FACTORS INFLUENCING SMALL CONSTRUCTION BUSINESSES FROM IMPLEMENTING INFORMATION SECURITY: A CASE STUDY

by

Carl A. Mayes

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University, School of Business

January 2021

Abstract

This qualitative study described the influence of small businesses' failure to properly implement information security technologies resulting in the loss of sensitive and proprietary business information. A collective case study approach was used to determine the most effective way to gain a holistic picture of how small construction businesses make security technology implementation decisions to support their workforce. The theory guiding this study was the Unified Theory of Acceptance and Use of Technology (UTAUT) model which is related to the Theory of Planned Behavior and the Technology Acceptance Model which helped explain the intentions of individuals to use information systems. Security policies and threats (insider and cyber) were also looked at during this study. Data collection methods included questionnaires, interviews, document reviews, journaling, and webpage scans to provide insight into security information technology use. The results of this study indicated small construction businesses rely heavily on third-party information technology venders to perform security functions. This security model has led to several of the businesses experiencing cyber security incidents and the businesses being more reactive in responding to cyber-attacks. Deficiencies with planning for system implementations also impacted how employees thought and used the businesses' security information systems. The study's results indicated employee's behavior intention and use behavior was highly impacted by the age moderator with older employees more likely to display a lower behavior intention and use behavior for using systems.

Key words: construction, cyber security, UTAUT, small business

FACTORS INFLUENCING SMALL CONSTRUCTION BUSINESSES FROM IMPLEMENTING INFORMATION SECURITY: A CASE STUDY

by

Carl A. Mayes

Dissertation

Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University, School of Business

January 2021

Approvals

_____	_____
Carl A. Mayes, Doctoral Candidate	Date
_____	_____
Dr. Gayle Jesse, Dissertation Chair	Date
_____	_____
Dr. Daniel O'Malley, Committee Member	Date
_____	_____
Edward M. Moore Ph.D, Director of Doctoral Programs	Date

Dedication

When we met in South Korea during our tours with the United States Air Force, I knew I had found the right person for me. I dedicate this to my caring and loving wife, Mitzi of 33 years. Her support and sacrifices over three decades have allowed me to accomplish this monumental goal. I love her more every day! To my children and grandchildren, it is never too late to accomplish your dreams!

Acknowledgments

God is good, God is great. These words seem so insignificant when compared to what God has given me. I thank God for his grace, love, and putting Godly people in my life. I want to thank my dissertation chair, Dr. Gayle Jesse, who offered encouragement to me as I went through this very trying process. Her unwavering support and guidance were critical to me in completing each phase of my study and ultimately reaching my personal goal of getting my degree. I believe God is using your talents to further his kingdom on this earth. There is no greater honor than doing God's work.

I want to recognize DBA director, Dr. Edward Moore, and my committee member, Dr. Daniel O'Malley, for their value-added feedback during this process. Dr. O'Malley was especially instrumental in getting me to think about how to use triangulation to develop a comprehensive understanding of the study. Thank you all for the support you have provided to make this experience the finest it could be.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

A growing concern in the United States involves hundreds of millions of consumer records purloined and hundreds of security breaches reported each year affecting financial institutions directly and indirectly (Mikhed & Vogan, 2018). Data breaches can cause class-action lawsuits (McSweeney, 2017) or trigger a businesses' loss of reputation as they are perceived to intentionally or unconsciously breach their written contract with customers (Breitinger & Bonardi, 2019). Ultimately, bankruptcy is the final consequence small businesses may suffer from the consequences of cyber-attacks (Man & Lam, 2016). Small businesses drive the United States economy, comprising 99.9% of all businesses, while employing 47.8% of all private sector employees (Cyber Crime: An Existential Threat to Small Business, 2019). The United States economy perpetually relies on small businesses to continually sustain economic advancement, as prime targets for criminal attacks, small businesses' powerlessness to protect their daily operations, places the business at risk and the economy in a perilous situation. This study explored small businesses and the factors affecting their ability to defend their business from internal and external threats by identifying the factors influencing their implementation of security information technologies.

Background of the Problem

Implementing information security technologies in today's business environment is a major concern for securing business transactions as complex project deployments can only be substantiated through a rational and explicit planning process (Kohnke & Shoemaker, 2015). For small businesses, information technology adoption often happens without any proper planning, subsequently leading to a low percentage of success (Nguyen et al., 2015). Information security continues to be a problem that plagues all businesses where security professionals are constantly

selecting and implementing countermeasures to combat new security threats (Nazareth & Choi, 2015). The number and the sophistication of cyber-attacks has significantly increased over recent years with cyber criminals targeting businesses where legacy computer networks are too hard to modernize (Birkinshaw et al., 2019). The level of sophistication in today's malicious agents can take advantage of a variety of weaknesses in a business's information and communication technology management systems, especially when systems are outdated (Kohnke & Shoemaker, 2015). In addition to external criminal activities, insider threats are hard to pinpoint, as there are often very few valid indicators to substantiate criminal activity as only a fraction of such activity can be electronically monitored, and detected (Ho & Warkentin, 2017).

Today's businesses are under a constant threat from increasingly severe and sophisticated forms of attacks where breaches cost businesses billions of dollars in lost revenue and loss productivity every year (National Institute of Standards and Technology, 2019). Many businesses admit malicious information security incidents perpetrated against private and public entities involving security breaches can damage a businesses' reputation and may cause substantial financial loss (Badenhorst, 2017). When businesses are criticized in the media for failing to implement technologies to protect customers or employees' privacy, the businesses' reputation might be damaged for deviating from current security norms (Breitinger & Bonardi, 2019). Businesses also become reluctant to disclose security-related inadequacies for fear of attacks and harm of their reputation where a deficiency of deep expertise and complete comprehension in information security can become a detriment.

Theft of proprietary data, intellectual property, and sensitive financial and strategic information cost the United States economy between $57 billion and $109 billion in 2016 (The Council of Economic Advisers, 2018). With cyber-attacks on the rise, cyber criminals are

targeting small businesses, which they consider the easiest prey in an environment where there are an abundant number of potential targets. The annual Hiscox 'Cyber Readiness Report' for calendar year 2018, shows both the cost and frequency of attacks have increased markedly against small businesses from the previous year, costing businesses on average $369,000 per incident (Hiscox, 2019). Half of all cyber-attacks are committed against small businesses where potential threats from criminal enterprises can negatively impact a business and its financial objectives (Stanciu & Tinca, 2017). Couple this with the absence of national boundaries in cyberspace and the relatively low probability of being caught and the risk/reward ratio makes cybercrime an attractive alternative to other types of criminal activities (Hall, 2016). The lack of a cybercrime incident architecture to identify threats and interconnect relevant stakeholders with preventive measures and response actions furthers the success rate for cyber incidents (Tsakalidis et al., 2019).

With a drastic increase in cyber-attacks, small businesses need access to up-to-date information on how to decide on implementing new information security technologies, so they become less of a target. The current information available to small businesses, identifies several factors involved with implementing information security; however, the studies provide data related to large businesses with a minute amount targeted towards small businesses (Hwang et al., 2017; Yeh et al., 2015). Smaller businesses encounter different challenges than their larger counterparts, so the factors identified in these studies may not be as relevant to smaller businesses. Reports like the Hiscox (2019) Cyber Readiness Report, usually show aggregate numbers but do not provide enough details behind the numbers to assist small businesses with improving their security operations. Noguerol and Branch (2018) identified factors such as, financial restrictions and inefficient leaders as reasons any size business can lead managers to

making poor decisions in securing the business' data and systems from external and internal threats. Attacks, poor management or other factors make it necessary for all businesses to have information readily available to them to assist in improving their operations, especially small businesses (Nguyen et al., 2015; Noguerol & Branch, 2018). After all, it is imperative for small businesses to realize that cyber criminals will continue to target their businesses into the foreseeable future.

Many businesses are aware of the security issues they face through Information Technology reporting (Stanciu & Tinca, 2017) and consult with security experts to institute proactive security measures to combat cyber threats (Osborn & Simpson, 2018). In addition, small businesses prefer focusing on high-risk low-loss threats over low-risk high-loss threats which require accurate estimation of the level of risk that each threat poses to determine, if implementation of a new security technology is required (Mayadunne & Park, 2016). Security investments are typically a response to perceived and materialized threats where information security management really becomes important to businesses after they suffer a security incident (Kim & Chang, 2014; Nazareth & Choi, 2015). Proactive business managers armed with the knowledge that implementation of security technologies can enhance the businesses' cybercrime incident architecture are able to make informed decisions to protect the business from cyber-attacks before their infrastructure is compromised (Tsakalidis et al., 2019). Previous studies involving the theory of planned behavior showed individual's intention to engage in set behaviors or their anticipated regret for reacting in a certain fashion can be predicted (Sommestad et al., 2015). Understanding how to predict a manager's behavior when assessing the implementation of information security technologies is essential to improving results. Kmieciak et al. (2018) indicated business managers are expected to make rational decisions that

increase and strengthen the business's ability to improve performance, requiring information technology investment decisions to be based on how these technologies might influence the business's performance. If specific factors affecting small businesses capabilities in implementing information security technologies can be identified and analyzed, then business leaders can assimilate the results and appy the lessons learned to implement information security technologies.

Problem Statement

The general problem to be addressed is the failure of small businesses to insulate operations from malicious criminal attacks. Specifically, the failure of a small business to properly implement information security technologies makes them vulnerable to bad actors interested in stealing business information to further their criminal enterprise. Even though hacking incidents continue to rise affecting small to medium-sized enterprises, businesses and their leaders seem to remain obstinate in their need for improving their information security technology architecture (Sen & Borle, 2015). Generally speaking, business leaders deal with a myriad of issues daily, postponing enhancements to information security under the false belief that criminal enterprises will target more important businesses first, so they do not see the value of investing capital to improve their information security technologies (Almeida et al., 2018). Additionally, small businesses leaders struggle to see implementation of information security as a management issue, leading to a businesses' failure to approach information security management from a holistic approach (Soomro et al., 2016). This is especially common in some industries, which traditionally lag behind in adopting technologies like information security owing to a wide range of cultural, organizational and institutional barriers (Sepasgozar et al., 2016). Dr. Charles H. Romine, Director, Information Technology Laboratory at the National

Institute of Standards and Technology testified in March 2019 to the U.S. Senate committee on Small Business and Entrepreneurship stating that small businesses comprise 99.9% of all firms in the U.S. and they need to be aware that cybersecurity breaches cost businesses billions of dollars in lost revenue and productivity every year (Cyber Crime: An Existential Threat to Small Business, 2019). Dr. Romine's testimony illuminated the threat to small businesses and the importance of insulating their operations from threats. The specific problem to be addressed is the failure of small businesses to properly implement information security technologies resulting in the loss of sensitive and proprietary business information for small businesses within the state of Virginia.

Purpose Statement

The purpose of this qualitative case study was to add to the body of knowledge by furthering the understanding of small businesses' failure to properly implement information security technologies resulting in the loss of sensitive and proprietary business information. The problem was explored within its own setting through an in-depth study of information security implementation at small businesses, assisted in identifying specific factors affecting business's deployment of information security technologies. Previous research identified leadership's role in the implementation of information and communication technologies where supervision, information, and training were identified as important factors in successfully implementing new technologies (Hansen & Nørup, 2017).

Leadership is also responsible for making investment decisions where business logic dictates putting a greater emphasis on efficiencies and profitability, leading to a symbolic adoption of new security technologies (Angst et al., 2017). Huang et al. (2014) cited costs, interoperability, security, and privacy concerns as major barriers to the growth of security

systems in healthcare. With shorter innovation cycles and the constant development of new security technologies, employees need to adapt to ongoing changes in the work environment that require permanent adaptations to the way they work (Guhr et al., 2019). These changes drive managers to demonstrate the importance of securing business data by appropriately instituting business structures to support information security in the organization (Guhr et al., 2019).

Research also shows managers of small businesses do not see the implementation of information security as an immediate problem because of a lack of knowledge, therefore the approach they use to resolve the problem is not examined from a holistic approach (Osborn & Simpson, 2018; Soomro et al., 2016). In addition, leadership demonstration that they support information security management is highly valued by large businesses, however, smaller business owners do not value it the same way (Santos-Olmo et al., 2016). The researcher sought to identify the factors and reasons small businesses continually discount the implementation of information security technologies to safeguard and protect their future survivability through this study.

Nature of the Study

A qualitative case study was conducted to investigate and try to better understand why small businesses fail to properly implement information security technologies resulting in the loss of sensitive and proprietary business information. The researcher compared the data collected against a review of the literature to explore and understand: (1) the factors affecting implementation of information security, (2) the reasons a small business may not be proactive in adoption of security technologies, and (3) what role information technology investment decisions have on the implementation of security technologies. This research will add to the body of

literature as it relates to small businesses and their shift towards implementing technologies designed to deal with cyber-crime and internal threats.

Discussion of Method

The nature of the research problem supports the researcher in determining what type of research approach to elect as their philosophical assumptions to the research help drive their research design and methodology decisions (Creswell, 2014). The researcher identified a specific research method to use for data collection, which included the type of interview method, any surveys and/or observations the researcher used in gathering information to complete the study. To effectively conduct research, the person designing the plan needed to choose between one of the three main research approaches of qualitative, quantitative, and mixed method studies to answer a particular problem. A comprehensive analysis was conducted to determine the optimal approach to perform this study.

Qualitative Method Design. Qualitative studies are similar to quantitative studies, except Stake (2010) distinguished the difference as being a matter of special importance more than limited to a distinct boundary. Qualitative research explores the understanding and meaning individuals or groups assign to a social or human problem (Creswell, 2014). A main feature of a qualitative study is the researcher's personal involvement in the study where they strive to discover, hear, and document stories (Roger et al., 2018). Creswell and Poth (2018) indicated the event takes place in a natural setting where participants are not interfered with by the researcher as they go about their daily lives. By allowing researchers to focus on a "case" and retain a holistic and real-world perspective about the event, researchers are allowed to concentrate on contemporary events and not have to control behavioral events (Yin, 2014).

The information and data being collected for this study is not statistical in nature and neither is it compulsory for small business to implement technologies the same way. For this study, using the most common methods of qualitative research of observations, interviewing, and examination of artifacts (including documents) is the optimal way to approach this study (Stake, 2010). Gupta et al. (2015) conducted a study to analyze the adoption of online tax filing using three widely utilized technology adoption theories/models: Theory of Planned Behavior (TPB), Technology Acceptance Model (TAM), and Information System Success Model. Gupta et al. (2015) looked at the perspectives of web service quality, web service content, convenience of service, and perceived risk using a survey-based study. In addition, the study showed technology adoption in developing countries based on some of the same theories/models as used in this study. TAM was upgraded to TAM2 (Venkatesh & Davis, 2000) and is recognized as robust and reliable mechanism for predicting user acceptance of a wide-range of new technologies (Sánchez et al., 2013). Bhattacherjee et al.'s (2018) qualitative study analyzed how the introduction of a new information technology system into a workplace often causes a wide range of responses among users also relied on the TPB (Ajzen, 1991). The original Unified Theory of Acceptance and Use of Technology model (UTAUT) explained intentions to use information systems based on perceptions following the technology acceptance model (Davis, 1986; Venkatesh et al., 2003) and was updated to include more contextual factors, such as price value and habit, known as UTAUT2 (Venkatesh et al., 2012). With the addition of the hedonic motivation in UTAUT2, the model went from a largely cognition-based model to one with a much-needed affective component (Tamilmani et al., 2019). The modified UTAUT2 model represents a comprehensive theoretical framework that is suited well to support both qualitative and quantitative research (Morosan & DeFranco, 2016; Venkatesh et al., 2012).

Quantitative Method Design. Creswell (2014) pointed out that people use quantitative research to objectively test theories through examining the relationship between the three main types of variables: dependent, independent and controlled. Quantitative examinations call for the use of statistical means in analyzing the variables, where the researcher manipulates the independent variable in an effort to understand to what degree, the changes affect the dependent or controlled variables (Creswell, 2014). The quantitative design attempts to remove any subjectivity from the collected data, requiring data to be assigned numeric values that can be measured so that comparisons can be made against the data set. Using closed-ended questions in the study to collect data through surveys, interviews and questionnaires will provide only slices of insight into issues that are often considerably more complex and the responses will be mostly descriptive without any additional evaluative component (Cabrera & Reiner, 2018). Schoonenboom's (2018) study highlighted surveys using closed-ended questions did not allow participants to fully answer questions based on their opinion but only to provide answers to preconceived questions. The practice of using open-ended questions in a case study allows the researcher to document the connection between specific pieces of evidence and various issues in the case study (Yin, 2014). Quantitative researchers are aware that the quality of questionnaire translations is critical to research outcomes and problems exist with translation mistakes, shifts due to different linguistic systems, or different understandings of apparently well-translated items due to different cultural backgrounds making it more difficult to assign values to the participants answers (Behr, 2015).

The quantitative research method uses hypothesis testing to prove or disprove the research goal in a controlled environment where specific variables are identified and isolated within the context of the study to try to find correlation, relationships, and causality between

them (Park & Park, 2016). The qualitative research method occurs within the natural environment where specific variables have not been identified in advance. The quantitative research method also relies on statistical data to assist in the triangulation of the study's outcome as an important part of a case study's design and data collection (Yin, 2014). A quantitative case study can be a useful method for doing an evaluation, however for this study the qualitative case study was chosen as it aligns better to collecting data to respond to the research questions following the pattern of previous studies (Bhattacherjee et al., 2018; Gupta et al., 2015).

Mixed Method Design. The mixed method design involves using a convergent parallel, explanatory sequential, exploratory sequential, and transformative, embedded, or multiphase approach to combine or integrate qualitative and quantitative research data together within a study (Creswell, 2014). The convergent parallel mixed methods involve the researcher collecting data at the same time for a quantitative and qualitative study, while the explanatory sequential mixed method has the researcher performing quantitative research first and qualitative research last (Creswell, 2014). Mixed method research design uses the quantitative method either at the start or end of the study with one of its biggest disadvantages being how much time and resources it takes to plan and implement the research (Guest et al., 2013; Schoonenboom, 2018). If a qualitative or quantitative research design can adequately answer the questions posed by the researcher then creating a larger and more complicated design is not justified (Guest et al., 2013). In addition, both the open-ended and closed-ended type questions from the qualitative and quantitative parts of the research study required the researcher to design the same and different types of questions to collect the data analyzed. Open-ended type questions will allow the interviewee to explain in-depth about any feelings they may have and their attitudes towards a specific subject matter (Behar-Horenstein & Feng, 2018; O'Cathain & Thomas, 2004). Closed-

ended type questions limit the feedback a researcher can receive because they truncate the communication process allowing the interviewee to answer only specific questions (Cabrera & Reiner, 2018; O'Cathain & Thomas, 2004). These specific questions can make it easier to collect and analyze participant answers by linking them to specific areas that can be measured as part of the quantitative study side of the mixed method research study. Since quantitative methods emphasize numerical data and measurable variables while qualitative methods emphasize observation and interpretation with data collected within the context of its natural setting, it is more appropriate to use a qualitative study for this research (Creswell, 2014; Park & Park, 2016).

Discussion of Design

The main design of this study will be based on a qualitative design. Past researchers (Creswell & Poth, 2018; Merriam, 1998; Stake, 2010; Yin, 2014) are well-known researchers who have provided a structure for researchers to follow when performing qualitative research. Assessing each of the following five qualitative approaches: narrative research, phenomenology research, grounded theory research, ethnographic research, and case study research allowed one to stand out above the others. The qualitative case study stood out as a research method that works well for studying an event or an activity and its unique strength in handling an assortment of collected data will be an important part of this study (Creswell & Poth, 2018; Yin, 2014).

Narrative Research. Narrative research is the study of experiences understood through the lives of individuals (Creswell & Poth, 2018). The narrative research design comes from the humanities field of study and involves a researcher focusing on the study's participants life, where one or more individuals relay through their life's stories the experiences they have lived (Creswell, 2014). The narrative research design allows the researcher to study an individual's story by interviewing them so they can hear it orally or read their stories through written

dialogue. The researcher can also use a visual representation of an individual's story to further their understanding. By bringing together the different stories from multiple individuals, the researcher is able to form a cohesive story portraying how personal descriptions of life experiences occurred. Narrative research has a valuable place in the qualitative research domain where it is mostly used qualitatively, however it can also be used in quantitative and mixed methods studies to express stories offering rich insights into a person's lived experiences making sense of events and actions in their lives (Carless & Douglas, 2017; McAlpine, 2016).

Phenomenology Research. Qualitative phenomenology research is grounded on two classical approaches of hermeneutic (interpretive) or descriptive (transcendental constitutive) phenomenology (Chan et al., 2013). The hermeneutic (interpretive) goal is to provide researchers an opportunity to understand how a person, in a certain context, makes sense of a given phenomenon, while the descriptive transcendental constitutive phenomenology describes the special method of the eidetic reduction where the research views a phenomena from how humans see mental images in their consciousness, vivid and detailed. As part of a phenomenology study, the researcher tries to break the experience of each individual down into what and how they experienced the event to gain an understanding of the core of what they experienced. All participants who experienced the event saw or felt it in a different way so the researcher's quest is to set aside their biases and preconceived assumptions about the experience and delve into experiences of the people who actually lived the event. When trying to describe an event, activity, or phenomenon from the participant's experiences, the aptly named phenomenological study is an appropriate qualitative method to use. However, the researcher's goal for this study is not to identify the essence of a perceived phenomenon focusing more on the users' experiences

but to understand why and how managers of small businesses make decisions about implementing information security technologies (Ghaffari & Lagzian, 2018).

Grounded Theory Research. Grounded theory research involves the collection and analysis of data to expand the understanding of a common experience or phenomenon to generate or discover a theory (Creswell & Poth, 2018). Rieger (2019) pointed out the key characteristics of a grounded theory clarifies a process beginning with inductive logic where the process involves collecting data, performing analysis and theory construction. In addition, grounded theory research incorporates constant comparisons while employing theoretical sampling to focus on the generation of a grounded theory (Rieger, 2019). The two most popular grounded theory approaches are the systematic and the constructivist approach (Creswell & Poth, 2018). Under the systematic approach, the researcher searches for a way to systematically develop a theory that explains a process, action, or interaction of a topic-using field interviews (Creswell & Poth, 2018). The constructivist approach acknowledges the subjectivist stance of researchers who use our past and present involvements and interactions with people, perspectives and the research practices to construct grounded theories (Lauckner et al., 2012). Whereas a phenomenological study looks to describe the essence of an activity or event, grounded theory looks to provide an explanation or theory behind the events. The researcher has not formed a hypothesis for this study and therefore is not prepared to perform test against a non-existent hypothesis, so using the grounded theory to consider theoretical sampling to assist in developing properties of an emergent analytic category is not practical for this study (Charmaz, 2015). Grounded theory's focus on theory construction therefore makes it unsuitable as a methodology for this study.

Ethnographic Research. Ethnographic research was used by anthropologists as a qualitative research method to observe and/or interact shared and learned behaviors, beliefs and language of a culture-sharing group in their real-life environment (Creswell & Poth, 2018). Ethnographic research is an approach to learning about the social and cultural life of communities in response to current society, in which systems of power, prestige, privilege, and authority serve to shape and constrain by marginalizing individuals who are from different classes, races and genders (Creswell & Poth, 2018; Forster, 2019). The two most popular forms of ethnography research are the realist and critical (Creswell & Poth, 2018). The realist ethnography is considered the traditional approach reflecting the researcher's objective approach to a particular stance towards the individuals being studied. The realist study focuses on the entire culture-sharing group where the researcher is trying to understand the shared patterns of the group. Critical ethnography takes on the normalization of structures in society where the qualitative approach draws on research and theory to critique control, oppression, and symmetrical power relations in order to potentially foster social change in direct or indirect ways (Palmer & Caldas, 2015). Since the ethnography approach deals with marginalized groups with the goal of promoting for the freedom of groups downgraded by society, it is not the best option for this current research.

Case Study. Qualitative case studies work well for studying an event, a program, or an activity (Creswell & Poth, 2018). The case study is an empirical inquiry in which a social problem is investigated and described in-depth within its real-life context (Schoonenboom, 2018; Yin, 2014). The case study's unique strength is its ability to deal with an assortment of collected data to include evidence-documents, artifacts, interviews, and observations (Yin, 2014). The research questions fit well with Yin's (2014) thoughts on using "how" and "why" questions as a

way to be more descriptive and "what" questions as a justifiable rationale for conducting an exploratory study. Using the qualitative case study to perform the research, Creswell and Poth (2018) noted a case study begins with one identifying the specific case or cases described and analyzed. Stake (2010) discussed making a strategic choice between interpretive data or aggregative data, where the interpretations of the data source comes from the people or aggregation scores and observations, respectively.

A case study allows all the different components of the research design to be connected. As a tool to sort through alternatives and competing theoretical accounts, the case study allows the researcher to explore and deepen the understanding of the causality in program outcomes (Longhofer et al., 2017). Exploring complex situations allows the researcher to gather multiple perspectives from different participants, including contextual information (Lauckner et al., 2012). Collecting both qualitative and quantitative data to gain a more comprehensive understanding of the case being researched, case studies have a long tradition of supporting both types of data collection (Stake, 2010; Yin, 2014). Some research may require both types of data to fully explore the research questions; however, for this study the focus will be on qualitative data collection. The case study also allows collection of data in its natural setting with the questions of why and how to be answered to the best extent possible with a comparatively full understanding of the nature and complexity of the issue (Farquhar, 2012; Merriam, 1998). The case study methodology would be a rational choice for a research study intended to understand a specific problem (Schoonenboom, 2018).

Summary of the Nature of the Study

In conclusion, this study utilized a qualitative case study design, as it will provide the needed understanding to solve the problem of why businesses fail to implement information

security. A case study involves real-life, contemporary context according to Yin (2014) where one or multiple cases can be looked at during the study. Stake (2010) took it further, suggesting it requires an understanding of other cases, things, and events to understand a case along with an emphasis on its uniqueness. When a problem or issue requires exploration and an understanding of a complex issue, Creswell and Poth (2018) proposed using a qualitative research approach. A case study focuses on a case, allowing the researcher to keep in mind a holistic and real-world perspective (Yin, 2014). Allowing the researcher to collect data in its natural setting with the questions of why and how to be answered to the best extent possible with a comparatively full understanding of the nature and complexity of the issue is an important part of the study (Farquhar, 2012; Merriam, 1998). By using a qualitative case study, the researcher can access the thoughts and feelings of research participants to help understand how and why a behavior takes place (Sutton & Austin, 2015).

Qualitative research explores the understanding and meaning individuals or groups assign to a social or human problem (Creswell, 2014). The research allows for the diversity of theoretical and epistemological frameworks along with the inclusion of many different kinds of data collection and analysis techniques (Guest et al., 2013). A main feature of a qualitative study is the researcher's personal involvement in the study where they strive to discover, hear, and document stories in a natural setting where participants are not interfered with (Creswell & Poth, 2018; Roger et al., 2018). Gupta et al. (2015) study analyzed the adoption of online tax software using the TPB and the TAM. Bhattacherjee et al. (2018) also used a qualitative study to analyze the deployment of a new information technology system into a workplace using the TPB (Ajzen, 1991). Aswani et al. (2018) performed a qualitative study to understand the possible reasons for a digital divide or the adoption of technology by people using a Public WiFi using the UTAUT2

theoretical model. Based on these qualitative studies, the qualitative research study of small businesses' failure to properly implement information security should be suitable using a case study methodology of multiple businesses.

Research Questions

RQ1. What factors impact a businesses' decision to implement information security technologies?

RQ1a. How do the internal investment processes that owners/managers institute assist in determining the best course of action for implementing security systems?

RQ1b. How does knowing that internal threats and cyber-attacks occur against small businesses on a routine basis have on implementing security information applications?

RQ2. What practices do business managers incorporate in the work environment to ease the transition of new information security technologies?

RQ2a. How do employees perceive changes to the work environment when new information security technologies are deployed?

RQ2b. What new stresses are introduced in the workplace when new information security technologies are deployed?

RQ2c. How do security policies assist employees in dealing with the deployment and acceptance of new security information systems?

Conceptual Framework

For over 25 years, the increasing threat of computer crime has made information technology security a great concern to companies, with the human factor considered the weakest link in the security solution (Jones et al., 2010). This weakness can have many root causes with employees following the norms of their peers and a belief that information security policies may

reduce worker efficiency (Hwang et al., 2017). In addition, information security creates conflicts with active sharing of critical information resources, interferes with standardization of business processes, and ambiguous security policies or poor performing systems can cause anxiety (Hwang et al., 2017). To eliminate some of these aforementioned weaknesses a business may determine it needs to do something different with its security architecture or business culture. Any changes will come with its own set of factors like organizational, economic, social, and strategic factors that a business will need to understand (Chou et al., 2015). As adoption of information technology security systems is important to all businesses, this study focused its data collection and analysis on different factors that may play into adopting new technologies.

For this research, following the logic of Yin (2014), the research design linked the data collected to the initial questions of study, where analysis of the data assisted in drawing the conclusions. Bounding the qualitative case study around small businesses allowed the research to focus on a unique problem designed for a case study. The in-depth study involved small businesses' inability to implement information security technologies assisting in identifying relevant factors affecting this issue. The qualitative case study allowed for a flexible design in which the researcher was personally involved in the study to assist in collecting and analyzing data in its natural setting (Creswell & Poth, 2018; Roger et al., 2018). The researcher arranged the research in an organized manner so the qualitative case study's results will add to the body of knowledge.

The goal of this study was to understand a small businesses' lack of properly implementing information security technologies in the U.S. with the conceptual framework model being designed to assist in meeting that goal. First, an understanding of why a business would decide to implement new security technologies needs to be understood (Man & Lam,

2016; Raban & Hauptman, 2018). Looking at the way a business determines how to make investments may provide more insight into how and why new technology decisions are made (Bolek et al., 2016; Weishäupl et al., 2018). The researcher will also investigate what role perceived usefulness, perceived ease of use, and subjective norms has in influencing the attitude of managers and employees in deploying security technologies (Ajzen, 1991, Cheng, 2019; Davis, 1986; Taylor & Todd, 1995; Sánchez et al., 2013). Employees' attitudes towards use of any new technology is different than their intention to use it as most decisions in small businesses are directed from leadership and mandatory (Bolek et al., 2016; Guhr et al., 2019; Jones et al., 2010). Relying on observations, questionnaires and interviews the researcher will delve into what practices managers perform to prepare employees for new systems like publishing new security policies or looking at stressors in the workplace (Kim & Chang, 2014; Nazareth & Choi, 2015; Ullaha et al., 2018). Gathering data to learn about the factors and employee's behavior will provide a better understanding of why some businesses do not implement new information security technologies (Ajzen, 2011; Cheng, 2019; Davis, 1989; Taylor & Todd, 1995). TAM2 and UTAUT2 could offer a roadmap to identify key factors that all businesses have to come to terms with when implementing information security technologies.

Discussion of Technology Acceptance Model

The TAM was developed by Davis (1986) which outlines perceived usefulness and usage intentions as they relate to the processes of social influence and cognitive instrumental processes. People are more likely to use a system if they believe it will help them perform their job better and believe the systems' benefits of usage are out-weighed by the effort of using the system (Davis, 1989). Perceived usefulness and perceived ease are the two factors proposed by Davis (1986) in the TAM which asserts that these two factors are of particular importance in the

decision of employees to adopt any particular technology. Davis' (1986) TAM made some fundamental assumptions about users' opinions in that they are static, never varying under different circumstances and the model limited technology adoption to only two relevant factors. The original TAM model was challenged by other studies (Legris et al., 2003; Mathieson, 1991) showing different factors not identified by Davis (1986) might influence a user's decision to adopt a particular technology. The original TAM also lacked a consideration of social norms, where Ajzen's (1991) TPB does account for norms. A further weakness identified with the TAM is it omits the user's perceived control as a factor influencing their decision to adopt technology (Mathieson, 1991). TAM is also limited in looking at the broader perspectives from human and social change processes in order to understand and predict a user's technology adoption decision (Legris et al., 2003). As new studies were performed, TAM was updated to account for some of the shortcomings pointed out by Mathieson (1991) and Legris et al. (2003).

The updated TAM2 (Venkatesh, 2000; Venkatesh & Davis, 2000) proposed a theoretical framework that describes the factors of system-specific perceived ease of use as individuals evolve over time in their experiences in using new technologies. TAM2 updates the original model to include anchors (control, intrinsic motivation, and emotion) which are general beliefs about computers and computer usage and adjustments (perceived enjoyment and objective usability) which are beliefs shaped by the direct use of a new system (Venkatesh, 2000). Control is divided into perceptions of internal control or computer self-efficacy and perceptions of external control or facilitating conditions (Bhattacherjee et al., 2018; Venkatesh, 2000). TAM2 also intellectualizes intrinsic motivation as computer playfulness and emotion as computer anxiety (Hwang et al., 2017; Macedo, 2017; Venkatesh, 2000). The four factors (computer self-efficacy, facilitating conditions, computer playfulness, and computer anxiety) that make up

control are system-independent anchoring constructs that play a significant role in shaping perceived ease of use about a new system (Venkatesh, 2000). As users gain experience using a new system, adjustments (objective usability and perceived enjoyment from system) will have an additional influence on system-specific perceived ease of use (Venkatesh, 2000).

The extended TAM2 accounted for 40% to 60% of the variance in usefulness perceptions and 34% to 52% of the variance in usage intentions during Venkatesh and Davis' (2000) study. This was an increase over the original TAM that consistently explained approximately 40% of the usage intentions and behavior variance. The perceived usefulness and the perceived ease of use of the technology assist in shaping the user's beliefs and behavioral intention towards a particular technology, playing a major part in influencing the behavioral outcome of adopting the new technology (Ho et al., 2017). Abbas (2016) investigated the social factors of interpersonal influence, external influence, and instructor influence using TAM2 to determine the intention of students towards using a new e-learning system in two different countries. TAM2 showed interpersonal influence, external influence and instructor quality had a significant effect in one country with a student's behavioral intention to use e-learning platforms and only instructor quality played a significant role in the other country. The TAM2 asserted that through subjective norms student's behavioral intention to accept the e-learning platforms (new technology) through the mediating influence of perceived usefulness and perceived ease of use would be impacted (Abbas, 2016; Venkatesh & Davis, 2000). Ho et al. (2017) also highlight factors such as social, environmental factors, and cognitive instrumental processes as other influencers in the adoption of technology in their study. The different studies showed that TAM2 can be extended to support many various factors.

Discussion of Unified Theory of Acceptance and Use of Technology

UTAUT proposed by Venkatesh et al. (2003) were primarily considered for this study for its ability to explain a user's acceptance of technology and the amount of variance in behavioral intention and usage behavior. The UTAUT model was originally theorized for organizational context concentrating on the critical factors and contingencies related to the prediction of behavioral intention and use of technology (Venkatesh et al., 2012). The model proposed four constructs to assess people's technology acceptance: performance expectancy, social influence, effort expectancy, and facilitating conditions (Venkatesh et al., 2003; Yuan et al., 2015). The relationships theorized that the original UTAUT model could not be applied in all contexts and moderators specified the model could only explain 70% of the variance in behavioral intention and 50% of the variance in technology use (Dwivedi et al., 2019; Venkatesh et al., 2003; Venkatesh et al., 2012).

The UTAUT model explained employee technology acceptance and use and was expanded over time by Venkatesh et al. (2012) to other context like consumer technologies. The model update called UTAUT2 incorporates three constructs into the original UTAUT: hedonic motivation, price value, and habit (Venkatesh et al., 2012). The new UTAUT2 prediction model's hedonic motivation construct is an important predictor for more stressing utility (Huang & Kao, 2015; Venkatesh et al., 2012). The price value construct was also introduced in the UTAUT2 model because product quality, cost, and price will influence adoption decisions (Huang & Kao, 2015; Venkatesh et al., 2012). Venkatesh et al. (2012) also introduced habit as another new theoretical construct within the UTAUT2 model where habit is regarded as prior behavior and the degree to which people believe the behavior to be automatic (Huang & Kao, 2015; Venkatesh et al., 2012).

Ravangard et al. (2017) involved using the UTAUT2 model to investigate the software usability of electronic portals for patient laboratory results. Identifying the effective factors in successful acceptance of information technology by focusing on parts of the UTAUT2 model allowed the researchers to discover the construct of intention to use the system had significant associations with price value, hedonic motivation, habit and usability (Ravangard et al., 2017). Shaw and Sergueeva modified the UTAUT2 model to look at perceived value replacing price value to represent the value of an information technology artifact that has no direct costs attributable to it. The study was performed by removing attitude from the UTAUT2 model where previous studies have found attitude mediates some of the paths influencing behavioral intention (Dwivedi et al., 2019; Shaw & Sergueeva, 2019). The investigation involved consumers who had already purchased a smartphone for mobile commerce, typically subscribe to a monthly service for internet, and download free apps to connect with service providers (Shaw & Sergueeva, 2019). Since the smartphone was already purchased and the internet service was acting as a utility for many activities, the consumer had no additional cost (Shaw & Sergueeva, 2019). This set-up allowed for replacing price value by perceived value, where the value took into account the non-monetary costs (Shaw & Sergueeva, 2019). The study concluded that perceived value significantly influenced intention to use. The aforementioned studies (Ravangard et al., 2017; Shaw & Sergueeva, 2019) showed how the UTAUT2 model could be extended or modified to account for new or changed factors. This ability, along with the additions made to the model from UTAUT to UTAUT2, arguably makes UTAUT2 the most comprehensive theory in understanding individual technology adoption and use (Tamilmani et al., 2019).

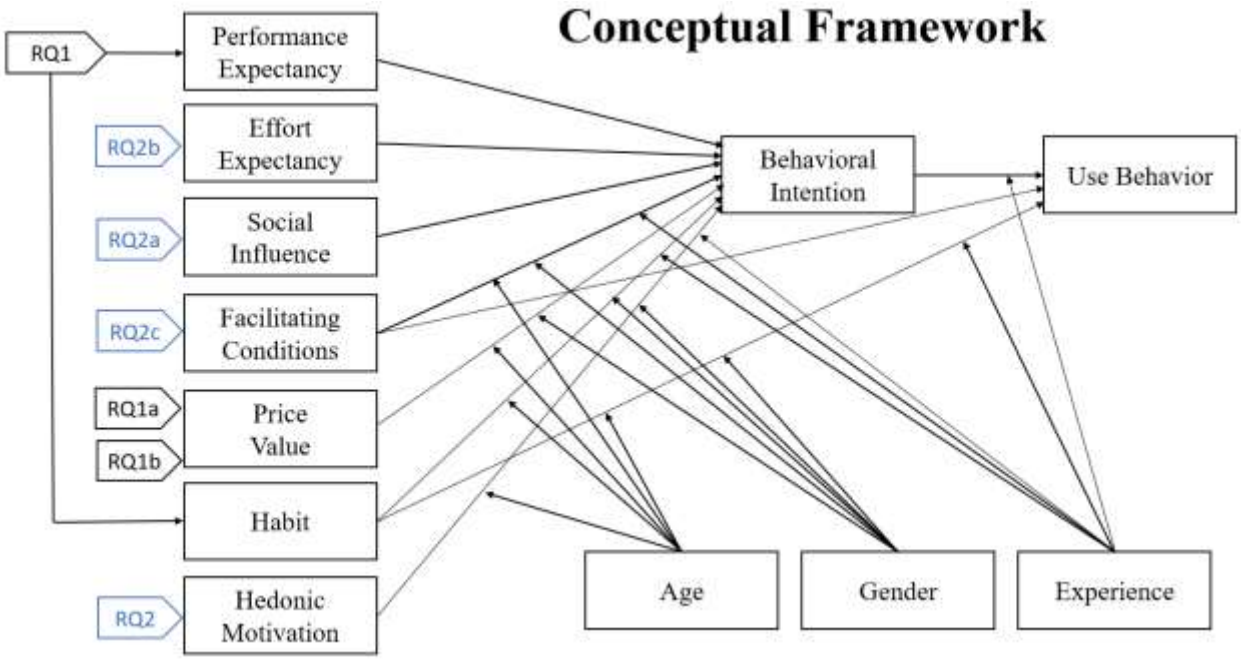
Discussion of UTAUT2 Versus TAM2

TAM2 can provide an understanding of user adoption behavior and how investments in new technologies are considered within the business (Venkatesh & Davis, 2000). Benbasat and Barki (2007) criticized TAM and suggested that there should be more emphasis on the antecedents of perceived usefulness and perceived ease of use (Shaw & Sergueeva, 2019). Based on criticism of TAM, numerous authors extended TAM in different contexts by adding theoretical constructs involving social influence processes of subjective norm, voluntariness, and image (Davis, 1986, 1989; Venkatesh & Davis, 2000; Venkatesh et al., 2012). In addition, cognitive instrumental processes of job relevance, output quality, result demonstrability, and perceived ease of use were added (Davis, 1986, 1989; Venkatesh & Davis, 2000; Venkatesh et al., 2012). The updated TAM2 model was used by Nadri et al. (2018) to investigate the key factors of adoption and use of hospital information systems in paraclinical departments. The case study concluded that several factors in the TAM2 were important like users' behavior factors which were essential for the successful adoption of systems but others were not significant in paraclinical departments and in government-owned hospitals (Nadri et al., 2018). Studies with TAM2, preserve the basic structure of TAM and add the predictors of "perceived usefulness" and "intention to use" under social influence (Onan & Simsek, 2019). Rondan-Cataluña et al. (2015) performed a study looking at the chronological view of the main models dealing with the acceptance and use of technology models staring from the 1970s to the present day. Using WarpPLS (non-linear model) and partial least squares (linear model) to test the TAM, TAM2, UTAUT, and UTAUT2 models found the UTAUT2 model obtained a better explanation power than the rest of technology acceptance models (TAMs). This was one reason the UTAUT2 model was chosen over the other models and theories for this study.

