work stations (three) are Dell computers	2/26/2018	6	0.3%
Tech Support Positives	Observation logs interview reflexive with participant removed	Work stations (three) are Dell computers with a firewall with anti-virus protection updated monthly and maintained by third party tech support. relies mostly on the third party (out-sourced) tech support for computer security and protection	3/1/2018	39	1.8%
Security	Observation logs interview reflexive with participant removed	Work stations (three) are Dell computers with a firewall	3/3/2018	9	0.4%
Security positives	Observation logs interview reflexive with participant removed	a firewall with anti-virus protection updated monthly and maintained by third party tech support.	2/26/2018	17	0.8%
Security	Observation logs interview reflexive with participant removed	anti-virus protection that updated monthly and maintained by third party tech support.	3/3/2018	14	0.6%
Security Negatives	Observation logs interview reflexive with participant removed	third party tech support. relies mostly on the third party (out-sourced) tech support for computer security and protection.	2/26/2018	19	0.9%
Tech Support	Observation logs interview reflexive with participant removed	relies mostly on the third party (out-sourced) tech support for computer security and protection.	3/3/2018	15	0.7%
Tech Support Negatives	Observation logs interview reflexive with participant removed	relies mostly on the third party (out-sourced) tech support for computer security and protection.	3/1/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	relies mostly on the third party (out-sourced) tech support for computer security and protection.	3/3/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	building stands approximately 200 feet from the two-lane main county thoroughfare	3/3/2018	12	0.5%

Security positives	Observation logs interview reflexive with participant removed	The building surrounded on three sides by a soy bean field	2/26/2018	12	0.5%
Security	Observation logs interview reflexive with participant removed	The building surrounded on three sides by a soy bean field.	3/3/2018	12	0.5%
Security	Observation logs interview reflexive with participant removed	The nearest cell tower is less than a half mile away	3/3/2018	11	0.5%
Security positives	Observation logs interview reflexive with participant removed	but the business internet and phone activity is through the DSL carrier only	2/26/2018	13	0.6%
Social Engineering	Observation logs interview reflexive with participant removed	but the business internet and phone activity is through the DSL carrier only.	2/26/2018	13	0.6%
Security	Observation logs interview reflexive with participant removed	t the business internet and phone activity is through the DSL carrier only.	3/3/2018	13	0.6%
Tech Support	Observation logs interview reflexive with participant removed	business internet and phone activity is through the DSL carrier only.	3/3/2018	11	0.5%
Security Negatives	Observation logs interview reflexive with participant removed	What is the difference between social engineering and hacking? Now that I do not know.	2/26/2018	15	0.7%
Social Engineering	Observation logs interview reflexive with participant removed	What is the difference between social engineering and hacking? Now that I do not know.	2/26/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	What is the difference between social engineering and hacking? Now that I do not know.	3/3/2018	15	0.7%
Security Negatives	Observation logs interview reflexive with participant removed	What do you think is the main way internet criminals access systems illegally? Through the internet connection	2/26/2018	17	0.8%
Social Engineering	Observation logs interview reflexive with participant removed	What do you think is the main way internet criminals access systems illegally? Through the internet connection	2/26/2018	17	0.8%
Security	Observation logs interview reflexive with participant removed	What do you think is the main way internet criminals access systems illegally? Through the internet connection	3/3/2018	17	0.8%
Security positives	Observation logs interview reflexive with participant removed	Who do you call if you suspect your system compromised? My IT support guy	2/26/2018	16	0.7%
Social Engineering	Observation logs interview reflexive with participant removed	Who do you call if you suspect your system compromised? My IT support guy	2/26/2018	16	0.7%
Tech Support Positives	Observation logs interview reflexive with participant removed	Who do you call if you suspect your system compromised? My IT support guy	3/1/2018	16	0.7%
Security	Observation logs interview reflexive with participant removed	Who do you call if you suspect your system compromised? My IT support guy	3/3/2018	16	0.7%
Tech Support	Observation logs interview reflexive with participant removed	Who do you call if you suspect your system compromised? My IT support guy	3/3/2018	16	0.7%
Security positives	Observation logs interview reflexive with participant removed	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	2/26/2018	17	0.8%
Security	Observation logs interview reflexive with participant removed	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/3/2018	17	0.8%

Tech Support	Observation logs interview reflexive with participant removed	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/3/2018	17	0.8%
Security positives	Observation logs interview reflexive with participant removed	Does he respond right away? Yes, that same day, usually within an hour or so.	2/26/2018	15	0.7%
Tech Support Positives	Observation logs interview reflexive with participant removed	Does he respond right away? Yes, that same day, usually within an hour or so.	3/1/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	Does he respond right away? Yes, that same day, usually within an hour or so.	3/3/2018	15	0.7%
Tech Support	Observation logs interview reflexive with participant removed	Does he respond right away? Yes, that same day, usually within an hour or so.	3/3/2018	15	0.7%
Security positives	Observation logs interview reflexive with participant removed	Who provides the tech support? The security software provider, it all comes under one package.	2/26/2018	15	0.7%
Tech Support Positives	Observation logs interview reflexive with participant removed	Who provides the tech support? The security software provider, it all comes under one package.	3/1/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	Who provides the tech support? The security software provider, it all comes under one package.	3/3/2018	15	0.7%
Tech Support	Observation logs interview reflexive with participant removed	Who provides the tech support? The security software provider, it all comes under one package	3/3/2018	15	0.7%
Cost	Observation logs interview reflexive with participant removed	No Wi-Fi at the facility. Strictly DSL	2/26/2018	8	0.4%
Tech Support Negatives	Observation logs interview reflexive with participant removed	No Wi-Fi at the facility. Strictly DSL.	3/1/2018	8	0.4%
Security	Observation logs interview reflexive with participant removed	No Wi-Fi at the facility	3/3/2018	6	0.3%
Tech Support	Observation logs interview reflexive with participant removed	No Wi-Fi at the facility. Strictly DSL. The Wi-Fi signal tested 5 times at random intervals with no signal detected	3/3/2018	23	1.0%
Security	Observation logs interview reflexive with participant removed	Strictly DSL	3/3/2018	2	0.1%
Security	Observation logs interview reflexive with participant removed	he Wi-Fi signal tested 5 times at random intervals with no signal detected.	3/3/2018	15	0.7%
Tech Support Negatives	Observation logs interview reflexive with participant removed	Using dedicated DOT Matrix printer to print receipts	3/1/2018	8	0.4%
Security	Observation logs interview reflexive with participant removed	Using dedicated DOT Matrix printer to print receipts.	3/3/2018	8	0.4%
Tech Support	Observation logs interview reflexive with participant removed	Using dedicated DOT Matrix printer to print receipts	3/3/2018	8	0.4%
Security positives	Observation logs interview reflexive with participant removed	Alarm system is good magnetic interlocks on door Like that laptop stolen was just an opportunity theft and not specifically sought out for info	2/26/2018	26	1.2%
Security	Observation logs interview reflexive with participant removed	alarm system is good magnetic interlocks on doors Like that laptop stolen was just an	3/3/2018	26	1.2%

		opportunity theft and not specifically sought out for info			
Tech Support	Observation logs interview reflexive with participant removed	alarm system is good magnetic interlocks on doors Like that laptop stolen was just an opportunity theft and not specifically sought out for info	3/3/2018	26	1.2%
Security	Observation logs interview reflexive with participant removed	Doors that laptop stolen was just an opportunity theft and not specifically sought out for info	3/3/2018	19	0.9%
Security	Observation logs interview reflexive with participant removed	Intruders would likely be after merchandise and electronic equipment would be opportunity	3/3/2018	12	0.5%
Security	Observation logs interview reflexive with participant removed	Intruders would likely be after merchandise and electronic equipment would be opportunity	3/3/2018	12	0.5%
Security	Observation logs interview reflexive with participant removed	The laptop recovered and being used by an acquaintance of the thief.	3/3/2018	14	0.6%
Security positives	Observation logs interview reflexive with participant removed	The laptop recovered	2/26/2018	4	0.2%
Security positives	Observation logs interview reflexive with participant removed	Work stations have a password timer	2/26/2018	6	0.3%
Social Engineering	Observation logs interview reflexive with participant removed	Work stations have a password timer, but it may need a shorter time out. Sometimes employees indisposed for long periods of time and unable to monitor the work stations.	2/26/2018	31	1.4%
Tech Support Negatives	Observation logs interview reflexive with participant removed	Work stations have a password timer, but it may need a shorter time out	3/1/2018	14	0.6%
Security	Observation logs interview reflexive with participant removed	Work stations have a password timer	3/3/2018	6	0.3%
Tech Support	Observation logs interview reflexive with participant removed	Work stations have a password timer, but it may need a shorter time out.	3/3/2018	14	0.6%
Security Negatives	Observation logs interview reflexive with participant removed	but it may need a shorter time out. Sometimes employees indisposed for long periods of time and unable to monitor the work stations	2/26/2018	25	1.1%
Security	Observation logs interview reflexive with participant removed	it may need a shorter time out.	3/3/2018	8	0.4%
Tech Support	Observation logs interview reflexive with participant removed	Sometimes employees indisposed for long periods of time and unable to monitor the work stations.	3/3/2018	17	0.8%
Security	Observation logs interview reflexive with participant removed	Sometimes employees indisposed for long periods of time and unable to monitor the work stations	3/3/2018	17	0.8%
Security positives	Observation logs interview reflexive with participant removed	The door ringer (a bird chirping) will trigger employees of customer entrances to the store if they are not out front	2/26/2018	21	1.0%
Tech Support	Observation logs interview reflexive with participant removed	The door ringer (a bird chirping) will trigger employees of customer entrances to the store if they are not out front.	3/3/2018	21	1.0%
Security	Observation logs interview reflexive with participant removed	Intruders would likely be after merchandise and electronic equipment would be opportunity	3/3/2018	12	0.5%
Social Engineering	Observation logs interview reflexive with participant removed	Customers would rarely have time to access the work stations without staff being present because of the chirping alarm	2/26/2018	19	0.9%