TPB was also considered for this study but was eliminated based on Chau and Hu's (2002) study of the acceptance of telemedicine where TPB appeared to be a weaker theory than TAM. Combining TPB and TAM into one integrated model in Chau and Hu's (2002) investigation found the new model resulted in marginal benefits. TPB was designed for finding the psychological factors influencing an individual's decisions and behavior (Pappa et al., 2018). Ajzen (1991) theorized the stronger the intention to participate in a behavior (intention) and the more control (behavioral control) an individual has over non-motivational factors, the more likely the behavior will occur. TAM2 will allow the same type of analysis and data collection to occur as TPB. Combining TAM2 and UTAUT2 could offer some additional benefits but UTAUT2 along with some other information will assist in understanding how the various factors affect a small businesses' ability to properly implement information security technologies by small businesses in Virginia. For the aforementioned reasons, UTAUT2 and the information dealing with external and internal threats, and security policies were chosen for this study. This study will benefit greatly by using the established model to complete a comprehensive assessment to identify the factors and reasons why businesses and their employees are falling short in protecting the business from bad actors (Cheng, 2019; Davis, 1986; Taylor & Todd, 1995; Sánchez et al., 2013).

Figure 1

UTAUT2 framework



Discussion of Relationships Between Concepts

Information security management has become a key strategic issue for many businesses since information is often one of the most important assets a business can own with information systems as the backbone of many public and private businesses to ensure information flow (Cisco, 2018; Hiscox, 2019; Karlsson et al., 2017; National Institute of Standards and Technology, 2019). To keep information safe, businesses need to implement security measures. Properly implementing security measures means getting everyone in the business behind them and sometimes external players.

Small businesses' implementation of security information technology can depend of many factors that can drive its acceptance and use. The TAM helps predict an employee's behavioral intention to use a system determined by the two beliefs of perceived usefulness and

perceived ease of use (Venkatesh & Davis, 2000). The TAM is widely accepted and provides different aspects to system implementation. Cheng (2019) referenced the predictive power of the TAM as being found to be slightly higher than that of the theory of planned behavior; however, the TPB arguably offers more useful information when developing a system. The theory and model's results can conflict sometimes as the Sánchez et al. (2013) study found the relationship between attitudes and intentions is insignificant when controlling for the influence of perceived ease of use and perceived usefulness on intentions. The TAM2 builds on the previous model by adding the theoretical constructs spanning social influence processes and cognitive instrumental processes (Venkatesh & Davis, 2000; Williams et al., 2015). The TAM and TAM2 model are viable alternatives to carry out this study; however, the UTAUT2 can perform most of the same functions and offers some flexibility with extending or modifying the model.

Previous UTAUT Findings

The UTAUT identified performance expectancy, effort expectancy, social influence, and facilitating conditions as key factors where the first three factors were theorized and found to influence behavioral intention to use a technology (Venkatesh et al., 2012). Behavioral intention combined with the last key factor of facilitating conditions assist in determining technology use (Venkatesh et al., 2012). UTAUT also used the four moderators of age, gender, experience, and voluntariness as a means to support predicting behavioral intention to use a technology within an organizational context (Venkatesh et al., 2012). UTAUT2 extended the model by adding salient predictor variables while examining more related consumer behavior by altering the prior perspective from organizations to individuals (Huang & Kao, 2015; Venkatesh et al., 2012). In addition, the new constructs of habit and price were added to consider the role of behavior and

take into account product quality, cost, and price as they influence technology adoption decisions, respectively (Huang & Kao, 2015; Venkatesh et al., 2012).

UTAUT2 Technology Adoption

UTAUT2 studies offer valuable insight into explaining technology adoption in different contexts. Gharaibeh et al. (2018) investigated the determinants that affect the adoption of mobile banking services. The shift by banks to self-service channels like ATMs and internet banking showed customers were willing to move away from the traditional banking cutomer interface and now banks are deciding to which degree to spend in mobile banking as a new fully interaction channel between the bank and its customers (Gharaibeh et al., 2018). Gharaibeh et al. (2018) added mass media and trust as two important factors to the UTAUT2 for their study. Gharaibeh et al. (2018) showed new factors can be added to the study to test new constructs.

UTAUT2 Price Value and Investment Behavior Modifications

For this study "price value" is considered the tradeoff between the perceived benefits of using an applications and the cost for using them or the investment behavior regarding the buying and deploying of security information technology systems (Venkatesh et al., 2012). Normally, the price value factor of the UTAUT2 model provides the purchase behavior assessing the trade-off between benefits and sacrifices (Huang & Kao, 2015). In this study, the business owner or manager's investment behavior is influenced by their attitudes, which may be influenced by cost-benefit evaluations and subjective perceptions of small businesses concerning the usefulness of security information technology systems (Heyder et al., 2012). Price value has both an internal influence where successful investment in technology can lead to improved productivity, while unsuccessful deployment of systems can lead to undesirable consequences such as employee frustration, loss revenue, or bankruptcy (Venkatesh, 2000; Weishäupl et al.,

2018). By looking at price value to investigate the attitudes of decision makers will allow the study to understand more than the monetary tradeoffs usually looked at in the UTAUT2 (Morosan & DeFranco, 2016; Ravangard et al., 2017; Venkatesh et al., 2012).

Tradeoff of Price vs Threats

Insider threats are increasingly becoming more detrimental and frequent, affecting critical infrastructure (Walker-Roberts et al., 2018). Cyber threats are so common that businesses have become numb to the headlines (Wilding, 2016). It is important for small businesses to recognize that cyber attackers can strike anywhere they wish, while the business's security defenses must attempt to defend the entire security perimeter (Fielder et al., 2016). The infrequency of large scale cyber attacks against a specific business provides decision makers with a limited sample of knowledge to form generalizations about cyber threats (Gomez & Villar, 2018). Like cyber security threats, insider threats represent a deviant behavior that is essentially difficult to predict (Ho & Warkentin, 2017). Both cyber and insider threats pose a major threat to small businesses where security practices typically fail to detect fraud, espionage, or theft of information at the earliest stages when the minimum amount of damage has occurred and the problem can be mitigated (Aldawood & Skinner, 2019; Ho & Warkentin, 2017). Technologies perceived to be less risky are also perceived to be more beneficial and vice versa, so small business leaders need to decide if the benefits of introducing new security technologies to counter cyber and insider threats is worth the risk or price (Van Schaik et al., 2017). By addressing this as a tradeoff dealing with price value, the study will delve into how business leaders perceive the tradeoff between price and the cost of dealing with insider and external threats. The model proposed by Venkatesh et al. (2012) and Huang and Kao (2015) looked at purchase behavior assessing the trade-off between benefits and sacrifices. The model used for this study will help determine if the

price value of dealing with insider and cyber threats play a role in management's decision to implement new security technologies.

Security Policies as a Facilitating Condition

Facilitating conditions will seek to understand the degree to which users can access organizational and technical resources needed to support information technology use (Venkatesh et al., 2012). Employees are more likely to use a new technology when they perceive their behavior will be supported with the availability of resources and conceptualized knowledge (Macedo, 2017; Shaw & Sergueeva, 2019). Individuals do not always have complete control over security systems due to external conditions but helpful facilitating conditions are positively related to IT acceptance when top management support them (Shaw & Sergueeva, 2019).

This study focused on security policies as a facilitating condition to help further our understanding of the impact they have on deploying security information technology. A business should use a top-down approach to define its overall security strategy and scope combining policies with technology to create a acceptable information security environment (Sohrabi Safa et al., 2016). Implementation of security policies is intended to help businesses manage their information security in an effective manner (Santos-Olmo et al., 2016). To ensure sustainable growth, businesses must exploit their core technologies to grow a reliable security environment where the integration of security policies, human resource management, facility management, and information technology security management are combined to achieve security compliance (Kim & Chang, 2014). Developing security policies along with business leaders allocating the appropriate funding for information security help build the businesses' information security culture (Santos-Olmo et al., 2016). The study's investigation illuminated a business manager's understanding of how security policies interact with the decision to deploy new technologies.

Understanding the relevance of security policies in a business leader's decision-making process to implement new security technolgies may play an important role.

Existing UTAUT2 Model

The framework also used effort expectancy, social influence, performance expectancy, hedonic motivation, and habit as part of the existing UTAUT2. Effort expectancy will look at the degree of ease related to a customer's use of technology (Venkatesh & Davis, 2000). Effort expectancy involves the employee as a customer evaluating the effort necessary to complete a task using a given information system (Morosan & DeFranco, 2016). Social influence defines the extent to which consumers perceive that others (e.g., family and friends) believe they should use a particular technology (Venkatesh et al., 2012). Social influence can positively contribute to a user's behavior where individuals exposed to higher levels of cues to action can positively effect an individuals' intention to adopt cybersecurity technologies (Li et al., 2019). Gupta et al. (2010) found that social influence positively affects adoption of technologies, whereas anxiety negatively influences a participants' intentions to adopt technology.

Hedonic motivation has been shown to play an important role in determining technology acceptance and use when an individual has fun or pleasure from using a technology (Venkatesh et al., 2012). Aswani et al. (2018) also showed hedonic motivation was a significant factor in deriving an individual's behavioral intention. Ravangard et al. (2017) and Venkatesh et al. (2012) showed that an individual's behavioral intention increased when their experience using technology was enjoyable.

Performance expectancy will seek to understand an employee's utilitarian value for using a new security information system that enables them to complete their activities (Macedo, 2017; Venkatesh et al., 2012). The utilitarian benefits (extrinsic motivation) from implementing a new

security system includes monitoring internal and external threats while managing and controlling particular types of attacks responsible for increasing a users' motivation to continue using the system (Venkatesh et al., 2012; Yuan et al., 2015). Previous studies have found that effort expectancy has a significant effect on performance expectancy but not on intention to use (Shaw & Sergueeva, 2019; Tamilmani et al., 2019; Venkatesh et al., 2012). According to UTAUT, performance expectancy and effort expectancy are theorized to influence behavioral intention to use a technology, while behavioral intention and facilitating conditions determine technology (Venkatesh et al., 2012).

Proposed Model

The proposed model will also look at the relationship between attitude and behavior, where behavioral intention is postulated to forecast user behavior, also referred to as a habit (Huang & Kao, 2015). The UTAUT model also uses the four moderators of age, gender, experience, and voluntariness as a means to support predicting behavioral intention to use a technology within an organizational context (Venkatesh et al., 2012). These moderators are expected to influence intentions and behavior indirectly by their effects on the theory's more proximal determinants (Ajzen, 2011).

The proposed model removed voluntariness from its moderators. Voluntariness shows the extent to which potential adopters perceive the adoption decision of a new technology to be non-mandatory (Venkatesh & Davis, 2000). Venkatesh et al. (2003) further illustrated that gender, age, and users' experience can show the moderating effects on the constructs of performance expectancy, effort expectancy, and social influence over users' intention to adopt without using voluntariness. Voluntariness was removed as being less relevant to the goals of this research study.

Summary of the Conceptual Framework

The TAM2 and the UTAUT2 are appropriate frameworks for this study, but the UTAUT2 was chosen. UTAUT2 is a powerful predicting framework that can effectively explain and analyze people's technology acceptance behaviors (Huang & Kao, 2015). The UTAUT2 will give insight to businesses on how employees will respond to implementation of new security systems based on their perceived ease of use and perceived usefulness. Hwang et al. (2017) mentioned spending on information technology security in 2014 increased to $71.1 billion or 7.9%, doubling information technology budgets over the same period. In addition, businesses continue the need to invest in information technology security to protect their vital resources and keep the business solvent. The Hiscox (2019) report outlines why this is such a major issue, almost half of small businesses underwent a cyber-attack in the past 12 months, an increase of 14% from the 2018. The purpose of this qualitative case study is to add to the body of knowledge by furthering the understanding of small businesses' failure to properly implement information security technologies resulting in the loss of sensitive and proprietary business information. When viewed within the framework of the UTAUT2, small businesses may understand why security implementation is lacking.

Definition of Terms

Availability. Ensuring timely and reliable access to and use of information in a specified location and in correct format (Nieles et al., 2017).

Behavior intention. Intention to use a technology, which in turn is determined by the person's attitudes and his/her subjective norms toward the behavior (Baptista & Oliveira, 2015).

Computer self-efficacy. One's ability to learn, use, and interact with computer systems (Bhattacherjee et al., 2018).

Confidential. Protecting information access and disclosure from unauthorized access, including means for protecting personal privacy and proprietary information (Nieles et al., 2017).

Cybercrimes. Term describing a broad range of criminal activities and linked to Internet- or technology-linked malicious acts such as cyberwarfare, cyberterrorism, and cyber threats (Tsakalidis et al., 2019).

Cyber threats. Any circumstance or event with the potential to adversely impact business operations (including mission, functions, image, or reputation), business assets, individuals, or other businesses through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service (Committee on National Security Systems, 2015).

Data integrity. The property refers to the protection of data against unauthorized access or corruption. Data integrity covers data in storage, during processing, and while in transit information (Nieles et al., 2017).

Effort expectancy. The degree of ease related to a customer's use of technology (Venkatesh & Davis, 2000).

Experience. The direct effect of subjective norm or intentions may diminish with increased system experience over time (Venkatesh & Davis, 2000).

Facilitating conditions. The degree to which users can access organizational and technical resources needed to support information technology use (Venkatesh et al., 2012).

Habit. Relationship between attitude and behavior, where behavioral intention is postulated to forecast user behavior (Huang & Kao, 2015).

Hedonic motivation. Fun or pleasure derived from using a technology (Venkatesh et al., 2012).

Image. Degree to which the use of a system is perceived to enhance one's social status with the workplace social environment (Venkatesh & Davis, 2000).

Insider threat. Insiders are employees, contractors, consultants and vendors who can be a targeted by outsiders or hackers to circumvent or betray the business by providing unauthorized access to the businesses' sensitive information (Yasin et al., 2018).

Integrity. Methods ensuring data are real, accurate, and guarding against improper information modification or destruction to ensure information non-repudiation and authenticity (Nieles et al., 2017).

Intentions. Are assumed to capture the motivational factors that influence a behavior; they are indications of how hard people are willing to try, of how much of an effort they are planning to exert, in order to perform the behavior (Ajzen, 1991).

Intention to use. Is determined by two beliefs: perceived usefulness and perceived ease of use (Venkatesh & Davis, 2000).

Job relevance. The individual's perception regarding the degree to which the information technology system is applicable to an individual's job (Venkatesh & Davis, 2000).

Objective usability. When the increased use of a specific system increases causing the user's knowledge and anxiety to be adjusted leading to independence of the user's experience (Venkatesh & Davis, 2000).

Output quality. How well an information system performs those activities it was designed to accomplish (Venkatesh & Davis, 2000).

Perceived ease of use. The degree to which a person believes that using information technology will be free of effort (Venkatesh & Bala, 2008).

Perceived enjoyment. Adjustments resulting from a user's system interaction having an added influence on system-specific perceived ease of use (Venkatesh & Davis, 2000).

Perceived usefulness. The extent to which a person believes that using information technology will enhance their job performance (Venkatesh & Bala, 2008).

Performance expectancy. An individual's perception that an Information System enables the completion of an assignment (Venkatesh et al., 2012).

Price value. Purchase behavior assessing the trade-off between benefits and sacrifices (Huang & Kao, 2015).

Result demonstrability. Tangible results based on using an information system (Venkatesh & Davis, 2000).

Security controls. The management, operational, and technical controls (i.e., safeguards or countermeasures) necessary for a robust security posture, prescribed for a system to protect the confidentiality, availability, and integrity of the system and its information (Nieles et al., 2017).

Small businesses. Businesses designated by the Small Business Administration as being small based on their size standards which vary by industry and are generally based on the number of employees or the amount of annual receipts the business produces (SBA Business Credit and Assistance, 2019).

Social influence. The extent to which consumers perceive that others (e.g., family, co-workers, and friends) believe they should use a specific technology (Venkatesh et al., 2012).

Subjective norm. A person's perception through perceived social pressure that they should perform or not to perform a behavior (Huang & Kao, 2015).

System integrity. The condition of a system wherein its mandated operational and technical parameters allow its intended functionality to occur in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental information (Nieles et al., 2017).

Usage behavior. The manner in which a person acts or performs (Venkatesh & Davis, 2000).

Voluntariness. The extent to which potential adopters perceive the adoption decision to be non-mandatory (Venkatesh & Davis, 2000).

Assumptions, Limitations, Delimitations

Notably, the researcher made some assumptions and encountered a number of limitations while performing this study. The researcher's assumptions were a lack of technology functionality by participants, a failure to understand security terminology, and knowledge of internal and external threats. The assumptions were required because small businesses operate in a multitude of organizational hierarchies, function using numerous differing business processes, and are subjected to variances in their market environments (United States Census Bureau, 2018). The researcher had to make assumptions that small business owners and managers would understand that businesses need to protect themselves and they may not understand the technologies available to accomplish this task. In addition, businesses should know if they have been attacked, which sometimes does not occur.

Predetermining certain assumptions about the research allowed the researcher to focus on certain aspects of each business, holding some of the unknowns' constant with the intent for the study's results to be more reliable. Additionally, the researcher recognized that the qualitative study would be influenced by limitations and sought to mitigate them. The limitations occurred

because the researcher could not account for every eventuality such as limiting the study to one type of business or ensuring the same technology was being deployed by all businesses involved in the study. Moreover, the researcher had limited control over the study's participants and their operating environment. The researcher investigated each unique businesses' security architecture and its funded plans for enhancements, as they existed at the time of the study. Delimitations also played a key role in this study with the geographic area of participants being limited. As a result, taking the limitations into account, the study was designed to thoroughly explore and understand the subject matter. The assumptions, limitations, and delimitations for this qualitative study and their impact on the study's findings are outlined in the next section.

Assumptions

To clarify, an assumption was made by the researcher that the owners of small businesses would understand that businesses need to protect themselves from internal and external threats dealing with their information system technologies. Rohn et al.'s (2016) study indicated that nonprofessional computer users find it difficult to understand the functions and practices of the various software and hardware security features and this has not improved much over time. Consequently, the lack of understanding has a significant negative impact on owners and managers, who are expected to make security decisions on the operations of the business without the knowledge of how security technology functions can serve to proactively identify and counter threats. The risk for the study is that managers may not understand security terminology, software or hardware functionality, so when interviewed, the interviewees may not be able to understand the questions to provide any relevant data to the research study. To remove some of the semantics from the study's questions during the interview process, generalized security terminology will also be incorporated.

A principal assumption used for the study is that owners will know if their small business have suffered an internal or external attack. Information security is about awareness at its most fundamental level with owners, managers and employees knowing what to protect and how to protect it, along with knowing how to respond when things go wrong (Kaila & Nyman, 2018). If managers do not understand information security and the numerous challenges they must defend against, then they may not even be aware they have been a victim of a crime. Managers are sometimes unaware of advanced persistent threats as the attacks are deliberate slow-moving cyberattacks designed to gain unauthorized system access and spread quickly through a businesses' network without their knowledge, stealing intellectual property and sensitive internal business documents in the background without interrupting network services (Friedberg et al., 2015). In other words, the scope of the assumption is that owners and their employees understand what a threat is and knowing there are numerous threats they may or may not be aware of, that exist. The risk for the study in the event this assumption is false means there may not be a fundamental understanding of information security measures and how they should be implemented to protect businesses' operations.

Limitations

The study's limitations are described below and future research using different methods can aid in overcoming some of the limitations described. The qualitative study's limitations involved time and funding. Within the short span of time this study, a broader look at the topic could not be investigated. No funding was provided for this study, so the researcher had access to limited resources to expand the research population. In addition, the qualitative study was limited to investigating only security technologies small businesses had previously or were currently implementing. Since each small business operated as a separate entity following their own

implementation schedules with different operating procedures and policies, the study was unable to investigate the similar technologies operating within the same type of business environment. Consequently, the limitation had implications on the comprehensiveness of the information collected for a specific security technology. The focus of this study applied to generalized security implementations of any security technology which limits its results from being applied on a broader scale. The findings of this qualitative study may also be limited in their replicability, as outsourcing security information security functions occurs at some businesses, technology continues to change at a rapid pace, and personnel training is unequal.

Delimitations

The emphasis of this qualitative study was to address the failure of small businesses to properly implement information security technologies resulting in the loss of sensitive and proprietary business information. The qualitative study's delimitations involved participation of mostly small businesses located within Virginia. Delimitations of the study's participants to a small geographic area restricted the sample size diversity of small businesses available throughout the Virginia area. Specifically, the delimitation was necessary to limit the scope of the study, so meaningful data could be collected and analyzed within a specified period of time. Deciding why a manager would implement information security technologies, the researcher choose to use the UTAUT2 over the value focused thinking approach, which often leads to development of objectives for evaluating alternatives or the creation of alternatives (Dhillon et al., 2016).

Significance of the Study

The purpose of the qualitative case study was to add to the body of knowledge by furthering the understanding of small businesses' failure to properly implement information

security technologies resulting in the loss of sensitive and proprietary business information. The significance of the qualitative study was its contribution to the existing knowledge by addressing some of the gaps noted by Nguyen et al. (2015) such as small businesses view that new information technology can be an opportunity or a threat. In addition, Santos-Olmo et al. (2016) pointed out businesses are more dependent on information security management systems today making them vital for the development of small and medium-sized enterprises. Since small business operate with more constrained budgets, this study's results may help with planning strategic and tactical decisions on protecting information (Mayadunne & Park, 2016). Additionally, small businesses adoption of Information Technology is relatively low and the failure rate for technologies implemented continues to be high. The study's significance can be seen in its incorporation of Biblical teachings whereby good stewardship and ethical principles are adhered to.

Reduction of Gaps

The study was designed for the researcher to understand small businesses' reluctance to appropriately implement information security technologies. The impact and scope of inadequately planning for security technologies is an important activity for small to medium size businesses to perform, as potentially one of the biggest issues a business faces today is how to defend itself from potential cyber-attacks, where approximately 72% of cyber breaches have occurred (Fielder et al., 2016). Factors affecting small businesses need to be considered in this area as gaps exist in improving an organization's information security culture and how to control employees' behavior that contributes to increasing problems with protecting business data, information, and knowledge, which makes the implementation of security technologies riskier (Santos-Olmo et al., 2016). The review of existing literature also emphasized several gaps with

regards to technology, employees and policies in small businesses dealing with internal and external threats affecting the implementation of security systems (Kim & Chang, 2014; Nazareth & Choi, 2015; Yasin et al., 2018). In addition, the literature has gaps in how implementation of security systems and their acceptance by employees translate into safeguarding a business from cyber threats created by social engineering threats that are dynamic and constantly evolving (Aldawood & Skinner, 2019).

Cybersecurity investment opportunities are generally a unique class of cost savings investments managers must decide on when trying to avoid the cost associated with cybersecurity breaches (Gordon et al., 2014). The decision to what degree to protect a business from internal and external threats is usually a decision based on risk. Threats and risks to information technology vary on how businesses will approach curbing their exposure depending on their risk assessment capabilities, level of risk tolerance, and business culture (Peterson et al., 2018). Researching the behaviors of employees' malicious non-compliance with security policies could have possibly prevented several high-profile insider threat cases from occurring, if risk assessment capabilities research could be advanced (Ho & Warkentin, 2017). For managers to proactively accept a level of risk requires the business to be able to perform or acquire services to complete an in-depth risk assessment. The lack of literature in this area severely affects the ability of managers to understand the significance of a risk assessment. Recent data suggests decision makers try to save as much money as possible by looking for costless or very cheap solutions, often ignoring the expected value approach when making investment decisions (Mayadunne & Park, 2016).

Implications for Biblical Integration

The prevalence of sophisticated, targeted, and malicious cyberattacks is growing on a global scale, forcing businesses to continually evolve their understanding of the cyber environment to re-evaluate and update the businesses' security posture to minimize risk. To minimize threats against business interest, infrastructure, and employees, a comprehensive cybersecurity strategy must include implementing technologies that assist businesses with overcoming technical issues, leadership challenges, and cultural problems in the business (Wirth, 2017). Colossians 3:23, telling us, "And whatsoever ye do, do it heartily, as to the Lord, and not unto men tells us work is for the Lord not us" (King James Bible, 2017). Business executives must inspire their employees to adopt a culture of security and challenge them to be the best they can be, by engaging in the businesses' mission and work efforts following God's commandments. This leadership will drive changes to the culture and lead personnel to put security at the forefront of their actions, overcoming technical issues as they are found.

God has a purpose for all businesses and individuals get to decide if they want to align their desires with God's plan or reject it and act in a rebellious fashion (Van Duzer, 2010). By allowing cyber criminals to steal proprietary information, businesses fail on two fronts. First, they are not good stewards of what has been given to them. The Lord gave five talents to a faithful servant who saw those talents grow and the Lord was pleased with his faithful servant, so much so, that he made him a ruler over many things (King James Bible, 2017, Mathew 25:20-21). God, teaches us that as stewards, leaders are responsible for the small and large things people entrust them with. By not implementing security technologies to protect the business from cyber threats, the business leaders fail to carry out God's commandments.

The second business failure involves denying God's will that a business should thrive to carry out his work. Van Duzer (2010) proposes that the paradigm of businesses equates to more than making a profit and should be strategically focused on achieving God's perspective of helping others. To make this happen, the executives leading a business need to live by God's teachings. Schouten et al. (2014) let executive's personal values and beliefs influence their own decisions and the values, beliefs, and behavior of their subordinates. It is true that non-Christians can be bestowed grace and be very successful in business; however, that does not free Christians from following God's commandments. Through personal convictions, executives following God's tenants may want to lead efforts like corporate social responsibility, environmental stewardship and protection of the business. These efforts are important in showing how businesses can be good stewards of what they are given; however, protecting the business from cyber-attacks by implementing the right tools is paramount to successfully completing any efforts.

Mello (2015) pointed out that businesses' strategic workforce planning should ensure the right employees are hired and trained with the right skill sets to make ensure they can be fully qualified to perform their jobs. Cyber criminals prey on the most vulnerable links in your company's security--employees. Understanding that the training of employees is necessary to support operations also holds the company together and when done successfully aligns an employee's skills up with God's intended goal for their lives. Businesses must use a combination of advanced technical measures along with managerial efforts to raise awareness of personnel to ensure the efficiency of the businesses' information systems by providing the right training to employees so they develop the right capabilities to fend off an attack (Aldawood & Skinner, 2019). This alignment pleases God because it prepares man to do God's will for their life,

leading to great works, which is like offering their prayers to God. It also prepares employees to accept implementation of new systems, knowing they are living a life supporting God's plan for their life.

Relationship to Field of Study

This study is directly related to the field of business administration due to the study's focus on the implementation of security information technology within the business environment. Roses et al. (2015) proposed business activities and information technology (IT) within the business must be strategically aligned to a degree that the business mission, objectives, and plans support the information technology strategic goals and objectives. Yeh et al. (2015) built on this further by relating the development of information technology capabilities has become a significant issue of information management in businesses where information technology capabilities influence business strategies, operations and services being offered by the business. In today's fast paced business world, the strategic alignment of business and information technology is a necessity, promoting the business' growth through prudent investments in technologies.

People are the most important asset most businesses possess. To obtain the maximum out of these resources, businesses must invest time and effort to properly train them on how to learn new job skills or improve their current skills. Maity et al. (2019) explained once trained, individual's habits of interacting with information technology should follow a normative behavior pattern, where behaviors are categorized as rules of prudence (i.e., judgment) or as categorical rules (i.e., choices), but this does not always happen. The UTAUT2 can assist in explaining how associations between the values of one behavior can relate to the values of another behavior (Venkatesh et al., 2012). Therefore, business managers can understand what

factors may be changed or needed to ensure employees follow a normative behavior pattern when dealing with the implementation or use of information technology. This study will bring add to the understanding of how small businesses make decisions about the implementation of security technologies.

Summary of the Significance of the Study

The significance of the study is to understand small businesses' reluctance to appropriately implement information security technologies. Peace be within your walls and security within your towers! (Psalms 122:7, English Standard Version). God wants us to be safe and secure in our houses and that extends to our businesses. With 72% of cyber breaches occurring against small and medium size businesses, the high risk of getting attacked is probable with the potential to fend off the attack, less plausible without properly installed security devices (Fielder et al., 2016). This study is intended to identify factors that may influence the behavior of business leaders and managers to motivate them into understanding what it takes to improve their businesses' security posture. The results of this qualitative case study can inform businesses on ways to increase their overall security culture. Business leaders can adopt strategic initiatives based on the factors identified, focusing their efforts toward finding ways to overcome the negative ones, to improve business operations.

A Review of the Professional and Academic Literature

The purpose of this literature review is to analyze the relationship between the proposed Unified Theory of Acceptance and Use of Technology model and the existing empirical literature on the implementation of information technology systems. The proposed model will build upon existing work in the field, furthering the research of Davis (1989) and Venkatesh et al. (2012) who presented data on the importance of understanding individual acceptance and use

of information technology. With small businesses under constant attacks in the U.S. at an ever-increasing rate and assailants costing small businesses billions of dollars in lost revenue and output it is critical that the research provide insights into the use of technology by individuals (Cyber Crime: An Existential Threat to Small Business, 2019; Sen & Borle, 2015; Wikina, 2014).

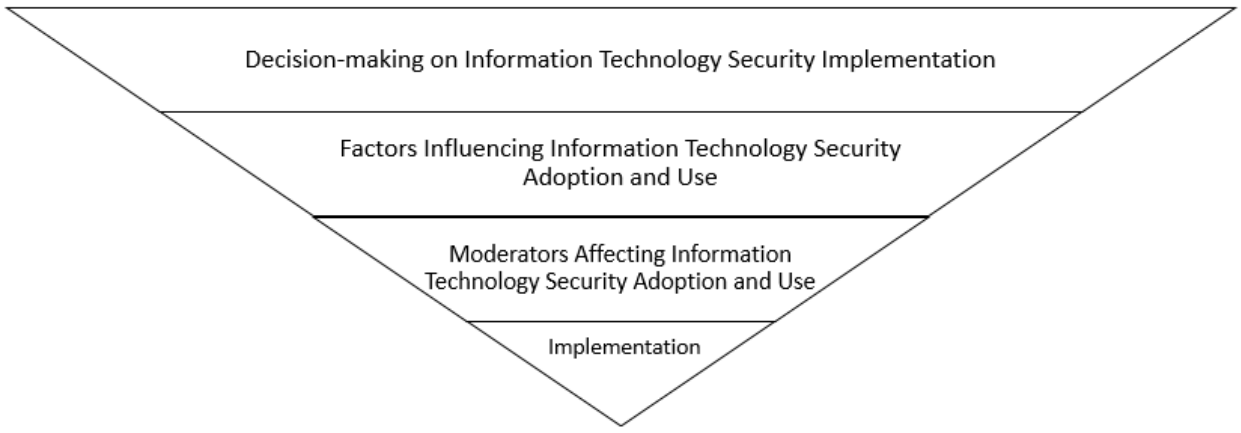
Prior research in the area of information technology use was introduced by Davis (1986) through the TAM, Ajzen (1991) through the TPB, and the original UTAUT model proposed by Venkatesh and Davis (2000). These models built upon Fishbein and Ajzen's (1975) Theory of Reasoned Action, which aimed to explain the relationship between attitudes and behaviors within human action. The Theory of Reasoned Action predicted an individual's behavioral intention and their behavior of taking part in a specific activity according to their attitude and subjective norms (Mi et al., 2018). Davis (1986) TAM built upon this by creating a reliable way to predict a user's acceptance of a wide-range of new technologies (Sánchez et al., 2013). Ajzen's (1991, 2011) TPB went further by looking at a user's attitude toward behavior, subjective norms, and perceived behavioral control and predicting how these constructs working together would shape an individual's behavioral intentions and behaviors (Cheng, 2019; Taylor & Todd, 1995). Venkatesh et al. (2012) expressed that attitudes and intentions once activated will automatically guide behavior unconsciously where the need for mental activities is unnecessary. The original UTAUT explained intentions to use information systems based on perceptions following the technology acceptance model (Davis, 1986; Venkatesh et al., 2003) and was updated to include more contextual factors, such as price value and habit, known as UTAUT2 (Venkatesh et al., 2012). The UTAUT2 model attempts to explain a user's intentions to use an information system and subsequent usage behavior with additional constructs designed

to take consumer use into account (Carter & Grover, 2015; Taherdoost, 2018; Venkatesh et al., 2012).

The conceptual framework section identified the UTAUT2 model (Davis, 1986; Venkatesh et al., 2003, 2012) as the foundation for this research and clarifies how the problem under investigation relates to the model. The literature review will involve an extensive overview and combination of existing literature related to the research topic using a comparison and contrast approach. The study is designed to understand small businesses' reluctance to appropriately implement information security technologies based on the UTAUT2 model and its extension. General and specific topics for the study will involve current literature on: (a) leadership, (b) facilitating conditions, (c) security policies, (d) effort expectancy, (e) social influence, (f) price value, (g) performance expectancy, (h) threats (insider and cyber), (i) habit, (j) Hedonic motivation, (k) UTAUT2 moderators: Age, gender, and experience, (l) behavioral intention, and (m) use behavior. Figure 2 illustrates how information technology implementation is affected by the different constructs and moderators.

Figure 2

Literature Review Visual Roadmap



Decision-Making

Small business owners can be firmly entrenched in their positions and often have wide-ranging latitude in managing the affairs of their businesses where insular decision-making is their preferred way of making decisions (Woods et al., 2017). Managers sometimes struggle with how to create information technology driven business decisions that add value to the business while controlling risks through suitable investment strategies (Kauffman et al., 2015). Business leaders need to set the preferred course for the business to follow, especially in acquiring information technology. There are several ways business leaders can make decisions about information technology and how that technology can impact their workforce.

Leadership

Business leaders are responsible for driving a firms' innovation performance by setting the strategic vision and direction of how a business will operate (Caridi-Zahavi et al., 2016; Woods et al., 2017). Businesses need to effectively implement competitive strategies in order to help ensure long-term growth and profitability, so the business will survive (Hardcopf et al., 2017). In small businesses, the owners or senior managers make most, if not all, of the strategic decisions that will guide how the business will operate and determine how information technology will be used (Nguyen et al., 2015). Their decisions are based on their current perspective of the situation, personal knowledge and judgment, and communication skills (Kim et al., 2017; Nguyen et al., 2015).

General Decision-making

Kurnia et al.'s (2017) data showed that decisions are made through the lens of "bounded rationality" or the strong influence that biases play in a manager's decision-making processes. The brain is undeniably not a computer, which can work with perfect knowledge and unbounded

rationality; therefore, it is an easy victim to all kinds of biases and lapses (Kurnia et al., 2017). Confirmation bias is pervasive throughout a leader's decision-making process where information that coincides with their existing beliefs tends to take on more relevance than other evidence collected (Von Bergen & Bressler, 2018). Cognitive biases can also have a positive impact on a leader's decision-making processes by putting less burden on their time and cognitive resources; however, leaders must always be aware that cognitive biases may lead to errors as information is disregarded in an irrational fashion (Von Bergen & Bressler, 2018).

Leadership Decision-making

Small business leader's reliance on their decision-making processes is critical to the business's investment in security technologies. Leaders are biased towards resolving business profit gaps by implementing short-term cost cutting tactics straying from long-term strategic goals (Hardcopf et al., 2017). Like the bias involved in resolving profit gaps, a small business leader's decision on security technology investment strategy can be affected, so long-term strategic goals dealing with security are superseded by short-term cost cutting tactics (Hardcopf et al., 2017). A leader's decision to purchase new security technologies or to upgrade existing security systems hinges on the belief the current system will perform the job in a satisfactory manner without the expense and aggravation of upgrading the system (Wang et al., 2018). Cognitive biases and short-term cost savings may lead business leaders to decide on continuing to use outdated technologies over protecting the business' assets more appropriately (Hardcopf et al., 2017; Wang et al., 2018).

Technology Impact on Decision-making. With technology playing such a pivotal role in modernizing businesses, more than half of small businesses in the U.S. do not have the right technologies to compete and stay current on global information technology security trends

(Olufemi, 2018; SBA, 2015). Hiscox (2019) confirmed through data research that barely half (52%) of small businesses had a clear strategy to deal with current or future cyber security issues. Currently, small businesses are facing a major issue related to identifying their technology adoption criteria, which helps guide their decision in the adoption of technology innovations to manage their information and big data (Olufemi, 2018). Numerous studies have shown that the decisions to adopt information technology is dependent on a leader's commitment to the adoption process (Kim et al., 2017; Nguyen et al., 2015). This commitment is further jeopardized, causing businesses to falter when leadership fails to apply the right type of leadership style for the type of business and the nature of the problem (Bonsu & Twum-Danso, 2018). Noguerol and Branch (2018) showed leadership styles could play an important part in making decisions with transformational leaders being more capable of making informed decisions in fields outside of their area of expertise.

Leadership Implementation of Technology. Small business leaders recognize the importance of information technology and make every effort to incorporate and utilize its power in order to increase the competitiveness of business and to create new business opportunities (Kim et al., 2017). Caution is essential in implementing or adopting any new technology where difficulties range from a lack of man-power, finances, other physical resources, and environment issues where technologies can be inherently besieged with security issues (Ghaffari & Lagzian, 2018; Kim et al., 2017). To overcome the risk in implementing new technologies, business leaders must develop investment strategies that promote the best path forward. This requires aligning information systems strategy with a well thought out business strategy that recognizes business risk can inhibit business success (Moon et al., 2018; Shao, 2019). Business leaders need to be aware of existing and emerging risks associated with the newest information technologies

to minimize issues with data leakage, cyber threats and fraud (Noguerol & Branch, 2018; Mikhed & Vogan, 2018; Tsakalidis et al., 2019). Business leaders are responsible for making investment decisions where an emphasis on efficiencies and profitability may require changes to a business' information architecture taking risk mitigation strategies into effect (Aldawood & Skinner, 2019; Angst et al., 2017; Tsakalidis et al., 2019). The tangible goal of a profit seeking business is to make money for its stakeholders, business leaders must make rational decisions that put the business's interest first by strengthening the company's position within the marketplace and to accomplish this, the deployment of information systems is reliant on employee's attitudes and behaviors (Bhattacherjee et al., 2018; Kmieciak et al., 2018; Nguyen et al., 2015).