Security positives	Observation logs interview reflexive with participant removed	Customers would rarely have time to access the work stations without staff being present because of the chirping alarm.	2/26/2018	19	0.9%
Security	Observation logs interview reflexive with participant removed	Customers would rarely have time to access the work stations without staff being present because of the chirping alarm	3/3/2018	19	0.9%
Tech Support	Observation logs interview reflexive with participant removed	Customers would rarely have time to access the work stations without staff being present because of the chirping alarm	3/3/2018	19	0.9%
Security Negatives	Observation logs interview reflexive with participant removed	They need a procedure to remove employee access from the system when terminated	2/26/2018	13	0.6%
Social Engineering	Observation logs interview reflexive with participant removed	They need a procedure to remove employee access from the system when terminated	2/26/2018	13	0.6%
Tech Support Negatives	Observation logs interview reflexive with participant removed	They need a procedure to remove employee access from the system when terminated.	3/1/2018	13	0.6%
Security	Observation logs interview reflexive with participant removed	They need a procedure to remove employee access from the system when terminated	3/3/2018	13	0.6%
Tech Support	Observation logs interview reflexive with participant removed	They need a procedure to remove employee access from the system when terminated	3/3/2018	13	0.6%
Security Negatives	Observation logs interview reflexive with participant removed	All the practices for security are informal,	2/26/2018	7	0.3%
Security	Observation logs interview reflexive with participant removed	All the practices for security are informal, but this can be beneficiary when it is not necessary to keep a lot of procedures and policy documents updated	3/3/2018	27	1.2%
Cost	Observation logs interview reflexive with participant removed	All the practices for security are informal	2/26/2018	7	0.3%
Security positives	Observation logs interview reflexive with participant removed	not necessary to keep a lot of procedures and policy documents updated	2/26/2018	12	0.5%
Security	Observation logs interview reflexive with participant removed	The down side is forgetting. Maybe a short check-list would be good.	3/3/2018	13	0.6%
Security Negatives	Observation logs interview reflexive with participant removed	Did not see a document shredder	2/26/2018	6	0.3%
Social Engineering	Observation logs interview reflexive with participant removed	Did not see a document shredder. The dumpster is outside and easily accessible	2/26/2018	13	0.6%
Security	Observation logs interview reflexive with participant removed	Did not see a document shredder	3/3/2018	6	0.3%
Security	Observation logs interview reflexive with participant removed	The dumpster is outside and easily accessible, but I saw no evidence of any confidential documents discarded	3/3/2018	18	0.8%
Security Negatives	Observation logs interview reflexive with participant removed	dumpster is outside and easily accessible	2/26/2018	6	0.3%
Security positives	Observation logs interview reflexive with participant removed	no evidence of any confidential documents discarded	2/26/2018	8	0.4%
Security positives	Observation logs interview reflexive with participant removed	The third-party tech-support provided by the supplier for data base issues and updates	2/26/2018	16	0.7%

Social Engineering	Observation logs interview reflexive with participant removed	The third-party tech-support provided by the supplier	2/26/2018	10	0.5%
Tech Support Negatives	Observation logs interview reflexive with participant removed	The third-party tech-support provided by the supplier for data base issues and updates	3/1/2018	16	0.7%
Security	Observation logs interview reflexive with participant removed	The third-party tech-support provided by the supplier for data base issues and updates.	3/3/2018	16	0.7%
Tech Support	Observation logs interview reflexive with participant removed	The third-party tech-support provided by the supplier for data base issues and updates	3/3/2018	16	0.7%
Security Negatives	Observation logs interview reflexive with participant removed	What is the difference between social engineering and hacking? Now that I do not know	2/26/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	What is the difference between social engineering and hacking? Now that I do not know.	3/3/2018	15	0.7%
Security Negatives	Observation logs interview reflexive with participant removed	What do you think is the main way internet criminals access systems illegally? Through the internet connection (the participant is very uncertain on this)	2/26/2018	24	1.1%
Security	Observation logs interview reflexive with participant removed	What do you think is the main way internet criminals access systems illegally? Through the internet connection	3/3/2018	17	0.8%
Security positives	Observation logs interview reflexive with participant removed	Who do you call if you suspect your system compromised? My IT support guy	2/26/2018	16	0.7%
Tech Support Positives	Observation logs interview reflexive with participant removed	Who do you call if you suspect your system compromised? My IT support guy	3/1/2018	16	0.7%
Security	Observation logs interview reflexive with participant removed	Who do you call if you suspect your system compromised? My IT support guy	3/3/2018	16	0.7%
Tech Support	Observation logs interview reflexive with participant removed	Who do you call if you suspect your system compromised? My IT support guy	3/3/2018	16	0.7%
Security positives	Observation logs interview reflexive with participant removed	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	2/26/2018	17	0.8%
Security	Observation logs interview reflexive with participant removed	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/3/2018	17	0.8%
Tech Support	Observation logs interview reflexive with participant removed	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/3/2018	17	0.8%
Security positives	Observation logs interview reflexive with participant removed	Does he respond right away? Yes, that same day, usually within an hour or so.	2/26/2018	15	0.7%
Tech Support Positives	Observation logs interview reflexive with participant removed	Does he respond right away? Yes, that same day, usually within an hour or so.	3/1/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	Does he respond right away? Yes, that same day, usually within an hour or so.	3/3/2018	15	0.7%
Tech Support	Observation logs interview reflexive with participant removed	Does he respond right away? Yes, that same day, usually within an hour or so.	3/3/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	Who provides the tech support? The security software provider, it all comes under one package	3/3/2018	15	0.7%

Security positives	Observation logs interview reflexive with participant removed	Who provides the tech support? The security software provider, it all comes under one package.	2/26/2018	15	0.7%
Tech Support Positives	Observation logs interview reflexive with participant removed	Who provides the tech support? The security software provider, it all comes under one package	3/1/2018	15	0.7%
Tech Support	Observation logs interview reflexive with participant removed	Who provides the tech support? The security software provider, it all comes under one package.	3/3/2018	15	0.7%
Social Engineering	Observation logs interview reflexive with participant removed	Uh, probably like use a firewall and kind of limit the access to internet	2/26/2018	14	0.6%
Tech Support Positives	Observation logs interview reflexive with participant removed	Uh, probably like use a firewall and kind of limit the access to internet.	3/1/2018	14	0.6%
Security	Observation logs interview reflexive with participant removed	Uh, probably like use a firewall and kind of limit the access to internet	3/3/2018	14	0.6%
Tech Support	Observation logs interview reflexive with participant removed	Uh, probably like use a firewall and kind of limit the access to internet	3/3/2018	14	0.6%
Security positives	Observation logs interview reflexive with participant removed	probably like use a firewall and kind of limit the access to internet.	2/26/2018	13	0.6%
Security	Observation logs interview reflexive with participant removed	Well, like our business there’s not that much I dont think that anybody would use, you know, we dont have that much information actually on our system, but you know, there’s always the chance.	3/3/2018	38	1.7%
Security positives	Observation logs interview reflexive with participant removed	business there’s not that much I dont think that anybody would use, you know, we dont have that much information actually on our system, but you know	2/26/2018	30	1.4%
Security Negatives	Observation logs interview reflexive with participant removed	there’s not that much I dont think that anybody would use, you know, we dont have that much information actually on our system, but you know, there’s always the chance.	2/26/2018	34	1.5%
Security	Observation logs interview reflexive with participant removed	Large corporations have got more information on the systems, they’ve got a lot more credit card activity and stuff than we do so I think that probably that would be a bigger target than a small business.	3/3/2018	38	1.7%
Security Negatives	Observation logs interview reflexive with participant removed	, they’ve got a lot more credit card activity and stuff than we do so I think that probably that would be a bigger target than a small business.	2/26/2018	29	1.3%
Security positives	Observation logs interview reflexive with participant removed	they’ve got a lot more credit card activity and stuff than we do so I think that probably that would be a bigger target than a small business.	2/26/2018	29	1.3%
Social Engineering	Observation logs interview reflexive with participant removed	stuff than we do so I think that probably that would be a bigger target than a small business.	2/26/2018	19	0.9%
Security	Observation logs interview reflexive with participant removed	Uh, I’ve just heard of the ones on the big corporations, the small ones, you know, I dont think they have that much trouble with it	3/3/2018	28	1.3%
Social Engineering	Observation logs interview reflexive with participant removed	I’ve just heard of the ones on the big corporations, the small ones, you know, I dont think they have that much trouble with it.	2/26/2018	27	1.2%