Business Goals. Understanding the goals of a business are important in deciding why a business might decide to support or not support implementation of information security technology. Rohn et al. (2016) pointed out that companies are segregated by their size which is influenced by the number of employees and revenue generation which impacts the environment the company operates within. This operating environment along with human resource skills and constraints are pivital in how a business may make decisions about implementing security technologies. Small business leaders, like any executive at a large corporation make management decisions daily. For good or bad, their value-added decisions are observed and interpreted by subordinates who positively or negatively react when those decisions are imposed on them (Mazereeuw-van der Duijn Schouten et al., 2014; Ruben & Gigliotti, 2016). Individuals are influenced by how they perceive their leaders would want them to act, causing a leader's influence to extend well beyond themselves and affect how an individual thinks about operations, group dynamics, organizational culture, and the introduction of new technologies

(Ruben & Gigliotti, 2016). This leadership influence also affects how employees' information security behavior is incorporated into the social fabric of the business making it an important focus for information systems deployment (Guhr et al., 2019; Hwang et al., 2017).

Facilitating Conditions

Facilitating conditions are the perceived degree to which users can access organizational and technical resources needed to support information technology use (Ho et al., 2017; Venkatesh et al., 2012). It is also the extent to which employees believe the business will support the system's use or impede its acceptance (Howard et al., 2017; Yuan et al., 2015). The UTAUT2 theory carried this construct further by incorporating consumer beliefs by expanding the construct from previous research where it was almost exclusively based on a user's internal belief system operating within an organization (Morosan & DeFranco, 2016; Venkatesh et al., 2008). Consumer's facilitating conditions under the UTAUT2 model exposed that the construct was a significant predictor of intentions of consumers to use information technology (Dwivedi et al., 2016; Venkatesh et al., 2008, 2012). This condition was based on consumers' needs to accomplish specific task-related behaviors requiring the use of information technology systems and without those systems being present in the environment, consumers would be incapable of performing the interactions necessary for them to complete their task (Baptista & Oliveira, 2015; Dwivedi et al., 2016; Huang & Kao, 2015; Venkatesh et al., 2008, 2012).

Facilitating Conditions With UTAUT and UTAUT2 Models. The UTAUT model theorized that researchers should expect facilitating conditions to predict behavioral intention when effort expectancy was not included in the model (Dwivedi et al., 2019; Venkatesh et al., 2003). Effort expectancy in the UTAUT2 model is an individual's estimation of the effort or ease of use it will take to complete a task using a specific information system (Baptista & Oliveira,

2015; Morosan & DeFranco, 2016; Venkatesh et al., 2003, 2012). Prior studies of technology acceptance explicitly showed the relationship between facilitating conditions and behavioral intention where facilitating conditions influenced the behavioral intention of individuals even in the presence of effort expectancy (Ajzen, 2011, 2012; Cheng, 2019; Venkatesh et al., 2003). Venkatesh et al. (2003) contended one could predict behavioral intention through facilitating conditions only if effort expectancy was not included in the model. When using the UTAUT2 model, facilitating conditions are factors found to be very important in adoption of technology when consumers perceive they have adequate knowledge about a service or product and the system has the proper help support to assist them when they encounter any issues with using the system, regardless of effort expectancy (Gharaibeh et al., 2018; Huang & Kao, 2015; Morosan & DeFranco, 2016). Low facilitating conditions such as the lack of top management support or failure to provide help support are often blamed for information technology resistance (Bhattacherjee et al., 2018; Dwivedi et al., 2019).

Technology Adoption. Using UTAUT2 as the basic model, facilitating conditions are significantly related to actual usage and do not influence the intention to use a technology (Palau-Saumell et al., 2019). An individual's intention to use a system is determined by two beliefs: perceived usefulness and perceived ease of use (Venkatesh & Davis, 2000). Yuan et al. (2015) found facilitating conditions did not predict a user's intention of continuing the use of a system countering previous studies that found facilitating conditions are an important factor in the adoption of technology (Dwivedi et al., 2016; Venkatesh et al., 2008, 2012). Tavares et al. (2018) hypothesized that facilitating conditions would have a significant influence on user behavior; however, their study's results showed that facilitating conditions were nonsignificant in predicting behavioral intention. Alalwan et al. (2017) identified behavioral intention and

facilitating conditions as two factors that were key predictors of adoption behavior. Alalwan et al. (2017) result aligned with most universal results from previous studies involving the UTAUT2 model which indicated facilitating conditions influenced behavioral intentions (Dwivedi et al., 2019; Gharaibeh et al., 2018; Huang & Kao, 2015; Morosan & DeFranco, 2016). In addition, when moderated by experience and age, facilitating conditions will have a significant influence on usage behavior (Venkatesh et al., 2003).

Security Policies

Businesses are strategically trying to gain an advantage over their competitors. This process in today's business environment requires businesses to improve productivity and reduce operating cost (Kim & Chang, 2014; Shao, 2019). One way to gain a strategic advantage over one's opponents is to use cloud computing, artificial intelligence or robotics to advance business operations and improve transactions (Chaâri et al., 2016; Duncan et al., 2015; Kauffman et al., 2015). When a company introduces new technologies into its environment, it must ensure security policies are also implemented so employees understand what management's expectations are with securely using new information systems (Sommestad et al., 2015). Implementing information security policies is one way to assist businesses in providing directions to employees to counter the risk of information technology systems being compromised, help reduce the probability of fraud, and prevent the loss of proprietary business information (Almeida et al., 2018; Bolek et al., 2016; Trim & Lee, 2019).

Trust Issues. Noguerol and Branch (2018) highlighted that leaders not in the information technology field described distrusting information technology and further do not fully understand security policies. This lack of knowledge when kept unaddressed can cause employees to place the blame on managers and leaders as an justification to not comply with security policies,

undermining the importance of the role policies play on the deployment and use of new information technology systems (Noguerol & Branch, 2018). Trust between employees and managers has shown to influence technology and cloud adoption, social media, and website usage decisions and privacy and security issues (Paliszkiewicz, 2019). A lack of trust (one party's confidence in an exchange partner's reliability and integrity) can be detrimental in security compliance where it is strategically important for managers of a business to lead employees in their adherance to information security policies, where an employee's non-compliance is commonly known as one of the most difficult aspects of information technology security (Hwang et al., 2017; Paliszkiewicz, 2019). Mao et al. (2017) pointed out that relying heavily on human knowledge and involvement alone is not sufficient to devise security policies for information system protection (Bélanger et al., 2017). If managers and leaders display a positive security posture emphasizing security awareness, then employees are more likely to adhere to security policies increasing security compliance (Angst et al., 2017; Paliszkiewicz, 2019).

Security Compliance. An employee's inability to comply with security policies, not only puts the business in jeopardy but can also impact their intention to use systems (Sommestad et al., 2015). Individuals who adapt and conform to new security policies early on actually benefit the business as opposed to late adopters who cost the business more money in last minute security changes that could cause the system to become inoperable or overwhelm the service desk with last minute calls (Bélanger et al., 2017). Early conformers of security policies are important as Bélanger et al. (2017) discovered TPB's suggested influence of subjective norm on intention does not apply to this group. Individuals who have adopted good information security awareness are more confident in using new technologies (Alharbi et al., 2017). Shillair et al.

(2015) found a strong factor in deciding whether or not individuals complied faithfully with security practices involved habits. Educating the workforce on security policies and how they impact work was a significant predictor in compliance which was strongly linked to habits and experiences (Shillair et al., 2015).

Social Acceptance. Social norms also influence an individual's decision to more readily comply with security practices, if perceptions of following security policies are considered "normative'' behavior (Shillair et al., 2015). Security awareness can facilitate employee social networks in favor of security policies and procedures that not only reduce security problems but help convey how important security enforcement is to system security, resulting in stronger group norms (Goo et al., 2014). Grimes and Marquardson (2019) confirmed that system quality induces positive social norms and increases evaluation to influence intentions of behavior (Woo et al., 2018). Sommestad et al. (2015) replaced perceived norms with anticipated regret, which theoretically is similar to unsafe expectations where individuals are more likely to comply with security policies when they perceive the probability and severity of incidents as high. This compliance better predicted an individuals intention to adopt technology (Sommestad et al., 2015).

Effort Expectancy

Attitudes contribute to shaping one's behavioral intention to use a technology, which inevitably will affect one's usage of the actual system (Howard et al., 2017; Taherdoost, 2018). Behavior intention towards using a technology is determined by a person's attitudes and his/her subjective norms toward the behavior (Baptista & Oliveira, 2015; Ghaffari & Lagzian, 2018). Some recent studies have indicated that effort expectancy has a significant effect on performance expectancy, but not on intention to use (Shaw & Sergueeva, 2019; Tarhini et al., 2016; Yuan et

al., 2015). These studies are contrary to other studies where performance expectancy, effort expectancy, and social influence were theorized and proven to influence behavioral intention to use a new technology (Macedo, 2017; Venkatesh et al., 2012).

UTAUT Behavior Intention Factors. UTAUT predicts that the behavior intention of an information system is affected by the three factors of performance expectancy, effort expectancy, and social influence (Howard et al., 2017; Venkatesh et al., 2012). As part of this three-way relationship, effort expectancy is defined as the ease related to an individual's use of a system (Macedo, 2017; Tavares et al., 2018; Venkatesh & Davis, 2000). This also applies to consumers' use of technology where its degree of ease determines effort expectancy (Aswani et al., 2018; Tavares et al., 2018; Venkatesh et al., 2012). Effort expectancy was part of the original TAM model where perceived ease of use was incorporated into the UTAUT2 model as effort expectancy (Davis, 1989; Tavares et al., 2018; Venkatesh & Davis, 2000).

Perceived Ease of Use. The perceived ease of use influences the perceived usefulness of a system, leading to individuals using the system more while adding to an individual's experiences with the system (Davis, 1989; Howard et al., 2017; Sheppard & Vibert, 2019). Couple perceived ease of use with an individual's attitude which helps shape their behavioral intentions to use a technology will add to an individual actually using a system more (Howard et al., 2017). These patterns of usage create a pattern of attitude-intention-behavior resulting in system acceptance and use based on the Theory of Reasoned Action (Davis, 1989; Sheppard & Vibert, 2019). As a branch of social psychology, the Theory of Reasoned Action predicts an individual's behavioral intention and their behavior of taking part in a specific activity according to their attitude and subjective norms (Mi et al., 2018). Venkatesh et al. (2012) articulated

attitudes and intentions once activated will automatically guide behavior unconsciously where the need for mental activities is unnecessary.

Technology Introduction. The usual pattern after introducing a technology follows a relatively simplistic path that leads individuals to use or not use an application based on their belief that it will help them accomplish their work better (Davis, 1989). Two separate studies by Oliveira et al. (2016) and Alalwan et al. (2017) found empirical evidence supporting a significant relationship between effort expectancy and behavioral intention, which leads to effort expectancy influencing the adoption of technology. If an individual perceives technology to be useful but believes that the technology's benefits are not worth the effort necessary to realize those benefits then the benefits derived from using the technology are not worth acquiring (Davis, 1989; Dwivedi et al., 2019; Venkatesh et al., 2012). In this case, perceived ease of use is not validated, so an individual would not want to adopt the system and the attitude-intention-behavior cycle would be interrupted causing experiences not to occur.

Social Influence

Venkatesh et al. (2012) described social influence as the extent to which consumers perceive that others (e.g., family, co-workers, and friends) believe they should use a particular technology. These social influence processes play a role in how UTAUT2 reflects the impacts of three interrelated social forces impinging on an individual facing the opportunity to adopt or reject a new system: subjective norm, voluntariness, and image (Ghaffari & Lagzian, 2018; Lai, 2017; Venkatesh & Davis, 2000). Social influence is in every part of a person's life from the mundane, everyday purchases to important life decisions where our choices are strongly influenced by the choices of others (Gershman et al., 2017). The influence of others is part of an ongoing process through which messages are sent to influence individuals where overtime these

messages help shape the sensibilities and responses of the receiver (Ruben & Gigliotti, 2016). Small business leaders like all people are socially influenced with those influences affecting how they will act towards acquiring security information technology for their business.

Subjective Norm. Subjective norm is an individual's perception of social normative pressure from influential peers that they should perform or not to perform a particular (Ajzen, 2012; Huang & Kao, 2015; Venkatesh et al., 2012). To understand how social norms, affect business leaders, one must understand how individual choices are influenced by shared affiliations with social groups. Studies and theories of social influence have an underlying assumption that individuals within a social group share a common set of utility functions or shared preferences (Gershman et al., 2017; Steffen et al., 2018). These shared preferences make group members believe that copying behaviors of one another will most likely lead to more rewarding outcomes (Gershman et al., 2017). Group members on the outside of a group's norm can feel like they are being punished for norm violations (Dannals & Miller, 2017; Gelfand et al., 2017). To feel part of a group, communication must take place among the group members.

Ruben and Gigliotti (2016) suggested communication encompass a complex arrangement of verbal and nonverbal messages that can lead to planned and unplanned messages that individuals need to decipher. The decoding of these messages involves both the sender and receiver constructing the meaning through cues based on a number of factors including past experiences, culture, previous learning, context, and their relationship history (Ruben & Gigliotti, 2016). Watching and understanding other group members' communications and choices may be the key to small business leaders determining their future course of action (Gershman et al., 2017).

Social Network Influence. Besides the actual messages, small business leaders' decisions are influenced by the groups they become part of. More than ever before with the fast growth of social network sites (SNSs) such as Twitter, LinkedIn, and Facebook, business leaders are able to easily find and join homogeneous groups with similar business goals and backgrounds (Horng & Wu, 2019). As members of these SNSs, over time members grow to identify closely with the group and as the union becomes stronger the extent to which they are influenced by the leader of that group increases (Steffen et al., 2018). It is important to understand that social influence plays a notable role in various domains of human behavior where influence from the group drives the human selection behavior of members (Pan et al., 2017). This means people tend to select what their friends select to be part of the group where the individual identity is forsaken for the group identity or norm (Pan et al., 2017; Steffen et al., 2018).

UTAUT Voluntariness. When the UTAUT model was modified the voluntariness was dropped from the moderating variables that influence the constructs which are now age, gender, and experience (Baptista & Oliveira, 2015; Venkatesh et al., 2012). The social force of voluntariness is now one of the three interrelated social forces impinging on an individual facing the opportunity to adopt or reject a new system (Ghaffari & Lagzian, 2018; Lai, 2017; Venkatesh & Davis, 2000). Under the original conceptualization of UTAUT, voluntariness assumed that individuals had a choice in using information systems because business leadership may not have made its adoption mandatory (Dwivedi et al., 2019; Venkatesh et al., 2012). With UTAUT2, by eliminating voluntariness from the moderating variables it only impacts the social influence–behavioral intention relationship by making voluntariness applicable to accepting voluntary technology acceptance and use among consumers (Venkatesh et al., 2012). This new relationship takes into account consumer behaviors as being entirely voluntary, resulting in no variance in the

voluntariness construct it making non-relevant for most situations (Dwivedi et al., 2019; Venkatesh et al., 2012).

Price Value

Small businesses are forced to make investment decisions constantly to further the business' existence and grow their markets. The Risks-Benefit framework is an analysis between risks and benefits of buying, leasing, outsourcing or staying the same as changes within the information technology environment that may affect the businesses' profit margins are disregarded (Kim et al., 2017). Motylska-Kuzma's (2017) pointed out that the scope of all financial decisions in family owned businesses was geared towards optimization of the capital structure, where limited funding affects investment decisions, with the intent to grow the businesses' wealth. Reliance on internal and bank financing can have an impact on a small businesses' ability to invest in information technology with sales, assets, business market value, age, location, and owner education as dominate influences that can impact a small businesses' information technology investments (Gill et al., 2019). To determine what types of information technology investments must occur, businesses must perform a risk assessment determining the likelihood their business will be attacked and the cost analysis that the attacks aftermath will cost them more money than the cost of implementing new security information technologies.

UTAUT2 Consumer Context. The UTAUT2 model extended the UTAUT model to the consumer context, by adding the 'price value' to the UTAUT2 model to represent the mental tradeoff between the perceived benefits of an application and the monetary cost for using it (Venkatesh et al., 2012). Price value was also incorporated in the UTAUT2 model because product quality, cost, and price will influence adoption decisions by consumers and managers (Huang & Kao, 2015). As information technology products geared towards consumers became

more prevalent in the marketplace, price became key factor as consumers bore more of the costs associated with the use of these products (Baptista & Oliveira, 2015). The tradeoff between benefits and sacrifices can be further emphasized by looking at the perceived value of what one gets for what one gives or the higher the cost of an item the more the perception can lead to the item having no net value (Shaw & Sergueeva, 2019). Baptista and Oliveira (2015) contend when the benefits of using an application are perceived to be greater than the associated monetary cost then the price value is positive.

Price Value Importance. When the price value is an important factor, price may influence the perception of value with other benefits being compared to it to determine a positive, negative, or neutral value (Shaw & Sergueeva, 2019). Perceived value has multiple dimensions, both positive and negative where benefits, such as quality perceived value, emotional perceived value, social perceived value, or price perceived value can be offset by the sacrifices of effort, relationships, brand loyalty or reliability to name a few (Dwivedi et al., 2016; Sampaio & Saramago, 2016; Shaw & Sergueeva, 2019). Most of these perceived values can play a factor in the "price value" that consumers believe a product should cost. These are important aspects as a business leader is a consumer but they must also consider Motylska-Kuzma's (2017) statement where the scope of financial decisions is targeted to optimize the businesses' capital structure to grow the businesses' wealth.

Investment Tradeoff Decisions. Investment tradeoff decisions by managers deciding to adopt innovative security technologies for a business are usually made under conditions of uncertainty and must account for benefits derived from its intrinsic payoff, but also the scope of the technologies use in the marketplace (Chulkov, 2017). Understanding the scope of the technologies used in the marketplace can help determine if the products lifecycle will be short or

long. Businesses are more likely to adopt existing technologies over newer technologies as they consider them safer assuming information technology adoption decisions by the firm is not reversible (Chulkov, 2017; Nie et al., 2018). This basically means once a security technology is implemented by a business it will be used by that business for a long period of time (Chulkov, 2017; Nie et al., 2018). The business must also take into account investment switching costs that can reduce or increase the businesses' overall costs (Nie et al., 2018).

Balancing Act. Business leaders often underestimate the cost of implementing technology changes while displaying a risk aversion or reluctance to transition from more mature technologies to newer technologies that can offer more benefits (Chronopoulos & Lumbreras, 2017). Balancing investment decisions to determine the level of securing its tangible and intangible assets requires the business leader to determine the implementation of new security technologies through a comparison of evaluating the current security level versus the projected security needs of the business while taking into account switching costs and business profits (Chronopoulos & Lumbreras, 2017; Kim & Chang, 2014; Nie et al., 2018). Information technology is evolving continuously and most small businesses do not keep abreast of current information security trends (Dor & Elovici, 2016; Weishäupl et al., 2018). This makes it necessary to design a formalized risk assessment structure that supports protecting the businessess' information while prioritizing its many information technology acquisitions (Dor & Elovici, 2016; Weishäupl et al., 2018).

Risk Assessment. To leverage the businesses' competitive advantage the risk assessment must answer the following questions: (a) What can go wrong?, (b) What is the likelihood that it would go wrong?, and (c) What are the consequences? (Cherdantseva et al., 2016). Small businesses in their decision-making processes are aware that not all cyber-attacks will affect their

business operations identically and are also very aware that some assets are more important than others requiring a higher level of protection. Business managers examining information security investments either take a riskier approach to investment or follow a more traditional approach of being risk neutral (Colicchia et al., 2019; Mayadunne & Park, 2016).

In both instances, business managers must address the questions posed by Cherdantseva et al. (2016) by looking at the breach probability. Mayadunne and Park (2016) described the breach probability where data are compromised being dependent on the two factors of threat probability and the information's vulnerability. The threat probability looks at the attempted breach of information, while the information vulnerability is the likelihood that the threat once comprehended will be successful (Mayadunne & Park, 2016). To address this, risk must be interpreted as a set of scenarios based on an undesirable event occurring, where the probability of the event occurring is measured by the consequences or damaged caused by it and the number of possible scenarios that might cause damage (Cherdantseva et al., 2016). This assists managers in their decision-making process of determining whether to implement new security technologies or rely on the status quo (Cherdantseva et al., 2016; Mayadunne & Park, 2016).

Performance Expectancy

The UTAUT model identified the following four significant determinants to explain user acceptance and usage behavior: performance expectancy, effort expectancy, social influence, and facilitating conditions (Dwivedi et al., 2016; Gharaibeh et al., 2018; Venkatesh et al., 2003, 2012). These constructors as they are known sometimes remained the same in the UTAUT2 model (Dwivedi et al., 2019; Macedo, 2017; Venkatesh et al., 2012). Performance expectancy is the degree to which using a technology will provide benefits to consumers in performing certain activities (Venkatesh et al., 2003, 2012). This means an individual's perception is that using a

new information security technology system will enable them to achieve gains in job performance (Rahi & Ghani, 2018; Venkatesh et al., 2003, 2012). These gains can be realized in a myriad of ways as information systems can provide benefits to users through improved performance, increased speed, more efficiency and accuracy in completing a task (Morosan & DeFranco, 2016).

Users' Intention. Based on the perceived gains individuals believe they receive while performing a variety of tasks with a new system, performance expectancy was found to influence their intentions to use the information technology system (Baptista & Oliveira, 2015; Morosan & DeFranco, 2016). Rahi and Ghani (2018) and Wang et al. (2017) uncovered through their studies that performance expectancy and effort expectancy were prominent factors in a user's intention. Morosan and DeFranco (2016) found that performance expectancy was the highest predictor of intentions while Tavares et al. (2018) study proved it to be an excellent predictor of behavioral intention to indicate an individual's intent to adopt new technologies.

Attitude. Dwivedi et al. (2019) believed attitude, as a mediator was needed between performance expectancy and behavioral intention and between effort expectancy and behavioral intention. This is because an individual's attitude when using an information system that is easy to use, beneficial, and accurate will lead them to use the system (Dwivedi et al., 2019). Prior studies illustrated that performance expectancy and effort expectancy significantly influence the intention to use new systems but data also showed the attitude's effect was weak, implying that attitude explains only part of an individual's intentions (Huang & Kao, 2015; Rahi & Ghani, 2018; Tamilmani et al., 2019). Dwivedi et al. (2019) also recognized attitude was central to behavioral intentions and usage behaviors with a direct effect on usage behaviors (Tamilmani et al., 2019).

Repetitive Behaviors. Venkatesh et al. (2012) pointed out that repetitive behaviors can result in establishing attitudes and intentions that can be prompted by signals in the environment. These mental cues unconsciously activate an individual's attitudes and intentions and once activated they automatically guide behavior without the need for conscious thought (Rahi & Ghani, 2018; Venkatesh et al., 2012). This behavior is also known as a habit were individuals automatically behave a specific way based on prior learning or experiences and it has also shown to be a good predictor of new technology adoption (Tavares et al., 2018). Tavares et al. (2018) and Ravangard et al. (2017) found that habit was a good predictor of behavioral intention having a significant impact on it while Morosan and DeFranco (2016) found that performance expectancy was the highest predictor of behavior intentions with habit being less of a predictor. Aligning with Morosan and DeFranco (2016) and Howard et al. (2017) found the moderator of experience strongly affected the relationship between performance expectancy and an individual's behavioral intention.

Threats (Insider and Cyber)

There is no doubt, according to Hiscox (2019) and the Council of Economic Advisers (2018), that recent trends demonstrate small businesses are more likely to be a victim of cyber-attacks now, than ever before. For this reason, mitigating the risk of a cyber-attack is a good business decision (Cisco, 2018; Stanciu & Tinca, 2017). Two threats on the rise that businesses are encountering today are cyber and insider threats (Almeida et al., 2018; Cisco, 2018; Fielder et al., 2016; Stanciu & Tinca, 2017). New types of electronic crimes or cybercrimes are being devised by criminal perpetrators as technology continues to evolve, leading to a variety of criminal offences based on the interested party's perspective (Brar & Kumar, 2018; Reep van den Bergh & Junger, 2018; Tsakalidis et al., 2019). Cybercrimes encompass a broad range of

criminal activities and the term is often interchangeable with other Internet-or technology-linked malicious acts such as cyberwarfare, cyberterrorism, and cyber threats (Li et al., 2019; Raban & Hauptman, 2018; Tsakalidis et al., 2019). The various terms used to describe the numerous types of cybercrimes make it difficult to classify or categorize cybercrime related offences and occurrences into standardized categories (Li et al., 2019; Raban & Hauptman, 2018; Tsakalidis et al., 2019).

Cybercrime. Reep-van den Bergh and Junger (2018) explained cybercrime as a broad and imprecise concept that may be categorized into three broad areas for clarification. First, crimes against computers (usually involves unauthorized access of the systems boundaries where accessing computer(s) is the perpetrators focus; Reep-van den Bergh & Junger, 2018). Second, crimes using computers (committing identity theft, phishing scams and the fraudulent use of credit online are types of crimes using information and communication technologies (Reep-van den Bergh & Junger, 2018). Last, crimes 'in' computers, where criminal content is the crime (may include pornography, threats of violence or terrorism; Reep-van den Bergh & Junger, 2018). When looking at cybercrimes one must represent them as a single or multiple events targeting a perspective target that may involve repeated interactions with the target (Stanciu & Tinca, 2017). Looking at cybercrimes from a risk perspective, Almeida et al. (2018) tries to categorize security risks and barriers into two categories of technical orientation (technical vulnerabilities of equipments, protocols and policies) and management orientation (security vulnerabilities from a social perspective). Under security vulnerabilities top managers and employees can play a central role in mitigating these vulnerabilities (Almeida et al., 2018; Cisco, 2018).

Insiders. Insiders are employees, contractors, consultants and vendors who can be a targeted by outsiders or hackers to circumvent or betray the business they are part of by providing unauthorized access to the businesses' sensitive information (Yasin et al., 2018). These insiders are commonly known to businesses as insider threats that must be accounted for in security operations. Cisco threat researchers investigated the insider threat phenomenon and discovered from January 2017 to June 2017, there were 7,500 users out of 150,000 users in 34 countries over 1. 5 months suspiciously downloaded more than 3. 9 million documents on the businesses' cloud networks (Cisco, 2018). Ho et al.'s (2018) research showed that insider threats pose a significant problem for businesses as trusted interactions in both physical and virtual organizations can be taken advantage of through cyber espionage which is on the rise and emphasizes the capture of trade secrets and proprietary information. With the move of business data to the cloud, cybercrime from insider threats poses the most significant source of risk as cloud service providers will possess large volumes of high-value data from many various sources (Duncan et al., 2015).

Various Business Threats. Small businesses can suffer cybercrime from an external perpetrator, internal employee (insider threat) or it can result from an insider threat working in unison with an external perpetrator (Trim & Lee, 2019). Insider threats that have elevated or privileged access to information systems and strategic information can have a graver impact on business operations as they have intimate knowledge of key business processes, which may exhibit information system flaws that a perpetrator could take advantage of (Ho & Warkentin, 2017). Understanding that the monitoring of employees and safeguarding business sensitive information is important, business leaders need to think in terms of how to reduce the risks associated with cybercrimes to reduce monetary losses and reputational damage (Sen & Borle,

2015; Trim & Lee, 2019). One way to identify organizational weaknesses is to perform a risk assessment that can address all types of threat sources, a single broad threat source, or a trusted insider where an employee's (insider threat) social networking on-line behavior is also accounted for when seeking to identify organizational vulnerabilities (National Institute of Standards and Technology, 2012; Trim & Lee, 2019). According to Aldawood and Skinner (2019), it is important to recognize social engineering as a social networking on-line behavior threat that seeks to exploit a weakness in human nature can be mitigated through implementation of modern preventive tools and the security systems.

Cyber Protection. Identifying insider threats is a difficult proposition as objective data sources only provide a fraction of the information needed on electrionic activity which is required to detect deceptive practices or breaches from outside perpetrators working jointly with insiders (Ho & Warkentin, 2017). As employees play the most important role in safeguarding the interest of busineses when it comes to attacks, providing them with the necessary tools they need such as newer security technologies may be the only way to implement countermeasures to identify and mitigate internal and external threats (Aldawood & Skinner, 2019; Tsakalidis et al., 2019; Ullaha et al., 2018). A businesses'goal when investing in cyber security is to select a set of cyber security controls that maximize protection of business assets while at the same time prioritizing budget requirements to acquire new security technologies (Fielder et al., 2016; Kohnke & Shoemaker, 2015). Within this decision, managers are determining if the reduction in risk to the business in implementing new security technologies is due to financial restrictions, limited resources, and adequate know-how is offset by their need to use technology to facilitate another process (Almeida et al., 2018; Osborn & Simpson, 2018).

COVID-19. A recent threat to small businesses' cyber security posture is the global COVID-19 pandemic. COVID-19 is responsible for prematurely terminating people's lives, destroying the social fabric of society, and closing the doors to many small businesses. Fairlie's (2020) study showed 3.3 million or 22% of active business in the United States ceased operations over the decisive 2-month window from February to April 2020. The pandemic impacted construction businesses especially hard leading to a 27% decline in the number of businesses operating between February and April 2020 (Fairlie, 2020). Businesses continuing to operate also suffered a decline in business income as government jurisdictions temporary closed down businesses in certain areas to combat the virus (Fairlie, 2020). A loss of revenue meant businesses today face a conundrum on what investments they will make which could impact their cyber security posture.

Selecting the Right Technologies. Sen and Borle (2015) found that implementation of information technology security is correlated with a higher risk of data breach within both a state and industry sectors, which is counter to what, should be expected. One explanation they offered for this problem is that managers decided to invest in the wrong security technologies that did not help employees secure resources (Sen & Borle, 2015). A business leader's deficiency in understanding network fundamentals is exacerbated by an absence of internal resources and employee expertise that can hinder the deployment of new security technologies (Cisco, 2018; Kim & Chang, 2014). This becomes even a bigger issue when dealing with enterprise systems where the complexity of implementing security system functionalities is associated with enormous monetary investment and a reliance on increasing labor requirements making the risk or probability of failure as high (Shao, 2019).

Habit

Habit is the extent to which people tend to perform behaviors automatically contingent upon them learning the process through repetition or based on experience of prior behavior (Dwivedi et al., 2016; Morosan & DeFranco, 2016; Venkatesh et al., 2012). Venkatesh et al. (2012) argued adding habit to the UTAUT2 model was necessary to account for unconscious actions as well as conscious intentions that behavioral intention are influenced by (Shaw & Sergueeva, 2019). Huang and Kao (2015) believed habit showed an individual's prior behavior and the degree to which people believe the behavior to be automatic making it a good predictor for the UTAUT2 model. Habit was added to the UTAUT2 model after being conceptualized within the UTAUT model by association with the user experience where it was thought to exert only a moderating role (Macedo, 2017; Venkatesh et al., 2012). It is theorized that habit is modelled as having both a direct and automatic effect on technology use and an indirect effect through influencing behavioral intention (Macedo, 2017; Tavares et al., 2018).

Habit as an Influencer. Prior studies have found that habit is a statistically significant driver directly affecting technology use between behavioral intention and technology use (Baptista & Oliveira, 2015; Tavares et al., 2018; Venkatesh et al., 2012). Morosan and DeFranco (2016) found habit, hedonic motivations, and social influences have relatively lower effects than those associated with performance expectancy which they found to be the highest predictor of intentions. According to Huang and Kao (2015), past behavior, the reflex behavior, and the individual experience make up the three parts of the habit construct. Past behavior is described as a user's prior behavior and is related to the probability of the user performing the same behavior under the same conditions repeatedly (Huang & Kao, 2015; Sommestad et al., 2015). Ajzen (2011) believed based on empirical evidence that there is a strong correlation between past and

later behavior supporting the rationale that past behavior is the best predictor of future behavior (Hagger et al., 2018). In addition, research has shown past behavior as a stronger predictor than other social factors when correlated with the user's past intentions (Brown et al., 2018; Hamilton et al., 2017).

Employee Habits. Implementation of new security technologies within a business structure requires employees to assimilate to the new applications over a period of time in order for employees to feel comfortable using the new tools in their work environment (this could take several weeks; Davis 1986). Employees who establish their own routines, norms and habits tend to gain experience over time, which leads to the accumulation of more experiences based on their established and stable interactions with using new technologies (Huang & Kao, 2015). Habits defined by past behaviors means an employee would have a tendency to perform the behavior on future occasions based on habitual rather than reasoned responses (Ajzen, 1991). Habitual intentions developed through experience of using information technology systems decreases the need for discussions and coordination demonstrating that a habit is a strong predictor of technology usages in promoting behavioral changes (Huang & Kao, 2015).

Habit Versus Behavioral Intention. Venkatesh et al. (2012) promoted within the UTAUT2 model that behavioral intention is influenced by unconscious actions as well as conscious intentions (Shaw & Sergueeva, 2019). Habit is an automatic behavior performed by an individual based on their past actions where behavioral intention refers to an individual making a conscious effort to perform or not perform a specific task in the future (Huang & Kao, 2015). Prior studies have found that habit had a positive and significant impact on behavioral intentions (Baptista & Oliveira, 2015; Morosan & DeFranco, 2016; Ravangard et al., 2017). Shaw and Sergueeva (2019) could not validate that habits caused individuals using a specific information

technology system over a period of time to develop habitual behaviors as prior studies had shown.

Positive and Negative Intentions. Ain et al. (2016) found an insignificant habit-behavioral intention relationship towards a specific information technology system based upon the fact that users perform routine tasks frequently and using the specific system frequently did not create a behavior that became habitual. For other users, even having a positive attitude toward using a new system and believing in its benefits is still not enough to actually adopt a new system as actual adoption is strongly impacted by other subconscious or automatic predictors of behavior, such as a strong incumbent system habit (Wang et al., 2018). In the incumbent system habit scenario, the employee's habits towards an existing system will likely reduce the extent to which positive attitudes affect their intentions to actually use a new system by impeding changes to their behavior (Lai & Wang, 2015; Wang et al., 2018). These habits are also impacted by gender where men may decide to use new technologies based on their perceptions of its usefulness, whereas women seek technologies that are perceived to be easier to use (ease of use) and meet subjective norms (Wang et al., 2017).

Hedonic Motivation

The original UTAUT model was extended by Venkatesh et al. (2012) to accont for the consumer context emphasizing on hedonic value (intrinsic motivation) of technology users (Tamilmani et al., 2017). Its purpose was to predict the behavioral intention and use behaviour of an individual who derived fun or pleasure from using a technology (Aswani et al., 2018; Tamilmani et al., 2017; Venkatesh et al., 2012). Huang and Kao's (2015) study found the essence of an individual's psychological and emotive experiences had the biggest influence compared to other factors to an individual's intention to use a technology. This was also

supported by Baptista and Oliveira (2015) and Shaw and Sergueeva (2019) whose studies found that hedonic motivation was found to be one of the most significant antecedents of behaviour intention. Palau-Saumell et al.'s (2019) study found that hedonic motivation and behavioral intentions relationships are moderated by gender, age, and experience.

UTAUT2 Moderators: Age, Gender, and Experience

The original UTAUT theory hypothesized that the moderators of gender, age, experience and voluntariness of use played a key role in the relationship amongst the various UTAUT constructs (Howard et al., 2017; Tamilmani et al., 2017). The UTAUT model explained intentions to use information systems looking at performance and effort expectancy, however the theory drew criticism for its complex interactions among the various attributes and moderators resulting in relatively less parsimony hindering its usage and necessitating the theory to be modified to include more contextual factors and moderators to make explaining the theory simplier (Morosan & DeFranco, 2016; Tamilmani et al., 2017). These limitations led to Venkatesh et al. (2012) modifying the UTAUT by identifying key additional constructs and relationships to better integrate the different parts. As part of this update, the modified UTAUT2 removed voluntariness of use as a moderator and attempted to explain the relationship between facilitating conditions (moderated by age, gender, and experience) and behavioral intention (Venkatesh et al., 2012). The UTAUT2 also included moderated relationships by age, gender, and experience pertaining to the three new constructs in the theory making UTAUT2 a more comprehensive theoretical framework (Tavares et al., 2018; Venkatesh et al., 2012). The UTAUT2 attempts to identify the most salient factors affecting relationship constructs; however, it may not be possible to enumerate all factors affecting construct relationships (Carter & Grover, 2015).

Importance of Moderators. According to Dwivedi et al. (2019), moderators can be relevant and add important data only when there are significant differences in moderators across individuals within the same context. Understanding how moderators influence the relationships between the UTAUT2 constructs can enlighten researchers on how individuals may act when new technologies are introduced. Age can be defined as the length of time that an indvidual has lived (Lexico.com, 2019a). As one of the UTAUT2 moderators, age moderates the relationships between effort expectancy, social influence, hedonic motivation, and behavioral intention (Chang et al., 2019). UTAUT research has shown that the degree to which individuals believe that using a technology will increase their task (performance expectancy) is particularly stronger for younger men, focused on performance achievement and driven by instrumental benefits making it more likely they will successfully acquire new technology-related skills over women and older individuals (Celik, 2016). Venkatesh et al. (2003) allude to this as an increase in age brings difficulties in processing task related information and acquiring the required computing skills for task completion. In addition, the difficulty in acquiring new computer skills brought on by age has been found to influence the amount of the anxiety an individual feels when adopting and using new information technologies with older individuals exhibiting higher levels of anxiety and resistance to technology adoption (Chang et al., 2019; Celik, 2016; Khatri et al., 2018).

Gender Moderator. Gender as a moderator refers to the two sexes (male or female) (Lexico.com, 2019b). Chang et al. (2019) concluded that gender moderates the relationships between performance expectancy, social influence, and behavioral intention (Tavares et al., 2018). Like age, gender can influence the amount of anxiety an individual may feel (Celik, 2016). Venkatesh et al. (2012) pointed out the moderating effect of gender was found to be in

conjunction with age and experience with the effect being stronger for older women in their early stages of experience with a new technology (Venkatesh et al., 2012). Experience as a modertor is intended to affect the relationships between social influence, price value, and behavioral intention and between habit behavior and use behavior (Chang et al., 2019). Experience like age and gender can negatively or positively influence the anxiety an individual feels (Celik, 2016).

Experience Moderator. As a moderator, a user's experience is considered as one of the main factors explaining an individual's behavior as experience is gained through time elapsed since the initial use of a technology by an individual (Palau-Saumell et al., 2019). In addition, perceptions and attitudes are more reliable when they are based on direct experience where indirect experiences do not provide as great a confidence (Davis, 1986; Yasin et al., 2018). Weishäupl et al. (2018) found business leaders rely heavily on past experiences to evaluate the effectiveness of their information security investments which can influence future investment decisions. This is supported by Li et al.'s (2019) investigation which showed employees are motivated through cues to action or triggers that make them react based on their past experiences. As a result, business owners who have had direct experience with cybercrimes are more likely to implement security technologies than their counterparts without similar experiences (Li et al., 2019; Weishäupl et al., 2018).

Moderator Impact. Using UTAUT2 model, Venkatesh et al. (2012) found that age, gender, and experience acted as moderators for performance expectancy, effort expectancy, and social influence on behavioral intention just as Venkatesh et al.'s (2003) prior study using UTAUT had shown. Macedo (2017) found gender and age had no significant impact on use behavior. Facilitating conditions on technology use was also moderated by age and experience; whereas, gender, age, and experience had a joint impact on the link between facilitating

conditions and intentions (Venkatesh et al., 2012). UTAUT2 suggests that gender, age, and experience significantly moderate the relationship among facilitating conditions, hedonic motivations, price value, habit, and behavioral intention; however, Yuan et al. (2015) found that these moderators had no statistically significant moderation effects. Tamilmani et al. (2019) found that moderators of gender and age offered no significant influence on an individual's adoption of technologies driven by hedonic motivation. This is a noteworthy change from Venkatesh et al.'s (2012) study's results (Tamilmani et al., 2019).