Security positives	Observation logs interview reflexive with participant removed	the small ones, you know, I dont think they have that much trouble with it.	2/26/2018	16	0.7%
Security Negatives	Observation logs interview reflexive with participant removed	the small ones, you know, I dont think they have that much trouble with it.	2/26/2018	16	0.7%
Social Engineering	Observation logs interview reflexive with participant removed	I dont know what, you know, they would jump in there and try to get that you know, you hadn't thought about. You know, I dont know	2/26/2018	30	1.4%
Security Negatives	Observation logs interview reflexive with participant removed	I dont know what, you know, they would jump in there and try to get that you know, you hadn't thought about. You know, I dont know.	2/26/2018	30	1.4%
Security	Observation logs interview reflexive with participant removed	Uh, I would say probably the bigger corporations you would have more people in the computer and have a better chance of somebody getting something that they shouldn't have out of it.	3/3/2018	33	1.5%
Social Engineering	Observation logs interview reflexive with participant removed	I would say probably the bigger corporations you would have more people in the computer and have a better chance of somebody getting something that they shouldn't have out of it.	2/26/2018	32	1.5%
Social Engineering	Observation logs interview reflexive with participant removed	Well, somebody could walk by that's not an employee and can get into the system and get stuff out of it.	2/26/2018	22	1.0%
Tech Support Negatives	Observation logs interview reflexive with participant removed	Well, somebody could walk by that's not an employee and can get into the system and get stuff out of it.	3/1/2018	22	1.0%
Security	Observation logs interview reflexive with participant removed	Well, somebody could walk by that's not an employee and can get into the system and get stuff out of it.	3/3/2018	22	1.0%
Tech Support	Observation logs interview reflexive with participant removed	Well, somebody could walk by that's not an employee and can get into the system and get stuff out of it.	3/3/2018	22	1.0%
Security	Observation logs interview reflexive with participant removed	Uh, Well I think, you know, that if you make a password that somebody wouldn't think of you know, I think you would be Okay, but you dont want to use your uh, uh, address or something like that.	3/3/2018	41	1.9%
Tech Support	Observation logs interview reflexive with participant removed	Uh, Well I think, you know, that if you make a password that somebody wouldn't think of you know, I think you would be Okay, but you dont want to use your uh, uh, address or something like that.	3/3/2018	41	1.9%
Security positives	Observation logs interview reflexive with participant removed	but you dont want to use your uh, uh, address or something like that.	2/26/2018	15	0.7%
Security	Observation logs interview reflexive with participant removed	I think most of your businesses have got some kind of plan in effect some, uh kind of uh, uh, somebody that's watching to kind of keep the security up on it you know to keep from having these deals happen.	3/3/2018	42	1.9%
Tech Support	Observation logs interview reflexive with participant removed	I think most of your businesses have got some kind of plan in effect some, uh kind of uh, uh, somebody that's watching to kind of keep the security up on it you know to keep from having these deals happen.	3/3/2018	42	1.9%
Tech Support Positives	Observation logs interview reflexive with participant removed	think most of your businesses have got some kind of plan in effect some, uh kind of uh, uh, somebody that's watching to kind of keep the	3/1/2018	41	1.9%

		security up on it you know to keep from having these deals happen.			
Security positives	Observation logs interview reflexive with participant removed	somebody that’s watching to kind of keep the security up on it you know to keep from having these deals happen	2/26/2018	22	1.0%
Security positives	Observation logs interview reflexive with participant removed	Ours has got a wall on it and uhm, and, I’m not sure about the brand of the uh anti-virus	2/26/2018	23	1.0%
Tech Support Positives	Observation logs interview reflexive with participant removed	Ours has got a firewall on it and uhm, and, I’m not sure about the brand of the uh anti-virus.	3/1/2018	23	1.0%
Security	Observation logs interview reflexive with participant removed	Ours has got a firewall on it and uhm, and, I’m not sure about the brand of the uh anti-virus	3/3/2018	23	1.0%
Tech Support	Observation logs interview reflexive with participant removed	ours has got a firewall on it and uhm, and, I’m not sure about the brand of the uh anti-virus.	3/3/2018	23	1.0%
Social Engineering	Observation logs interview reflexive with participant removed	and, I’m not sure about the brand of the uh anti-virus	2/26/2018	13	0.6%
Security positives	Transcript revision for coding	Uh, probably like use a firewall and kind of limit the access to internet	3/1/2018	14	2.9%
Tech Support Positives	Transcript revision for coding	Uh, probably like use a firewall and kind of limit the access to internet.	3/1/2018	14	2.9%
Security Negatives	Transcript revision for coding	Well, like our business there’s not that much I dont think that anybody would use, you know, we dont have that much information actually on our system, but you know, there’s always the chance.	3/1/2018	38	7.8%
Social Engineering	Transcript revision for coding	Well, like our business there’s not that much I dont think that anybody would use, you know, we dont have that much information actually on our system, but you know, there’s always the chance.	3/1/2018	38	7.8%
Security Negatives	Transcript revision for coding	Large corporations have got more information on the systems, they’ve got a lot more credit card activity and stuff than we do so I think that probably that would be a bigger target than a small business.	3/1/2018	38	7.8%
Social Engineering	Transcript revision for coding	large corporations have got more information on the systems, they’ve got a lot more credit card activity and stuff than we do so I think that probably that would be a bigger target than a small business.	3/1/2018	38	7.8%
Security Negatives	Transcript revision for coding	Uh, I’ve just heard of the ones on the big corporations, the small ones, you know, I dont think they have that much trouble with it.	3/1/2018	28	5.8%
Social Engineering	Transcript revision for coding	Uh, I’ve just heard of the ones on the big corporations, the small ones, you know, I dont think they have that much trouble with it.	3/1/2018	28	5.8%
Social Engineering	Transcript revision for coding	I think that if somebody wants in the system they can get in and get what they want if, uh I dont think you’re going to be able to just totally stop it. If they want in, they’re going to get in. Uh, That I dont know, I dont know what, you know, they would jump in there and try to get that you know, you hadnt thought about. You know, I dont know.	3/1/2018	81	16.7%
Cost	Transcript revision for coding	think that if somebody wants in the system they can get in and get what they want if, uh I dont think you’re going to be able to just	3/1/2018	80	16.5%

		totally stop it. If they want in, they're going to get in. Uh, That I dont know, I dont know what, you know, they would jump in there and try to get that you know, you hadnt thought about. You know, I dont know.			
Security Negatives	Transcript revision for coding	think that if somebody wants in the system they can get in and get what they want if, uh I dont think you're going to be able to just totally stop it. If they want in, they're going to get in. Uh, That I dont know, I dont know what, you know, they would jump in there and try to get that you know, you hadn't thought about. You know, I dont know.	3/1/2018	80	16.5%
Social Engineering	Transcript revision for coding	Uh, I would say probably the bigger corporations you would have more people in the computer and have a better chance of somebody getting something that they shouldn't have out of it.	3/1/2018	33	6.8%
Cost	Transcript revision for coding	Well, somebody could walk by that's not an employee and can get into the system and get stuff out of it.	3/1/2018	22	4.5%
Security positives	Transcript revision for coding	Well, somebody could walk by that's not an employee and can get into the system and get stuff out of it.	3/1/2018	22	4.5%
Tech Support Negatives	Transcript revision for coding	Well, somebody could walk by that's not an employee and can get into the system and get stuff out of it.	3/1/2018	22	4.5%
Security positives	Transcript revision for coding	Uh, Well I think, you know, that if you make a password that somebody wouldn't think of you know, I think you would be Okay, but you dont want to use your uh, uh, address or something like that.	3/1/2018	41	8.4%
Security positives	Transcript revision for coding	I think most of your businesses have got some kind of plan in effect some, uh kind of uh, uh, somebody that's watching to kind of keep the security up on it you know to keep from having these deals happen.	3/1/2018	42	8.6%
Cost	Transcript revision for coding	think most of your businesses have got some kind of plan in effect some, uh kind of uh, uh, somebody that's watching to kind of keep the security up on it you know to keep from having these deals happen.	3/1/2018	41	8.4%
Security positives	Transcript revision for coding	Ours has got a firewall on it and uhm, and, I'm not sure about the brand of the uh anti-virus	3/1/2018	23	4.7%
Security Negatives	Transcript revision for coding	Ours has got a firewall on it and uhm, and, I'm not sure about the brand of the uh anti-virus.	3/1/2018	23	4.7%
Social Engineering	Transcript revision for coding	Ours has got a firewall on it and uhm, and, I'm not sure about the brand of the uh anti-virus.	3/1/2018	23	4.7%
Tech Support Negatives	Transcript revision for coding	Ours has got a firewall on it and uhm, and, I'm not sure about the brand of the uh anti-virus.	3/1/2018	23	4.7%
Tech Support Positives	Transcript revision for coding	Ours has got a firewall on it and uhm, and, I'm not sure about the brand of the uh anti-virus.	3/1/2018	23	4.7%
Security positives	Transcript revision for coding	Uh, monthly	3/1/2018	2	0.4%
Security Negatives	Transcript revision for coding	What is the difference between social engineering and hacking? Now that I do not know.	3/1/2018	15	3.1%
Social Engineering	Transcript revision for coding	What is the difference between social engineering and hacking? Now that I do not know.	3/1/2018	15	3.1%