Behavioral Intention

Behavioral intention to use a technology using the UTAUT model is defined as a conscious plan to perform a behavior determined by the person's attitudes and his/her subjective norms toward the behavior (Baptista & Oliveira, 2015; Gupta et al., 2015). Normally, behavior is determined by intention to perform the behavior where the individual's attitude toward a behavior, their subjective norms, and their perceived behavioral control assist in predicting how they will act (Ajzen, 2012; Mazereeuw-van der Duijn Schouten et al., 2014; Pappa et al., 2018). Ajzen (1991) pointed out those intentions are the motivational factors that influence a behavior and indicate how hard people are willing to exert themselves in order to perform that behavior (Aswani et al., 2018; Guhr et al., 2019). Behavioral intention is considered one of the most important determinants of one's actual behavior, which is determined by one's attitude (positive or negative feelings) towards performing the behavior (Shropshire et al., 2015; Zhang et al., 2012). Typically, the stronger the intention to engage in a behavior, the more likely it will occur (Ajzen, 1991; Kim et al., 2016).

Mandatory Influence. In developing the UTAUT2 model, Venkatesh et al. (2012) theorized that behavioral intention is influenced by unconscious actions as well as conscious

intentions when habit was added as a construct (Santos-Olmo et al., 2016; Shaw & Sergueeva, 2019; Taherdoost, 2018). Macedo (2017) pointed out that an important distinction made using the UTAUT2 model between behavioral intention to use a technology and its actual use is behavioral intention, which is the closest proxy for use behavior (Bhattacherjee et al., 2018). This aligns to previous quantitative studies that typically measured information technology use in terms of how often the targeted system is used and a user's intention to actually use the system as a proxy for actual use behavior (Alalwan et al., 2017; Bhattacherjee et al., 2018; Ravangard et al., 2017). It is important to realize that within mandatory settings, information technology users have very little to no choice in using a particular information technology system, so the users' intention can be severely skewed during a study (Bhattacherjee et al., 2018). Jones et al. (2010) pointed out in mandatory settings perceived ease of use was shown to have a greater degree of significance on intention to use than intention to use which could mean under strict mandatory settings, behavioral intention may not be an appropriate construct (Howard et al., 2017). Measuring intention rather than actual behaviors can be difficult sometimes, as a person's intentions do not always lead to explicit behaviors (Venkatesh et al., 2003).

UTAUT2 Constructs. Studies have shown subjective norms have a significant direct effect on behavioral intention for mandatory use but they did not have the same effect for voluntary usage (Shaw & Sergueeva, 2019; Venkatesh & Davis, 2000; Venkatesh et al., 2003). With UTAUT2 changes geared towards consumers, studies have shown facilitating conditions had only a significant effect in mandatory settings, while effort expectancy has a significant effect on consumers' attitude of use in both mandatory and voluntary usage (Dwivedi et al., 2019; Huang & Kao, 2015). Saumell et al. (2019) contradicted this by showing that higher facilitating conditions had a significant and positive influence on the intention to use. Saumell et

al.'s (2019) results showed performance expectancy, effort expectancy, facilitating conditions, hedonic motivation, habit, and social influence had a significant effect on the actual intention to use. Dwivedi et al. (2019) found attitude had a direct effect on behavioral intention and was influenced by facilitating conditions and social influence. Social influence elements of personality (agreeableness and conscientiousness) have been shown to have a moderating effect on user's behavioral intention to adopt security software (Ho et al., 2017; Shropshire et al., 2015). Previous research also showed that perceived ease of use affects perceived usefulness and, in turn, behavioral intention to use (Bhattacherjee & Lin, 2015; Venkatesh, 2000). This may be significant as managers look to implement security systems, where easier navigation of the system creates an ease of use that is perceived as making the system more useful to its users (Dhillon et al., 2016).

Technology Implementation. Intention determines behavior where intention is reliant on the three factors of subjective norms, perceived behavioral control, and attitude toward the behavior (Ajzen, 2012; Dwivedi et al., 2019; Mathieson, 1991; Pappa et al., 2018). With information technology adoption studies characteristically used to predict behavioral outcomes through the relationship between attitudes and intentions, this relationship may not actually be the best predictor of actual behavior (Shropshire et al., 2015). Palau-Saumell et al. (2019) reinforced Venkatesh et al.'s (2003) findings that performance expectancy was one of the main predictors of the intention to adopt a technology. Behavioral intention and facilitating conditions were significant in predicting usage behavior with facilitating conditions being moderated by age (Venkatesh et al., 2003). Leadership has also been found to be a critical factor in implementing information security technologies as more financial and technical resources are most likely needed to be successful (Goo et al., 2014). Implementation of a strong security culture to

strengthen the businesses' security posture can lead to significant gains in security awareness and employee behaviors towards security implementation (AlHogail, 2015). By combining new technology use with enforcement of new information security policies, businesses can avoid both voluntary and involuntary nonconforming behavior and improve technology acceptance (Bélanger et al., 2017).

Use Behavior

Usage behavior is typically the manner in which a person acts or performs (Venkatesh & Davis, 2000). Tamilmani et al. (2017) and Chang et al. (2019) show behavioral intention and facilitating conditions influence use behavior which is positively influenced by hedonic motivation. Behavioral intention's direct effect on use behavior was insignificant in Chang et al. (2019) when moderated by experience. Ravangard et al. (2017) found price value, hedonic motivation, habit, and usability have positive and significant impact on the behavioral intention, albeit, behavioral intention and usability play a significant role in use behavior. As mentioned by Ravangard et al. (2017), habit impacts use behavior when it is moderated by experience and age (Chang et al., 2019). Huang and Kao (2015) found that both hedonic motivation and use behavior are the main dimensions that influence relationships between the UTAUT2 constructs where usage frequency is predicted to be the most important criterion for enhancing the use behavior.

Consumers. UTAUT2 was expanded to incorporate the use patterns of consumers into the UTAUT model (Venkatesh et al., 2012). Consumer behavior looks at the way people look, buy, use, and evaluate goods and services they perceive will fulfill their needs (Huang & Kao, 2015). When consumers trust an e-commerce website their trust intention is increased which in turn will influence their perception of the sites usefulness, which affects their use of e-commerce

systems (Ho et al., 2017). A consumer can be an employee, manager or leader in the process that Ho et al. (2017) explained is similar to adoption of any technology. In addition, a user's behavior when adopting a new technology is impacted by their emotional, subconscious and rational decision-making responses (Ho et al., 2017). This can be seen when implementing e-commerce systems where information security concerns impact buyer's decisions on using the technology by consciously being skeptical of a systems security status and unconsciously worried about data breaches that may have never occurred (Oliveira et al., 2016).

Businesses. Business organizations usually fall into the following three categories when adopting new technologies: adopters, prospectors, and laggards (Alam et al., 2016). Focusing on the businesses that take the adopter path, their technology implementations are affected by a user's attitude (Alam et al., 2016). Businesses that adopt and implement systems are impacted by the environment the business operates within where the adoption of systems is more complex at the business level than with individual employees (Olufemi, 2018). Making the implementation of technology easier for employees could have something to do with the social influences that employees are subject to where managers, co-workers, and friends affected their beliefs on use behavior (Venkatesh et al., 2003). Ain et al. (2016) also support this view where employees are socially influenced by their peers' beliefs about services, which then influences their behavioral intention. As mentioned earlier, under mandatory settings, users may have no choice in using a security system, so social influences may have no role in behavioral intention (Bhattacherjee et al., 2018).

Potential Themes and Perceptions

The literature review identified certain themes and/or perceptions that emerged through prior studies completed on implementation of information technology and its acceptance. These

themes showed that certain factors had a profound influence on an individual's behavior to use new technologies. Common themes were found regarding how valuable social influence are in the workplace, impact of security awareness on system adoption, and the dual role consumer awareness of technology plays in the workplace (Angst et al., 2017; Dwivedi et al., 2016, 2019; Hwang et al., 2017; Venkatesh et al., 2003, 2012).

Social Influence. Employees become confident with their actions when peers within the organization perform similar tasks (Hwang et al., 2017). This social process is known as subjective norms, which shows an individual's reaction to social preferences when they perform a particular behavior (Cheng, 2019). Studies have shown social identity can affect individual behavior within a group setting for better or worse (Cheng, 2019; Gupta et al., 2015). Carter and Grover (2015) pointed out that social structures and information technology have become, so intertwined they are inseparable. This can affect an individual's integrity, work habits and technology acceptance, if left to the wrong social influences (Ho & Warkentin, 2017; Howard et al., 2007). This social discounting bias can be overcome by management support and leadership influence (Ho et al., 2017; Moussaïd et al., 2018; Ruben & Gigliotti, 2016).

Security Awareness. In today's business environment, small businesses are continually under attack through social engineering designed to exploit their employee's weaknesses by taking advantage of their naivety (Aldawood & Skinner, 2019). This type of attack has a profound influence on an individual's behavior causing businesses to invest in technologies and human security resources (Santos-Olmo et al., 2016; Weishäupl et al., 2018). Most small and medium businesses dealing with cyber security deal with resource constraints where there is a scarcity of cyber security experts (Grimes & Marquardson, 2019; Kim & Chang, 2014; Osborn & Simpson, 2018). To counter these issues, businesses turn towards security awareness training

where several factors come into effect (e.g., cultural diversity and varying knowledge level of employee) (Hwang et al., 2017; Weishäupl et al., 2018).

Ninety-nine percent of business executives responsible for cyber awareness learning convey that security awareness learning is essential to minimize security breaches (Wilding, 2016). Additionally, managers know that for employees to understand information security issues, they need to be trained and the business needs skilled information technology people to assist (Akman & Mishra, 2015; Bolek et al., 2016). This becomes especially difficult as new technologies are invented in shorter technology innovation cycles, meaning employees are exposed to ongoing changes at an ever-increasing pace in their work environments (Guhr et al., 2019; Li et al., 2019). The continuous cycle of launching new technologies in a relatively short period of time results in employees' feeling their daily work demands are more complex and to combat this they should receive a high degree of information security awareness training (Guhr et al., 2019). When new information technology is introduced, Li et al. (2019) found that it is also important to enhance employee awareness. Security awareness and acceptance of new technologies by employees are tied together, especially as information technology security investments are mandated (Angst et al., 2017; Hwang et al., 2017; Osborn & Simpson, 2018).

Consumer Duality. Performance expectancy provides consumers with benefits when they perform certain activities while effort expectancy is the ease associated with a system (Dhillon et al., 2016; Dwivedi et al., 2019; Venkatesh et al., 2012). Using the UTAUT2 model facilitating conditions acts as a significant predictor of consumers' intention to use information technology (Dwivedi et al., 2016; Venkatesh et al., 2008, 2012). Consumers are more likely to use a system when they perceive they have adequate knowledge about the service or product and the system has adequate help support to assist them (Gharaibeh et al., 2018; Huang & Kao, 2015;

Morosan & DeFranco, 2016). It is important to recognize that consumers play a dual role when they are also employees. As employees, facilitating conditions, performance expectancy, effort expectancy, and other constructs can play the same role as they do when thinking of an employee as a consumer (Dhillon et al., 2016; Dwivedi et al., 2016, 2019; Gharaibeh et al., 2018; Venkatesh et al., 2012). The dual role consumers' play as insiders and outsiders of a business can show how their expectations can encourage technology adoption or refuse adoption of new technologies, when something is perceived as skewed (Ghaffari & Lagzian, 2018).

Summary of the Literature Review

Leaders need to understand how all the UTAUT2 constructs and moderators work together to influence employees' use of new technologies. The constructs of facilitating conditions, security policies, threats, and habit have an influence on behavioral intention and use behavior. Facilitating conditions and habit are influenced by the moderators of age, gender, and experience when dealing with use behavior while habit is also impacted by the moderators when dealing with behavioral intention. Effort expectancy, social influence, investments, and performance expectancy influence behavioral intention. Behavioral intention influences use behavior and is moderated by experience. The various studies showed significant and insignificant influences by the various constructs using the UTAUT and UTAUT2 models (Alalwan et al., 2017; Aswani et al., 2018; Baptista & Oliveira, 2015; Sheppard & Vibert, 2019; Venkatesh et al., 2012).

Transition and Summary of Section 1

The purpose of this qualitative case study is to further the understanding of small businesses' failure to properly implement information security technologies resulting in the loss of sensitive and proprietary business information. Research has identified leadership's role in the

implementation of information and communication technologies with supervision and security training identified as important factors in successfully implementing new technologies (Dwivedi et al., 2019; Goo et al., 2014; Hansen & Nørup, 2017; Hwang et al., 2017; Weishäupl et al., 2018; Wilding, 2016). The modified UTAUT2 model represents a comprehensive theoretical framework that offers a roadmap to identify key factors that all businesses have to come to terms with when implementing information security technologies (Morosan & DeFranco, 2016; Venkatesh et al., 2012). The UTAUT2 model will use facilitating conditions, effort expectancy, social influence, performance expectancy, and habit as part of the original model with the additional constructs of security policies, investments, and threats (insider and cyber).

To understand adoption of technology by small businesses, a literature review was conducted to determine the why businesses decide to deploy or not deploy security information technology (Angst, 2017; Morosan & DeFranco, 2016; Ravangard et al., 2017; Venkatesh et al., 2012). The research explored the factors affecting implementation of information security and the reasons small businesses are not proactive in adoption of security technologies to protect their enterprise. Previous studies considering the body of knowledge established theoretical support for reasons small businesses may decide to implement security technologies, but it also showed a gap in the literature regarding the impact and scope of inadequately planning for security technologies. Factors affecting small businesses need to be considered in this area as gaps exist in improving an organization's information security culture and how to control employees' behavior that contributes to increasing problems with protecting business data, information, and knowledge (Santos-Olmo et al., 2016).

This study focused on two primary areas to understand the practices that business managers incorporate in the work environment to ease the transition of new information security

technologies and how do employees perceive changes to the work environment when new information security technologies are deployed. For this research, following the logic of Yin (2014), the research design attempted to link the data collected to the initial questions of study. Bounding the qualitative case study around small businesses allowed an in-depth study on the relevant factors affecting this issue involving small businesses' inability to implement information security technologies. The next section presents the methodology and procedures related to the field study, offering the researcher a framework for answering the study's questions.

Section 2: The Project

To securely compete in the U.S. economy, small business leaders will want to continually invest in security technologies that make their workforce more productive, while ensuring business' transactions are secure and data are protected (Shao, 2019; Taherdoost, 2018; Venkatesh et al., 2008). The introduction of new security technologies within a business environment requires the business to adopt to changes within its technology architecture and at the same time meet the workforce challenges imposed by their deployment (AlHogail, 2015; Dwivedi et al., 2016; Yeh et al., 2015). This section describes the research process chosen to examine small businesses and the factors affecting their ability to defend the business from internal and external threats by identifying the factors influencing their implementation of security information technologies.

This qualitative study was intended to identify the factors influencing a small construction business' implementation of security information technologies. Section 1 of the study focused on defining the problem, identifying the purpose of the research while understanding the underlying information from previous studies. Section 2 identified the research methodology and design that was used to further understand the factors small businesses' need to deal with successfully implementing security technologies. Following a structured roadmap, Section 2 will connect the research design, research questions, data collection and analysis while ensuring reliability and validity are infused throughout this qualitative study's research.

Purpose Statement

The purpose of this qualitative case study is to add to the body of knowledge by furthering the understanding of small businesses' failure to properly implement information security technologies resulting in the loss of sensitive and proprietary business information. The

problem is explored within its own setting through an in-depth study of information security implementation at small businesses will assist in identifying specific factors affecting businesses' deployment of information security technologies. Previous research identified leadership's role in the implementation of information and communication technologies where supervision, information, and training were identified as important factors in successfully implementing new technologies (Goo et al., 2014; Hansen & Nørup, 2017; Paliszkiewicz, 2019).

Leadership is also responsible for making investment decisions where business logic dictates putting a greater emphasis on efficiencies and profitability, leading to a symbolic adoption of new security technologies (Angst et al., 2017). Huang et al. (2014) cited costs, interoperability, security, and privacy concerns as major barriers to the growth of security systems in healthcare. With shorter innovation cycles and the constant development of new security technologies, employees need to adapt to ongoing changes in the work environment that require permanent adaptations to the way they work (Guhr et al., 2019). These changes drive managers to demonstrate the importance of securing business data by appropriately instituting business structures to support information security in the organization (Guhr et al., 2019).

Research also shows managers of small businesses do not see the implementation of information security as an immediate problem because of a lack of knowledge, therefore the approach they use to resolve the problem is not examined from a holistic approach (Osborn & Simpson, 2018; Soomro et al., 2016). In addition, leadership demonstration that they support information security management is highly valued by large businesses, however smaller business owners do not value it the same way (Santos-Olmo et al., 2016). The researcher sought to identify the factors and reasons small businesses continually discount the implementation of

information security technologies to safeguard and protect their future survivability through this study.

Role of the Researcher

The purpose of this qualitative case study is to add to the body of knowledge by furthering the understanding of small businesses' failure to properly implement information security technologies resulting in the loss of sensitive and proprietary business information. The problem is explored within its own setting through an in-depth study of information security implementation at small businesses will assist in identifying specific factors affecting businesses' deployment of information security technologies. Previous research identified leadership's role in the implementation of information and communication technologies where supervision, information, and training were identified as important factors in successfully implementing new technologies (Goo et al., 2014; Hansen & Nørup, 2017; Paliszkiewicz, 2019).

Leadership is also responsible for making investment decisions where business logic dictates putting a greater emphasis on efficiencies and profitability, leading to a symbolic adoption of new security technologies (Angst et al., 2017). Huang et al. (2014) cited costs, interoperability, security, and privacy concerns as major barriers to the growth of security systems in healthcare. With shorter innovation cycles and the constant development of new security technologies, employees need to adapt to ongoing changes in the work environment that require permanent adaptations to the way they work (Guhr et al., 2019). These changes drive managers to demonstrate the importance of securing business data by appropriately instituting business structures to support information security in the organization (Guhr et al., 2019).

Research also shows managers of small businesses do not see the implementation of information security as an immediate problem because of a lack of knowledge, therefore the

approach they use to resolve the problem is not examined from a holistic approach (Osborn & Simpson, 2018; Soomro et al., 2016). In addition, leadership demonstration that they support information security management is highly valued by large businesses, however smaller business owners do not value it the same way (Santos-Olmo et al., 2016). The researcher sought to identify the factors and reasons small businesses continually discount the implementation of information security technologies to safeguard and protect their future survivability through this study.

Designing the Study

The researcher must design the study to allow data collection, analysis, and reporting to occur in an unbiased manner exploring the activity or event as fully as possible (Creswell, 2014). Using a multiple or collective case study to gather data will assist the researcher in identifying the procedures and analysis that will be used for this case study. Collective case studies are intended to examine an issue, population or general condition across multiple cases (Goddard, 2012; Stake, 2006). In this study, small businesses' implementation of security technologies will be explored through a collective case study design method as the most effective way to gain a holistic picture of how these businesses make technology implementation decisions. The researcher intends to select enough businesses and participants until a saturation point is reached, so an in-depth analysis of the research problem can occur (Creswell & Poth, 2018).

One of the major challenges encountered by researchers performing qualitative studies is the standardization of data collection (Yin, 2014). In qualitative research, data collection usually occurs simultaneously with data analysis where various techniques such as interviews, focus groups, observations, record reviews, and an examination of electronic devices is used as a means by the researcher to gather and document information (Rimando et al., 2015). To

assemble quality data, the researcher will be objective in their data collection activities by asking questions to elicit responses to the research questions, be observant and an attentive listener while always being open to new ideas to understand the issue being investigated (Yin, 2014). Farquhar (2012) and Stake (2010) described the researcher's role in data collection as one of maintaining their integrity, avoidance of conflicts of interest, adhering to ethical procedures, and employing effective data handling procedures while at all times planning how the data will be collected and analyzed. Before data can be collected, the researcher identifies the relevant boundaries of the study ahead of time while making sure the sample population will meet the needs of the study (Forster, 2019). For this study the boundary was small businesses within the state of Virginia and the researcher utilized the interviews, observations, documents, and social networking applications, where appropriate. Establishing the data collection methods was only part of what the researcher needed to outline. The researcher also identified the possible participants and the means by which they were selected.

Participants

The goal of any qualitative study should be to select participants equitably, attempting to bias the study's outcome by including or excluding any particular groups of people from the research would be unethical (Yin, 2014). Participants should voluntarily want to participate in the study while willing to engage interactively with the researcher in trying to pull together information. Forming a trusting researcher–participant relationship allows for the free flow of communication between the different parties with untethered collaboration leading to individuals sharing personal stories that can contradict widely held assumptions about a particular situation (Carless & Douglas, 2017). Personal narratives, being observed, filling out questionnaires, and

participating in experiments are a few of the way's participants can actively be involved in the process.

When recruiting participants for this study, the researcher established criteria for the participants to have some type of knowledge or interaction with the study's objective (Creswell, 2014). As a collective case study, several different businesses as well as various individuals within each business will need to participate. The proper identification of the participant pool was especially important for this study to ensure the researcher had identified potential participants who could support the study through their qualifications and willingness to join in the study. Potential participants who met certain criteria and possessed certain characteristics were selected to be involved in this research study. The following selection criteria was used to identify potential participant pool for this study: (1) identified as a small business, (2) interested in better understanding the implementation of security technologies, (3) experience and/or adoption of any kind of security technology in the business environment, (4) willingness to participate in digitally recorded interview, and (5) granted the researcher the right to publish data. These criteria would be used to develop the pool of potential participants once the researcher receives approval from the Institutional Review Board.

Institutional Review Board

The Institutional Review Board (IRB) fulfills the role of overseer for the university as all human subject research is regulated by the federal government (Liberty University, 2019). Prior to recruiting participants to a study, the researcher must be granted permission to conduct the research by the IRB. The researcher is responsible for submitting a comprehensive research proposal to the IRB whose function is to review all research involving human participants. The IRB's function helps to ensure the privacy, confidentiality, and safety of all participants who are

recruited for the study (Liberty University, 2019). The IRB as part of Liberty University's Research Ethics Office is responsible for ensuring federal regulations and university policies dealing with all research conducted by Liberty University faculty, staff, and students is carried out in an ethical manner accordance with these policies and regulations (Creswell, 2014; Liberty University, 2019).

Recruitment

Recruitment is a key function a researcher must perform to educate potential participants about the research. Participants selected for this study sign an informed consent agreement stating that they voluntarily agree without any form of constraint or coercion to participate in research (Creswell, 2014). This agreement is signed by the participant before they participate in the study with the reservation they can voluntary withdrawal from the study at any time. Informed consent usually involves the signing or reading of the consent form describing the limitations and the boundaries of the study. This process involves the researcher educating the prospective participants about the study and what is to be expected. Potential participants who decline to participate in the study are removed from the potential participants list without prejudice and the researcher tries to ensure the remaining participants fulfill the requirements of the sample population. Potential participants failing to meet the initial criteria set by the sampling strategy are also removed from the sampling pool.

Participant Selection

Following the IRB approval, the pool of participants is created by the researcher using the selection criteria for the research study. All participants receive information about the study and are provided with an informed consent agreement. Ensuring IRB guidelines are followed, the researcher insured participants' rights are protected throughout the study. These early stages in

recruiting participants help to form the trusting researcher–participant relationship (Carless & Douglas, 2017). The researcher discussed the informed consent form with each participant ensuring all questions were answered before the participant endorsed the form (Guest et al., 2013; Seidman, 2013). This question and answer period by the researcher will promote a collegial environment where developing a relationship built on trust will enhance unconstrained communication between the different parties (Carless & Douglas, 2017). The pool of potential participants was solicited from small business listings, professional contacts, and professional social groups. For this study, the participants were recruited from the pool of potential participants based on the study's selection criteria.

Participant Privacy

Since the UTAUT2 suggests that gender, age, and experience significantly moderate different relationships, the researcher must ensure participants concerned with these privacy issues understand how the data will be used and their privacy protected (Venkatesh et al., 2003; Yuan et al., 2015). In addition, the study also collected data on the participant's experience dealing with security systems. This information may be considered highly sensitive to most participants, so the researcher had to explain how it would be protected. Critical sensitive information was being shared through the study's survey and participants responses to questions. As such, the researcher described how private information would be treated and securely stored to keep a respondent's confidentiality and anonymity. Participant identifying information, recordings, and transcripts were stored in a secure location with access only by the researcher. A universal serial bus (USB) drive was used to secure digital information with an encryption at rest solution implemented to ensure data were protected on the device from inadvertent access, if the device happened to be stolen or lost. Participant's interview(s) were conducted in privacy when

possible and a safe distance away from others when no private room was available. Personal details that may have revealed a respondent's identity were used when a participant's information was shared. When information was used from a transcript, the researcher took care in interpreting the information and presenting it in a manner that did not identify any particular participant or business to protect the identity of each (Reep-van den Bergh & Junger, 2018). The researcher followed ethical standards and advocated for an unbiased study dealing with all participants (Stake, 2010).

Relationship Building

Recruiting from a pool of participants who are most likely strangers to the researcher can be an arduous task. Initially, with participants spread throughout the state the researcher's initial contact was by email. The researcher followed up the email by phone contact to any participant who might be interested in participating in the study and met the study's criteria for participating. By discussing the study with the potential participant by phone, the researcher found an opportunity to build rapport and answer any initial questions with the potential participant. Future contacts with actual participants selected for the study occurred in person, by phone, via email or through social networking applications depending on the location and technology limitations of the participant. Communications between the researcher and participants was documented and collected for the study's analysis and report.

Data Collection and Analysis Role

The researcher analyzes and describes a complex situation in terms of its fundamental constituents to bind it as small as possible for discrete testing (Creswell, 2014). This bounding of the problem into more manageable parts leads to the researcher being able to create hypotheses or research questions that can be delved into by a study (Creswell, 2014). The researcher is the

main person in this qualitative study, collecting data through interviews, observations, and questionnaires that will be analyzed and written about to form the study's conclusions. The researcher for this study was responsible for recognizing the important factors related to data collection methods which involved identifying a target population, sample size, method, location, tools/measures (new, existing, modified), and collection duration (Rimando et al., 2015).

When planned and correctly implemented, data collection plays a critical role for the researcher to carry out their qualitative study (Rimando et al., 2015). The researcher's goal is to use the data gathering techniques to refine information, collect and analyze data to shape knowledge based on evidence and rational considerations (Creswell, 2014). As data are collected, the process of analyzing and interpreting the data collected takes place. The researcher during the qualitative study is continually observing and analyzing the data being collected to try and explore all aspects of the event. By performing collection, coding, analysis, and interpreting throughout the study, the researcher is better prepared to perform a final analysis on the data collected to prepare the study's report. The researcher used a mixture of data collection techniques in this study to collect and analyze data in preparation for providing their final analysis of the collective cases used for this study.

Research Method and Design

The principal goal of this research is to understand small businesses' lack of properly implementing information security technologies within U.S. businesses using a qualitative case study. The qualitative case study works well for studying an event, a program, or an activity (Creswell & Poth, 2018). Qualitative research seeks to include a participant's voice, meaning, and experience while the case study's empirical inquiry is a creditable way to investigate and

described an in-depth social issue within its real-life context (Creswell, 2014; Creswell & Poth, 2018; Schoonenboom, 2018; Yin, 2014).

Discussion of Method

Qualitative research methods are an inductive methodology often employed to answer the "how" and "why" of human behavior, opinion, and experience while exploring the causal connections between and among phenomena (Creswell & Poth, 2018; Guest et al., 2013). The inductive researcher using the "theory-later" approach ends up with a causal network as opposed to a deductive researcher who starts with a preliminary causal network (Miles & Huberman, 1994). Using the flexibility of the qualitative research design in this study allowed the researcher to start with the research questions were the primary determinant of the design allowed purposeful observation and interviews to occur for data collection making this a theory-later approach to describe the situation being studied (Cypress, 2018; Miles & Huberman, 1994). This study's movement away from a strictly social research prominence emphasizing cause-and-effect explanations, allowed the researcher to focus on the holistic treatment of the phenomena (Boblin et al., 2013). The movement towards a personal interpretation makes qualitative studies more geared towards a constructivist view.

Constructivist Worldview. Constructivist worldview hypothesizes that learning is an active, constructive process that individuals go through as they live their lives (Boblin et al., 2013; Creswell & Poth, 2018; Stake, 2010). Since mental representations are subjective, people actively construct their own subjective meanings of their reality and researchers try to understand as many of these as possible (Charmaz, 2015). The constructivist's inductions are informed by a personal conceptual universe (Miles & Huberman, 1994). Using qualitative research, the constructivist researcher tries to analyze the processes of interaction among individuals

(Creswell, 2014). These processes are also impacted by the person's culture and the way they live and work (Creswell, 2014; Guest et al., 2013; Seidman, 2013). Interpreting how others view the world starts with thinking about a theory or pattern of how they might think. Expounding on that process by collecting information and drawing conclusions from what the researcher observes is an important part of the qualitative process. Miles and Huberman (1994) believed both inductive and deductive researchers end up in the same place after they complete their data gathering, where the constructivist has a built-up cause-and-effect map. Additionally, it is important for the researcher to understand their own biases and backgrounds, so results are not influenced by any biases they may have from related experiences. In this study, the researcher took care to identify their biases to lessen the effect of any biases that may have been present.

Qualitative Research. The qualitative research methodology used for this study provided the researcher a reliable mechanism to attain data to better understand how business leaders and managers think about securing their data through the use of information technology. Since qualitative case studies work well for studying an event, a program, or an activity using the case study to further our understanding of why businesses do not follow security measures that may protect their business made the most sense to look at this situation (Creswell & Poth, 2018). This study was less structured, so a qualitative research design worked better than a quantitative design and offered the researcher more latitude in how to interact with participants, collect data and analyze the results. The research was not intended to generalize why every business does or does not implement security technologies to protect their information but was intended to help understand a particular situation (Stake, 2010). By specifically focusing on the small business context the researcher is able to better understand why and how small business leaders make their decisions about implementing security technologies and preparing their workforce for

changes (Stake, 2010). The qualitative research design allows the researcher to explore participants' decisions in depth which aids in understanding the holistic approach to technology implementation.

Discussion of Design

Creswell and Poth (2018) identified five approaches to qualitative research design with each research design having a different research focus. The phenomenology, grounded, ethnographic, narrative, and case study research designs all have in common the universal process of research starting with a research problem that leads to questions needing to be answered by collecting data, performing data analysis and interpretations, and authoring a research report (Creswell & Poth, 2018). For this study, the researcher decided to select the case study design as the best way to answer the questions and collect data to be analyzed.

Case Study. The case study design allows a researcher to delve into an individual, business, entity or event using one case or multiple cases to analyze what caused the occurrence. Case study research can be distinguished by the focus of the analysis for the bounded case where the single instrumental case study, the collective or multiple case study, and the intrinsic case study can be chosen based on the intent of the study (Creswell & Poth, 2018). The researcher decided not to use the instrumental case study because it focuses on one bounded case study and this research was going to involve more than one single case study (Creswell & Poth, 2018). The researcher also eliminated the intrinsic case study because its focus is on studying a case itself for uniqueness (Creswell & Poth, 2018). The researcher chose to perform a collective case study for this research to examine the situation across multiple cases.

Multiple Case Study. By selecting the collective case study for this research, the researcher is able to use multiple case studies to delve into the issue. During the collective case

study research, the researcher will use interviews, documents, questionnaires, and observations as a way to collect data. These data collection instruments allowed the researcher to maximize their data collection. In addition, the researcher's selection of the collective case study allows them to assemble enough information to perform an in-depth understanding of the issue by using multiple cases (Creswell & Poth, 2018; Lauckner et al., 2012; Stake, 2010). By looking at the problem through multiple cases the researcher is able to analyze why one small business might introduce a robust security information architecture and another business might just implement an out of the box firewall to prevent intruders.

Real-life Data Collection. The ability of the researcher to operate within the contexts of real-life situations with little to no control over the events happenings (Weishäupl, 2018; Yin, 2014) is positive and negative. Weishäupl (2018) and Yin (2014) pointed out that an advantage can be derived from collecting large amounts of data when the situation's understanding grows through real-life situations. The researcher viewed this as a strength when selecting the collective case study design. Since multiple cases are being used a better result can be had when the researcher is collecting more data across differing cases. The researcher understood that the study's results may not lead to generalizability of the research findings, however they hoped the results would lead to new avenues of thoughts being opened (Turner et al., 2017; Yin, 2014).

Seeking Answers. Why small businesses' fail to implement information security technologies properly is the main focus of this study. Seeking to understand what business practices leaders and managers incorporate in their workplace to ease the transition of employees in using new information security technologies will also be looked at. The factors that impact a businesses' decision to implement information security technologies may be identified by the researcher's data collection efforts whereby the study's analysis may prove that each factor plays

a role in the businesses' technology decisions. By simplify the situation being investigated into its unique parts, the researcher is able to better understand the data's aggregate parts and their interrelationships. Collecting and analyzing information based on the collective case study was an excellent way for the researcher to complete this activity.

Summary of Research Method and Design

Merriam (2009) and Yin (2014) believed a qualitative case study was an intensive, holistic description within its real-world context where the boundaries between the situation and context may not be clear. The inductive methodology of the qualitative research method can explore the causal connections between and among phenomena while answering the "how" and "why" of human behavior, opinion, and experience (Creswell & Poth, 2018; Guest et al., 2013). The study's empirical setting of small businesses' failure to implement information security technologies was an excellent way to answer the "how" and "why" within a bounded environment. Performing a thorough assessment of the advantages and disadvantages of using a qualitative case study, the researcher decided it was clear that the qualitative case study could readily support this research. For that reason, the researcher performed a collective case study to examine the issue across multiple cases which allowed the researcher to gain a holistic view of the situation (Boblin et al., 2013; Goddard, 2012; Stake, 2006).

Population and Sampling

The researcher designed the study to acquire an understanding of why small businesses' fail to fully implement information security technologies that would protect their business activities. All businesses in today's global economy whether they are corporations like Procter and Gamble or a small local independent store use technology to further their goals (The Procter & Gamble Company, 2019). Technology can improve a businesses' supply chain management,

human resource management, marketing, sales, transaction management, and customer support. As splendid as technology advancements can be, the risks associated with technology are even graver as information can be compromised from within or externally by bad actors without the proper compensating controls in place. This study's focus on small businesses is intended to identify a population and sample of small construction businesses that made strategic decisions on how they would deal with their security information technology using purposeful sampling. The purposeful sampling approach as pointed out by Creswell (2014) and Merriam (2009) is one of the most credible non-probable sampling strategies for qualitative studies. By using purposeful sampling, the researcher was able to select participants consistent with the study's methodology (Creswell, 2014; Merriam, 2009).

Discussion of Population

By focusing on the factors influencing the implementation of security information technologies in small construction businesses, the researcher must identify the proper population to gather data from. Employed as an information technologist for over 31 years with the last 20 years working in Virginia, the researcher has a keen awareness of local businesses and security technologies that will assist in making participant selections. The population from which the sample will be drawn will be small construction businesses within the state of Virginia. As of 2016, the U.S. Small Business Administration estimates there are 681,517 small businesses operating within the state of Virginia (U.S. Small Business Administration Office of Advocacy, 2016). Within Virginia businesses are segregated into eighteen industries with the top six firm types shown in Table 1 (U.S. Small Business Administration Office of Advocacy, 2016).

Table 1

Virginia Small Firms by Industry, 2013

Industry	Total Small Firms
Professional, Scientific, and Technical Services	112,035
Other Services (except Public Administration)	98,034
Construction	77,130
Real Estate and Rental and Leasing	67,913
Retail Trade	56,934
Health Care and Social Assistance	54,598

Note. Adapted from https://www.sba.gov/sites/default/files/advocacy/Virginia.pdf. Copyright 2016 by U.S. Small Business Administration Office of Advocacy.

Aiming to explore this particular issue within a contemporary context in-depth, the researcher decided to limit the participant business type to Construction or General Contractor as one of the top six small business types identified by the U.S. Small Business Administration's Office of Advocacy's 2016 data (Farquhar, 2012; U.S. Small Business Administration Office of Advocacy, 2016). To create the pool of potential participants, the researcher used various means including business listings (e.g., https://us-business. info/), professional contacts, and professional social groups concentrating mostly on small construction businesses located in Virginia.

The researcher intends to select enough small construction businesses and participants from the construction business type identified in Table 1 until a saturation point is reached (Creswell & Poth, 2018; Saunders et al., 2018). Each business participant was selected based on their involvement with implementing security technology projects or lack thereof. Selection criteria for each participant was based on the following selection criteria: (1) identified as a small business, (2) interested in better understanding the implementation of security technologies, (3) experience and/or adoption of any kind of security technology in the business environment, (4) willingness to participate in digitally recorded interview, and (5) granted the researcher the right

to publish data. Initial contact by the researcher was through the use of email, phone call, or in person contact. Business participants agreeing to participate in the study received an email confirmation letter explaining the study, study expectations, and a copy of the study's release form to be signed.

Discussion of Sampling

Primary businesses and management participants were identified using purposive sampling as it is the most important kind of non-probability sampling (Ghaffari & Lagzian, 2018). Purposive sampling, also known as judgmental, selective, or subjective sampling is a form of non-probability sampling that the researcher selected to choose participants based on their characteristics and objectives of the study. The researcher's use of the purposive sampling technique was to identify and select information-rich cases for the most effective use of his limited time and resources (Patton, 2015). This involved identifying and selecting construction businesses and individuals within the business that were involved with implementing security technologies and had knowledge about or experience in this area. Besides knowledge and experience, the researcher sought to recruit willing participants who were able to communicate experiences in a clear, expressive, and thoughtful manner while making themselves available for the study.

Since one of the main goals of purposive sampling is to focus on particular characteristics of a population that are of interest, the researcher selected participants he thought would best be able to answer the research questions. Using the purposive sampling technique at the beginning stage of the study, he was able to identify initial participants who were responsible for making IT decisions and may have participated in the evaluation, planning, execution, and implementation of security technologies within the business environment. The researcher understood that using

this technique for the study would lead to a sample that was not representative of the population, however this is not considered a weakness for researchers pursuing qualitative research designs (Onuekwe, 2015). The researcher was also aware that purposive sampling was prone to researcher bias, so they had to take that into account. To mitigate the possibility of bias, the researcher made sure judgements were based on an accepted criterion that was clear. For this study, the researcher's goal in using purposive sampling was not to randomly select participants from the population to create a sample with the intention of making generalizations about the population but to fully answer the research questions.

Sample Size. Case studies can have a flaw when a researcher considers statistical generalization to be the way of generalizing the findings from their case study because the sample size is usually too small to represent any larger population (Yin, 2014). In this study, the researcher saw using the case study and its sampling as an opportunity to shed empirical light on the study's theme. Developing an estimate of the sample size would be needed for this study, the researcher agreed with Saunders et al. (2018) that specifying the specific number of participants for the study at the start without sufficient understanding of the matter being investigated was illogical. As the researcher developed an increasingly comprehensive picture of the themes involved, he performed an iterative, context-dependent analytical process to help determine if enough information was gathered to reach saturation on each (Creswell, 2014). This process determined if more interviews or information needed to be collected to reach a saturation point. To begin, the researcher based his rough sampling size on Boddy (2016) and Sim et al. (2018) where the proposed rule of thumb for sample size in qualitative research, based on methodological considerations and past experience with similar studies could be 15-30

interviews for case studies. The researcher set the minimum starting number of participants for this study at 30.

Summary of Population and Sampling

The sampling frame consisted of businesses in the construction industry which is one of the top six small industries within the state of Virginia. The study's participants were recruited and selected from this sampling frame. Not all construction businesses had participants selected and the number of participants from each business may not have been the same. Relying on purposive sampling to select participants allowed the researcher to choose participants he thought would best be able to answer the research questions. The researcher also understood according to Farquhar's (2012) research that they may need to limit their research to in-depth interviews and the study of documents for smaller businesses.

Data Collection

The case study samples were taken from small business managers that dealt, implemented, or were currently participating in IT security adoption initiatives in the construction business sector in Virginia. The researcher used interviews, documents, observations, and questionnaires to gather data (Yin, 2014). Data collection from multiple cases offered the researcher constructive insights into the many perspectives of the participants.

Instruments

The general problem addressed by this study was the failure of small businesses to insulate operations from malicious criminal attacks. Specifically, the failure of a small business to properly implement information security technologies that make them vulnerable to bad actors interested in stealing business information to further their criminal enterprise. The researcher acted as the focal point to collect and analyze data during the study, so the study's main research

questions could be answered. Performing semi-structured face-to-face interviews as the main way to collect data allowed the researcher to gather different perspectives on why small businesses make themselves vulnerable to bad actors. The researcher developed an interview guide to act as a blueprint in how data collection during the interview process should take place. The interview guide was only a starting point and did not limit participants from freely sharing their perspectives on the subject being studied but helped with bounding the discussions to keep on track. Participating in all aspects of the data collection process, the researcher was a major factor in ensuring the study stayed on track and participants remained attentive to the study's goals.

Interviews. The researcher's primary instrument during this study was the use of semi-structured face-to-face interviews. These face-to-face interviews allowed the participants to provide details and information that would be important to the study's outcome. When in-person interviews occurred, the researcher used a Dell Inspiron laptop or a Microsoft Surface Pro tablet to record the interview. This allowed the researcher to capture the conversations using an audio mic for future reference.

Audio Recordings. When the researcher and participant could not meet at the same location, the interviews were captured using Zoom conferencing App. Zoom is a web-based video conferencing tool that allows users to meet online securely with the ability to record conversations for future reference (Zoom Meetings & Chat, 2019).

Note Taking. The key to first-rate note taking is listening to what the participants had to say. Listening involved receiving information through multiple modalities that helped the researcher sense what was happening around him (Yin, 2014). Exceptional listening allowed the

researcher to take meticulous notes collecting meaningful information without bias to help with the study's eventual analysis.

Observations. Researcher' observations proved to be a valuable asset during the field interviews. Observations of real-world events allowed the researcher to gain insight into how participants acted in their workplace. Sometimes acting as an observer can constrain a researcher's behavior but the researcher took care to ensure observations were unconstrained and participants were always put at ease and unencumbered (Yin, 2014).

Data Collection Techniques

Using the modified UTAUT2 model as the framework to collect data for this study, the researcher used a two-prong approach to collect data from participants. The first approach involved developing a participant profile questionnaire (Appendix A) that allowed the participants to answer up to seven questions designed to provide some initial basic information to the researcher. At this point in the study, the researcher had the participants read and sign the informed consent agreement stating they voluntarily agree without any form of constraint or coercion to participate in research (Creswell, 2014). The participant profile questionnaire involved participants answering questions about their gender, age, security awareness training, security information policies, interaction with information systems, and length of time with the business. These particular questions allowed the researcher to collect answers dealing with the study's moderators (age, gender, and experience) of the modified UTAUT2 model and initial data dealing with security policies. The security policy questions are directly tied to one of the main research questions in how do security policies assist employees in dealing with the deployment and acceptance of new security information systems. If a participant answered no to this question, they would not be asked during their interview other specific questions about this

area. The participant profile questionnaire was distributed to all study participants before their interviews took place. The researcher also had an idea based on question #6 of the participant profile questionnaire whether individuals dealt with any information security systems. Based on their answer to that particular question the researcher determined what further questions they might be asked during the interview portion of the study.

The second approach the researcher used to gather data was performing actual interviews with the participants in person or through a web conference. The research questions and the modified UTAUT2 framework was integral in developing the interview guide. Interview questions were intended to uncover information on the main research questions, facilitating conditions, security policies, effort expectancy, social influence, investments, performance expectancy, threats (cyber and insider threats), and habit. The semi-structured face-to-face interview questions (Appendix B) were asked of all participants.

From the information obtained, analysis of the data assisted the researcher in determining how behavioral intention and use behavior were impacted by participant's actions and perceptions. The participants' interviews also provided insight into the role of perceived usefulness, perceived ease of use, and subjective norms in influencing the attitude of managers and employees in deploying security technologies (Ajzen, 1991; Cheng, 2019; Davis, 1986; Taylor & Todd, 1995; Sánchez et al., 2013). Relying mainly on the participant's interview, the researcher delved into what practices managers performed to prepare employees for implementation of new security systems (Kim & Chang, 2014; Nazareth & Choi, 2015; Ullaha et al., 2018). Gathering data to learn about the factors and employee's behavior provided the researcher with a better understanding of why some businesses do not implement new

information security technologies (Ajzen, 2011; Cheng, 2019; Davis, 1989; Taylor & Todd, 1995).

Data Organization Techniques

The researcher primary means to record, track and document information for this study involved the use of Microsoft Office© suite. Within this suite of tools, Microsoft Word© was the preferred tool to document journal entries, produce participant handouts (participant questionnaire), compile reports, and generate all archival records. Microsoft Excel© primarily use was to perform any statistical analysis, manage and track artifacts, and manage coordination with the study's participants. Microsoft PowerPoint© provided the researcher a simple tool to create graphics for reports. ATLAS.ti© software was also used as a powerful tool capable of storing, tracking, coding, visualizing, and linking data in a semantically meaningful way.

Privacy. Privacy is an important concern today by individuals and business entities. As such, the researcher described to each participant how their confidentiality and anonymity would be maintained. This was made possible through securing all video, audio, and artifacts that could identify the participant. All participant identifying information was stored in a central secure location with access only by the researcher. Computers that were used to record video and audio of participant's interview were password protected. A universal serial bus (USB) drive was used to secure digital information with an encryption at rest solution implemented to ensure data were protected on the device from inadvertent access, if the device happened to be stolen or lost.

Participants' interviews were conducted in privacy when possible and a safe distance away from others when no private room was available. Personal details that may have revealed a respondent's identity were used when a participant's information was shared. When information was used from a transcript, the researcher took care in interpreting the information and

presenting it in a manner that did not identify any particular participant or business to protect the identity of each (Reep-van den Bergh & Junger, 2018).

Summary of Data Collection

The researcher took great care in ensuring all data were collected in an ethical manner. In addition, the researcher understood the importance of keeping participants privacy protected. Using the modified UTAUT2 model as the framework to collect data for this study, the researcher was able to collect meaningful data from participants for this study. Semi-structured face-to-face interviews proved to be a valuable instrument for participants to answer questions in an open free flowing environment.

Data Analysis

Data analysis of case study evidence consist of examining, categorizing, tabulating, testing, or otherwise recombining evidence, to produce empirically based findings (Yin, 2014). Using techniques such as coding to perform this function allows the researcher to compile evidence to identify particular themes or perceptions of importance in the study (Creswell, 2014; Yin, 2014). Compiling and searching for associations between the different elements, the researcher was able to take things apart and methodically sort evidence to determine the strength of the empirical support for the study's themes and perceptions (Stake, 2010; Yin, 2014). Subsequently, the researcher's ability to collect data, sort and classify the data, and interpret data clusters will affect the quality of the study's data analysis (Stake, 2010).

The research focused on the study's seven questions (two primary and five secondary). The primary questions: First, what factors impact a businesses' decision to implement information security technologies? Second, what practices do business managers incorporate in the work environment to ease the transition of new information security technologies? The five

sub-questions: First, how do the internal investment processes that owners/managers institute assist in determining the best course of action for implementing security systems? Second, how does knowing that internal threats and cyber-attacks occur against small businesses on a routine basis have on implementing security information applications? Third, how do employees perceive changes to the work environment when new information security technologies are deployed? Fourth, what new stresses are introduced in the workplace when new information security technologies are deployed? Fifth, how do security policies assist employees in dealing with the deployment and acceptance of new security information systems?

By concentrating on significant quotes, statements, and sentences that participants made during their interviews and assessing the field data that the researcher observed, the researcher was able to start shaping an understanding of the context of the participant's interactions with the study's subject matter. The researcher developed seminal impressions that were derived from the coding process. This was the data analysis process by which the researcher developed clusters of meaning. Using the interview questions, the researcher was able to interpret themes based on the participant's responses. This thematic categorization along with the setting and field data allowed the researcher to integrate the multiple parts of the study together, developing a composite description to describe the participant's situation.

As part of the data analysis process the researcher used numerous software tools. To assist in the organization of the data, the researcher used ATLAS.ti© software, Microsoft Word©, and Microsoft Excel© to track participants' information, consolidate audio/video recordings of the interviews, transcripts, field notes, and journal information. Leveraging ATLAS.ti© software allowed the researcher to track and monitor all information from participants in a very

manageable way. In addition, the ATLAS.ti© software assisted in building the themes for the study.

Coding Process

Data collection begins the analysis process where the researcher tries to establish a relationship with participants. Establishing rapport with participants allowed them to be more open during the interview process. This made it easier to collect data and get participant's views and experiences in dealing with the study's subject matter. This process began with the researcher collecting data through a single questionnaire instrument that was designed to collect basic data on the participant's gender, age, and work tenure. In addition, the questionnaire was used to gather information on the business's security awareness training, security policies, participant's perception of policies, and interactions with security systems. These questions were chosen to allow the researcher to gather some initial data and get to know some basic facts about the participants before they were actually interviewed. Using the information garnered from the questionnaire the interviewer was able to assimilate the data in their conversations with the participants to put them at ease during the start of the interviews.

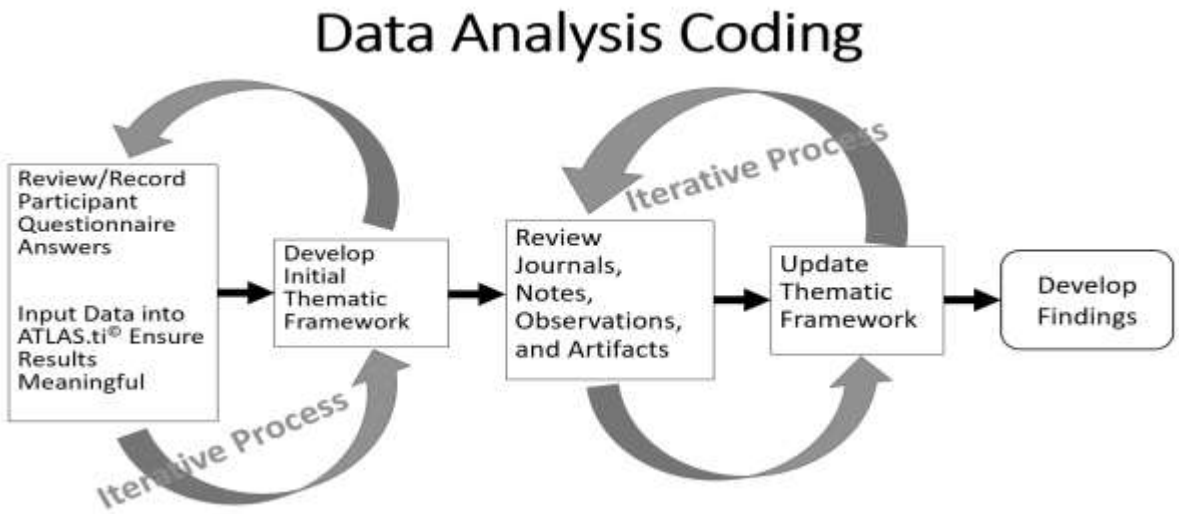
Data collection continued with the researcher carrying out interviews with the participants. Interviews were conducted using the interview guide which was based on a modified UTAUT2 model developed by Venkatesh et al. (2012) with additional factors (e.g., security policies, investments, and threats [insider and cyber]) added for this study. Along with the interview transcripts, observation field notes, journals, and other documents the researcher had the data to begin the coding exercise. Coding is a ubiquitous part of the qualitative research process, whereby the researcher labeled and organized the data collected to identify different themes and relationships that existed between them (Creswell, 2014). Identifying common

themes between the participants, allowed the researcher to categorize the ideas being collected, so a framework of thematic ideas could be developed. Using this process, the researcher was able to find common themes and concepts to further understand how each factor contributed to security information technology adoption.

Thematic Framework. The coding process began with an analysis of the collected data using ATLAS.ti© software. The participant interviews had to be transcribed line-by-line by the researcher. During this process the researcher began the initial coding by looking for key words, phrases, events, and occurrences that appeared in the transcripts from the participant's interviews. This was a painstakingly slow process as some recordings were of a better quality of audio than others. Listening to the recorded interviews several times provided the researcher a means to verify the transcriptions were accurate. From the transcribed interviews, the researcher using ATLAS.ti© software ensured the coding is meaningful. Categorizing the main ideas of each participant into meaningful gerunds was critical to building the thematic framework. Assigning gerunds to a portion of data, word, or short phrase helped the researcher identify important characteristics of that piece of data. The participant questionnaire was also reviewed and any main ideas that could be gleaned from it were added to the framework. This became an iterative process by the researcher to ensure he captured the most critical aspects of the discussions and answers. Once the initial thematic framework was built, the researcher reviewed and analyzed his journal entries, notes, observations, and any artifacts that were collected to add any additional information to the thematic framework. This updated thematic framework produced many ideas that needed to be analyzed to develop the study's findings. The coding process as outlined in Figure 3, identified ideas and perceptions from participants to develop the thematic framework.

Figure 3

Thematic Coding Flowchart



When performing the analysis, the researcher took great care in trying to identify areas dealing with the factors of the modified UTAUT2 model. In addition to the factors and modifiers mentioned previously information on the following factors was being sought: (1) facilitating conditions, (2) effort expectancy, (3) social influence, (4) performance expectancy, (5) habit, (6) behavioral intention, and (7) use behavior. The researcher's data analysis was shaped by the content of the data received from the study's participants. Microsoft Word©, Microsoft Excel©, and ATLAS.ti© software were the primary tools used during the coding process to develop the thematic themes. The researcher was familiar with the software's functionality and these tools could easily handle the amount of data being analyzed based on the number of participants. Throughout this process the researcher took care to respect the participant's perspectives and opinions which were essential in furthering the study's goals.

Summary of Data Analysis

Conducting a case study analysis involves having a general analytic strategy that links the case study's data together looking at both elements and associations (Stake, 2010; Yin, 2014).

This study's iterative coding process allowed the researcher to create a thematic framework to understand the participant's views and perceptions better. By identifying the elements and associations through the coding process, the researcher was able to see associations and form decisions about the data collected.

Reliability and Validity

Qualitative studies need to establish credibility and thoroughness just like quantitative studies. Performing qualitative validity and reliability checks helped the researcher be more accurate with the study's findings where consistency, credibility, transferability, dependability and confirmability for the study's findings was being sought (Creswell, 2014; Merriam, 2009; Yin, 2014). This was accomplished through validation of the data collected, so the researcher could ensure the findings of the study accurately represented the participant's perspectives and experiences.

Reliability

Reliability refers to the consistency of a researcher's measurements where other researchers can exactly replicate the processes and the results of their study (Creswell, 2014; Yin, 2014). Using the same interview guide and questionnaire as the main instruments to gather responses from participants allowed data to be gathered in a similar fashion each time it was used under comparable conditions. Allowing data to be collected in a repeatable manner strengthened the study's validity by improving its internal consistency. Consistency is considered the very essence of reliability for a qualitative research study. According to Creswell and Poth (2018), consistency can be improved through accurate transcription of interviews. Listening to the recorded interviews several times allowed the researcher to verify the interviewers' statements to increase the consistency of the transcripts. In addition, the researcher was the sole coder and

analyst for this study. This allowed more consistency in the coding of transcripts and analysis of the questionnaires and other data being gathered.

Validity

Validity in qualitative research means "suitability" of the tools, processes, and data where the research question is valid for the desired outcome (Creswell & Poth, 2018; Leung, 2015; Yin, 2014). In addition, the methodology is suitable for responding to the research question, the design supports the methodology, sampling and data analysis are suitable, and the study's findings are valid for the information collected within a specific context (Creswell & Poth, 2018; Leung, 2015; Yin, 2014). To validate the current study, the researcher investigated the research questions using a methodology and design that were suited to appropriately lead to findings that could be reliable and validated. The researcher ensured enough data were collected to reach a data saturation point. This was necessary for the researcher to make an informed decision about the study's research questions. Through triangulation and analysis, the researcher was able to validate the study's findings by looking at the extracted data.

Data Saturation. Validating data also involved the collection of data to a juncture where no new themes or information could be observed by collecting additional data (Creswell & Poth, 2018; Wray et al., 2007). At a certain point, the researcher determined that data saturation had occurred where the quality and quantity of information collected was enough for the researcher to determine there was sufficient information for them to make an informed decision about the research questions. The process started with the researcher interviewing all participants with structured questions which facilitated the researcher in achieving data saturation (Fusch & Ness, 2015). Performing preliminary data analysis concurrently with the data collection allowed the researcher to see initial themes and track them as more interviews occurred.

Developing clustering codes into central categories, the researcher was able to compare data from the various interview transcripts, questionnaire responses, and observational data against the central categories to determine their placement or if a new category had to be created. Using the iterative process to compare new data to the established coding clusters allowed the researcher to identify similarities, variances, and general patterns between the data sources. Examining and comparing previously collected data with the newly collected data and matching it against the initial codes was an excellent process to organize ideas and continually pinpoint concepts that seemed to cluster together. This iterative process added rigor to the study's analysis and meant the quality of the research conducted was improved while data saturation was reached (Saunders et al., 2018).

Triangulation. Triangulation is a validity procedure where the researcher searches for convergence among the different sources of information collected in order to provide corroborating evidence and form themes for the study (Creswell & Poth, 2018; Stake, 2010; Yin, 2014). During this study, data were gathered from approximately 30 participants representing small businesses within the construction industry throughout Virginia. Through a thorough examination of the data collected from the various participants using the same method, the researcher was able to triangulate patterns and contradictions beyond their individual experiences. Comparing different levels of the semi-structured participants' interview details along with data from scans of the businesses' websites permitted the researcher to use triangulation to integrate the study's data. Since all data from this study went through the process of triangulation viewing each participant as a unique individual with their own worldview, the researcher was able to perform an in-depth analysis on the multiple participants to validate the data collected.

Data source triangulation in this study was based on using semi-structured face-to-face interviews and a passive scan of the businesses' website as the main ways to collect data, which allowed the researcher to gather different perspectives from participants and independent data on why small construction businesses may make themselves vulnerable to bad actors. Comparing the data collected during the interviews with data from the previously issued questionnaires allowed the researcher to make an independent assessment of whether the participants' words matched their previous answers. This would show the researcher any incongruities between the two data sources. Since interviews and questionnaires were taken at different times and from different physical locations, the data source triangulation can be derived as if these were two different, independent data sources being used. In addition, the researcher used observations and notes on any artifacts reviewed to support the participant's perspectives. During the study the researcher also reviewed documents from the company. Performing observations, the researcher was able to independently verify what participants were stating during their interviews and validate answers on the questionnaires against documents reviewed and observed data.

The other source of the study's triangulation was the use of Zed Attack Proxy (ZAP©) developed by the Open Web Application Security Project® which is a nonprofit foundation that works to improve the security of software and is the world's most wide used web app scanner (OWASP Foundation, Inc., 2020). The researcher performed a passive scan using ZAP© against each businesses' website to determine how they controlled their website application risk determining how much security emphasis was placed on protecting their sites.

Summary of Reliability and Validity

The importance of qualitative research comes from the role it plays in exploring the reasons behind why something occurs. Making sure the results of the research are valid and

reliable gives a study credibility. To accomplish this, the researcher tried to reach saturation in their study to uncover the different reasons the situation occurred. Supporting this through triangulation allowed the study's evidence to be corroborated.

Transition and Summary of Section 2

The focus of Section 1 was to identify the problem to being studied and outline the research questions to be answered to provide a more in-depth understanding of the issues surrounding implementation of new security technologies within a small business. The literature review provided information on past studies and areas that may be in need of further study. Section 2 built upon this information and delineated how the study would be conducted. In Section 2, the researcher discussed the role of the researcher along with the study's design and method, population and sampling, privacy concerns, data collection, analysis, and the reliability and validity of the findings. Section 1 and Section 2 set the foundation for the researcher to be successful in carrying out the actual study and prepare for the data analysis occurring in Section 3.

Section 3: Application to Professional Practice and Implications for Change

The goal of this qualitative case study was to understand a small businesses' lack of properly implementing information security technologies in the U.S. The lack of implementing security technologies in today's business environment could have a detrimental effect on a businesses' survival. By analyzing the collection of data from the participants' experiences and perceptions, the researcher was able to document the findings of this qualitative case study research involving thirty businesses involved in the construction industry. By identifying the themes that emerged from the participants, the researchers' findings will add to the body of knowledge on small businesses and information security technology.

The purpose of Section 3 is to present the study's results from a thorough analysis of the data collected. Section 3 starts with a brief overview followed by the presentation of the findings, applications to professional practice, recommendations for action, recommendations for further study, reflections, and the summary and study conclusions.

Overview of the Study

This qualitative research study was conducted to answer specific research questions to gain further insight into why small business owners or managers do not think it is necessary to properly implement information security technologies within their business. By exploring thirty businesses operating in the construction industry, the researcher was able to collect data to discover the different ways these businesses conducted their security practices, made investment decisions, trained personnel, and implemented security systems and policies.

Participants

Selecting to use a qualitative collective case study was determined to be the preeminent method in answering the research questions posed. It provided the researcher the ability to use

multiple case studies to delve into the issue. Primarily using Facebook and the Blue Book (The Blue Book building and construction network, 2020) a building and construction social networking site, the researcher was able to identify construction businesses located and operating within Virginia. Combining data from both sites and the internet, the researcher was able to collect data on the principal owners/managers of the business, email(s), phone numbers, and addresses. By means of the acquired data, the researcher distributed information on the study, along with the profile questionnaire which was either electronically emailed or personally delivered with the informed consent letter that explained the purpose of the questionnaire and study to all participants.

Data were obtained from 30 businesses in the construction industry operating within the state of Virginia. Information was primarily gathered through interviews, questionnaires, observations, and documents. With 30 different businesses at 30 different locations the researcher was able to perform triangulation by converging the different data sources of information collected in order to provide corroborating evidence to form the themes for this study (Creswell & Poth, 2018; Stake, 2010; Yin, 2014). The researcher ensured enough data were collected to reach a data saturation point by ensuring to fill any gaps that may have occurred due to fewer participants being involved in the study. This allowed for a stronger case study through triangulation and analysis, which allowed the researcher to better validate the study's findings making them more comprehensive.

Twenty-three of the participants were owners of the businesses with the remaining participants being managers within their business. Eighty-six percent of participants were directly involved in decision-making on how investments were decided, which included determining how the business would respond to cyber security threats. Twenty-five participants

were male and five were female. Ninety percent of participants were over the age of 35 with 37% being over 55 years old. Seventy-three percent of the participants had been with their company for 11 or more years. Individual participant demographic data are shown in Table 2.

Table 2

Participant Demographics

Name	Gender	Age	Business Longevity	Family Started	Family Owned
Participant 1	Male	35 - 44	11 – 15 years	Yes	Yes
Participant 2	Male	35 - 44	6 – 10 years	Yes	Yes
Participant 3	Male	Over 64	21 – 25 years	Yes	No
Participant 4	Male	55 - 64	36 – 40 years	Yes	Yes
Participant 5	Male	Over 64	Over > 40 years	Yes	Yes
Participant 6	Female	45 - 54	6 – 10 years	Yes	Yes
Participant 7	Male	35 - 44	11 – 15 years	Yes	Yes
Participant 8	Male	35 - 44	16 – 20 years	Yes	Yes
Participant 9	Male	45 - 54	16 – 20 years	Yes	Yes
Participant 10	Male	Over 64	16 – 20 years	Yes	Yes
Participant 11	Male	45 - 54	16 – 20 years	Yes	Yes
Participant 12	Male	55 - 64	21 – 25 years	Yes	Yes
Participant 13	Male	Over 64	Over > 40 years	Yes	Yes
Participant 14	Male	25 - 34	6 – 10 years	Yes	Yes
Participant 15	Male	45 - 54	16 – 20 years	Yes	Yes
Participant 16	Male	Over 64	26 – 30 years	Yes	Yes
Participant 17	Male	18 - 24	6 – 10 years	No	No
Participant 18	Male	25 - 34	1 – 5 years	Yes	Yes
Participant 19	Male	35 - 44	21 – 25 years	Yes	Yes
Participant 20	Male	35 - 44	11 – 15 years	Yes	Yes
Participant 21	Male	55 - 64	36 – 40 years	Yes	Yes
Participant 22	Male	55 - 64	16 – 20 years	No	No
Participant 23	Male	35 - 44	11 – 15 years	Yes	Yes
Participant 24	Female	45 - 54	11 – 15 years	Yes	Yes
Participant 25	Male	45 - 54	26 – 30 years	Yes	Yes
Participant 26	Female	35 - 44	16 – 20 years	Yes	Yes
Participant 27	Male	35 - 44	1 – 5 years	No	No
Participant 28	Male	55 - 64	31 – 35 years	Yes	Yes
Participant 29	Female	55 - 64	1 – 5 years	No	No
Participant 30	Female	35 - 44	1 – 5 years	Yes	Yes

Each participant was contacted via email, phone, or in person and agreed to participate in the study. The participant questionnaire along with the appropriate consent form was distributed and documented. The participants provided the researcher access to documentation and the business premises. The study's interviews were conducted in person when possible or via telephone, as necessary.

Evidence Collection

The case study's unique strength is its ability to deal with an assortment of collected data to include documents, observations, and interviews (Yin, 2014). The researcher used a form of these methods for gathering evidence for this collective case study for each business involved in the study. The details and description of the how these methods were incorporated and used within the study follows.

Interviews. Performing semi-structured face-to-face interviews is one of the most important sources of evidence in a case study research (Yin, 2014). As such, the researcher was able to use this method to collect data from the different participants to gather their diverse perspectives. The researcher had developed an interview guide to act as a blueprint in how data collection would occur during the interview process and allowed it to guide the conversations. Before the interviewees participated in the interview session, the researcher administered a profile questionnaire. This questionnaire allowed the interviewer to learn some small facts about the interviewee and collect demographic data on each participant. In addition, the questionnaire was used as a filter to determine what questions in the interview should be eliminated. For example, if a business had no written security policies, then questions in that area during the interview were not detailed in nature. Once the interviewer had determined the appropriate questions to focus the interviewee on, the interview guide was used as the starting point.

Interviewees were not limited to discussing material only about the questions being asked but could freely share their perspectives on the subject matter. The interview guide was an excellent tool in assisting the interviewer in keeping the interviewee focused on the pertinent areas being studied. By bounding the discussion with the questionnaire, it helped keep interviews on track. The interviewer recorded the guided conversations and at a later date transcribed them into a Word document. Once the interviews were transcribed, the researcher went about the task of coding the conversations where ideas and key phrases could be identified. Creswell (2014) and Yin (2014) pointed out that using techniques such as coding allows a researcher to compile evidence to identify particular themes or perceptions of importance in a study. Through coding the researcher was able to identify themes that illuminated certain factors that had a profound influence on an individual's behavior to implement and use security technologies. The researcher's categorization of codes into themes allowed for analysis to take place. By analyzing and interpreting the data from the emerging themes, the researcher was able to connect the various data points together to form a cohesive story.

By means of the interview guide (Appendix B), the researcher interviewed the participants from each business. The researcher's questions were intended to collect evidence to answer the following two major research questions:

RQ1. What factors impact a businesses' decision to implement information security technologies?

RQ2. What practices do business managers incorporate in the work environment to ease the transition of new information security technologies?

Before performing face to face interviews the researcher eliminated questions that the participants answered no to in the profile questionnaire (Appendix A). These questions dealt with

the use of security information policies within the company. When a participant responded that the business did not employ security information policies, they were not asked to describe how important security policies are to you (Question #17 Interview Guide, Appendix B) and to describe how security policies may help you in dealing with the security system (Question #18 Interview Guide, Appendix B). Both questions were intended to get feedback on the use of security policies within the business. Since the business did not employ any security policies these questions were not asked. If during the interview the participant mentioned documentation usually associated with security policies, the researcher followed up to find out if they used security policies but called them something different in the company. If participants answered "Yes" to interacting with any information security system (Question #6, Profile Questionnaire, Appendix A) then they were asked the set of the following questions from the Interview Guide (Appendix B):

11. Describe how easy or hard it is to use the information security technology system?
12. Describe how you may influence other employees' use of the security system?
13. Describe any influence other employees have on your use of using security technologies?
14. Describe how long you have been using the security technology and your comfort with it?
15. Explain how you may help other employees with the security system?
16. Explain how you perceive your co-workers view the security systems?

This set of questions was intended to explore the factors that influenced an employee's behavior. The collected data would provide the researcher with a better understanding of why some businesses do not implement information security technologies and how employees would perceive their use. The remaining questions in the interview guide assisted the researcher in

further understanding both RQ1 and RQ2. The data collected also shed light on the sub-questions associated with the main questions. The researcher used the main qualitative research questions to clarify the purpose of the study and make connections between the data collected and the participants' perceptions. The sub-questions used during the interview were narrower in scope and allowed the researcher to use that information to answer the main research questions.

Documentation. One way the researcher added validity to this study was by reviewing documentation at the different businesses. This is considered a fundamental practice when conducting qualitative inquirers as a means to provide corroborating evidence with the other areas of interviewing and observations to collect data through multiple methods. The researcher using multiple forms of evidence rather than a single business or data point for this study assisted with the triangulation of the study. Yin (2014) pointed out that documentary evidence is likely relevant in every single case study performed. The different types of documentary information reviewed by the researcher dealt with policies, training, and third-party venders providing cybersecurity services to the businesses.

Observations. Qualitative studies emphasize observation and interpretation with data collected within the context of its natural setting (Creswell, 2014; Park & Park, 2016). Because of this, the case study research took place in real-world settings which provided the researcher an opportunity for direct observations. The COVID-19 pandemic and the availability of some business owners at their business locations, did interfere with some direct on-site observations, however the researcher felt this had a de minimis effect on the data collection overall because data saturation had been reached before the 30 interviews took place. In addition, the study's observations were casual in nature and provided supplemental information for the researcher to gain a better understanding of the business setting and how participants perceived the interview

questions. The researcher's observations extended to the participants' reactions during the interviews as well as when the researcher was engaged in asking clarifying questions of examined documents. Observations allowed the researcher to gain insight into how participants acted in their real-world workplaces as an additional data source for this study.

Risk Assessment. In the security realm, businesses often use penetration testing to gain confidence in their ability to identify vulnerabilities in their networks which could lead to cyber-attacks. A business that implements a robust penetration testing program allows their cyber security program to be proactive by identifying possible vectors for cyber-attacks and applying fixes to mitigate the risk. Determining vulnerabilities is important to a business so they can reduce their risk before a cybercriminal targets their systems. To determine the risk to the participants businesses the researcher used the ZAP© software to run passive scans against each businesses' website. A passive scan relies on the software tool collecting information from the businesses' network data about possible vulnerabilities that may exist on the target computer without direct interaction of manipulation. Data collected assisted the researcher in determining a businesses' risk acceptance and how that was associated with their security perspective.

Summary

The researcher interviewed personnel from 30 businesses in the construction industry and performed a passive scan of their websites for known vulnerabilities. The data gathered were from unique individuals within the management tier of the business with all businesses being distinctly unique from each other, so no management decisions were influenced by the same business management structure. In addition, the businesses were located in different geographic locations around Virginia, to remove any localized influences that may have occurred. Incorporating the differences in the study allowed the researcher to obtain a suitable level of

saturation to develop convergence. These differences lead to improved validity and reliability to assist the researcher in being more accurate with the study's findings where consistency, credibility, transferability, dependability and confirmability for the study's findings was being sought (Creswell, 2014; Merriam, 2009; Yin, 2014). The degree of saturation obtained from the study was sufficient to support the findings. The researcher discovered no known comparative studies in this area; however, the researcher supported his findings with pertinent literature to provide further support.

Anticipated Themes/Perceptions

The review of previous literature identified themes and/or perceptions that emerged through prior studies completed on implementation of information technology. This study discovered certain themes/perceptions through its findings and analysis. The major themes will be presented in the presentation of findings where a detailed description of the analysis will be discussed.

Presentation of the Findings

The study's findings indicate that small businesses are less concerned with cybersecurity thefts than carrying out their core business of construction. The main factors involved in making information technology decisions dealt with return on investment and risk of compromise. Most businesses relied on third-party contractors to support their operations while providing minimal training and policies to support their workforce. The larger the construction business the more important information security technology seemed to become. Within the construction industry when dealing with small businesses, decision making is usually top-down. Almost always, the decision makers are adept at the construction business but have very little experience in the information technology field. For this reason, most business operations relied on outsourcing

their support to a myriad of companies offering information security type support. The following section on the presentation of findings will explain these findings in more detail.

Saturation

The researcher ensured enough data were collected to reach a data saturation point. Data saturation was the point at which no new information was discoverable in the data analysis portion of the study and indicated to the researcher that data collection could terminate (Creswell, 2014). This was necessary for the researcher to make an informed decision about the study's research questions. The researcher's study involved 30 construction businesses where one participant from each company was interviewed. The participants were all managers with most of them holding the role of owner or president. The researcher had reached saturation with five interviews left where no new information came to light. As a result, the researcher is confident data saturation had been achieved when reviewing small construction businesses in Virginia.

ZAP© Triangulation

The researcher's goal in triangulation was to validate the data collected searching for convergence among the different sources of information collected in order to provide corroborating evidence that formed the study's themes. Data were gathered from 30 small construction businesses representing companies throughout Virginia. Through a thorough examination of the data collected from the various participants using the same method, the researcher was able to triangulate patterns and contradictions beyond their individual experiences. The researcher was able to take the results from the semi-structured data collected through the participants' interviews along with a review of documents from the independent businesses geographically located in different areas of Virginia to start the triangulation. The

researcher then performed passive scans of the businesses' websites to determine how valid the information collected on security status matched the other information collected.

The ZAP© passive scans allowed the researcher to determine how the businesses used technology to protect their businesses' websites. The scans showed the following information from 29 websites (one business shutdown their website in preparation owner retiring) in Table 3. Appendix D shows a description for each alert description.

Table 3

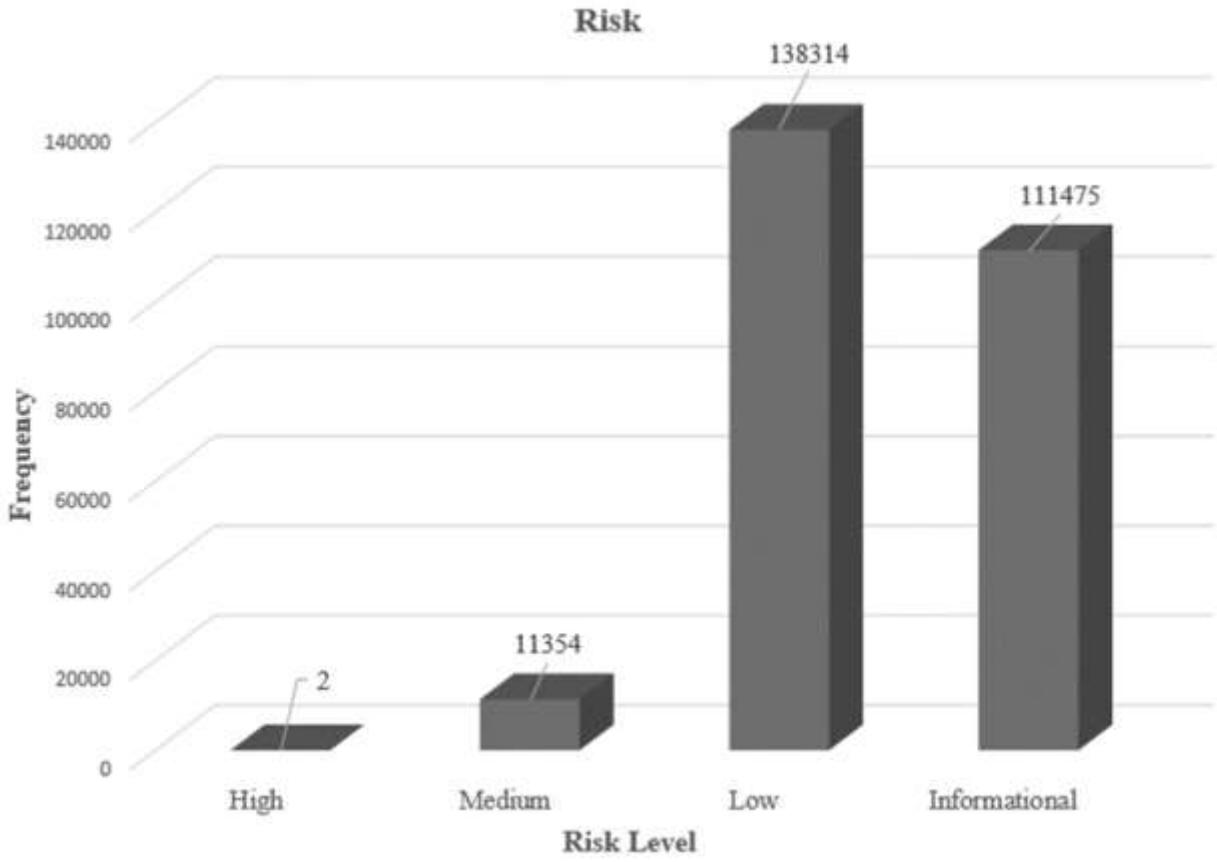
ZAP© Number of Alerts

Alert Description	Number of Instances
Absence of Anti-CSRF Tokens	20,086
Application Error Disclosure	607
Charset Mismatch	867
Content-Type Header Missing	3
Cookie No HTTPOnly Flag	2,433
Cookie Without SameSite Attribute	3,687
Cookie Without Secure Flag	2,323
Cross Domain Misconfiguration	1,544
Cross-Domain JavaScript Source File inclusion	54,510
CSP Scanner Notices	5,610
CSP Scanner Wildcard Directive	5,675
Incomplete or No Cache-control and Pragma HTTP Header Set	12,356
Information Disclosure - Debug Error Messages	109
Informational Disclosure - Sensitive Information in URL	59
Informational Disclosure - Suspicious Comments	12,139
Loosely Scoped Cookie	48
Old ASP Net Version in Use	1
Private IP Disclosure	6
Secure Pages Include Mixed Content	39
Sever Leaks Information via "X-Powered-By" HTTP Response Header Fields(s)	6,352
Timestamp Disclosure - Unix	98,359
Viewstate Without MAC Signature (Unsure)	2
X-AspNet-Version Response Header Scanner	13,775
X-Content-Type-Options Header Missing	16,985
X-Frame-Options Header Not Set	3,570
Grand Total	261,145

A passive scan of the websites showed a total of 261,145 alerts. Each alert represents a high, medium, low or informational issue with the website. Figure 4 shows how many alerts fell into the high, medium, low or informational category. The high-risk alerts are based on possible exposure of information to potential malicious users such as potential impact of access to confidential information. Only two alerts fell in this area but this is the most critical alert possible. Normally, circumstances leading to these types of alerts should be corrected immediately. There were over eleven thousand medium alerts which can lead to breach of data or interruption of service. If a bad actor took advantage of one of these risks, the business could face legal challenges or monetary losses. With over two-hundred and forty alerts in the low to informational category these businesses still face a stout challenge because of the tiering issue. Bad actors use tiering to take advantage of one deficiency that allows them to take advantage of another deficiency that eventually elevates them to access the system. The number of ZAP© alerts show that the small construction businesses do not place a premium on securing their websites. This aligns with the interview and artifact data where interviewees put a higher premium on their core services than their security status.