Security Negatives	Transcript revision for coding	What do you think is the main way internet criminals access systems illegally? Through the internet connection	3/1/2018	17	3.5%
Social Engineering	Transcript revision for coding	What do you think is the main way internet criminals access systems illegally? Through the internet connection	3/1/2018	17	3.5%
Security positives	Transcript revision for coding	Who do you call if you suspect your system compromised? My IT support guy	3/1/2018	16	3.3%
Tech Support Positives	Transcript revision for coding	Who do you call if you suspect your system compromised? My IT support guy	3/1/2018	16	3.3%
Social Engineering	Transcript revision for coding	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/1/2018	17	3.5%
Security Negatives	Transcript revision for coding	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/1/2018	17	3.5%
Tech Support Negatives	Transcript revision for coding	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/1/2018	17	3.5%
Tech Support Positives	Transcript revision for coding	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/1/2018	17	3.5%
Security positives	Transcript revision for coding	Does he respond right away? Yes, that same day, usually within an hour or so.	3/1/2018	15	3.1%
Tech Support Positives	Transcript revision for coding	Does he respond right away? Yes, that same day, usually within an hour or so.	3/1/2018	15	3.1%
Cost	Transcript revision for coding	Who provides the tech support? The security software provider, it all comes under one package.	3/1/2018	15	3.1%
Security positives	Transcript revision for coding	Who provides the tech support? The security software provider, it all comes under one package	3/1/2018	15	3.1%
Security Negatives	Transcript revision for coding	Who provides the tech support? The security software provider, it all comes under one package. (he gave me the name of the company, but I did not bother to write it down since I cannot use it anyway)	3/1/2018	38	7.8%
Social Engineering	Transcript revision for coding	Who provides the tech support? The security software provider, it all comes under one package.	3/1/2018	15	3.1%
Tech Support Negatives	Transcript revision for coding	Who provides the tech support? The security software provider, it all comes under one package.	3/1/2018	15	3.1%
Tech Support Positives	Transcript revision for coding	Who provides the tech support? The security software provider, it all comes under one package.	3/1/2018	15	3.1%

Appendix O: Cost Emergent Theme

Code	Method(s)	Text	Date	Words	%Words
Cost	Observation logs reflexive notes member checking	. Printer is a hole fed dot matrix printer for printing hardcopy receipts	2/26/2018	12	0.5%
Cost	Observation logs interview member checking	All the practices for security are informal	2/26/2018	7	0.3%
Cost	Observation logs reflexive notes and member checking	Dot matrix printer	2/26/2018	3	0.1%
Cost	Observation logs reflexive and member checking	I noticed that the can not print when talking on the phone (DSL)	2/26/2018	13	0.6%
Cost	Reflexive notes and member checking	No scanning system point and click system for receipt print out	2/26/2018	11	0.5%
Cost	Observation logs interview reflexive notes and member checking	No wi-fi	2/26/2018	3	0.1%
Cost	Observation logs interview reflexive and member checking	No Wi-Fi at the facility. Strictly DSL	2/26/2018	8	0.4%
Cost	Observation logs interview and member checking	phone and electrical egress to the building is under ground with no exterior access	2/26/2018	14	0.6%
Cost	Observation logs reflexive and member checking	Phone operation prevents printer operation	2/26/2018	5	0.2%
Cost	Observation logs interview and member checking	The absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall	2/26/2018	23	1.0%
Cost	Observation logs member checking	Wi-fi scan produced no results	2/26/2018	6	0.3%
Cost	Observation logs interview and member checking	Work stations (three) are Dell computers	2/26/2018	6	0.3%

Appendix P: Security Emergent Theme

Code	Methods(s)	Text	Date	Words	%Words
Security	Observation logs interview reflexive notes and member checking	(no wi-fi signals within range)	3/3/2018	6	0.3%
Security	Observation logs reflexive and member checking	. Customer can access most of the merchandise in the front of the store for shopping.	3/3/2018	15	0.7%
Security	interview	. I noted that there are a lot of county employees making purchases on store credit. There are two possible charges- to the truck or to the shop.	3/3/2018	27	1.2%
Security	Observation logs reflexive and member checking	. Magnetic security devices on three bay doors as well as the front entry doors	3/3/2018	14	0.6%
Security	Observation logs interview member checking	. Plumbing, phone and electrical egress to the building is under ground with no exterior access.	3/3/2018	15	0.7%
Security	Observation logs interview and member checking	access to the system requires a password and user name	3/3/2018	11	0.5%
Security	Observation logs and member checking	Activity at the work stations recorded	3/3/2018	8	0.4%
Security	Observation logs and member checking	Adequate fluorescent lighting	3/3/2018	3	0.1%
Security	Observation logs interview and member checking	Alarm system connected to a motion and magnetic interlock system that activates an alarm. All service connections are inside the building	3/3/2018	22	1.0%
Security	Observation logs and member checking	alarm system is good magnetic interlocks on doors Like that laptop stolen was just an opportunity theft and not specifically sought out for info	3/3/2018	26	1.2%
Security	Observation logs and member checking	All the practices for security are informal, but this can be beneficiary when it is not necessary to keep a lot of procedures and policy documents updated	3/3/2018	27	1.2%
Security	Observation logs member checking	and the time of the activity which would be enough to provide any information for an inquiry.	3/3/2018	17	0.8%
Security	Observation logs interview member checking	anti-virus protection that updated monthly and maintained by third party tech support.	3/3/2018	14	0.6%
Security	Observation logs interview member checking	AT&T provides the DSL service and phone. Line service	3/3/2018	10	0.5%
Security	Observation logs member checking	building stands approximately 200 feet from the two-lane main county thoroughfare	3/3/2018	12	0.5%
Security	Observation logs member checking	but no details of work station would be available with the exception of the person at the station	3/3/2018	18	0.8%
Security	Observation logs interview member checking	Cable and phone	3/3/2018	3	0.1%
Security	Observation logs reflexive and member checking	Cameras and motion detector well placed (see security map	3/3/2018	9	0.4%
Security	Observation logs interview reflexive and member checking	Customers would rarely have time to access the work stations without staff being present because of the chirping alarm	3/3/2018	19	0.9%
Security	Observation logs reflexive notes and member checking	Did not see a document shredder	3/3/2018	6	0.3%

Security	interview and member checking	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/3/2018	17	0.8%
Security	interview and member checking	Does he respond right away? Yes, that same day, usually within an hour or so.	3/3/2018	15	0.7%
Security	Observation logs interview reflexive and member checking	Doors that laptop stolen was just an opportunity theft and not specifically sought out for info	3/3/2018	19	0.9%
Security	Observation logs member checking	farmers swapping stories and gossip about each other	3/3/2018	8	0.4%
Security	Observation logs interview member checking	For a fuel dispenser costs almost $500.00.	3/3/2018	8	0.4%
Security	Observation logs interview reflexive and member checking	the absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall.	3/3/2018	23	1.0%
Security	Observation logs interview and member checking	The participant is on a first name basis with all of the patrons with the exception of a scant few.	3/3/2018	20	0.9%
Security	Observation logs interview reflexive notes and member checking	the Wi-Fi signal tested 5 times at random intervals with no signal detected.	3/3/2018	15	0.7%
Security	Observation logs interview and member checking	I also learned that some farmers are very superstitious and will not perform some farm activities if the signs are not right. (Full moon etc.)	3/3/2018	25	1.1%
Security	Observation logs interview reflexive and member checking	I noted that if any work stations are left unattended	3/3/2018	10	0.5%
Security	interview and member checking	I think most of your businesses have got some kind of plan in effect some, uh kind of uh, uh, somebody that's watching to kind of keep the security up on it you know to keep from having these deals happen.	3/3/2018	42	1.9%
Security	Observation logs interview member checking	in other words, no useful information or any information of value).	3/3/2018	12	0.5%
Security	Observation logs interview reflexive and member checking	ethernet internet service by separate line such that there is no interference during transaction processing	3/3/2018	16	0.7%
Security	Observation logs interview member checking	Intruders would likely be after merchandise and electronic equipment would be opportunity	3/3/2018	12	0.5%
Security	interview reflexive and member checking	It is an expectation that the laptop stolen for use and not data because of the nature of the recovery	3/3/2018	19	0.9%
Security	Observation logs interview reflexive and member checking	password may need a shorter time out.	3/3/2018	8	0.4%
Security	interview and member checking	Large corporations have got more information on the systems, they've got a lot more credit card activity and stuff than we do so I think that probably that would be a bigger target than a small business.	3/3/2018	38	1.7%
Security	Observation logs and member checking	Lot of activity from uniform service. Changing out uniforms and replacing carpets.	3/3/2018	12	0.5%
Security	Observation logs member checking	makes custom hydraulic hoses which takes some time with work stations unattended	3/3/2018	12	0.5%
Security	Observation logs and member checking	monitored by security video camera at the rear of the store.	3/3/2018	13	0.6%
Security	Observation logs interview reflexive notes and member checking	noticed that they cannot print when talking on the phone (DSL)	3/3/2018	12	0.5%