Figure 4

Alert category



Research Question 1 Themes

Three themes were derived for RQ1, "What factors impact a businesses' decision to implement information security technologies?" These themes include Theme 1: Dependence, Theme 2: Knowledge Deficiencies, and Theme 3: Old School. According to existing research, technology plays a critical role in modernizing businesses with more than half of small businesses in the U.S. not implementing the right technologies to protect their businesses (Olufemi, 2018; SBA, 2015). Past studies have indicated the decision to adopt information technology is dependent on a leader's commitment to implementing a technology where leaders of small businesses sometimes struggle to identify what technologies to adopt (Kim et al., 2017;

Nguyen et al., 2015; Olufemi, 2018). Prior studies have shown small business leaders recognize the importance of information technology and make every effort to incorporate and utilize its power (Kim et al., 2017). Leaders also are responsible for making investment decisions based on gaining efficiencies and increasing profitability which can require enactment of risk mitigation strategies (Aldawood & Skinner, 2019; Angst et al., 2017; Tsakalidis et al., 2019). When responding to research question 1 and its two sub questions, respondents did not always agree with previous research findings. The results of this study will build upon previous studies and elucidate how small construction owners and managers perceive security in their industry. Through the analysis, the researcher discovered several prevalent themes throughtout the small construction businesses which each finding being consistent with the body of literature.

Theme 1: Dependence. For an industry dominated by the male gender (United States Department of Labor, 2019), small construction businesses take pride in being independent and self-reliant. This study showed that when it comes to cyber-security the industry has outsourced its cyber-security role relying on others to protect it from cyber-threats abdicating its independence. Twenty-seven of the 30 businesses participating in the study decided to outsource their information technology services and become dependent on third-party venders to protect their interest. The decision to outsource the implementation and management of their information security technologies within these small construction businesses was based on more than a few reasons.

Small businesses did not consider information technology as a core service of their construction business which by virtue of them being small limited the number of personnel resources they had to perform daily operations. Participant 5 noted, “We do not have that many people in the office.” Participant 4 stated they only have three people in the office with most of

their assets located out in the field and participant 6 indicated, "…as far as our personnel, most of our guys are in the field. There is nobody in the office but me." Participant 21 said he was the sole owner and president of the business which meant "And so, that means pretty much running the day to day operations." Participant 7 expressed, "We do not employ a significant number of office personnel." Participant 14 noted, "…probably 80 percent of the company is out in the field…" Participant 25 summed it up the best when he expressed, "I am everywhere, I'm a man of many hats. So, if it is Summer time, I am in the van, I am in the field. If it is not, here I am." Since construction businesses depend on generating their income from the services they offer in the field, the smaller businesses are dependent on third-party venders to do their cyber security work. Some businesses like participant 22 noted, "We do not have any security measures," relying solely on third-party companies for protection. This allows the small businesses to keep their money-making resources (employees) in the field doing the actual construction duties that create revenue for the business.

Theme 2: Knowledge Deficiencies. Small businesses also rely on third-party information technology venders because of their internal information technology knowledge gaps. Research has shown managers of small businesses do not see the implementation of information security as an immediate problem because of a lack of knowledge (Osborn & Simpson, 2018; Soomro et al., 2016). The majority of businesses had very few administrative people that worked in the office. These individuals were responsible for performing many functions within the office. Participant 6 related, "My job is to make sure all the paperwork is done correctly, I do payroll, I do everything." This was not just limited to office managers but included owners as well. Participant 24, the owner of one of the businesses emphasized, "I am the president, secretary, treasurer, but basically my job position is just the office manager." This

dual hat positioning is normal in a large amount of small businesses (Howard et al., 2019; Wetzel, 2019). Participant 25 stated, “I am everywhere, I’m a man of many hats.” This sentiment was also expressed by participant 2 who noted, “I wear multiple hats within my business.” Participant 29 relayed she was one of the owner’s and was responsible for the books and everything outside of the field work. The issue in the construction industry is the majority of employees operating in the industry have not been trained to be information technology experts and therefore cannot perform those specialized functions as an additional job. Some businesses recognized this and tried to hire internal computer experts, but these were the larger of the small businesses involved in the study. Computer expertise was also not important to many of the smaller businesses involved in the study as they believed the traditional or old school way of doing business was preferable.

Theme 3: Old School. Twenty-six of the businesses were started as family owned businesses with 23 still being owned by the same family. This family model of ownership has kept the original entrepreneur in the business still making most of the investment decisions. Age was also a factor here as many of the older owners know they are ill equipped to deal with the cyber security challenges that continue to grow exponentially. In many instances, the owners and managers have no desire to deal with the security challenges imposed by cybercriminals and would prefer to go back in time, when things were simpler and less complicated.

Participant 4 discussed his distrust of computer systems when they were first implemented in the business and how his doubts ruled his behavior. For the first year after implementation of a new system, he kept a separate set of books on hand in case the system failed. He also acknowledged, “… my son just started working with us about five years ago, and he is brought in new technology that we have been looking at utilizing a little bit of.” He

understood that the next generation is more prepared to use technology in the business than he is. Participant 6 described herself as the person that knows the most about computers within their business and relayed that the owner, "… is old school, he does not use the computer, at all." This sentiment is shared by more of the owners as participant 5, an older interviewee expressed they would prefer to do things the way they did in the past with paper but commented, "… but that is not the way of the world, so either the phones or the communications through email and things like that are a necessary evil and even point of sale has got to be a necessary evil." Additionally, participant 15 articulated that their business was still paper based and they've been trying to implement more technologies but are just starting to move towards technology to protect operations. Participant 30 relayed, "There is no need for any security it's just ah proposals," believing the construction business was operating like in the past were cybersecurity was not a concern. Most of these individuals understood information technology is a necessity for the business but sometimes they believed like participant 28 who voiced, "I know there is hackers out there, and if they want to get in, they are going to get in." His was not a prevalent idea among the interviewees were most thought they could protect their systems. However, this protection comes at a cost and interviewees highlighted the need to level set risk with what it cost to protect their businesses' information.

Research Question RQ1a Themes

Five themes were derived for RQ1a, "How do the internal investment processes that owners/managers institute assist in determining the best course of action for implementing security systems?" These themes include Theme 4**:** Top-down Decision Making**,** Theme 5: No Formal Plan, Theme 6: Cost Driver, Theme 7: Privacy, and Theme 8: Risk Driver. Prior research has shown business security investments typically are in response to perceived and materialized

threats where many businesses prioritize implementing security systems only after they suffer a security incident (Kim & Chang, 2014; Nazareth & Choi, 2015). Data has shown proactive managers implement security technologies that can enhance the businesses' infrastructure before cybercrime incidents occur (Tsakalidis et al., 2019). Research involving the theory of planned behavior has shown that a manager's behavior can be predicted to be proactive or reactive (Sommestad et al., 2015). Internal investment decisions by owners/managers has shown it is more complicated than just cost when it comes to construction businesses which is consistent with the body of literature.

Theme 4: Top-down Decision Making. Interviewees' disclosed that decision making was based on a top-down approach where cost was considered. The top-down approach was implemented by the owners or managers in all instances. Most decision makers said they took advice from others in the business but the final decision on the way to move forward was theirs and they expected everyone in the businesses' lower hierarchy to follow those decisions. Participant 7 said, "Anything that needs to be done within security would, would come to me first and I make the final decision." Participant 10 explained, "All, all the decisions," are made by him. Participant 8 enthusiastically portrayed he was the ultimate decision maker while participant 17 noted, "…as far as what this branch does, as far as security, it all relies on me. I make the ultimate decision." Participant 25 explained, "I do make the decisions on 98% of what happens around here." While many interviewees claimed to be the ultimate decision makers, over half believed getting input from others around them only made sense. Participant 4 noted they play the main decision role. As participant 15 recognized, "Well, I would think, anybody who is smart would use the resources you have around you to make the best decision for the business." This was reinforced by participant 3 who believed he could make a decision between

two computer systems, but if a majority of his managers believed in the opposite system than he choose, he would have a hard time implementing the one he thought was best for the business. At that point, he believed convincing other managers of the merits of the system he liked or they needed to convince him of the advanatages of the system they liked was the only way to resolve this conundrum. Attaining their buy-in was important for the system implementation to be successful. Participant 20 explained, “Our company makes these decisions on a very, very higher level.”

Theme 5: No Formal Plan. None of the interviewees had a formal risk-analysis process to identify cyber risk to the business. Instead, they used word of mouth and sometimes when seeing newspaper, television or other stories about data breaches or cyber thefts against small businesses, some interviewees said they put a little more thought into it. Participant 25 noted, “No, we don’t use any risk analysis.” Participant 7 stated, “Nothing with risk analysis, I mean it’s nothing we would document.” Participant 9 relayed, “I wouldn’t think anything formal we probably jot some stuff down on the whiteboard and weigh the pros and cons.” Participant 14 was the only interviewee whose business does a yearly risk assessment against their business pointed out, “Yes, you know, we have like I said minimal things we do on our side that when something comes out like a data breach or something like that. . .” With participant 27 saying, “We at least think about it.” Being candid, participant 4 admitted, “I will be honest with you, we do not, we do not think about it that, that much.” Because of a lack of information security planning, cost was not as big a driver as expected in the implementation of security systems.

Theme 6: Cost Driver. Six businesses directly mentioned cost as a major factor in their decision-making processes as participant 3 explained, “… how much time and savings can I get.” Cost was a driver in other interviewees’ decision making processes as participant 8 pointed out,

"I make most of the decisions around here so when it comes to the cost of something that has to weigh in heavily on our yearly budget, so our finances, cash flow all that comes into play." This cost philosophy was reinforced by other interviewees in how it affected their small businesses as participant 15 stated, "One obviously is cost relative to most small, you know, small businesses and what they feel they can afford. The other is the necessity of it." Participant 15 mentioned the necessity of cost with a more succinct answer being provided by participant 4 were he said, "I base my decision on price and functionality." These replies seem like participants were cognizant of their decisions to protect their data depending on the price of new technologies. When responding to the question of what the impact was when they knew that cyber-attacks occur against small businesses on a routine basis have on their implementing security information applications (RQ1b), the majority of interviewees did not really think about it much.

Theme 7: Privacy. Privacy vs cost was on the mind of a lot of the business leaders interviewed as they contemplated how to protect their businesses' data. Small construction businesses operate within a very competitive marketplace where participant 28 pointed out. "…it is a cutthroat type of business." This directly impacted how that manager and others thought about making privacy decisions on implementing systems. Interviewees wanted to protect internal and external data. Participant 9 noted, "I would say financial and client personal information security." Participant 10 stated, "Private, private information is private." Statements from participant 2 highlighted, "I would have to protect would be some of my employee's information and my customer's information," while participant 1 said, "I think the most important thing would be my responsibility of keeping the people's information protected," and participant 26 relayed, "You want to protect your staff and any customers from any kind of hacking." Participant 20 mentioned, "Most of the secure information that we have is mostly how

we bid the jobs and how we win the projects and how we do our work," which meant this was their most secure information and it really needed to be locked down. Participant 22 stated, "You don't want people getting into your computers and getting customer information, addresses and phone numbers, your accounting information, banking information." Participant 7 explained, "I would say protection of customer data as well as employee and company financial data" while participant 8 stated, "the protection of information as much as possible. Within reason. You can not spend a million dollars to protect a hundred thousand dollars." These were common sentiments among the different interviewees.

Theme 8: Risk Driver. The construction businesses involved in this study operated in the following three types of areas: residential, commercial and government. Each business sought a niche for their particular type of services with some operating within all three at the same time while at other times operating within only one. The goal of the businesses was to earn a profit with the ones operating in the government construction space accepting the least amount of risk. As participant 19 said on moving into the government space said:

> We are actually swapping over currently because we, we have delved into the government agencies side of work more than anything else now. And as a result, obviously, we want our systems, systems to be more secure because some of the stuff is secure, classified that we are looking at. So, we were with a private you know, third-party company that was mainly for commercial small business and stuff like that. But we are doing a joint venture currently with a company that specializes in information technology security for the government, and they are going to be upgrading our system to, to match government standards.

Since the government has standardized requirements that businesses winning government construction contracts have to adhere to, their systems are required to be more secure. Participant 19 who was getting into the business stated, “We are doing a joint venture currently with a company that specializes in information technology security for the government, and they're going to be upgrading our system to, to match government standards.”

The businesses involved with residential sales accepted the most amount of risk because there are no standardized security requirements. Participant 5 pointed out,

> Well, for our purposes, we really do not have much that a need to be totally secure… I am not, you know worried about security from that end, if someone wants to make a copy of it, that is fine.

The sentiment ran deeper with some interviewees where participant 28 saying, “No, like I said we do not really worry about security.” Participant 12 mentioned, “There is really not, I mean, there is just not a big market on the black market for construction information.” These behaviors about information security led to the businesses being dependent on the third-party information technology companies to protect them and think about the risk.

Research Question RQ1b Theme

One theme was derived for RQ1b, “How does knowing that internal threats and cyber-attacks occur against small businesses on a routine basis have on implementing security information applications?” The theme consisted of Theme 9: Insider Threat. There is a cost involved with businesses either proactively implementing security to protect the business or financially dealing with the aftermath of a successful attack. Noguerol and Branch (2018) identified financial restrictions and inefficient leadership as factors that affected businesses from properly implementing security information systems. According to Mayadunne and Park’s

(2016) research, small businesses are more likely to focus on high-risk low-loss threats over low-risk high-loss threats which require accurate estimation of the level of risk that each threat poses to determine. This information may not be readily available at the time decisions are being made. Nguyen et al. (2015) found that poor management practices also played a role in a business leaders' inability to make informed security implementations decisions. The following theme highlighted some of these issues which was consistent with the current literature.

Theme 9: Insider Threat. Twenty-three interviewees believed keeping information safe was one of the most important factors a company could do. Many times, smaller companies feel they can trust their employees and may not feel they need security measures in place. This sentiment was dispelled by participant 19 who stated:

> All the construction industry is one of the largest, if you look at the what trades, get embezzled upon, construction industries or embezzled from within more than any other company in the world. It is really easy to have employees steal from a construction company in one way, shape or form. I do not know how that would relate to outside sources and then being able to embezzle funds, but the biggest, the biggest money lost to the construction industry, sees is actually from embezzlement from within.

This data proved factual in participant 23's business as it had suffered two separate incidents of embezzlement and forgery from business employees. These insider threats caused the business to loss $150,000 from the first incident between January 2016 and January 2018 and in the second incident nearly $93,000 in business funds. This business was in the middle of finding a new information technology expert. No other businesses claimed to have been compromised from the inside and did not place a value on this risk. Only three interviewees

placed much concern on insider threat situations even though twenty-three interviewees mentioned protection of data as a concern. Participant 19 noted, “if you look at what trades, get embezzled upon, construction industries or embezzled from within more than any other company in the world.” Participant 1 believed, “No one has access to anybody’s computer except for me. I have a, I have a like the master passcode for all the computers,” believing this would prevent an insider threat issue. Participant 11 stated, “It is a risky industry. It only takes a breach of that information to get out to, you know, subcontractors, employees taking files, things of that nature.” Participant 13 noted, “We build things, we don't pay much attention to, the computer system.” He believed they had no worries about insider threats as long as they had a cloud backup and virus protection software. Like participant 13, three-quarters of interviewees believed the third-party contractors were protecting their interest either through QuickBooks® or other cloud-based systems implemented by their banks. As participant 15 said that their company follows the third-party suggestions on “…what different software seem to be most effective and we've always invested kind of heavily on that.”

Protecting the business from internal or external threats was couched with financial concerns. Participant 3 stated, “Before you make a decision on implementing any type of system. You need to know the cost benefit of that system.” As other interviewees made known, cost weighed heavily on their budgets, finances, and cash flow. Participant 11 described how his business has gone from doing 20 to 30 million dollars in construction work down to five or ten. This decline in projects lead to less revenue which in turn made the participant 11 say, “I do not, I do not quite look at it the same or that concern anymore,” referring to security. Participant 15 summed it up well when he clarified, “…cost relative to most small, you know, small businesses and what they feel they can afford. The other is the necessity of it.”

Research Question 2 Theme

One theme was derived for RQ2, "What practices do business managers incorporate in the work environment to ease the transition of new information security technologies?" The theme consisted of Theme 10: Training and Support. Previous research identified a leader's role in implementing security technologies as one where supervision, communication, and training were important factors to successfully implement technologies (Hansen & Nørup, 2017). Leadership's demonstration that they support information technologies was highly valued by larger businesses over smaller businesses (Santos-Olmo et al., 2016). A manager's commitment on the importance of securing business information by aligning business structures to support that goal was also a factor to easing the transition to new information security technologies (Guhr et al., 2019).

Theme 10: Training and Support. The majority of businesses when introducing new security systems required employees to receive their training either in person or on-line. When presented in person the company who the system was purchased from usually brought in an information technology expert on the system to the purchasing business to train their employees. Participant 8 said, "Once a system is in place, we have our information technology company come in and do a training session to all our employees." Participant 15 pointed out, "There have been a couple of webinars and information technology guys came and, you know, showed he is giving tutorials, if needed at the office." Participant 26 noted, "We use a third-party IT company. They have come in done, have done in person training on security items." Participant 27 stated, "We usually just have an individual basis on training on each individual program." Participant 13 detailed they only make their employees familiar with what is in place. One business was unique in that the participant 16 stated, "We use training provided by the government. Security agency

is online training." Participant 17 who belonged to the largest business in the study actually required each individual employee when onboard to attend a training course on how to use the network safely. This was a rare occurrence as 53% of the small businesses said they did not offer any training to their employees. Participant 9 was one of those where the owner said they offered no training or other resources to their employees to learn about security systems. This was due mainly to managers believing all security systems were being run in the background and the employees had no direct access to them. Participant 19 was introducing a new system in the business and had not decided on how training would be conducted. Finally, some managers felt that employees could learn on their own usually these involved systems dealing with email, credit card purchases and virus scanner programs. Participant 23 stated, "Usually, it is up to the individual who is at that computer but a lot of times the office manager has to step in." Participant 28 put it like this, "We do not, we do not do any training." Participant 14 stated, "I can tell you that we do not have any specific training."

Besides third-party and individual training, some companies offered their employees help desk support through either the direct vender they purchased their systems through or through an independent vender. Participant 29 allowed employees to request "assistance through Geek Squad and just calling the helpdesk." Still multiple interviewees used QuickBooks® as there help desk because of the contractual relationship they had. With participant 29 saying "Just on the job training and assistance through QuickBooks®" is how they resolved their security issues. Participant 28 also said, "QuickBooks® we work through them." Participant 21 said they usually rely on the security measures that come with their store-bought computers and whatever there would be with QuickBooks®. While participant 2 also used QuickBooks® for its security and support. Another unique way one business received security training from an outside source was

through pop up training. Participant 11 explained, “As we get, you know, pop ups and different things coming from our information technology folks, we have one young lady that kind of reviews those things and can provide me with some recommendations at times.” The pop-up training is not planned but is just offered in a short time period and the business only takes advantage of it, if they think it will help them in some way.

Research Question RQ2a Theme

One theme was derived for RQ2a, “How do employees perceive changes to the work environment when new information security technologies are deployed?” The theme consisted of Theme 11: Change Perception. Akman and Mishra (2015) and Bolek et al. (2016) recognized managers understood that for employees to understand information security changes, they needed to be trained and the businesses needed to hire skilled information technology personnel to assist (Akman & Mishra, 2015; Bolek et al., 2016). Employees can feel overwhelemed as technology changes are accelerated to combat the increases in cybercrime incidents leaving them in a state of exhaustion (Guhr et al., 2019; Li et al., 2019). Passwords also add to an employee’s stress as the number of passwords is on the rise creating frustration and inconvenience with users who learn to circumvent password security rules by engaging in risky password behaviors to aid them in managing a multitude of passwords (Woods & Siponen, 2019). Prior studies have also found that it is important for employees to receive communication on information technology changes to make them more accepting of the changes being imposed (Guhr et al., 2019; Li et al., 2019). Employees at all levels react positively or negatively when the hierarchy of the business imposes information technology solutions on them (Mazereeuw-van der Duijn Schouten et al., 2014; Ruben & Gigliotti, 2016). Past research has shown employees are also influenced by how

they perceive their leaders want them to act when technology changes take place (Ruben & Gigliotti, 2016). An evaluation of the finding showed it was consistent with prior literature.

Theme 11: Change Perception. The majority of interviewees said their employees accept changes to their work environment when new information technology systems are implemented. Acceptance of new security systems was not always easy as stress played an important role. Participant 26 thought, “I think they are useful. I don’t think they cause stress to anybody.” Describing implementation of a system, participant 8 said, “There is always a strain to whenever there is change.” Participant 3 believed until employees figured out that the change that took place was not that horrible, they are in a learning curve phase. Participant 16 explained that changes are never easy with any of the work they have to accomplish. Participant 17 described, “If I feel that there's something that needs to be changed as far as security goes, I make that change.” Participant 11 stated, “There is always a strain to whenever there is change.” Participant 19, a manager switching to a new security system discussed how he did not know how much volatility the change would bring and how it would impact employees work. Many interviewees discussed the issue with the number and frequency of password changes and how they impacted employees’ acceptance of systems. Participant 6 noted, “I do something that I know that I am going to do to remember, remember you know as far as the password.” This went against the businesses security policy but he felt violating password rules was not as important as being able to access the system to do his job. While participant 6 also relayed, “I will update the system every 30 days because there will be somebody that can figure out what my password is.” In several instances, interviewees talked about how they lead the change as participant 24 stressed she wanted to implement credit card readers for her field workforce but the stress was

too much on the employees, so they cancelled the project that would have provided improved data security.

Research Question RQ2b Theme

One theme was derived for RQ2b, "What new stresses are introduced in the workplace when new information security technologies are deployed?" The theme consisted of Theme 12: Stress. Previous studies confirmed stress has a negative effect on employees' productivity emphasizing how important it is to manage employee stress while implementing information security (Lee et al., 2016). Other research has shown employees must devote time and effort to comprehend and learn how to work with new technologies causing confusion and stress from job insecurity, privacy concerns and job insecurity (Ament & Haag, 2016). The fact employees believe they are being watched introduces mistrust into the work environment. Along with mistrust employees who are older may fear job insecurity with the rapid job changes. Studies have shown age differences especially for older adults have more difficulties in adopting to new technologies, which can lead to more stress (Berg-Beckhoff et al., 2017). Findings showed that some managers thought stress was important and other managers did not which is consistent with prior research.

Theme 12: Stress. Stress was a constant when discussing implementation of security technologies. Participant 11 was very accurate when he discussed stress and the age of his workers.

> There is always a strain to whenever there is change. Typically, we find that with our personnel that is older. We are talking about 45 and older. They seem to not like certain things when things get changed and where the younger folks seem to going with the flow.

Participant 1 discussed the stress level for one particular employee when her computer was updated that, "…it causes her a lot of stress, for her. She is not in to having new stuff come in she is pretty much set in her ways and if I change something it stresses her out really bad." This was a common statement from several interviewees where participant 3 basically stated, "…all new technologies cause stress from the standpoint of them, they have, everybody, not everybody likes change." Participant 8 explained he is under stress because he has to "Weigh the risk of do I need to purchase it or do I take the risk of, of not spending that money at this time and continue, continuing down the path I am on. That is stress." Participant 27 clarified, "I think there is a little bit of stress to the workforce as far as employees using new technologies for security purposes." Participant 12 said, "There is no, there is no stress really involved in the employee's day to day unless something goes really wrong with an install and really wrong with the implementation of the security." Participant 18 stated, "I mean, of course, using any program could be a little bit stressful, but the whole goal of using a lot of these programs is to reduce the amount of work that you have, which makes your work easier." Participant 19 detailed, "Any time you are looking at a new system and everybody has to be trained and learn a new process for doing something, it's always a little bit stressful." Participant 22 stated, "No, it does not cause any kind of stress." Participant 15 noted, "Well, there have not been any stressors and you know." Both participant 22 and participant 15 contradicted what a lot of other participants believed.

Research Question RQ1c Theme

One theme was derived for RQ2c, "How do security policies assist employees in dealing with the deployment and acceptance of new security information systems?" The theme consisted of Theme 13: Security Policies. Santos-Olmo et al. (2016) found security policies are intended to

help businesses manage their information security in an effective manner. Emphasizing information security policies with the launch of a new security system, businesses can gain voluntary and involuntary conformance and improve technology acceptance (Bélanger et al., 2017). Leadership was also found to be a critical factor in implementing information security technologies as policies help change the security culture which is needed to strengthen the businesses' security posture leading to substantial gains in security awareness and employee behaviors towards security implementation (AlHogail, 2015; Goo et al., 2014). Angst et al. (2017), Hwang et al. (2017), and Osborn and Simpson (2018) discovered security awareness and acceptance of new technologies by employees happens concurrently, especially as information technology security investments are mandated. An evaluation of the finding showed it was consistent with previous literature.

Theme 13: Security Policies. When ask about security policies only seven businesses had internal written security policies. Like many other particpants involved in the study, participants 1, 2, 4, 10, 15, 18, 21, and 30 admitted to not having policies. Participant 8 whose business had written security policies said the following:

> We do have written security policies and employee policies. When I purchased the company, I felt like it was, we needed more formal procedures in place, so we took on the initiative to put several policies, manuals and what not in place, so there was never any question in what, what should take place.

Participant 16 stated, "…we have both, we have government security policies and we have our internal processes, the ISO 9000, one 2015 certified business." Participant 16 explained, "…we have personal privacy policies with all of our, you know, NDAs and things like that that we go through with everyone that we work with, depending on, you know, who it is."

Participant 12 noted, “Policies largely regard users, you know, that don't, you know, certain sites don't visit social media and things that are known to harbor exploits or have been traditionally places that exploits may be harbored online.” Participant 11 described his role, “As the president of the company, I implement, you know, some of those policies to protect and to provide checks and balances.”

Kim and Chang (2014) mentioned to ensure sustainable growth, businesses should integrate security policies, human resource management, facility management, and information technology security management to achieve security compliance. Instead small construction businesses were relying on external businesses like credit card companies and banks they had a fiduciary duty with to develop policies they were required to follow. These external policies were enforced by penalties sometimes as participant 24 noted, “If I were to hold your credit card and say throw it in my desk or save it on my computer, that is a problem for me because that could be up to $20,000 fine.” Participant 16 noted, “It is very important because there is the weak link, if people don't follow policies and procedures. There could be a breach.” The majority of businesses did not have written security policies and used word of mouth to tell employees what to do. Participant 2 stated, “Yeah, it’s all up in your head.” Along with written communications on the business security policies and performing training activities, compliance with the security may subsequently rise when these are in place (Cram et al., 2018). Failing to provide written security policies along with not providing adequate training did show to have an adverse effect on employee’s behavior intention, which in turn impacted how some interviewees felt about security technologies.

Analysis of the Findings

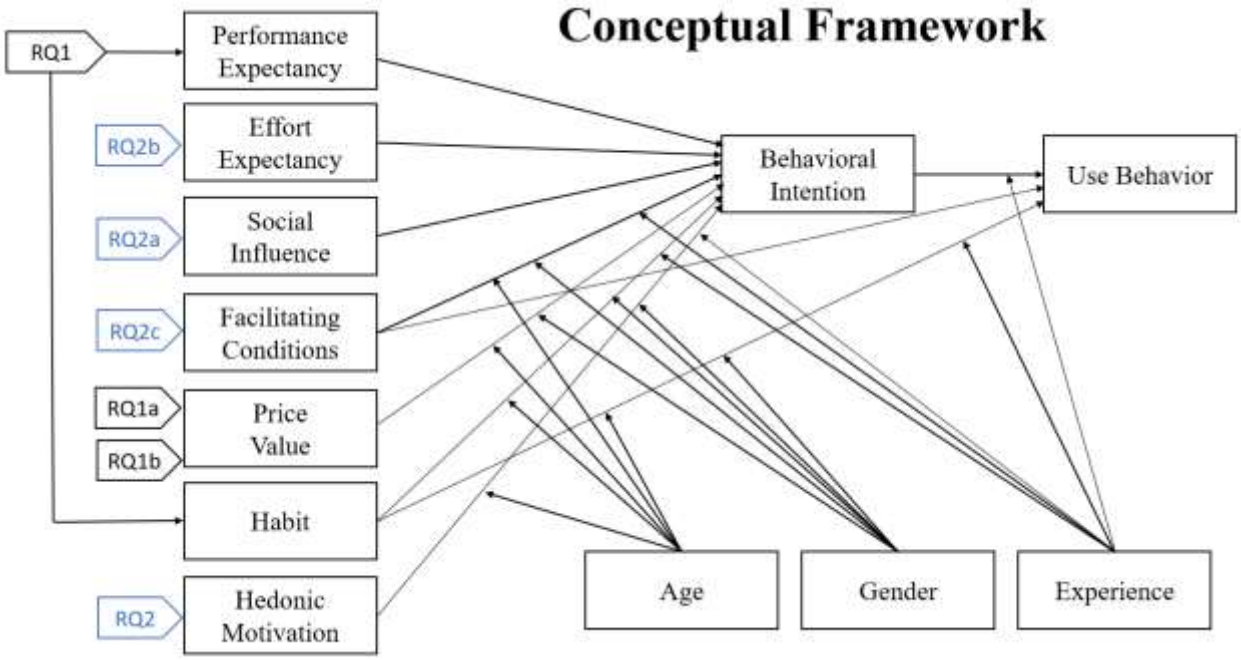
Supplementary analysis of the conceptual framework and how it impacts this study of small construction businesses. The conceptual framework is compared and contrasted against the information collected to see how the data compares against previous data collected in similar research. The modified UTAUT2 framework will add new data to the discussion points as new elements were added and some of the prior elements removed.

Research Question 1 Conceptual Framework

Analyzing RQ1, "What factors impact a businesses' decision to implement information security technologies?" through the conceptual framework allowed the researcher to look at performance expectancy and habit which can affect behavioral intention, and use behavior. In addition, the modifiers of age, gender, and experience were incorporated. The sub questions RQ1a, "How do the internal investment processes that owners/managers institute assist in determining the best course of action for implementing security systems?" and RQ1b, "How does knowing that internal threats and cyber-attacks occur against small businesses on a routine basis have on implementing security information?" both allowed an in-depth view of price value. Using the main question and sub questions allowed this research to identify some key data to support the UTAUT2 framework. Figure 5, visually displays the UTAUT2 framework and how these elements are aligned to each other. The findings in the study were also consistent with the research surrounding prior UTAUT2 studies.

Figure 5

UTAUT2 framework



Performance Expectancy Findings. Venkatesh et al. (2012) described performance expectancy as an individual's perception that an information system enables the completion of an assignment. This study found that owners and managers involved with using security systems used them without thinking about their functions. Macedo (2017) and Venkatesh et al. (2012) discussed the employee's utilitarian value for using a security information system while this study's results found the utilitarian benefits (extrinsic motivation) from implementing a new security system came from previous exposures to cyber threats and third-party requirements, if not followed could result in fines or loss of system use. Participant 30 described how credit card machines in the past would show you the complete credit card number and name but today, "It might show you the last name but it does not show the credit card." Because of this the business

ensures nothing is kept for that part of a transaction securely protecting the transaction. Participant 1 stated, “They are very important to me because of the liability that I have. You know that’s the only thing I worry about the liability that I have if I leak that information for my guys.” Having systems work that protect the employee’s information was important. Participant 3 discussed his businesses issue with a system working and a subcontractor not ensuring it was operating which cost the business to file a large insurance claim. Without the insurance policy the company could have been out tens of thousands of dollars. Participant 8 noted that someone hacked into their bank account and made an ACH withdrawal from their business bank account. This failure of the bank’s security system required the business to find a larger bank with improved security protocols with multi layers of security. The business relied on the smaller banks security protocols to protect their funds and the system did not. Participant 14 discussed their reliance on their security system’s ability to protect non-confidential and confidential information that the business needs to disseminate to different people but must remain under strict control. The employees believe the system will operate as intended so data can be secured. Participant 16 explained how they rely on their supplier logistics system to securely track shipments because they have to follow certain guidelines. The business dependence on the system is the only way they can secure the shipping locations from other suppliers. Participant 29 stated when asked about the importance of their computer systems what they thought and she declared, “Really important because our business is really growing at a very rapid pace and we are dependent on our computer systems.” Her belief that they were dependent on their computer systems like many other interviewees

had a positive effect on performance expectancy which increased behavioral intention to use the systems.

Habit Findings. Maity et al. (2019) explained once trained, individual's habits of interacting with information technology should follow a normative behavior pattern. This habit was described by Venkatesh et al. (2012) and Huang and Kao (2015) as prior behavior and the degree to which people believed the behavior to be automatic. During the interviews most interviewees held they did not think much about the systems they used or how they functioned. Instead they were more worried about other aspects of their jobs. Participant 1 reinforced this thinking when he said he did a lot of on-line banking transactions and reiterated he was not that concerned with data breaches. He relied on the banking system to protect his business transactions. Participant 8 discussed the benefits of their server filters to prevent spam emails as they had a ransomware attacks previously and these filters cut down on erroneous information. They also allow employees to focus on more productive task by preventing email overload from outside. This type of technology improves an individual's habit of using the technology, but they are strictly in passive mode.

Participant 12 mentioned that the employees really do not interact with the security systems functionality, so there is no need to train them. The age did show an impact on behavior intention and use behavior as older interviewees did not like using the systems and, in some instances, avoided them altogether. Participant 11 stated, "We're talking about 45 and older. They seem to not like certain things when things get changed and where the younger folks seem to go with the flow." Interviewees used the systems that the company purchased with gender and experience not showing anything that could be construed as negatively impacting behavior intention and use behavior.

Research Question 1a Conceptual Framework

For this study, "investment behavior" regarding the buying and deploying of security information technology systems was assessed as part of price value. The findings indicated that investment behavior was influenced by the attitudes of decision makers. These depended sometimes on their cost-benefit evaluations and the subjective nature of their perceptions on the usefulness of security information technology systems which Heyder et al. (2012) had found. Price, risk and return was the mantra of participant 4 who believed the all three had to be aligned for him to make a decision on implementing a security system. Participant 1 layed out why he let his third-party contractor make decisions on investments by saying, "I have had the same guy for 20 years and he is always, he is always done what is best for me, you know. . . I let him handle all my computer stuff."

Kim and Chang (2014) and Nazareth and Choi (2015) comtemplated that security investments are typically a response to perceived and materialized threats where information security management really becomes important to businesses after they suffer a security incident. Exposure was believed by participant 12 who had 60 odd employees working in the business important, but he also noted that a bank has very high exposure as opposed to a construction company. Participant 12 also believed it was important to protect the businesses' information in a layered approach using active firewalls to defend against viruses, malware and other known exploits but procuring additional security technologies to protect against one off websites was not parctical. Six businesses had suffered some type of cyber incident and in each case they took actions but always did not necessarily increase their security posture. Participant 6 said after the business owner had gotten taken advantage of, "I think he does need to upgrade it." While participant 3's business suffered a large insurance claim, so the business according to the

interviewee noted, ". . . and after that point we implemented some really strong protective things for the company." Participant 10 said, "I got caught into a trap once and I do not want it to a happen again," implemented tougher security after the incident to prevent repeat occurrences. Participant 14 stated, "Yes, you know, we have like I said minimal things we do on our side that when something comes out like a data breach or something like that, you know, we've had a risk assessment done to our business." The study showed investments in most instances did drive behavioral intention when incidents occurred.

Research Question 1b Conceptual Framework

Half of all cyber-attacks are committed against small businesses where these actions can have a damagingly impact on the business's financial objectives (Stanciu & Tinca, 2017). Insider threats are increasingly becoming more detrimental and frequent, affecting critical infrastructure (Walker-Roberts et al., 2018). The price value factor of the conceptual framework comes into play here by businesses who deteremine they want to proactively or reactively pay out to prevent security incidents or pay for the consequences of those incidents. Only two businesses in this study thought about insider threats while the majority focused more on external threats. The manager operating at the buisness that suffered two insider threats attacks believed information security was important as everything was going to a digital format, however the company did not have security training or other resources in place for its employees. In addition, they were having a hard time finding an internal computer specialist for the business. Some businesses just accepted that they would not be able to stop external actors from accessing their information. During the interview, the participant 28 stated when asked about hacking, "… just take it each day as it comes. So, I am not really too worried about

it.” This was an outlier in the data but most businesses did think they were too small to worry about being attacked.

Fielder et al. (2016) showed how important it was for small businesses to recognize that cyber attackers can strike anywhere they wish. Most of these small businesses did not take that warning into account as participant 9 said, “We have not made any, any plans in the future to have it. I do hear about breaches of people's personal, you know, personal stuff, but not that much on businesses.” While participant 12 explained after an employee had released sensitive information to a bad actor pointed out, “…when the breach was discovered, we implemented training for people…” This reactive response was usually the norm as participant 3 spoke of their big cyber incident and how they, “had already implemented something that would protect us against like a cyber hit.” Participant 18 relayed, “We don't really have a lot of security that we can implement now within our business plan.” This lack of pre-planning to deal with internal and external threats seemed to be the norm for the smaller construction businesses. The findings showed after an incident that use behavior and their behavior intention would increase for a period of time.

Research Question 2 Conceptual Framework

Analyzing RQ2, “What practices do business managers incorporate in the work environment to ease the transition of new information security technologies?” through the conceptual framework allowed the researcher to look at hedonic motivation. In addition, the modifiers of age, gender, and experience were incorporated. The sub questions RQ2a, “How do employees perceive changes to the work environment when new information security technologies are deployed?,” RQ2b, “What new stresses are introduced in the workplace when

new information security technologies are deployed?" both allowed an in-depth view of price value?," and RQ2c, "How do security policies assist employees in dealing with the deployment and acceptance of new security information systems?" allowed the researcher to analyze social influence, effort expectancy, and facilitating conditions, respectively. Figure 5, visually displays the UTAUT2 framework and how these elements are aligned to each other. The findings in the study were also consistent with the research surrounding prior UTAUT2 studies.

Hedonic Motivation. Venkatesh et al. (2012) defined hedonic motivation as the fun or pleasure derived from using a technology. Aswani et al. (2018) and Venkatesh et al. (2012) studies showed hedonic motivation was a significant factor in deriving an individual's behavioral intention and determining technology acceptance. Ravangard et al. (2017) and Venkatesh et al. (2012) showed that an individual's behavioral intention increased when their experience using technology was enjoyable. Participant 27 noted, "For instance, we have an app right now that we check in, it's a clocking in app basically but at least I know where they are at if something happens. Which is fantastic to have." The businesses' use of securely tracking employees' locations assists with complaints and participant 27 believes, "…it is nice to have that information if something does happen or come awry or we have a complaint or something like that." Participant 25 believed his job was easier with their secure systems in paying the business's bills and sending people's information back and forth through the systems. The ease made it less stressful to use the system. Participant 17 discussed his role in network intrusion and said, "… like somebody breaching our network, I can see that because all that information comes through me and I can push it on to our IT department, say something needs to happen here." He found his role important and he was enthusiastic about carrying it out which meant he continually used the tools at his disposal. Participant 12 described his role in finding and hiring security vendors with a reputation of being reputable vendors who have a history within the

industry of being active and forward thinking on managing exploits. This allowed him to feel comfortable using the security standards and equipment the business implemented. Participant 10 found his business's anti-virus software easy to manage and believed it protected him from cyber-attacks. The ease of use made using the systems more enjoyable which lead to increased behavior intent and use behavior.

Research Question 2a Conceptual Framework

Social Influence. This study looked at how social influence impacted the extent to which employees perceive that co-workers believe they should use a specific technology. Focusing on co-workers, the researcher asked two questions to gather data in this area. Interviewees were asked to describe how they may influence other employees' use of the security system (Question #12, Interview Guide, Appendix B) and to describe any influence other employees have on their use of using security technologies (Question #12, Interview Guide, Appendix B). In both instances interviewees thought they influenced others by providing guidance on the system. Participant 24 relayed she was very strict with her employees in a totalitarian way to make them follow the businesses' processes. Other interviewees used more positive management styles like when he noticed employees writing down passwords because the passwords had become unwieldy to many employees because they had to be continually updated and the number of passwords for the different systems seemed to keep increasing. Participant 17 tried to remind them that "…there is a lot that we do on a normal basis that people do not feel like it is a big deal, but it really is." This approach by participant 17 worked sometimes and other times it did not. Since a large majority of the offices had few employees' they felt that the close working relationship had a positive influence in learning to use and implement their system(s).

As Li et al. (2019) explained, social influence can positively contribute to a user's behavior where individuals exposed to higher levels of cues to action can positively effect an individuals' intention to adopt cybersecurity technologies. This was characterized by participant 12 who detailed when a problem occurred people immeditely got a hold of him and he immediately went to discuss the issue and how or why it occurred and what to look for next time. The study showed that these types of social interactions did have a positive influence on the behavioral intentions of employees within the business.

Research Question 2b Conceptual Framework

Venkatesh and Davis (2000) defined effort expectancy as the degree of ease related to a customer's use of technology. During the interviews some interviewees complained of technology in general but not the difficulty or ease of using it. The bigger problem managers saw was the stress involved when new systems were implemented. Participant 18 said, "I mean, of course, using any program could be a little bit stressful, but the whole goal of using a lot of these programs is to reduce the amount of work that you have, which makes your work easier." Implementing security technologies should make protecting the businesses' data easier. Participant 1 noted the following:

> … the stress level is, because if anytime someone comes in and messes with any of our computers, my secretary it causes her to go, it causes her a lot of stress for her. She is not in to having new stuff come in she is pretty much set in her ways and if I change something it stresses her out really bad.

Along with this sentiment participant 3 opinioned that all new technologies caused stress from the standpoint that not everybody likes to change. He went on to say, "So, until they figure out that this is not that horrible, you know, you know it is, it there is, there is a learning curve."

This sentiment was echoed by participant 16 where they pointed out, “Yeah, there's always you know a learning curve. Some people are going to learn it. Other people struggle.” Participant 18 explained, “I mean, of course, using any program could be a little bit stressful, but the whole goal of using a lot of these programs is to reduce the amount of work that you have, which makes your work easier.” Stress could be minimized, and the learning curve reduced with the proper emphasis of training by managers. Participant 12 noted, “Well, those of us who interact with the bank go through the banks, you know, security system, and it is, it is a, it is relatively straightforward, especially what you become comfortable with using it.” This study showed with a lack of training, manager’s thought stress remained at a higher rate which impacted the ease of use of certain technologies. Stress impacted effort expectancy as it made it more difficult for employees to use technology.

Research Question 2c Conceptual Framework

Facilitating conditions are the degree to which users can access organizational and technical resources needed to support information technology use (Venkatesh et al., 2012). The training and service support provided to employees in small construction businesses was found to be non-existent for over half the businesses in this study. The other businesses provided the minimal level of training support employees needed to perform their functions. Prior studies have shown that employees are more likely to use a new technology when they perceive their behavior will be supported with the availability of resources (Macedo, 2017; Shaw & Sergueeva, 2019). This study showed that individual employees did not always have complete control over the security systems they used. This was in agreement with what Shaw and Sergueeva (2019) found about facilitating conditions and that employees perception of information technology systems would be more favorably accepted when top management supported them. Managers not

providing training was one way employees did not believe they were being supported. Participant 6 when talking about security training wanted more training saying “I would love to have more training on this,” referring to security training.

When linking behavioral intention with facilitating conditions one extrapolate that making a conscious plan to perform a behavior is determined by an employees’ attitude toward the behavior (Baptista & Oliveira, 2015; Gupta et al., 2015). Typically, the stronger the behavior intention to engage in a behavior, the more likely it will occur (Ajzen, 1991; Kim et al., 2016). Several owners discussed incidents were their or other employee’s behaviors negatively impacted behavior intention. Participant 3 discussed his partner who retired a year ago. His partner was never a computer guy but he always talked about being a computer guy. He acted more like a technophobe where he feared or disliked computers so he was the last person in the business to sign up for direct deposit. Another owner admitted, “Basically I think that I do not do a whole lot of online banking, my main concern would be online banking.” Showing a negative behavioral intention is considered one of the most important determinants of one’s actual behavior and these were coming from the business leaders. Venkatesh et al. (2012) discussed behavioral intention combined with facilitating conditions assist in determining technology use and as this study’s data showed those were trending negatively.

Security Policies as Facilitating Condition. Security awareness can be fostered through several mechanisms such as leadership, employee social networks, and training, all of which can reduce security problems by conveying how important security policies are (Goo et al., 2014). Adopting business strategies to improve security compliance can be done through written communications and training (Cram et al., 2018). The majority of businesses in this study did not

have written security policies and used word of mouth to communicate their businesses' security intentions.

Alharbi et al., (2017) found employees who have adopted good information security awareness are more confident in using new technologies leading to a positive affect on behavioral use and use behavior. Educating the workforce on security policies and how they impact work was a significant predictor in compliance which was strongly linked in previous studies to habits and experiences (Shillair et al., 2015). One business was out of the norm in this study as they implemented written security policies for their employees. Participant 8 explained after they purchased the business, "…we needed more formal procedures in place, so we took on the initiative to put several policies, manuals and what not in place, so there was never any question in what, what should take place." Participant 14 noted, "We have personal privacy policies with all of our, you know, NDAs and things like that that we go through with everyone that we work with, depending on, you know, who it is." Other businesses used external policies to guide employees in how to secure credit card information and bank transactions. Participant 1 relayed when they perform phone sales and don't use their credit card machine but the internet, the bank charges the business additional fees. This same bank implemented security procedures on how his checks had to clear the bank without his say. He said he just accepts their policies, even though they cost his business more money. Participant 24 and participant 30 mentioned how they had to follow the policies of their credit card companies or loss the ability to do credit card transactions. These policies were reinforced with fines as participant 24 stated they could suffer a $20,000 fine up to $200,000. Internal written policies were not the norm but the exception. More businesses offered training through third-party contractors but not at a level necessary for employees to feel comfortable. Failing to provide written security policies along

with not providing adequate training did show to have an adverse effect on employee's behavior intention, which in turn impacted how some interviewees felt about security technologies.

Research Questions With Moderators

The three moderators of age, gender, and experience were looked at to see how they supported predicting use behavior to use a technology within a business context (Venkatesh et al., 2012). The majority of interviewees were over the age of 45 (Table 4). Six interviewess said they directly interacted with security systems and five interviewees answered they did not know with the remaining 19 saying they did not interact with security systems (Table 4). During the interviews it was determined that 28 of the interviewees used anti-virus software and email systems with security filters on them. Most interviewees felt comfortable with using these types of tools with the older interviewees feeling the least comfortable. Of the five women who participated in the study, they all felt comfortable with the technology they were required to use. The study's findings indicated that older participants were less comfortable in using the security tools provided. All the women felt comfortable in using their technology but their average age was slightly less than the average age of men in the study. The interviewees all had at least three years experience using their current or prior systems. Participant 28 when asked about the employee's expectation to use the current or new system stated, "It is another day at work, they got to do what they have to do. They come to work, they have to do what they have to do."

Table 4

Profile Questionnaire Data

1. What is your gender?	2. What is your age?	3. Are you familiar with your business's Security Awareness Training (SAT)?	4. Does the business employ security information policies?	5. Do you believe the security information policies are effective?	6. Do you interact with any information security systems?	7. How long have you been working for the business? (In Years)
Male	35 - 44	No	No	N/A	No	11 – 15
Male	35 - 44	No	No	N/A	No	6 – 10
Male	Over 64	No	No	N/A	No	21 – 25
Male	55 - 64	No	No	Don't Know	Don't Know	36 – 40
Male	Over 64	No	No	N/A	No	Over > 40
Female	45 - 54	No	No	N/A	Don't Know	6 – 10
Male	35 - 44	No	N/A	N/A	No	11 – 15
Male	35 - 44	Yes	Yes	Yes	Yes	16 – 20
Male	45 - 54	No	No	N/A	No	16 – 20
Male	Over 64	No	No	Yes	No	16 – 20
Male	45 - 54	No	No	N/A	No	16 – 20
Male	55 - 64	No	Yes	Yes	Yes	21 – 25
Male	Over 64	No	No	N/A	No	Over > 40
Male	25 - 34	No	Yes	Don't Know	No	6 – 10
Male	45 - 54	No	No	N/A	No	16 – 20
Male	Over 64	Yes	Yes	Yes	Yes	26 – 30
Male	18 - 24	Yes	Yes	Yes	Yes	6 – 10
Male	25 - 34	No	No	Don't Know	No	1 – 5
Male	35 - 44	No	No	Don't Know	No	21 – 25
Male	35 - 44	No	No	No	No	11 – 15
Male	55 - 64	No	No	Don't Know	Don't Know	36 – 40
Male	55 - 64	No	No	No	Don't Know	16 – 20
Male	35 - 44	No	No	Don't Know	No	11 – 15
Female	45 - 54	Yes	Yes	Yes	No	11 – 15
Male	45 - 54	No	N/A	N/A	No	26 – 30

Female	35 - 44	No	No	N/A	No	16 – 20
Male	35 - 44	No	Yes	Yes	No	1 – 5
Male	55 - 64	No	N/A	No	Don't Know	31 – 35
Female	55 - 64	No	No	Don't Know	Yes	1 – 5
Female	35 - 44	No	No	N/A	Yes	1 – 5

Shaw and Sergueeva (2019) showed that facilitating conditions are positively related to information technology acceptance when top management supports them. A manager's attitude, lack of resources in these small businesses, and the age moderator did seem to have an undesirable impact on facilitating conditions and use behavior. This aligned with previous quantitative studies that typically measured information technology use in terms of how often the targeted system is used and a user's intention to actually use the system (Alalwan et al., 2017; Bhattacherjee et al., 2018; Ravangard et al., 2017).

Summary of the Findings

Small construction businesses have very few administrative people that work in the administrative offices. This means personnel working in the office perform multiple functions which has led to businesses being dependent on third-party information technology venders to perform their specialized information technology functions. This reliance on third-party venders allows the businesses to focus on their core services of delivering value-added activities in the field. It also reinforces a mindset that planning for cyber security issues is not needed because the venders will take care of all issues. This has led to several of the businesses experiencing cyber security issues and being reactive in how they responded to them.

Without proper planning for implementing security technologies the businesses impacted how their employees thought and used the businesses' information systems. In addition, a lack of assertiveness in prioritizing security technologies within the business meant activities that could

help employees ease the transition of new information security technologies was lacking. The findings also showed an employee's behavior intention and use behavior was highly impacted by the age moderator. The older an employee the more likely they would be having a lower behavior intention and use behavior for using systems. Other factors such as facilitating conditions, written security policies, and effort expectancy lead to a negative response behavior intention of employees with training and the moderator of age having an impact. Social influence, investments, performance expectancy, threats, and habit seemed to show a more positive response on influencing an employees' behavior intention and use behavior.

Applications to Professional Practice

The practical implication of this study's findings can be applied to any small business in the United States. As the annual Hiscox 'Cyber Readiness Report' showed both the cost and frequency of attacks have increased markedly against small businesses, costing businesses on average $369,000 per incident (Hiscox, 2019). Half of these cyber-attacks are committed against small businesses who probably thought they would never be attacked by criminal enterprises (Stanciu & Tinca, 2017). Similar to small construction businesses who believed their operations are not important enough to draw the attention of cybercriminals. The small business owners and managers in this study lived with their businesses suffering internal and external cyber-attacks but still did not think cyber security was as important an issue as the Hiscox 'Cyber Readiness Report' and the U.S. Senate testimony provided by Dr. Charles H. Romine showed it to be. Dr. Romaine testified small businesses comprise 99.9% of all firms in the U.S. and cybercriminals cost these businesses billions of dollars in lost revenue and productivity every year (Cyber Crime: An Existential Threat to Small Business, 2019). The study's results should guide businesses into taking action so they can prevent their business from becoming another

cybercriminal statistic. To assist in improving their cyber security business posture, small businesses should think about the following.

Business Losses

When a business manager thinks about the factors that impact a businesses' decision to implement information security technologies, they should focus on stopping businesses losses. Both internal and external losses can add up quickly in a small business as one business in this study suffered $243,000 in losses involving two insider threat incidents. Another business pointed out they had suffered a large insurance claim based on the failure of their third-party information technology partner to carry out their fiduciary duties. External attacks can cost businesses tens of thousands of dollars or involve a data breach that can lead to significant lawsuits and government fines. Limited resources and budgets are some of the main reasons small businesses accept the risk of a security attack. Most of the interviewees in this study would tell you that their information technology budgets are constrained and there are more important things to worry about than security. This mindset is the same for many of the small businesses in the United States where managers have to make difficult decisions every day so the business can remain viable. These judgements have consequences and discounting cybercrime as a threat may lead the business to becoming insolvent sooner than later. A culture change on how small businesses managers think about protecting their information systems is critical to successfully defend the business against future threats. This change can only take place with a change in how managers make decisions and implement security technologies.

Management Style

The study's results showed that small business managers are more prone to use a top down management style. This means decisions about security technologies are predominately

being made by construction leaders who are most likely not experts in security information systems. To counter this problem, leaders must move from a top down management approach to one of inclusion. Inclusive leaders are good listeners, people-oriented, and able to bring out the talents and motivations of those around them. Being visibly committed to implementing security technologies shows employees that security is important and management is fully behind any systems being deployed. To successfully implement this, leaders need to be aware of their bias towards security technologies, by admitting their personal blind spots as well as their short comings in understanding security technologies and how to implement them.

The study's findings showed that when decisions about security were required, leaders leaned heavily on their third-party contractors and to some extent other managers within the business (may lack same security expertise) and/or external resources (e.g., magazines, sales brochures, internet searches, etc…). The third-party security contractors provided leadership with an external generic view of how to protect their businesses. This homogenous view is the norm as third-party venders to save money and reduce their cost offer small businesses similar type security services they apply across all their third-party clientele without any detailed deep dive into the actual businesses' threats. These generic offerings allow third-party security businesses to offer small businesses at lower cost services they can afford to protect their systems and it lets the security provider reach a sort of economies of scale.

Leaders also got internal information from their managers who most likely are not any more adept at cyber security systems than their leaders. They do however have a fundamental understanding of the businesses operations that could be invaluable in identifying different threats to the businesses' operations. By being an inclusive leader, the internal and external people can coordinate to figure out what the best solution is for the business to identify specific

risk to those types of businesses. Participant 13 relayed, “I would rely on, you know, people that were more into the computers and books, but as, as I would get information from them, I just would decide based on what they were recommending.” As participant 15 stated, “Well, I would think, anybody who is smart would use the resources you have around you to make the best decision for the business.” Leaders should use all available resources at their disposal to identify risk and make the best plan to mitigate them. One way to start this process is to make sure people are trained in security.

Security Training and Support

Small construction businesses did a lackluster job in providing security training to their employees. Ninety-nine percent of business managers responsible for cyber security training conveyed that security awareness learning is essential to minimize security threats (Wilding, 2016). The failure to provide training may be occurring because of managers’ aversion to security in general, high cost of training, employee availability, de-emphasis on security training, or several other reasons. Prior research recognized leaders play a key role in the implementation of information technologies by delivering training to successfully implement new technologies (Hansen & Nørup, 2017). Businesses of all sizes know the importance of training their personnel to do functions within the business. The current study showed that within the construction industry, most small businesses hire third-party contractors to provide security services to the business. These contractors provide some security training but not enough to make employees feel they have the experience to handle any major security incidents. Leaders need to comprehend that information security is part of today’s business environment. They need to make it part of the culture, so employees will develop good habits. As they gain more experience, employees will feel more comfortable in dealing with security systems, incidents,

and the aftermath of a security attack. Preparing employees for the inevitable security attack is a proactive business practice that will go a long way in fortifying the business against threats. Training is only one aspect of changing the businesses security readiness as written security policies will also be needed.

Written Security Policies

What practices do business managers incorporate in the work environment to ease the transition of new information security technologies? As mentioned previously, training to instill in the workforce the importance of security is a major motivator of employees. Additionally, managers must communicate their policies and beliefs so employees know what is expected. Employees cannot be expected to know what to do in a security situation when they occur, so infrequently and the employee has never been properly trained. To ensure employees are prepared for security incidents, employers should have written security policies in place to further educate employees on what is expected to prevent an incident or react to one. This is especially important when security incidents occur rapidly and they need to respond quickly to disrupt or halt the incident as soon as possible.

By preparing their workforce and giving them the tools, they need to do their jobs, small business managers are more likely to profit from their efforts. Understanding that employees who are better prepared are more able to respond to threats, only benefits the small business in the end. Written policies also provide a training mechanism for employees to look up information improving their habits. The more they improve their habits the more they will gain experience which will lead employees to increasing their behavior intention. Leaders need to link their businesses' strategy, communication, management style, security training, and written

policies together to create a fundamental shift in the business' security posture, leading to a new security culture.

Biblical Framework

"All scripture is given by inspiration of God, and is profitable for doctrine, for reproof, for correction, for instruction in righteousness: That the man of God may be perfect, thoroughly furnished unto all good works" (King James Bible, 2017, 2 Timothy 3:16-17). God's word tells us he wanted to teach us to be good and competent to do his work. His biblical framework is how we should live our lives just as small businesses should emulate his desires by taking care of their employees. Schouten et al. (2014) recounted executive's personal values and beliefs influence their own decisions and the values, beliefs, and behavior of their subordinates. Leaders should communicate, guide, and train their employees to inspire them to adopt a culture of security and challenge them to be the best they can be. The study showed from a biblical framework perspective, a few small construction businesses followed God's example, but most fell short and this is probably the same problem throughout small businesses in the United States. Small business leaders would benefit from following God's biblical framework by having their employees better trained making them more competent in protecting the business from cyber-attacks.

Recommendations for Action

Based on the study's conclusions a series of recommendations has been developed. The three recommendations that the researcher offers here affect multiple areas that a business should want to improve in. These recommendations are by no means the only areas that a reader may see that needs improvement, however the researcher felt that these could have some of the most consequential impacts to a small businesses' security preparedness.

The three recommendations could impact any small business struggling with how to deal with implementing security systems or wanting to change and adopt a security information culture. The study's results can be disseminated through online articles or journals targeted towards small businesses. These communication channels provide an excellent venue to reach a large number of dispersed small businesses swiftly with the study's findings. The articles should also be focused to clearly depict the benefits of the study's findings.

Recommendation 1: Planning and Investments

Businesses must account for all cost within their budgets and recoup that cost by passing on those charges to their customers. Accounting for the implementation of security technologies and training employees are part of the cost managers should be trying to recover. Managers must strategically plan on how to pay for security improvements while determining how they can spread the cost of those initiatives over their jobs. Implementing a security fee spread out equally over all projects the business is involved with would allow the businesses to plan for security and at the same time account for the cost involved in implementing it. It is important to recognize as one owner said, "…it is a cutthroat type of business," so the amount of the businesses' fees may not always be optimal to win bids, which means businesses will also need a way to prioritize their security spending. This security fee surcharge will allow the businesses to implement security technologies that will mitigate security threats to their businesses. Business leaders will also need to learn how to prioritize the threats they will want to protect the business from since the fees collected will still need to remain limited to keep the businesses competitive in their marketplace. Planning on what risk to address can be accomplished through a simple security risk framework.

Recommendation 2: Security Risk Framework

Formalization of a security risk framework will assist businesses in determining what risk should be mitigated. Employing a formal security risk framework would allow any new threats to be addressed quickly allowing leaders to have a simple way to evaluate and track risk. One simple way to do this would be to use a five-step risk plan to identify, analyze, mitigate, monitor, and reassess mitigation strategies. To identify risk, business owners must first identify the risk exist by asking themselves what are the risk the business may be facing. This can be asked to both internal employees and external sources. Once small businesses know the risk, they can evaluate what is the likelihood that the risk will occur in their business. Using a scale of 1 - high, 2 - medium, and 3 - low managers can determine a cutoff point for dealing with any risk. They may determine high risk need to be mitigated immediately as these will have the biggest impact on the business. Low risk is less of an impact to the business, so managers may perceive these risks may not need to be mitigated in the short-run or at all. Medium risk may seem not as important as high risk but sometimes they can be just as critical to mitigate to prevent cyber thieves from accessing information. Once the list of threats is ranked, the business managers can work with their third-party security contractors or internal information technology staff to estimate the cost it will take to mitigate the threats. Business mitigation efforts will be based on what resources are available and the cost to implement any security measures. At this point, leadership will need to perform a cost analysis on how much money they can afford to spend on security measures based upon competing requirements and any fee they could charge their customers to recoup expenses for their security technologies.

The business can monitor its mitigation strategies or a have their third-party business do the monitoring for them, depending on their resource constraints. Finally, at some point the

mitigation strategies will need to be assessed to make sure they are working. This should be done in conjunction with the information technology specialist to determine what changes might need to be, if any. This iterative process should be run at different times of the year to identify any new threats and verify the prioritized threats are still a concern. This is a very simple and quick process that would help focus non-technical people on a very important topic that should concern any business. Businesses in this study demonstrated through the ZAP© business alerts and participant interviews, identifying and mitigating risk was not a high priority to most of these small businesses but the consequences of not evaluating these security risk could be very detrimental to the businesses' overall viability. Risk planning to mitigate threats is needed by all small businesses before they become victim to a cybercrime that forces them to dissolve.

Recommendation 3: Support Functions

Reinforcement of security training engrains within a workforce a habit of following the rules to keep systems secure which can only take place with management's support. Managers know that for employees to be successful in protecting the business from security threats, they need to be trained, so their experience levels can increase making them more capable in the security arena (Akman & Mishra, 2015; Bolek et al., 2016). Businesses must use a combination of training and managerial encouragement to inspire employees to raise their awareness of security by making it part of the culture. This is a problem for small businesses, especially when the managers are older and less prone to perceive information technology security as a priority.

Subsequently, since managers are not always present written security policies are a valuable tool for employees to reference, when needed. It is known that the learning curve is not the same for everyone and sometimes age can play a role in employees picking up security technologies quickly. Written security policies can help in this area by providing employees a

means to work at their own pace to learn a new system. Hwang et al. (2017) found that security policies may reduce worker efficiency when employees believe they slow down their work activities. Managers need to be aware of these perceptions as ambiguous security policies can lead to personnel performing poorly and in turn reinforce negative stereotypes that the culture takes on as the norm (Hwang et al., 2017). To counter these non-productive views, managers should try to mitigate them through a change in the businesses' culture. Written security policies that are well written, factual and provide clear guidance to employees are critical to this endeavor. As small businesses adopt information technology security systems it is crucial to all businesses that they have repeatable processes that can be easily followed, allowing employees to seek guidance when managers are not on-site. Clear written security policies are a positive influence on the workforce and cost very little to develop. Their use will assist in changing the businesses' culture by providing stability among employees of all ages, origins, and genders so they know how to respond when a security incident happens. Leaders supporting training and written policies will improve facilitating conditions along with effort expectancy leading to a more positive behavior intention response towards security systems.

Recommendations for Further Study

This qualitative study sought to explore examine the failure of small construction businesses to properly implement information security technologies resulting in the loss of sensitive and proprietary business information for small construction businesses within the state of Virginia. There was an acceptable amount of literature describing theories such as the TAM, TPB, UTAUT, and UTAUT2 which provided explanatory information on the intentions of individuals to use information systems. When applied to small construction businesses, there was sparse research available for the researcher to draw on. With miniscule research and information

available on small construction businesses dealing with information security technology, further research in the area of security risk management and decision-making on the implementation of security technologies would be beneficial.

The research showed that small construction businesses fail to use a repeatable process to determine security risk against their businesses. This lack of a formalized risk management process assists small businesses in reinforcing their top down management style which was proven in this study to not be insufficient in getting security systems deployed and protecting the company from threats. Additional research is needed in this area.

Another area that needs to be delved into more is small businesses reliance on third-party contractors. Managers in small construction businesses basically abdicated their responsibilities in the security arena and let the third-party companies determine what needed to be done. In one instance this led to a large lawsuit and in other instances the data showed that the websites were not being protected to a level they should have been. Was this abdication of responsibilities adopted because of a lack of security knowledge by management or based more on the age of the decision makers? Delving into this area more would provide better understanding of why business might do this while every other part of the construction business is tightly controlled. Further research in these areas would help small businesses improve deployment of security technologies and maybe increase adoption by their workforce of security systems.

Reflections

When this research started, I did not have any concerns about managers in small construction businesses supporting the study's goals. Reflecting on the difficulties of getting participants involved, there were early signs in the conversations with some managers who indicated construction people are very secretive. The reasons varied as some managers hinted

that many construction businesses employ foreigners under the H-1B visa program but not all play fairly as some hire citizens and non-citizen employees under the table to reduce cost. Others opined that a lot of these family run businesses did not want anyone to know what or how they were doing. This made the recruitment of participants very challenging and required a belief by the researcher that trusting in God's will, would get him through this process. I also had the challenge of limiting the influence of personal bias and preconceived ideas about small construction businesses.

Personal Biases

I understood that bias could occur at any phase of this research, including my study's design, data collection or data analysis phases. The need to not introduce errors to sway the outcome of this research in one way or another was always at the forefront of my actions. When I started this study, I had no preconceived ideas about why small businesses do not fully protect their information technology operations from cybercriminals. Throughout the study, I continued to recruit businesses randomly that did not prove or disprove data that had been collected from earlier participants. This ensured the study's results were not being biased towards the collection of information from sources that I might have pre-determined would lean in a direction I wanted them to. This was also applied to interviews, where I continued to asked open ended questions as to not influence their responses to a pre-determined inference. Overall, I believed my actions mitigated bias during this study where it did not have an influence on the study's outcome.

Changed Thinking

My experiences have led me to a profound understanding of how the construction industry sees their core business. As this study progressed, I saw how small construction businesses varied in sizes and were still mainly influenced by the patriarch of the family who

started the original business. Some of these businesses had already gone through a transition phase were a younger family member had taken over and I could perceive that they brought a different mindset about security awareness than their predecessors. As this change continues to occur within the industry with owners growing younger and the leadership roles being filled by more women, I believe the results of this study, if done again in ten years will be markedly different. As cyber-attacks continue to increase year after year, a younger more diverse generation will be more likely to adopt their work environments to counter insider and outsider threats. I believe this will be possible only through changes like the ones proposed in this study, otherwise the new generation will make the same mistakes as those that came before them.

Biblical Principles

Throughout this study, I thought about how students are taught in business classes that for-profit businesses exist to make money. The owners and managers in these small businesses saw the core of their business as a means to make money to support their hearts desires. This singular focus to make money may nourish a monetary craving but as God's words tell us, "No man can serve two masters: for either he will hate the one, and love the other; or else he will hold to the one, and despise the other. Ye cannot serve God and mammon" (King James Bible, 2017, Mathew 6:24). Knowing personally that a desire to walk with God and fellowship with Jesus Christ will help fortify us against temptations and in turbulent times. Some business owners did not heed the warming, "Trust in the Lord, and do good; so shalt thou dwell in the land, and verily thou shalt be fed. Delight thyself also in the Lord; and he shall give thee the desires of thine heart" (King James Bible, 2017, Psalm 37:3–4). Instead by not relying on God's words, managers may believe putting their trust in themselves or their business strategy will save them. Ultimately, this self-reliance will fail because only through our daily walk with God, can we

learn new knowledge and wisdom to make faithful decisions that will make us better stewards of the resources God has bestowed upon us. Managers desiring to be better stewards will seek to take care of their employees by preparing them against future cyber-attacks.

Summary and Study Conclusions

This study involved 30 businesses in the construction industry operating within the state of Virginia. Information was primarily gathered through interviews, questionnaires, observations, and documents. With 30 different businesses at 30 different locations the researcher was able to perform triangulation by converging the different data sources of information collected in order to provide corroborating evidence to form the themes for this study (Creswell & Poth, 2018; Stake, 2010; Yin, 2014). The practical implication of this study's findings can be applied to any small business in the United States. Small businesses can improve their cyber security business posture by diligently looking at their business losses, changing the organization's management style, arranging security training and support, implementing written security policies, and following a biblical framework to prepare their employees to be competent. Finally, improvements will only last when leaders communicate, guide, and inspire their employees to adopt a culture of security and challenge them to be the best they can be.

The researcher also made recommendations for action which were based on the study's findings. Based on the study's conclusions businesses should pay more attention to planning and investments within the business. Businesses should develop a security risk framework to guide their application of mitigation strategies while controlling security spending. Managers must also learn to improve their support to their employees to increase their behavior to use the deployed security systems. In addition to these recommendations, the researcher feels that further study is

still needed in the areas of security risk management and decision-making on the implementation of security technologies would be beneficial to small businesses.

References

Abbas, T. (2016). Social factors affecting students' acceptance of e-learning environments in developing and developed countries: A structural equation modeling approach. *Journal of Hospitality and Tourism Technology*, *7*(2), 200–212. https://doi.org/10.1108/JHTT-11-2015-0042

Ain, N., Kaur, K., & Waheed, M. (2016). The influence of learning value on learning management system use: An extension of UTAUT2. *Information Development*, *32*(5), 1306–1321. https://doi.org/10.1177/0266666915597546

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50,* 179–211. https://www.dphu.org/uploads/attachements/books/books_4931_0.pdf

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, *26*(9), 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Ajzen, I. (2012). Martin Fishbein's legacy: The reasoned action approach. *The Annals of the American Academy of Political and Social Science*, *640*, 11–27. https://www.jstor.org/stable/23218420

Akman, I., & Mishra, A. (2015). Sector diversity in green information technology practices: Technology acceptance model perspective. *Computers in Human Behavior*, *49*, 477–486. https://doi.org/10.1016/j.chb.2015.03.009

Alalwan, A. A., Dwivedi, Y. K., & Rana, N. P. (2017). Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *International Journal of Information Management*, *37*(3), 99–110. https://doi.org/10.1016/j.ijinfomgt.2017.01.002

Alam, M. G., Masum, A. K., Beh, L. S., & Hong, C. S. (2016). Critical factors influencing decision to adopt human resource information system (HRIS) in hospitals. *PLoS One*, *11*(8), 1–22. https://doi.org/10.1371/journal.pone.0160366

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73–88. https://doi.org/10.3390/fi11030073

Alharbi, N., Papadaki, M., & Dowland, P. (2017). The impact of security and its antecedents in behaviour intention of using e-government services. *Behaviour & Information Technology*, *36*(6), 620–636. https://doi.org/10.1080/0144929X.2016.1269198

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Almeida, F., Carvalho, I., & Cruz, F. (2018). Structure and challenges of a security policy on small and medium enterprises. *KSII Transactions on Internet and Information Systems*, *12*(2), 747–763. https://doi.org/10.3837/tiis.2018.02.012

Ament, C., & Haag, S. (2016). How information security requirements stress employees. *Thirty Seventh International Conference on Information Systems* (pp. 1–17). Dublin: Association for Information Systems (AIS) eLibrary. https://core.ac.uk/download/pdf/301370436.pdf

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, *41*(3), 893–916. https://doi.org/10.25300/MISQ/2017/41.3.10

Aswani, R., Ilavarasan, P. V., Kar, A. K., & Vijayan, S. (2018). Adoption of public WiFi using UTAUT2: An exploration in an emerging economy. *Procedia Computer Science, 132*, 297–306. https://doi.org/10.1016/j.procs.2018.05.180

Badenhorst, R. (2017). Cybersecurity: saves financial organisations. *Accountancy SA*, 32–33. http://ezproxy.liberty.edu/login?url=https://search-proquest-com.ezproxy.liberty.edu/docview/1903041609?accountid=12085

Baptista, G., & Oliveira, T. (2015). Understanding mobile banking: The unified theory of acceptance and use of technology combined with cultural moderators. *Computers in Human Behavior, 50*, 418–430. https://doi.org/10.1016/j.chb.2015.04.024

Behar-Horenstein, L. S., & Feng, X. (2018). What open-ended comments reveal: An analysis of a clinical translational science institute's annual surveys. *The Qualitative Report, 23*(8), 2003–2018. https://nsuworks.nova.edu/tqr/vol23/iss8/15

Behr, D. (2015). Translating answers to open-ended survey questions in cross-cultural research: A case study on the interplay between translation, coding, and analysis. *Field Methods, 27*(3), 284–299. https://doi.org/10.1177/1525822X14553175

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management, 54*(7), 887–901. https://doi.org/10.1016/j.im.2017.01.003

Benbasat, I., & Barki, H. (2007). Quo vadis, TAM? *Journal of the Association for Information Systems, 8*(4), 211–218. https://doi.org/10.17705/1jais.00126

Berg-Beckhoff, G., Nielsen, G., & Larsen, E. L. (2017). Use of information communication technology and stress, burnout, and mental health in older, middle-aged, and younger

workers – results from a systematic review. *International Journal of Occupational and Environmental Health, 23*(2), 160–171. https://doi.org/10.1080/10773525.2018.1436015

Bhattacherjee, A., Davis, C. J., Connolly, A. J., & Hikmet, N. (2018). User response to mandatory IT use: A coping theory perspective. *European Journal of Information SystemsI, 27*(4), 395–414. https://doi.org/10.1057/s41303-017-0047-0

Birkinshaw, C., Rouka, E., & Vassilakis, V. G. (2019). Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. *Journal of Network and Computer Applications, 136*, 71–85. https://doi.org/10.1016/j.jnca.2019.03.005

Boblin, S. L., Ireland, S., Kirkpatrick, H., & Robertson, K. (2013). Using Stake's qualitative case study approach to explore implementation of evidence-based practice. *Qualitative Health Research, 23*(9), 1–9. https://doi.org/10.1177/1049732313502128

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journa, 19*(4), 426–432. https://doi.org/10.1108/QMR-06-2016-0053

Bolek, V., Látečková, A., Romanová, A., & Korček, F. (2016). Factors affecting information security focused on SME and agricultural enterprises. *AGRIS on-line Papers in Economics and Informatics, 8*(4), 37–50. https://doi.org/10.7160/aol.2016.080404

Bonsu, S., & Twum-Danso, E. (2018). Leadership style in the global economy: A focus on cross-cultural and transformational leadership. *Journal of Marketing and Management, 9*(2), 37–52. https://gsmi-ijgb.com/wp-content/uploads/JMM-V9-N2-P04-Samuel-Bonsu-Global-Economy.pdf

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

Breitinger, D., & Bonardi, J. P. (2019). Firms, breach of norms, and reputation damage. *Business & Society*, *58*(6), 1143–1176. https://doi.org/10.1177/0007650317695531

Brown, D., Hagger, M., Morrissey, S., & Hamilton, K. (2018). Predicting fruit and vegetable consumption in long-haul heavy goods vehicle drivers: Application of a multi-theory, dual-phase model and the contribution of past behaviour. *Appetite*, *121,* 326–336. https://doi.org/10.1016/j.appet.2017.11.106

Cabrera, L. Y., & Reiner, P. B. (2018). A novel sequential mixed-method technique for contrastive analysis of unscripted qualitative data: Contrastive quantitized content analysis. *Sociological Methods & Research, 47*(3), 432–548. https://doi.org/10.1177/0049124116661575

Caridi-Zahavi, O., Carmeli, A., & Arazy, O. (2016). The influence of CEOs' visionary innovation leadership on the performance of high-technology ventures: The mediating roles of connectivity and knowledge integration. *Journal of Product Innovation Management*, *33*(3), 356–376. https://doi.org/10.1111/jpim.12275

Carless, D., & Douglas, K. (2017). Narrative research. *The Journal of Positive Psychology, 12*(3), 307–308. https://doi.org/10.1080/17439760.2016.1262611

Carter, M., & Grover, V. (2015). Me, my self, and I(T): Conceptualizing information technology identity and its implications. *MIS Quarterly*, *39*(4), 931–957. https://doi.org/10.25300/MISQ/2015/39.4.9

Celik, H. (2016). Customer online shopping anxiety within the Unified Theory of Acceptance and Use Technology (UTAUT) framework. *Asia Pacific Journal of Marketing and Logistics*, *28*(2), 278–307. https://doi.org/10.1108/APJML-05-2015-0077

Chaâri, R., Ellouze, F., Koubâa, A., Qureshi, B., Pereira, N., Youssef, H., & Tovar, E. (2016). Cyber-physical systems clouds: A survey. *Computer Networks*, *108*, 260–278. https://doi.org/10.1016/j.comnet.2016.08.017

Chan, Z. C., Fung, Y. L., & Chien, W. T. (2013). Bracketing in phenomenology: Only undertaken in the data collection and analysis process? *The Qualitative Report*, *18*(30), 1–9. https://nsuworks.nova.edu/tqr/vol18/iss30/1/

Chang, C. M., Liu, L. W., Huang, H. C., & Hsieh, H. H. (2019). Factors influencing online hotel booking: Extending UTAUT2 with age, gender, and experience as moderators. *Information*, *10*(9), 1–18. https://doi.org/10.3390/info10090281

Charmaz, K. (2015). Teaching theory construction with initial grounded theory tools: A reflection on lessons and learning. *Qualitative Health Research*, *25*(12), 1610–1622. https://doi.org/10.1177/1049732315613982

Chau, P. Y., & Hu, P. J. H. (2002). Investigating healthcare professionals' decisions to accept telemedicine technology: an empirical test of competing theories. *Information & Management*, *39*, 297–311. https://doi.org/10.1016/S0378-7206(01)00098-2

Cheng, E. W. (2019). Choosing between the theory of planned behavior (TPB) and the technology acceptance model (TAM). *Education Tech Research Dev*, *67*, 21–37. https://doi.org/10.1007/s11423-018-9598-6

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

Chou, S., Techatassanasoontorn, A., & Hung, I. (2015). Understanding commitment in business process outsourcing relationships. *Information & Management*, *52*(1), 30–43. https://doi.org/10.1016/j.im.2014.10.003

Chronopoulos, M., & Lumbreras, S. (2017). Optimal regime switching under risk aversion and uncertainty. *European Journal of Operational Research*, *256*(2), 543–555. https://doi.org/10.1016/j.ejor.2016.06.027

Chulkov, D. V. (2017). On the role of switching costs and decision reversibility in information technology adoption and investment. *Journal of Information Systems and Technology Management*, *14*(3), 309–321. https://doi.org/10.4301/S1807-17752017000300001

Cisco. (2018). *Cybersecurity Special Report.* Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf

Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal*, *24*(2), 215–240. https://doi.org/10.1108/SCM-09-2017-0289

Committee on National Security Systems. (2015). *Committee on National Security Systems (CNSS) Glossary.* Ft Meade: National Security Agency. https://www.cnss.gov/CNSS/openDoc.cfm?1IADI91ZNhIm3Z8w++PdnA==

Cram, A. W., Proudfoot, J. G., & D'Arcy, J. (2018). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, *26*(6), 605–641. https://doi.org/10.1057/s41303-017-0059-9

Creswell, J. (2014). *Research design : Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design : Choosing among five approaches* (4th ed.). Sage.

Cyber Crime: An Existential Threat to Small Business: Hearings before the Committee on Small Business and Entrepreneurship, Senate, 116th Cong. (2019). (Testimony of Charles H. Romine, Ph.D.). (n.d.). 1–10.