Security	Observation logs interview member checking	Observed a wide-angle security camera attached to the drop ceiling on the back-left corner from the entrance of the building.	3/3/2018	22	1.0%
Security	Observation logs interview and member checking	Observed two work station CRTS with keyboards on customer service counter	3/3/2018	11	0.5%
Security	Observation logs and member checking	on a first name basis with the owner,	3/3/2018	8	0.4%
Security	interview and member checking	One instance a lap-top stolen with employee personal information taken	3/3/2018	11	0.5%
Security	interview and member checking	Ours has got a firewall on it and uhm, and, I'm not sure about the brand of the uh anti-virus	3/3/2018	23	1.0%
Security	Observation logs interview reflexive and member checking	Phone operation prevents printer operation	3/3/2018	5	0.2%
Security	Observation logs and member checking	power supply generator	3/3/2018	2	0.1%
Security	Observation logs reflexive and member checking	Printer is a hole fed dot matrix printer for printing hardcopy receipts.	3/3/2018	12	0.5%
Security	interview and member checking	Procedure changed to not leave lap-top overnight. The laptop recovered.	3/3/2018	12	0.5%
Security	Observation logs and member checking	Receipts discarded in waste receptacle upon payment	3/3/2018	8	0.4%
Security	interview and member checking	relies mostly on the third party (out-sourced) tech support for computer security and protection.	3/3/2018	15	0.7%
Security	Observation logs member checking	security layout	3/3/2018	2	0.1%
Security	Observation logs interview reflexive and member checking	Smart phone Wi-fi scan produced no results	3/3/2018	8	0.4%
Security	Observation logs member checking	Some merchandise can be very expensive	3/3/2018	6	0.3%
Security	Observation logs interview reflexive and member checking	Sometimes employees indisposed for long periods of time and unable to monitor the work stations	3/3/2018	17	0.8%
Security	Observation logs interview member checking	states that 98% are farmers.	3/3/2018	5	0.2%
Security	Observation logs interview and member checking	store inventory can be accessed on-line. No scanning system point and click system for receipt print out	3/3/2018	18	0.8%
Security	Observation logs member checking	Store walls lined with product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door	3/3/2018	23	1.0%
Security	Observation logs interview reflexive and member checking	Strictly DSL	3/3/2018	2	0.1%
Security	Observation logs interview reflexive and member checking	tthe business internet and phone activity is through the DSL carrier only.	3/3/2018	13	0.6%
Security	Observation logs interview member checking	The building is metal construction on a concrete slab.	3/3/2018	9	0.4%
Security	Observation logs interview and member checking	The building surrounded on three sides by a soy bean field.	3/3/2018	12	0.5%
Security	Observation logs interview reflexive and member checking	The camera covers the entire store including the counter work stations. Activity on the work stations not observed, but a person using the system can be and a date and time established as to when a person is at the workstation.	3/3/2018	44	2.0%
Security	Observation logs interview and member checking	The down side is forgetting. Maybe a short check-list would be good.	3/3/2018	13	0.6%

Security	Observation logs interview and member checking	The dumpster is outside and easily accessible, but I saw no evidence of any confidential documents discarded	3/3/2018	18	0.8%
Security	Observation logs member checking	The exterior of the building is corrugated steel construction with about a 20-degree pitch roof with plumbing and heating vents only	3/3/2018	22	1.0%
Security	interview and member checking	He has indicated that he is aware of the necessity of a strong password.	3/3/2018	14	0.6%
Security	interview and member checking	The laptop recovered and being used by an acquaintance of the thief.	3/3/2018	14	0.6%
Security	Observation logs and member checking	The main floor of the store divided three shelves about six feet high and double sided with the circular displays arranged around the perimeter	3/3/2018	25	1.1%
Security	Observation logs interview member checking	The nearest cell tower is less than a half mile away	3/3/2018	11	0.5%
Security	Observation logs interview member checking	the potential still exists for retaliation from disgruntled customers over money or merchandise dissatisfaction	3/3/2018	14	0.6%
Security	interview and member checking	The security video recording device is located out of sight and disguised by covered by an empty cardboard container giving it the appearance of regular store merchandise.	3/3/2018	29	1.3%
Security	Observation logs reflexive notes and member checking	The shelves dividing the main floor contain plumbing, electrical painting, body repair brackets and assorted brackets and fluids and chemicals, safety equipment, light bulbs, etc.	3/3/2018	25	1.1%
Security	Interview and member checking	The third-party tech-support provided by the supplier for data base issues and updates.	3/3/2018	16	0.7%
Security	Observation logs member checking	Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches.	3/3/2018	57	2.6%
Security	Observation logs reflexive notes and member checking	There are customer store credits but only the purchase receipts stored for records. No billing, customer or payment information kept in-house	3/3/2018	24	1.1%
Security	Observation logs reflexive notes and member checking	There is an audible chirping thru out the facility when the front door is opened to alert staff of an entry	3/3/2018	21	1.0%
Security	Observation logs member checking	There is standard emergency lighting and exit signs t activated by an emergency generator.	3/3/2018	16	0.7%
Security	interview and member checking	they have had three break-ins in the 19 years that have been in business	3/3/2018	15	0.7%
Security	Observation logs reflexive notes and member checking	They need a procedure to remove employee access from the system when terminated	3/3/2018	13	0.6%
Security	interview and member checking	Uh, I would say probably the bigger corporations you would have more people in the computer and have a better chance of somebody getting something that they shouldn't have out of it.	3/3/2018	33	1.5%
Security	interview and member checking	Uh, I've just heard of the ones on the big corporations, the small ones, you know, I dont think they have that much trouble with it	3/3/2018	28	1.3%
Security	interview and member checking	Uh, probably like use a firewall and kind of limit the access to internet	3/3/2018	14	0.6%

Security	interview and member checking	Uh, Well I think, you know, that if you make a password that somebody wouldn't think of you know, I think you would be Okay, but you dont want to use your uh, uh, address or something like that.	3/3/2018	41	1.9%
Security	Observation logs interview reflexive and member checking	Using dedicated DOT Matrix printer to print receipts.	3/3/2018	8	0.4%
Security	Observation logs member checking	We worked in back putting away stock	3/3/2018	7	0.3%
Security	interview and member checking	Well, like our business there's not that much I dont think that anybody would use, you know, we dont have that much information actually on our system, but you know, there's always the chance.	3/3/2018	38	1.7%
Security	interview and member checking	Well, somebody could walk by that's not an employee and can get into the system and get stuff out of it.	3/3/2018	22	1.0%
Security	interview and member checking	What do you think is the main way internet criminals access systems illegally? Through the internet connection	3/3/2018	17	0.8%
Security	interview and member checking	What do you think is the main way internet criminals access systems illegally? Through the internet connection	3/3/2018	17	0.8%
Security	interview and member checking	What is the difference between social engineering and hacking? Now that I do not know.	3/3/2018	15	0.7%
Security	interview and member checking	Who do you call if you suspect your system compromised? My IT support guy	3/3/2018	16	0.7%
Security	interview and member checking	Who provides the tech support? The security software provider, it all comes under one package.	3/3/2018	15	0.7%
Security	Observation logs interview reflexive and member checking	Work stations (three) are Dell computers with a firewall	3/3/2018	9	0.4%
Security	Observation logs interview reflexive and member checking	Work stations have a password timer	3/3/2018	6	0.3%
Security	Observation logs and member checking	(customer traffic and phone calls are heaviest early in the morning).	3/3/2018	11	0.5%
Security	Observation logs interview reflexive and member checking	(no wi-fi signals within range)	3/3/2018	6	0.3%
Security	Observation logs interview and member checking	. Customer can access most of the merchandise in the front of the store for shopping.	3/3/2018	15	0.7%
Security	Observation logs reflexive notes and member checking	. Door alert goes off when customers enter and leave (chirping & tweeting sounds).	3/3/2018	12	0.5%
Security	Observation logs interview reflexive and member checking	. Magnetic security devices on three bay doors as well as the front entry doors	3/3/2018	14	0.6%
Security	Observation logs interview reflexive and member checking	. Plumbing, phone and electrical egress to the building is under ground with no exterior access.	3/3/2018	15	0.7%
Security	Observation logs interview and member checking	access to the system requires a password and user name	3/3/2018	11	0.5%

Security	Observation logs interview reflexive and member checking	Activity at the work stations recorded	3/3/2018	8	0.4%
Security	Observation logs interview reflexive and member checking	Adequate fluorescent lighting	3/3/2018	3	0.1%
Security	Observation logs interview reflexive and member checking	Alarm system connected to a motion and magnetic interlock system that activates an alarm. All service connections are inside the building	3/3/2018	22	1.0%
Security	Observation logs interview reflexive and member checking	alarm system is good magnetic interlocks on doors Like that laptop stolen was just an opportunity theft and not specifically sought out for info	3/3/2018	26	1.2%
Security	Observation logs and member checking	All the practices for security are informal, but this can be beneficiary when it is not necessary to keep a lot of procedures and policy documents updated	3/3/2018	27	1.2%
Security	Observation logs interview and member checking	Date and the time of the activity which would be enough to provide any information for an inquiry.	3/3/2018	17	0.8%
Security	interview and member checking	anti-virus protection that updated monthly and maintained by third party tech support.	3/3/2018	14	0.6%
Security	interview and member checking	AT&T provides the DSL service and phone. Line service	3/3/2018	10	0.5%
Security	Observation logs reflexive and member checking	but no details of work station would be available with the exception of the person at the station	3/3/2018	18	0.8%
Security	Observation logs interview reflexive and member checking	Cameras and motion detector well placed (see security map)	3/3/2018	9	0.4%
Security	Observation logs interview and member checking	Customers would rarely have time to access the work stations without staff being present because of the chirping alarm	3/3/2018	19	0.9%
Security	Observation logs interview reflexive notes and member checking	Did not see a document shredder	3/3/2018	6	0.3%
Security	interview reflexive and member checking	Does he do all the IT support services like trouble shooting? Yes, we just e-mail him	3/3/2018	17	0.8%
Security	Observation logs member checking	farmers swapping stories and gossip about each other	3/3/2018	8	0.4%
Security	Observation logs interview member checking	For a fuel dispenser costs almost $500.00.	3/3/2018	8	0.4%
Security	Observation logs interview reflexive notes and member checking	The absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall.	3/3/2018	23	1.0%
Security	Observation logs interview and member checking	he participant is on a first name basis with all of the patrons with the exception of a scant few.	3/3/2018	20	0.9%
Security	Observation logs interview and member checking	The Wi-Fi signal tested 5 times at random intervals with no signal detected.	3/3/2018	15	0.7%
Security	Observation logs interview and member checking	I also learned that some farmers are very superstitious and will not perform some farm activities if the signs are not right. (Full moon etc.)	3/3/2018	25	1.1%
Security	Observation logs interview reflexive notes and member checking	I noted that if any work stations are left unattended	3/3/2018	10	0.5%
Security	Observation logs interview reflexive and member checking	I think most of your businesses have got some kind of plan in effect some, uh kind of uh, uh, somebody that's watching to kind of	3/3/2018	42	1.9%

Security	Observation logs and member checking	keep the security up on it you know to keep from having these deals happen. in other words, no useful information or any information of value). R	3/3/2018	12	0.5%
Security	Observation logs interview reflexive notes and member checking	ethernet internet service by separate line such that there is no interference during transaction processing	3/3/2018	16	0.7%
Security	Observation logs interview and member checking	Intruders would likely be after merchandise and electronic equipment would be opportunity	3/3/2018	12	0.5%
Security	interview reflexive notes and member checking	It is an expectation that the laptop stolen for use and not data because of the nature of the recovery	3/3/2018	19	0.9%
Security	Observation logs member checking	password may need a shorter time out.	3/3/2018	8	0.4%
Security	Observation logs interview and member checking	Large corporations have got more information on the systems, they've got a lot more credit card activity and stuff than we do so I think that probably that would be a bigger target than a small business.	3/3/2018	38	1.7%
Security	Observation logs member checking	Lot of activity from uniform service. Changing out uniforms and replacing carpets.	3/3/2018	12	0.5%
Security	Observation logs interview reflexive and member checking	makes custom hydraulic hoses which takes some time with work stations unattended	3/3/2018	12	0.5%
Security	Observation logs interview reflexive and member checking	monitored by security video camera at the rear of the store.	3/3/2018	13	0.6%
Security	Observation logs interview reflexive and member checking	No Wi-Fi at the facility	3/3/2018	6	0.3%
Security	Observation logs interview reflexive and member checking	No wi-fi. Dot matrix printer.	3/3/2018	6	0.3%
Security	Observation logs interview reflexive and member checking	noticed that the can not print when talking on the phone (DSL	3/3/2018	12	0.5%
Security	Observation logs interview reflexive and member checking	Observed a wide-angle security camera attached to the drop ceiling on the back-left corner from the entrance of the building.	3/3/2018	22	1.0%
Security	Observation logs and member checking	Observed two work station CRTS with keyboards on customer service counter	3/3/2018	11	0.5%
Security	Observation logs interview member checking	on a first name basis with the owner,	3/3/2018	8	0.4%
Security	interview member checking	One instance a lap-top with employee personal information taken	3/3/2018	11	0.5%
Security	interview and member checking	Ours has got a firewall on it and uhm, and, I'm not sure about the brand of the uh anti-virus	3/3/2018	23	1.0%
Security	Observation logs interview reflexive notes and member checking	Phone operation prevents printer operation	3/3/2018	5	0.2%
Security	Observation logs interview member checking	power supply	3/3/2018	2	0.1%
Security	Observation logs interview reflexive and member checking	Printer is a hole fed dot matrix printer for printing hardcopy receipts.	3/3/2018	12	0.5%
Security	interview and member checking	Procedure changed to not leave lap-top overnight. The laptop recovered.	3/3/2018	12	0.5%
Security	Observation logs interview reflexive notes and member checking	Receipts discarded in waste receptacle upon payment	3/3/2018	8	0.4%

Security	Observation logs interview reflexive and member checking	relies mostly on the third party (out-sourced) tech support for computer security and protection.	3/3/2018	15	0.7%
Security	Observation logs interview reflexive notes and member checking	security layout	3/3/2018	2	0.1%
Security	Observation logs interview reflexive and member checking	Smart phone Wi-fi scan produced no results	3/3/2018	8	0.4%
Security	Observation member checking	Some merchandise can be very expensive	3/3/2018	6	0.3%
Security	Observation member checking	Sometimes employees indisposed for long periods of time and unable to monitor the work stations	3/3/2018	17	0.8%
Security	interview and member checking	states that 98% are farmers.	3/3/2018	5	0.2%
Security	Observation logs and member checking	store inventory can be accessed on-line. No scanning system point and click system for receipt print out	3/3/2018	18	0.8%
Security	Observation logs reflexive notes and member checking	Store walls lined with product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door	3/3/2018	23	1.0%
Security	Observation logs interview reflexive and member checking	Strictly DSL	3/3/2018	2	0.1%
Security	Observation logs interview reflexive notes and member checking	the business internet and phone activity is through the DSL carrier only.	3/3/2018	13	0.6%
Security	Observation logs interview reflexive notes and member checking	The building is metal construction on a concrete slab.	3/3/2018	9	0.4%
Security	Observation member checking	The building surrounded on three sides by a soy bean field.	3/3/2018	12	0.5%
Security	Observation logs interview reflexive and member checking	The camera covers the entire store including the counter work stations. Activity on the work stations not observed, but a person using the system can be and a date and time established as to when a person is at the workstation.	3/3/2018	44	2.0%
Security	Observation logs reflexive notes and member checking	The down side is forgetting. Maybe a short check-list would be good.	3/3/2018	13	0.6%
Security	Observation logs reflexive notes and member checking	The dumpster is outside and easily accessible, but I saw no evidence of any confidential documents discarded	3/3/2018	18	0.8%
Security	Observation logs member checking	The exterior of the building is corrugated steel construction with about a 20-degree pitch roof with plumbing and heating vents only	3/3/2018	22	1.0%
Security	interview and member checking	The participant has indicated that he is aware of the necessity of a strong password.	3/3/2018	14	0.6%
Security	interview and member checking	The laptop recovered and being used by an acquaintance of the thief.	3/3/2018	14	0.6%
Security	Observation logs reflexive notes and member checking	The main floor of the store divided three shelves about six feet high and double sided with the circular displays arranged around the perimeter	3/3/2018	25	1.1%
Security	Observation logs interview and member checking	The nearest cell tower is less than a half mile away	3/3/2018	11	0.5%
Security	Observation logs interview member checking	the potential still exists for retaliation from disgruntled customers over money or merchandise dissatisfaction	3/3/2018	14	0.6%

Security	Observation logs interview and member checking	The security video recording device is located out of sight and disguised by covered by an empty cardboard container giving it the appearance of regular store merchandise.	3/3/2018	29	1.3%
Security	Observation logs interview reflexive notes and member checking	The shelves dividing the main floor contain plumbing, electrical painting, body repair brackets and assorted brackets and fluids and chemicals, safety equipment, light bulbs, etc.	3/3/2018	25	1.1%
Security	Observation logs interview reflexive and member checking	The third-party tech-support provided by the supplier for data base issues and updates.	3/3/2018	16	0.7%
Security	Observation logs reflexive notes and member checking	Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches.	3/3/2018	57	2.6%
Security	Observation logs interview reflexive and member checking	There are customer store credits but only the purchase receipts stored for records. No billing, customer or payment information kept in-house	3/3/2018	24	1.1%
Security	Observation logs interview reflexive and member checking	There is an audible chirping thru out the facility when the front door is opened to alert staff of an entry	3/3/2018	21	1.0%
Security	Observation logs interview and member checking	There is standard emergency lighting and exit signs t activated by an emergency generator.	3/3/2018	16	0.7%
Security	interview and member checking	they have had three break-ins in the 19 years that have been in business	3/3/2018	15	0.7%
Security	Observation logs reflexive and member checking	They need a procedure to remove employee access from the system when terminated	3/3/2018	13	0.6%
Security	interview and member checking	Uh, I would say probably the bigger corporations you would have more people in the computer and have a better chance of somebody getting something that they shouldn't have out of it.	3/3/2018	33	1.5%
Security	Interview and member checking	Uh, I've just heard of the ones on the big corporations, the small ones, you know, I dont think they have that much trouble with it	3/3/2018	28	1.3%
Security	interview and member checking	Uh, probably like use a firewall and kind of limit the access to internet	3/3/2018	14	0.6%
Security	interview and member checking	Uh, Well I think, you know, that if you make a password that somebody wouldn't think of you know, I think you would be Okay, but you dont want to use your uh, uh, address or something like that.	3/3/2018	41	1.9%
Security	Observation reflexive notes and member checking	Using dedicated DOT Matrix printer to print receipts.	3/3/2018	8	0.4%
Security	Observation logs and member checking	We worked in back putting away stock	3/3/2018	7	0.3%
Security	interview and member checking	Well, like our business there's not that much I dont think that anybody would use, you know, we dont have that much information actually on our system, but you know, there's always the chance.	3/3/2018	38	1.7%
Security	interview and member checking	Well, somebody could walk by that's not an employee and can get into the system and get stuff out of it.	3/3/2018	22	1.0%

Security	interview and member checking	What do you think is the main way internet criminals access systems illegally? Through the internet connection	3/3/2018	17	0.8%
Security	Observation logs interview reflexive and member checking	What do you think is the main way internet criminals access systems illegally? Through the internet connection	3/3/2018	17	0.8%
Security	interview and member checking	What is the difference between social engineering and hacking? Now that I do not know.	3/3/2018	15	0.7%
Security	interview and member checking	What is the difference between social engineering and hacking? Now that I do not know.	3/3/2018	15	0.7%
Security	interview and member checking	Who do you call if you suspect your system compromised? My IT support guy	3/3/2018	16	0.7%
Security	Interview and member checking	Who do you call if you suspect your system compromised? My IT support guy	3/3/2018	16	0.7%
Security	interview and member checking	Who provides the tech support? The security software provider, it all comes under one package.	3/3/2018	15	0.7%
Security	interview and member checking	Who provides the tech support? The security software provider, it all comes under one package	3/3/2018	15	0.7%
Security	Observation logs reflexive notes and member checking	Work stations (three) are Dell computers with a firewall	3/3/2018	9	0.4%
Security	Observation logs interview reflexive notes and member checking	Work stations have a password timer	3/3/2018	6	0.3%

Appendix Q: Social Engineering Emergent Theme

Code	Method(s)	Text	Date	Words	%Words
Social Engineering	Observation logs interview reflexive and member checking	9:00-10:00- Work stations (three) are Dell computers with a firewall with anti-virus protection updated monthly and maintained by third party tech support. relies mostly on the third party (out-sourced) tech support for computer security and protection	2/26/2018	43	2.0%
Social Engineering	Observation logs interview reflexive and member checking	access to the system requires a password and user name	2/26/2018	11	0.5%
Social Engineering	Observation logs reflexive notes and member checking	Activity on the work stations not observed	2/26/2018	8	0.4%
Social Engineering	Observation logs interview Reflexive note and member checking	All service connections are inside the building	2/26/2018	7	0.3%
Social Engineering	interview and member checking	and, I'm not sure about the brand of the uh anti-virus	2/26/2018	13	0.6%
Social Engineering	Observation logs reflexive notes and member checking	but the business internet and phone activity is through the DSL carrier only.	2/26/2018	13	0.6%
Social Engineering	Observation logs reflexive and member checking	customer traffic and phone calls are heaviest early in the morning	2/26/2018	11	0.5%
Social Engineering	Observation logs interview and member checking	Customers would rarely have time to access the work stations without staff being present because of the chirping alarm	2/26/2018	19	0.9%
Social Engineering	Observation logs reflexive and member checking	Did not see a document shredder. The dumpster is outside and easily accessible	2/26/2018	13	0.6%
Social Engineering	Observation logs interview and member checking	expressed that tech support is a third-party IT rep from the supplier.	2/26/2018	13	0.6%
Social Engineering	Observation logs reflexive notes and member checking	Heavy customer traffic	2/26/2018	3	0.1%
Social Engineering	interview and member checking	I dont know what, you know, they would jump in there and try to get that you know, you hadn't thought about. You know, I dont know	2/26/2018	30	1.4%

Social Engineering	Observation logs interview reflexive and member checking	I noticed that the can not print when talking on the phone (DSL). No wi-fi.	2/26/2018	16	0.7%
Social Engineering	interview and member checking	I would say probably the bigger corporations you would have more people in the computer and have a better chance of somebody getting something that they shouldn’t have out of it.	2/26/2018	32	1.5%
Social Engineering	interview and member checking	I’ve just heard of the ones on the big corporations, the small ones, you know, I dont think they have that much trouble with it.	2/26/2018	27	1.2%
Social Engineering	Observation logs reflexive and member checking	no details of work station would be available with the exception of the person at the station	2/26/2018	17	0.8%
Social Engineering	interview and member checking	One instance a lap-top with employee personal information taken	2/26/2018	11	0.5%
Social Engineering	Observation logs interview reflexive and member checking	receipts discarded in waste receptacle upon payment.	2/26/2018	8	0.4%
Social Engineering	Observation logs reflexive and member checking	Small talk with farmers swapping stories and gossip about each other	2/26/2018	11	0.5%
Social Engineering	Observation logs reflexive and member checking	Store walls lined with product that begins with a welding equipment display (tips, wire, helmets) at the entrance (left of the door). Then wiper blades to the right of the entrance, then specialty tools (brakes, engine repair etc.) and a discount tool bin. Then a soda machine and then higher end tools on the wall after the soda machine and around behind the counter. There are eight revolving displays with accessories and nuts and bolts as well as wrenches	2/26/2018	80	3.6%
Social Engineering	interview and member checking	stuff than we do so I think that probably that would be a bigger target than a small business.	2/26/2018	19	0.9%
Social Engineering	Observation logs reflexive and member checking	The main floor of the store divided three shelves about six feet high and double sided with the circular displays arranged around the perimeter.	2/26/2018	25	1.1%
Social Engineering	Observation logs interview reflexive and member checking	The participant is on a first name basis with all of the patrons with the exception of a scant few.	2/26/2018	20	0.9%
Social Engineering	Observation logs interview reflexive	the potential still exists for retaliation from disgruntled customers over	2/26/2018	28	1.3%

	and member checking	money or merchandise dissatisfaction. Some merchandise can be very expensive. For a fuel dispenser costs almost $500.00.			
Social Engineering	interview and member checking	The rep is located off site and offers help desk type support but will come in as required	2/26/2018	18	0.8%
Social Engineering	Observation logs interview reflexive and member checking	The third-party tech-support provided by the supplier	2/26/2018	10	0.5%
Social Engineering	Observation logs interview and member checking	There are customer store credits	2/26/2018	5	0.2%
Social Engineering	interview and member checking	they have had three break-ins in the 19 years that have been in business	2/26/2018	15	0.7%
Social Engineering	Observation logs i reflexive and member checking	They need a procedure to remove employee access from the system when terminated	2/26/2018	13	0.6%
Social Engineering	interview and member checking	Uh, probably like use a firewall and kind of limit the access to internet	2/26/2018	14	0.6%
Social Engineering	interview and member checking	Well, somebody could walk by that's not an employee and can get into the system and get stuff out of it.	2/26/2018	22	1.0%
Social Engineering	interview and member checking	What do you think is the main way internet criminals access systems illegally? Through the internet connection	2/26/2018	17	0.8%
Social Engineering	interview and member checking	What is the difference between social engineering and hacking? Now that I do not know.	2/26/2018	15	0.7%
Social Engineering	interview and member checking	Who do you call if you suspect your system compromised? My IT support guy	2/26/2018	16	0.7%
Social Engineering	Observation logs interview reflexive and member checking	Work stations have a password timer, but it may need a shorter time out. Sometimes employees indisposed for long periods of time and unable to monitor the work stations.	2/26/2018	31	1.4%
Social Engineering	Observation logs interview reflexive and member checking	work stations unattended	2/26/2018	3	0.1%
Social Engineering	Observation logs interview reflexive and member checking	9:00-10:00- Work stations (three) are Dell computers with a firewall with anti-virus protection that updated monthly and maintained by third party tech support. relies mostly on the third party (out-sourced) tech support for computer security and protection	2/26/2018	43	3.2%

Appendix R: Tech Support Emergent Theme

Code	Method(s)	Text	Date	%Words	
Tech Support	Observation logs interview reflexive and member checking	Activity at the work stations recorded	3/3/2018	8	0.4%
Tech Support	Observation logs reflexive notes and member checking	Alarm system connected to a motion and magnetic interlock system that activates an alarm	3/3/2018	15	0.7%
Tech Support	Observation logs reflexive notes and member checking	alarm system is good magnetic interlocks on doors Like that laptop stolen was just an opportunity theft and not specifically sought out for info	3/3/2018	26	1.2%
Tech Support	Observation logs interview reflexive and member checking	All service connections are inside the building	3/3/2018	7	0.3%
Tech Support	Observation logs interview reflexive and member checking	AT&T provides the DSL service and phone	3/3/2018	8	0.4%
Tech Support	Observation logs interview reflexive and member checking	business internet and phone activity is through the DSL carrier only.	3/3/2018	11	0.5%
Tech Support	Observation logs interview reflexive and member checking	but a person using the system can be and a date and time established as to when a person is at the workstation	3/3/2018	25	1.1%
Tech Support	Observation logs interview reflexive and member checking	but no details of work station would be available with the exception of the person at the station and the time of the activity which would be enough to provide any information for an inquiry.	3/3/2018	35	1.6%
Tech Support	Observation logs interview reflexive and member checking	Cable and phone	3/3/2018	3	0.1%
Tech Support	Observation logs interview reflexive and member checking	Cameras and motion detector well placed (see security map).	3/3/2018	9	0.4%
Tech Support	Observation logs reflexive and member checking	Customers would rarely have time to access the work stations without staff being present because of the chirping alarm	3/3/2018	19	0.9%
Tech Support	Observation logs interview and member checking	Discussed power supply	3/3/2018	3	0.1%
Tech Support	interview and member checking	Does he respond right away? Yes, that same day, usually within an hour or so.	3/3/2018	15	0.7%
Tech Support	Observation logs reflexive and member checking	Door alert goes off when customers enter and leave (chirping & tweeting sounds).	3/3/2018	12	0.5%
Tech Support	Interview and member checking	expressed that tech support is a third-party IT rep from the supplier	3/3/2018	13	0.6%
Tech Support	interview and member checking	For on-line issues	3/3/2018	4	0.2%
Tech Support	interview and member checking	The security video recording device is located out of sight and disguised by covered by an empty	3/3/2018	29	1.3%

		cardboard container giving it the appearance of regular store merchandise			
Tech Support	Observation logs reflexive and member checking	I noted that if any work stations are left unattended	3/3/2018	10	0.5%
Tech Support	Observation logs reflexive and member checking	I noticed that the can not print when talking on the phone (DSL	3/3/2018	13	0.6%
Tech Support	interview and member checking	I think most of your businesses have got some kind of plan in effect some, uh kind of uh, uh, somebody that's watching to kind of keep the security up on it you know to keep from having these deals happen.	3/3/2018	42	1.9%
Tech Support	Observation logs reflexive and member checking	Internet ethernet internet service by separate line such that there is no interference during transaction processing	3/3/2018	16	0.7%
Tech Support	Observation logs reflexive and member checking	On-Line service.	3/3/2018	2	0.1%
Tech Support	Observation logs interview and member checking	Magnetic security devices on three bay doors as well as the front entry doors.	3/3/2018	14	0.6%
Tech Support	Observation logs reflexive and member checking	monitored by security video camera at the rear of the store	3/3/2018	13	0.6%
Tech Support	Observation logs interview and member checking	No scanning system point and click system for receipt print out.	3/3/2018	11	0.5%
Tech Support	Observation logs interview reflexive and member checking	No Wi-Fi at the facility. Strictly DSL. The Wi-Fi signal tested 5 times at random intervals with no signal detected	3/3/2018	23	1.0%
Tech Support	Observation logs interview reflexive and member checking	No wi-fi. Dot matrix printer.	3/3/2018	6	0.3%
Tech Support	Observation logs interview reflexive and member checking	Observed a wide-angle security camera attached to the drop ceiling on the back-left corner from the entrance of the building.	3/3/2018	22	1.0%
Tech Support	Observation logs interview reflexive and member checking	Observed two work station CRTS with keyboards on customer service counter	3/3/2018	11	0.5%
Tech Support	interview and member checking	ours has got a firewall on it and uhm, and, I'm not sure about the brand of the uh anti-virus.	3/3/2018	23	1.0%
Tech Support	Observation logs interview reflexive and member checking	phone and electrical egress to the building is under ground with no exterior access.	3/3/2018	14	0.6%
Tech Support	Observation logs interview reflexive and member checking	Phone operation prevents printer operation	3/3/2018	5	0.2%
Tech Support	Observation logs interview reflexive and member checking	Printer is a hole fed dot matrix printer for printing hardcopy receipts.	3/3/2018	12	0.5%
Tech Support	Observation logs interview reflexive and member checking	relies mostly on the third party (out-sourced) tech support for computer security and protection.	3/3/2018	15	0.7%
Tech Support	Observation log reflexive and member checking	Smart phone Wi-fi scan produced no results	3/3/2018	8	0.4%
Tech Support	Observation logs reflexive and member checking	Sometimes employees indisposed for long periods of time and	3/3/2018	17	0.8%

		unable to monitor the work stations.			
Tech Support	Observation logs interview and member checking	store inventory can be accessed on-line	3/3/2018	7	0.3%
Tech Support	Observation logs interview reflexive and member checking	The absence of any wi-fi signal indicates that all access to the system is through the DSL lines and subsequently the firewall	3/3/2018	23	1.0%
Tech Support	Observation logs interview reflexive and member checking	The camera covers the entire store including the counter work stations. Activity on the work stations not observed	3/3/2018	19	0.9%
Tech Support	Observation logs interview reflexive and member checking	The door ringer (a bird chirping) will trigger employees of customer entrances to the store if they are not out front.	3/3/2018	21	1.0%
Tech Support	interview and member checking	The rep is located off site and offers help desk type support but will come in as required.	3/3/2018	18	0.8%
Tech Support	interview and member checking	The third-party tech-support provided by the supplier for data base issues and updates	3/3/2018	16	0.7%
Tech Support	Observation log reflexive and member checking	There is an audible chirping thru out the facility when the front door opened to alert staff of an entry.	3/3/2018	21	1.0%
Tech Support	Observation logs reflexive and member checking	They need a procedure to remove employee access from the system when terminated	3/3/2018	13	0.6%
Tech Support	interview and member checking	Uh, probably like use a firewall and kind of limit the access to internet	3/3/2018	14	0.6%
Tech Support	interview and member checking	Uh, Well I think, you know, that if you make a password that somebody wouldn’t think of you know, I think you would be Okay, but you dont want to use your uh, uh, address or something like that.	3/3/2018	41	1.9%
Tech Support	Observation logs interview reflexive and member checking	Using dedicated DOT Matrix printer to print receipts	3/3/2018	8	0.4%
Tech Support	interview and member checking	Well, somebody could walk by that’s not an employee and can get into the system and get stuff out of it.	3/3/2018	22	1.0%
Tech Support	interview and member checking	Who do you call if you suspect your system compromised? My IT support guy	3/3/2018	16	0.7%
Tech Support	interview and member checking	Who do you call if you suspect your system compromised? My IT support guy	3/3/2018	16	0.7%
Tech Support	Interview and member checking	Who provides the tech support? The security software provider, it all comes under one package	3/3/2018	15	0.7%
Tech Support	interview and member checking	Who provides the tech support? The security software provider, it all comes under one package.	3/3/2018	15	0.7%
Tech Support	Observation logs interview reflexive and member checking	Work stations (three) are Dell computers with a firewall with anti-virus protection updated monthly and maintained by third party tech support	3/3/2018	24	1.1%

Tech Support	Observation logs interview reflexive and member checking	Work stations have a password timer, but it may need a shorter time out.	3/3/2018	14	0.6%