Cypress, B. (2018). Qualitative research methods: A phenomenological focus. *Dimensions of Critical Care Nursing*, *37*(6), 302–309. https://doi.org/10.1097/DCC.0000000000000322

Dannals, J. E., & Miller, D. T. (2017). Social norm perception in groups with outliers. *Journal of Experimental Psychology: General*, *146*(9), 1342–1359. https://doi.org/10.1037/xge0000336

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Publication No. 1557992034) [Doctoral dissertation, MIT Sloan School of Management]. https://scinapse.io/papers/1557992034

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information. *MIS Quarterly*, *13*(3), 319–340. https://www.jstor.org/stable/249008

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. *Computers in Human Behavior*, *61*, 656–666. https://doi.org/10.1016/j.chb.2016.03.068

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security*, *63*, 1–13. https://doi.org/10.1016/j.cose.2016.09.006

Duncan, A., Creese, S., & Goldsmith, M. (2015). An overview of insider attacks in cloud computing. *Concurrency and Computation: Practice and Experience*, *27*(12), 2964–2981. https://doi.org/10.1002/cpe.3243

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2019). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers*, *21*(3), 719–734. https://doi.org/10.1007/s10796-017-9774-y

Dwivedi, Y. K., Shareef, M. A., Simintiras, A. C., Lal, B., & Weerakkody, V. (2016). A generalised adoption model for services: A cross-country comparison of mobile health (m-health). *Government Information Quarterly*, *33*(1), 174–187. https://doi.org/10.1016/j.giq.2015.06.003

Fairlie, R. (2020). The impact of COVID-19 on small business owners: Evidence from the first three months after widespread social-distancing restrictions. *Journal of Economics & Management Strategy*, *29*(4), 727–-740. https://doi.org/10.1111/jems.12400

Farquhar, J. D. (2012). *Case study research for business.* Sage.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23. https://doi.org/10.1016/j.dss.2016.02.012

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to Theory and research.* Addison-Wesley.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative*, *12*(2), 219–245. https://doi.org/10.1177/1077800405284363

Forster, M. (2019). “Ethnographic” thematic phenomenography: A methodological adaptation for the study of information literacy in an ontologically complex workplace. *Journal of Documentation*, *75*(2), 349–365. https://doi.org/10.1108/JD-05-2018-0079

Friedberg, I., Skopik, F., Settanni, G., & Fiedler, R. (2015). Combating advanced persistent threats: From network event correlation to incident detection. *Computers & Security*, *48*, 35–57. https://doi.org/10.1016/j.cose.2014.09.006

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*(9), 1408–1416. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2281&context=tqr

Gelfand, M. J., Harrington, J. R., & Jackson, J. C. (2017). The strength of social norms across human groups. *Perspectives on Psychological Science*, *12*(5), 800–809. https://doi.org/10.1177/1745691617708631

Gershman, S. J., Pouncy, H. T., & Gweon, H. (2017). Learning the structure of social influence. *Cognitive Science*, *41*, 545–575. https://doi.org/10.1111/cogs.12480

Ghaffari, K., & Lagzian, M. (2018). Exploring users’ experiences of using personal cloud storage services: A phenomenological study. *Behaviour & Information Technology*, *37*(3), 295–309. https://doi.org/10.1080/0144929X.2018.1435722

Gharaibeh, M. K., Arshad, M. R., & Gharaibh, N. K. (2018). Using the UTAUT2 model to determine factors affecting adoption of mobile banking services: A qualitative approach. *International Journal of Interactive Mobile Technologies*, *12*(4), 123–134. https://doi.org/10.3991/ijim.v12i4.8525

Gill, A., Mand, H. S., Amiraslany, A., & Obradovich, J. D. (2019). The Impact of Internal Financing Sources and Bank Financing on Information Technology Investment.

International Journal of Business and Economics, *18*(1), 1–16. The Impact of Internal Financing Sources and Bank Financing on Information Technology Investment. https://ideas.repec.org/a/ijb/journl/v18y2019i1p1-16.html

Goddard, J. T. (2012). Collective case study. In J. T. Goddard, *Encyclopedia of Case Study Research* (pp. 1–5). Thousand Oaks: Sage. https://doi.org/10.4135/9781412957397

Gomez, M. A., & Villar, E. B. (2018). Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats. *Politics and Governance, 6*(2), 61–72. https://doi.org/10.17645/pag.v6i2.1279

Goo, J., Yim, M. S., & Kim, D. J. (2014). A path to successful management of employee security Compliance: An empirical study of information security climate. *IEEE Transactions on Professional Communication*, *57*(4), 286–308. https://doi.org/10.1109/TPC.2014.2374011

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2014). Cybersecurity Investments in the private sector: The role of governments. *Georgetown Journal of International Affairs*, *15*(SI), 79–88. http://www.jstor.org/stable/43773651

Grimes, M., & Marquardson, J. (2019). Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions. *Decision Support Systems*, *119*, 23–34. https://doi.org/10.1016/j.dss.2019.02.010

Guest, G., Namey, E. E., & Mitchell, M. L. (2013). *Qualitative research: Defining and designing.* Sage. https://doi.org/10.4135/9781506374680.n1

Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal*, *29*(2), 340–362. https://doi.org/10.1111/isj.12202

Gupta, G., Zaidi, S. K., Udo, G., & Bagchi, K. (2015). The influence of theory of planned behavior, technology acceptance model, and information system success model on the acceptance of electronic tax filing system in an emerging economy. *The International Journal of Digital Accounting Research*, *15*, 155–185. https://doi.org/10.4192/1577-8517-v15_6

Gustafsson, J. T. (2017). Single case studies vs. multiple case studies: A comparative study. 1–15. https://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf

Hagger, M. S., Polet, J., & Lintunen, T. (2018). The reasoned action approach applied to health behavior: Role of past behavior and tests of some key moderators using meta-analytic structural equation modeling. *Social Science & Medicine*, *213*, 85–94. https://doi.org/10.1016/j.socscimed.2018.07.038

Hall, M. (2016). Why people are key to cyber-security. *Network Security*, *2016*(6), 9–10. https://doi.org/10.1016/S1353-4858(16)30057-5

Hamilton, K., Kirkpatrick, A., Rebar, A., & Hagger, M. S. (2017). Child sun safety: Application of an Integrated Behavior Change model. *American Psychological Association, Inc.*, *36*(9), 916–926. https://doi.org/10.1037/hea0000533

Hansen, M. B., & Nørup, I. (2017). Leading the implementation of ICT innovations. *Public Administration Review*, *77*(6), 851–860. https://doi.org/10.1111/puar.12807

Hardcopf, R., Gonçalves, P., Linderman, K., & Bendoly, E. (2017). Short-term bias and strategic misalignment in operational solutions: Perceptions, tendencies, and traps. *European Journal of Operational Research*, *258*(3), 1004–1021. https://doi.org/10.1016/j.ejor.2016.09.036

Heyder, M., Theuvsena, L., & Hollmann-Hespos, T. (2012). Investments in tracking and tracing systems in the food industry: A PLS analysis. *Food Policy, 37*, 102–113. https://doi.org/10.1016/j.foodpol.2011.11.006

Hiscox. (2019). *Hiscox Cyber Readiness Report 2019.* Hamilton HM 12: hiscoxgroup.com.

Ho, S. M., Kaarst-Brown, M., & Benbasat, I. (2018). Trustworthiness attribution: Inquiry into insider threat detection. *Journal of the Association for Information Science and Technology*, *69*(2), 271–280. https://doi.org/10.1002/asi.23938

Ho, S. M., Ocasio-Velázquez, M., & Booth, C. (2017). Trust or consequences? Causal effects of perceived risk and subjective norms on cloud technology adoption. *Computers & Security*, *70*, 581–595. https://doi.org/10.1016/j.cose.2017.08.004

Ho, S. M., & Warkentin, M. (2017). Leader's dilemma game: An experimental design for cyber insider threat research. *Information Systems Frontiers*, *19*(2), 377–396. https://doi.org/10.1007/s10796-015-9599-5

Horng, S. M., & Wu, C. L. (2019). How behaviors on social network sites and online social capital influence social commerce intentions. *Information & Management*, 1–13. https://doi.org/10.1016/j.im.2019.103176

Howard, R., Restrepo, L., & Chang, C. Y. (2017). Addressing individual perceptions: An application of the unified theory of acceptance and use of technology to building information modelling. *International Journal of Project Management*, *35*, 107–120. https://doi.org/10.1016/j.ijproman.2016.10.012

Howard, T. L., Ulferts, G. W., & Hannon, J. (2019). Leadership styles of small business Owners: linking theory to application. *Journal of Leadership, Accountability and Ethics*, *16*(2), 47–55. https://doi.org/10.33423/jlae.v16i2.2021

Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a healthcare information exchange: An economic analysis. *Decision Support Systems*, *61*, 1–11. https://doi.org/10.1016/j.dss.2013.10.011

Huang, C. Y., & Kao, Y. S. (2015). UTAUT2 based predictions of factors influencing the technology acceptance of phablets by DNP. *Mathematical Problems in Engineering*, *2015*. https://doi.org/10.1155/2015/603747

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2–18. https://doi.org/10.1108/OIR-11-2015-0358

Jones, C. M., McCarthy, R. V., Halawi, L., & Mujtaba, B. (2010). Utilizing the technology acceptance model to assess the employee adoption of information systems security measures. *Issues in Information Systems*, *11*(1), 9–16. https://commons.erau.edu/publication/310

Kaila, U., & Nyman, L. (2018). Information security best practices: First steps for startups and SMEs. *Technology Innovation Management Review*, *8*(11), 32–42. https://doi.org/10.22215/timreview/1198

Karlsson, F., Karlsson, M., & Åström, J. (2017). Measuring employees' compliance – The importance of value pluralism. *Information & Computer Security*, *25*(3), 279–299. https://doi.org/10.1108/ICS-11-2016-0084

Kauffman, R. J., Liu, J., & Ma, D. (2015). Technology investment decision-making under uncertainty. *Information Technology and Management*, *16*(2), 153–172. https://doi.org/10.1007/s10799-014-0212-2

Khatri, V., Samuel, B. M., & Dennis, A. R. (2018). System 1 and System 2 cognition in the decision to adopt and use a new technology. *Information & Management, 55*, 709–724. https://doi.org/10.1016/j.im.2018.03.002

Kim, S. H., Jang, S. Y., & Yang, K. H. (2017). Software-as-a-service adoption in small businesses: Risks, benefits, and organizational and environmental factors. *Journal of Small Business Management*, *55*(2), 303–325. https://doi.org/10.1111/jsbm.12304

Kim, S. H., Lee, K. H., Hwang, H., & Yoo, S. (2016). Analysis of the factors influencing healthcare professionals' adoption of mobile electronic medical record (EMR) using the unified theory of acceptance and use of technology (UTAUT) in a tertiary hospital. *BMC Medical Informatics and Decision Making*, *16*(12), 1–12. https://doi.org/10.1186/s12911-016-0249-8

Kim, Y., & Chang, H. (2014). Human centric security policy and management design for small and medium business. *Security and Communication Networks, 7*, 1622–1632. https://doi.org/10.1002/sec.814

King James Bible. (2017). King James Bible Online. https://www.kingjamesbibleonline.org (original work published 1769). Retrieved from King James Bible Online.

Kmieciak, R., Michna, A., & Felden, C. (2018). A Comparison of information technology capability, employee empowerment and innovativeness in German and Polish firms. *Information Technology Capability, Employee Empowerment and Innovativeness*, *23*(4), 642–672. https://doi.org/10.5771/0949-6181-2018-4-642

Kohnke, A., & Shoemaker, D. (2015). Making cybersecurity effective: The five governing principles for implementing practical IT governance and control. *The EDP Audit,*

Control, and Security Newsletter, *52*(3), 9–17. https://doi.org/10.1080/07366981.2015.1087799

Kurnia, S., Constantinidis, D., Parkes, A. J., & Seddon, P. B. (2017). Is there a prescription for strategic IT decisions? *Journal of Information Technology Teaching Cases*, *7*(1), 1–8. https://doi.org/10.1057/s41266-016-0011-1

Lai, J. Y., & Wang, J. (2015). Switching attitudes of Taiwanese middle-aged and elderly patients toward cloud healthcare services: An exploratory study. *Technological Forecasting and Social Change*, *92*, 155–167. https://doi.org/10.1016/j.techfore.2014.06.004

Lai, P. (2017). The literature review of technology adoption models and theories for the novelty technology. *Journal of Information Systems and Technology Management*, *14*(1), 21–38. https://doi.org/10.4301/S1807-17752017000100002

Lauckner, H., Paterson, M., & Krupa, T. (2012). Using constructivist case study methodology to understand community development pocesses: Proposed methodological questions to guide the research process. *The Qualitative Report*, *17*(13), 1–22. https://nsuworks.nova.edu/tqr/vol17/iss13/1

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, *59*, 60–70. https://doi.org/10.1016/j.cose.2016.02.004

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management*, *40*(3), 191–204. https://doi.org/10.1016/S0378-7206(01)00143-4

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324–327. https://doi.org/10.4103/2249-4863.161306

Lexico.com. (2019a). *Definition of age in English*. https://www.lexico.com/en/definition/age

Lexico.com. (2019b). *Definition of gender in English*. https://www.lexico.com/en/definition/gender

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Liberty University. (2019). *Institutional review board*. https://www.liberty.edu/graduate/institutional-review-board/

Longhofer, J., Floersch, J., & Hartmann, E. (2017). A case for the case study: How and why they matter. *Clinical Social Work Journal*, *45*(3), 189–200. https://doi.org/10.1007/s10615-017-0631-8

Macedo, I. M. (2017). Predicting the acceptance and use of information and communication technology by older adults: An empirical examination of the UTAUT2. *Computers in Human Behavior*, *75*, 935–948. https://doi.org/10.1016/j.chb.2017.06.013

Maity, M., Bagchi, K., Shah, A., & Misra, A. (2019). Explaining normative behavior in information technology use. *Information Technology & People*, *32*(1), 94–117. https://doi.org/10.1108/ITP-11-2017-0384

Man, W., & Lam, W. (2016). Attack-prevention and damage-control investments in cybersecurity. *Information Economics and Policy, 37,* 42–51. https://doi.org/10.1016/j.infoecopol.2016.10.003

Mao, W., Cai, Z., Towsley, D., Feng, Q., & Guan, X. (2017). Security importance assessment for system objects and malware detection. *Computers & Security*, *68*, 47–68. https://doi.org/10.1016/j.cose.2017.02.009

Mathieson, K. (1991). Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research*, *2*(3), 173–191. https://doi.org/10.1287/isre.2.3.173

Mayadunne, S., & Park, S. (2016). An economic model to evaluate information security investment of risk-taking small and medium enterprises. *Intternational Journal of Production Economics*, *182*, 519–530. https://doi.org/10.1016/j.ijpe.2016.09.018

Mazereeuw-van der Duijn Schouten, C., Graafland, J., & Kaptein, M. (2014). Religiosity, CSR attitudes, and CSR behavior: An empirical study of executives' Religiosity and CSR. *Journal of Business Ethics*, *123*(3), 437–459. https://www.jstor.org/stable/42921504

McAlpine, L. (2016). Why might you use narrative methodology? A story about narrative. *Estonian Journal of Education*, *4*(1), 32–57. https://doi.org/10.12697/eha.2016.4.1.02b

McSweeney, C. L. (2017). Defending with clapper: applying the supreme court's article iii standing interpretation to data breach lawsuits. *The Journal of High Technology Law*, *18*(1), 71–97. https://www.law.suffolk.edu/highlights/stuorgs/jhtl/

Mello, J. A. (2015). *Strategic human resource management* (4th ed.). South-Western.

Merriam, S. B. (1998). *Qualitative research and case study applications in education.* Jossey-Bass.

Merriam, S. B. (2009). *Qualitative research: A guide to design and implementation.* Jossey-Bass.

Mi, C., Chang, F., Lin, C., & Chang, Y. (2018). The theory of reasoned action to CSR behavioral intentions: The role of CSR expected benefit, CSR expected effort and stakeholders. *Sustainability*, *10*(12), 4462–4479. https://doi.org/10.3390/su10124462

Mikhed, V., & Vogan, M. (2018). How data breaches affect consumer credit. *Journal of Banking and Finance*, *88*, 192–207. https://doi.org/10.1016/j.jbankfin.2017.12.002

Miles, M. B., & Huberman, A. M. (1994). *An expanded sourcebook: Qualitative data analysis* (2nd ed.). Sage.

Moon, Y. J., Choi, M., & Armstrong, D. J. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. *International Journal of Information Management*, *40*, 54–66. https://doi.org/10.1016/j.ijinfomgt.2018.01.001

Morosan, C., & DeFranco, A. (2016). It's about time: Revisiting UTAUT2 to examine consumers' intentionsto use NFC mobile payments in hotels. *International Journal of Hospitality Management*, *53*, 17–29. https://doi.org/10.1016/j.ijhm.2015.11.003

Motylska-Kuzma, A. (2017). The financial decisions of family businesses. *Journal of Family Business Management*, *7*(3), 351–373. https://doi.org/10.1108/JFBM-07-2017-0019

Moussaïd, M., Campero, A. N., & Almaatouq, A. (2018). Dynamical networks of influence in small group discussions. *PLoS One*, *13*(1), 1–13. https://doi.org/10.1371/journal.pone.0190541

Nadri, H., Rahimi, B., Lotfnezhad Afshar, H., Samadbeik, M., & Garavand, A. (2018). Factors affecting acceptance of hospital information systems based on extended technology

acceptance model: A case study in three paraclinical departments. *Applied Clinical Informatics, 9*(2), 238–247. https://doi.org/10.1055/s-0038-1641595

National Institute of Standards and Technology. (2012). *NIST Special Publication 800-30 (Guide for ConductingRisk Assessments) Revision 1*. National Institute of Standards and Technology, United States Department of Commerce. Gaithersburg: Computer Security Division National Information Technology Laboratory National Institute of Standards and Technology.

National Institute of Standards and Technology. (2019, March 13). Cyber Crime: An Existential Threat to Small Business . Washington, District of Columbia, United States. https://www.nist.gov/speech-testimony/cyber-crime-existential-threat-small-business

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*(1), 123–134. https://doi.org/10.1016/j.im.2014.10.009

Nguyen, T. H., Newby, M., & Macaulay, M. J. (2015). Information technology adoption in small business: Confirmation of a proposed framework. *Journal of Small Business Management*, *53*(1), 207–227. https://doi.org/10.1111/jsbm.12058

Nie, P. Y., Wang, C., Chen, Y. H., & Yang, Y. C. (2018). Effects of switching costs on innovative investment. *Technological and Economic Development of Economy*, *24*(3), 933–949. https://doi.org/10.3846/tede.2018.1430

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *NIST Special Publication 800-12, Revision 1: An Introduction to Information Security*. National Institute of Standards and Technology, U.S. Department of Commerce. Gaithersburg: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1

Noguerol, L. O., & Branch, R. (2018). Leadership and electronic data security within small businesses: An exploratory case study. *Journal of Economic Development, Management, IT, Finance, and Marketing*, *10*(2), 7–35. https://gsmi-ijgb.com/wp-content/uploads/JEDMITFM-V10-N2-P02-Luis-Noguerol-Electronic-Data-Security.pdf

O'Cathain, A., & Thomas, K. J. (2004). "Any other comments?" Open questions on questionnaires – a bane or a bonus to research? *BMC Medical Research Methodology*, *4*(25), 1–7. https://doi.org/10.1186/1471-2288-4-25

Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior*, *61*, 404–414. https://doi.org/10.1016/j.chb.2016.03.030

Olufemi, A. (2018). Considerations for the adoption of cloud-based big data analytics in small business enterprises. *Electronic Journal of Information Systems Evaluation, 21*(2), 63–79. https://issuu.com/academic-conferences.org/docs/ejise-volume21-issue2-article1063

Onan, A., & Simsek, N. (2019). Interprofessional education and social interaction: The use of automated external defibrillators in team-based basic life support. *Health Informatics Journal*, *25*(1), 139–148. https://doi.org/10.1177/1460458217704252

Onuekwe, C. E. (2015). *Entertainment-education for health behaviour change.* FriesenPress.

Osborn, E., & Simpson, A. (2018). Risk and the small-scale cyber security decision making dialogue - A UK case study. *The Computer Journal*, *61*(4), 472–495. https://doi.org/10.1093/comjnl/bxx093

OWASP Foundation, Inc. (2020). Retrieved from Open Web Application Security Project: https://owasp.org/

Palau-Saumell, R., Forgas-Coll, S., Sánchez-García, J., & Robres, E. (2019). User acceptance of mobile apps for restaurants: An expanded and extended UTAUT-2. *Sustainability, 11*(4), 1–24. https://doi.org/10.3390/su11041210

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems*, *59*(3), 211–217. https://doi.org/10.1080/08874417.2019.1571459

Palmer, D., & Caldas, B. (2015). Research Methods in Language and Education. In S. I. 2017, *Research Methods in Language and Education* (3rd ed., pp. 1–12). New York, NY: Springer, Cham. https://doi.org/10.1007/978-3-319-02329-8

Pan, X., Hou, L., & Liu, K. (2017). Social influence on selection behaviour: Distinguishing local- and global-driven preferential attachment. *PloS One*, *12*(4), 1–12. https://doi.org/10.1371/journal.pone.0175761

Pappa, I. C., Iliopoulos, C., & Massouras, T. (2018). What determines the acceptance and use of electronic traceability systems in agri-food supply chains? *Journal of Rural Studies*, *58*, 123–135. https://doi.org/10.1016/j.jrurstud.2018.01.001

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

Patton, M. Q. (2015). *Qualitative research & evaluation methods.* Sage.

Peterson, D. C., Adams, A., Sanders, S., & Sanford, B. (2018). Assessing and addressing threats and risks to cybersecurity. *Frontiers of Health Services Management*, *35*(1), 23–29. https://doi.org/10.1097/HAP.0000000000000040

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *Foresight*, *20*(4), 353–363. https://doi.org/10.1108/FS-02-2018-0020

Rahi, S., & Ghani, M. (2018). The role of UTAUT, DOI, perceived technology security and game elements in internet banking adoption. *World Journal of Science, Technology and Sustainable Development*, *15*(4), 338–356. https://doi.org/10.1108/WJSTSD-05-2018-0040

Ravangard, R., Kazemi, Z., Kazemi, A. S., Sharifian, R., & Monem, H. (2017). Development of the UTAUT2 model to measure the acceptance of medical laboratory portals by patients in. *Electronic Physician*, *9*(2), 3862–3869. https://doi.org/10.19082/3862

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in europe: A review of victim surveys. *Crime Science*, *7*(5), 1–15. https://doi.org/10.1186/s40163-018-0079-3

Rieger, K. L. (2019). Discriminating among grounded theory approaches. *Nursing Inquiry*, *26*(1), 1–12. https://doi.org/10.1111/nin.12261

Rimando, M., Brace, A., Namageyo-Funa, A., Parr, T. L., Sealy, D. A., Davis, T. L., Martinez, L. M., & Christiana, R. W. (2015). Data collection challenges and recommendations for early career researchers. *The Qualitative Report*, *20*(12), 2025–2036. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2428&context=tqr

Roger, K., Bone, T., Heinonen, T., Schwartz, K., Slater, J., & Thakrar, S. (2018). Exploring identity: What we do as qualitative researchers. *The Qualitative Report*, *23*(3), 532–546. https://nsuworks.nova.edu/tqr/vol23/iss3/3

Rohn, E., Sabari, G., & Leshem, G. (2016). Explaining small business InfoSec posture using social theories. *Information and Computer Security*, *24*(5), 534–556. https://doi.org/10.1108/ICS-09-2015-0041

Rondan-Cataluña, F. J., Arenas-Gaitán, J., & Ramírez-Correa, P. E. (2015). A comparison of the different versions of popular technology acceptance models: A non-linear perspective. *Kybernetes*, *44*(5), 788–805. https://doi.org/10.1108/K-09-2014-0184

Roses, L. K., Brito, J. C., & Lucena Filho, G. J. (2015). Conversational competences model for information technology and business strategic alignment. *JISTEM - Journal of Information Systems and Technology Management*, *12*(1), 125–144. https://doi.org/10.4301/S1807-17752015000100007

Ruben, B. D., & Gigliotti, R. A. (2016). Leadership as social influence: An expanded view of leadership communication theory and practice. *Journal of Leadership & Organizational Studies*, *23*(4), 467–479. https://doi.org/10.1177/1548051816641876

Saldaña, J. (2009). *The coding manual for qualitative researchers.* Sage.

Sampaio, A., & Saramago, J. (2016). Loyalty in retailing: Multidimensional approach to customer perceived value. *European Journal of Applied Business Management*, *2*(2), 96–114. https://pdfs.semanticscholar.org/38bb/92bd0129c55510d8b55ef1ae849334308eb7.pdf

Sánchez, A. R., Hueros, D. A., & Ordaz, G. M. (2013). E-learning and the university of huelva: A study of WebCT and the technological acceptance model. *Campus-Wide Information Systems*, *30*(2), 135–160. https://doi.org/10.1108/10650741311306318

Santos-Olmo, A., Sánchez, L., Caballero, I., Camacho, S., & Fernandez-Medina, E. (2016). The importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet*, *8*(4), 30–56. https://doi.org/10.3390/fi8030030

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and

operationalization. *Quality & Quantity*, *52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

SBA Business Credit and Assistance. (2019). (13 C.F.R. § 121.201).

Schoonenboom, J. (2018). Designing mixed methods research by mixing and merging methodologies: A 13-Step Model. *American Behavioral Scientist*, *67*(2), 998–1015. https://doi.org/10.1177/0002764218772674

Schouten, C. M.-v., Graafland, J., & Kaptein, M. (2014). Religiosity, CSR attitudes, and CSR behavior: An empirical study of executives' religiosity and CSR. *Journal of Business Ethics*, *123*(3), 437–459. https://doi.org/10.1007/s10551-013-1847-3

Seidman, I. (2013). *Interviewing as qualitative research: A guide for researchers in education and the social sciences.* Teachers College Press.

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

Sepasgozar, S. M., Loosemore, M., & Davis, S. R. (2016). Conceptualising information and equipment technology adoption in construction. *Engineering, Construction and Architectural Management*, *23*(2), 158–176. https://doi.org/10.1108/ECAM-05-2015-0083

Shao, Z. (2019). Interaction effect of strategic leadership behaviors and organizational culture on IS-Business strategic alignment and Enterprise Systems assimilation. *International Journal of Information Management*, *44*, 96–108. https://doi.org/10.1016/j.ijinfomgt.2018.09.010

Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International Journal of Information Management, 45*, 44–55. https://doi.org/10.1016/j.ijinfomgt.2018.10.024

Sheppard, M., & Vibert, C. (2019). Re-examining the relationship between ease of use and usefulness for the net generation. *Education and Information Technologies*, *24*(5), 3205–3218. https://doi.org/10.1007/s10639-019-09916-0

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior, 48*, 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Sim, J., Saunders, B., Waterfield, J., & Kingstone, T. (2018). Can sample size in qualitative research be determined a priori? *International Journal of Social Research Methodology*, *21*(5), 619–634. https://doi.org/10.1080/13645579.2018.1454643

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

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*, *23*(2), 200–217. https://doi.org/10.1108/ICS-04-2014-0025

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*, 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stake, R. E. (2003). *Case studies. In* N. K. Denzin & Y. S. Lincoln (Eds.). Sage.

Stake, R. E. (2006). *Multiple case study analysis.* Guilford Press.

Stake, R. E. (2010). *Qualitative research: Studying how things work.* Guilford Press.

Stanciu, V., & Tinca, A. (2017). Exploring cybercrime – realities and challenges. *Accounting and Management Information Systems*, *16*(4), 610–632. https://doi.org/10.24818/jamis.2017.04009

Steffen, N. K., Haslam, S. A., Jetten, J., & Mols, F. (2018). Our followers are lions, theirs are sheep: How social identity shapes theories about followership and social influence. *Political Psychology*, *39*(1), 23–42. https://doi.org/10.1111/pops.12387

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, *68*(3), 226–231. https://www-ncbi-nlm-nih-gov.ezproxy.liberty.edu/pmc/articles/PMC4485510/

Taherdoost, H. (2018). Development of an adoption model to assess user acceptance of e-service technology: E-Service technology acceptance model. *Behaviour & Information Technology*, *37*(2), 173–197. https://doi.org/10.1080/0144929X.2018.1427793

Tamilmani, K., Dwivedi, Y. K., & Rana, N. (2017). *A systematic review of citations of UTAUT2 article and its usage trends.* Springer International Publishing AG. https://doi.org/10.1007/978-3-319-68557-1_5

Tamilmani, K., Rana, N. P., Prakasam, N., & Dwivedi, Y. K. (2019). The battle of brain vs. heart: A literature review and meta-analysis of "hedonic motivation" use in UTAUT2.

International Journal of Information Management, *46*, 222–235. https://doi.org/10.1016/j.ijinfomgt.2019.01.008

Tarhini, A., El-Masri, M., Ali, M., & Serrano, A. (2016). Extending the UTAUT model to understand the customers' acceptance and use of internet banking in Lebanon: A structural equation modeling approach. *Information Technology & People*, *29*(4), 830-849. https://doi.org/10.1108/ITP-02-2014-0034

Tavares, J., Goulão, A., & Oliveira, T. (2018). Electronic health record portals adoption: Empirical model based on UTAUT2. *Informatics for Health & Social Care, 43*(2), 109–125. https://doi.org/10.1080/17538157.2017.1363759

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, *6*(2), 144–176. https://www.jstor.org/stable/23011007?seq=1#page_scan_tab_contents

The Blue Book building and construction network. (2020). *The Blue Book building and construction network.* http://www.thebluebook.com/

The Council of Economic Advisers. (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy.* The Council of Economic Advisers. Washington: Executive Office of the President. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

The Procter & Gamble Company. (2019). *P&G 2019 Annual Report.* Cincinnati: The Procter & Gamble Company. https://www.pg.com/annualreport2019/download/PG-2019-Annual-Report.pdf

Trim, P. R., & Lee, Y. I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, 1–15. https://doi.org/10.1016/j.indmarman.2019.04.003

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A cybercrime incident architecture with adaptive response policy. *Computers & Security*, *83*, 22–37. https://doi.org/10.1016/j.cose.2019.01.011

Turner, S. F., Cardinal, L. B., & Burton, R. M. (2017). Research design for mixed methods: A triangulation-based framework and roadmap. *Organizational Research Methods*, *20*(2), 243–267. https://doi.org/10.1177/1094428115610808

U.S. Small Business Administration Office of Advocacy. (2016). *Small Business Profile Virginia.* https://www.sba.gov/sites/default/files/advocacy/Virginia.pdf

Ullaha, F., Edwards, M., Ramdhany, R., Chitchyan, R., Ali Babar, M., & Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications*, *101*, 18–54. https://doi.org/10.1016/j.jnca.2017.10.016

United States Census Bureau. (2018, December). *2016 SUSB Annual Data Tables by Establishment Industry*. https://www.census.gov/data/tables/2016/econ/susb/2016-susb-annual.html

United States Department of Labor. (2019). *Employed persons by occupation, sex, and age.* U.S. Burea of Labor Statistics. https://www.bls.gov/cps/tables.htm#annual

Van Duzer, J. (2010). *Why business matters to God: (And what still needs to be fixed).* IVP Academic.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research*, *11*(4), 342–365. https://doi.org/10.1287/isre.11.4.342.11872

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Venkatesh, V., Brown, S. A., Maruping, L. M., & Bala, H. (2008). Predicting different conceptualizations of system use: the competing roles of behavioral intention, facilitating conditions, and behavioral expectation. *MIS Quarterly*, *32*(3), 483–502. https://doi.org/10.2307/25148853

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 57–178. https://doi.org/10.2307/41410412

Von Bergen, C. W., & Bressler, M. S. (2018). Confirmation bias in entrepreneurship. *Journal of Management Policy and Practice, 19*(3), 74–84. https://doi.org/10.33423/jmpp.v19i3.49

Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access, 6,* 25167–25177. https://doi.org/10.1109/ACCESS.2018.2817560

Wang, C., Harris, J., & Patterson, P. G. (2017). Modeling the habit of self-service technology usage. *Australian Journal of Managemen, 42*(3), 462–481. https://doi.org/10.1177/0312896216640862

Wang, M., Cho, S., & Denton, T. (2017). The impact of personalization and compatibility with past experience on e-banking usage. *International Journal of Bank Marketing, 35*(1), 45–55. https://doi.org/10.1108/IJBM-04-2015-0046

Wang, Y. Y., Wang, Y. S., & Lin, T. C. (2018). Developing and validating a technology upgrade model. *International Journal of Information Management, 38*(1), 7–26. https://doi.org/10.1016/j.ijinfomgt.2017.07.003

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security, 77*, 807–823. https://doi.org/10.1016/j.cose.2018.02.001

Wetzel, S. (2019). Modern casting. *American Foundry Society, Inc.*, *109*(4), 32–36. http://ezproxy.liberty.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F2222494487%3Faccountid%3D12085

Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management*, *11*(Fall), 1–16. https://pdfs.semanticscholar.org/f6f2/c79ebc546933960ea4675c1e857398b75e7f.pdf

Wilding, N. (2016). Cyber resilience: How important is your reputation? How effective are your people? *Business Information Review*, *33*(2), 94–99. https://doi.org/10.1177/0266382116650299

Williams, M. D., Rana, N. P., & Dwivedi, Y. K. (2015). The unified theory of acceptance and use of technology (UTAUT): A literature review. *Journal of Enterprise Information Management*, *28*(3), 443–488. https://doi.org/10.1108/JEIM-09-2014-0088

Wirth, A. (2017). The economics of cybersecurity. *Biomedical Instrumentation and Technology*, *51*(s6), 52–59. https://doi.org/10.2345/0899-8205-51.s6.52

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

Woods, J. A., Gottschall, R., Matthews, C. H., & Carsrud, A. L. (2017). The influence of industry association involvement on technology decision-making in small businesses. *Journal of Enterprising Culture*, *25*(3), 317–337. https://doi.org/10.1142/S0218495817500121

Woods, N., & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies*, *128*, 61–71. https://doi.org/10.1016/j.ijhcs.2019.02.003

Wray, N., Markovic, M., & Manderson, L. (2007). “Researcher saturation”: The impact of data triangulation and intensive-research practices on the rsearcher and qalitative rsearch pocess. *Qualitative Health Research*, *17*(10), 1392–1402. https://doi.org/10.1177/1049732307308308

Yasin, M. M., Czuchry, A. J., & Small, M. H. (2018). Organizational security: A conceptual framework and implementation issues. *Competition Forum*, *16*(1), 38–49. https://www.questia.com/library/journal/1P4-2133361299/organizational-security-a-conceptual-framework-and

Yeh, C. H., Lee, G. G., & Pai, J. C. (2015). Using a technology-organization-environment framework to investigate the factors influencing e-businessinformation technology capabilities. *Information Development*, *31*(5), 435–450. https://doi.org/10.1177/0266666913516027

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

Yuan, S., Ma, W., Kanthawala, S., & Peng, W. (2015). Keep using my health apps: Discover users’ perception of health and fitness apps with the UTAUT2 model. *Telemedicine and e-Health*, *21*(9), 735–741. https://doi.org/10.1089/tmj.2014.0148

Zhang, L., Zhu, J., & Liu, Q. (2012). A meta-analysis of mobile commerce adoption and the moderating effect of culture. *Computers in Human Behavior*, *28*, 1902–2911. https://doi.org/10.1016/j.chb.2012.05.008

Zoom Meetings & Chat. (2019). Retrieved from Zoom: https://zoom.us/meetings

Appendix A: Participant Profile Questionnaire

Participant Profile Questionnaire

Business Name: _____ **Date:** _____

Participant Name (First/Last Name): _____

Please fill in the blanks or place an X or check mark next to the word or phrase that best matches your response.

1. What is your gender?

- ☐ Male
- ☐ Female
- ☐ Other

2. What is your age?

- ☐ Under 18
- ☐ 18 - 24
- ☐ 25 - 34
- ☐ 35 - 44
- ☐ 45 –-54
- ☐ 55 - 64
- ☐ Over 64

3. Are you familiar with your business's Security Awareness Training (SAT)?

- ☐ Yes
- ☐ No
- ☐ No SAT Program Exists

4. Does the business employ security information policies?

- ☐ Yes
- ☐ No (If No, Skip to Question # 6)

5. Do you believe the security information policies are effective?

- ☐ Yes
- ☐ No
- ☐ Don't Know

6. Do you interact with any information security systems?

- ☐ Yes
- ☐ No
- ☐ Don't Know

7. How long have you been working for the business?

- ☐ Less than < 1 year
- ☐ 1 – 5 years
- ☐ 6 – 10 years
- ☐ 11 – 15 years
- ☐ 16 – 20 years
- ☐ 21 – 25 years
- ☐ 26 – 30 years
- ☐ 31 – 35 years
- ☐ 36 – 40 years
- ☐ Over > 40 years

Appendix B: Interview Guide

Interview Questions: Implementing Information Security

Date: _____

Location: _____

Interviewer: _____

Interviewee (Number): _____

Time of Interview: **Start:** _____ **End:** _____

Thank you for agreeing to meet with me today for this interview. Qualitative researchers often view the interview process as a focused conversation about the subject of interest they are studying. I intend for this interview to be a conversation and want you to feel comfortable throughout our meeting and feel free to ask questions as we go.

Do you have any questions before we move forward and record our conversation?

Before we get started with the interview questions, I want to know if you have any questions about the informed consent form or how this interview process will be conducted.

As part of this interview session, I will be recording our conversation.

Turn On Recorder

1. To start with, will you please tell me what your job title is and about your current job position?

Interview Questions

2. Describe what role you play in deciding to implement information security measures?
    a. Even if you are not responsible for implementing information security measures, can you describe how their implementation may affect your work habits?
3. Explain to me what you think are the most important factors in deciding to implement information security measures?
4. Do you play any role in deciding business investment strategies?
    a. How do business investment strategies come into play when deciding on implementing information security strategies?

   b. When deciding on new information security investments, describe the process that is used to make investment decisions?
   c. Is this process based on any type of formal risk-analysis?

5. Do newspaper, television or other stories about data breaches or cyber thefts against small businesses affect how you make decisions on information security?

6. Can you describe any losses the business may have suffered from information security breaches?

   a. Describe any changes that the business made because of this incident?

7. What role do you think managers or employees should play in getting people to use new information security technologies?

8. When new information security technologies are implemented in the business, how do you feel about their use?

   a. Do you believe there are any benefits to using information security technologies and if so, please describe them?

   b. Please describe any new stressors you feel when new information security technologies are implemented?

9. Please describe any training you have in place for any security systems you are implementing or have installed?

10. Can you describe any other resources besides training, the business uses for employees to help them with the introduction of new security systems?

Only ask if Participant answered <u>Yes</u> to Question #6, Participant Profile Questionnaire

11. Describe how easy or hard it is to use the information security technology system?

12. Describe how you may influence other employees' use of the security system?

13. Describe any influence other employees have on your use of using security technologies?

14. Describe how long you've been using the security technology and your comfort with it?

15. Explain how you may help other employees with the security system?

16. Explain how you perceive your co-workers view the security systems?

Only ask if Participant answered <u>Yes</u> to Question #4, Participant Profile Questionnaire

17. Describe how important security policies are to you?

18. Describe how security policies may help you in dealing with the security system?

This concludes our interview. I want to thank you for participating in this study. The questions you so graciously answered will provide valuable information from which themes can be developed for further analysis. This will help the researcher further their understanding of small businesses and their implementation of information security technologies. The data collected during the interviews will be analyzed in conjunction with the other information collected to assists in answering the research questions.

Appendix C: Participant Profile Questionnaire Responses

1. What is your gender?	2. What is your age?	3. Are you familiar with your business's Security Awareness Training (SAT)?	4. Does the business employ security information policies?	5. Do you believe the security information policies are effective?	6. Do you interact with any information security systems?	7. How long have you been working for the business? (In Years)
Male	35 - 44	No	No	N/A	No	11 – 15
Male	35 - 44	No	No	N/A	No	6 – 10
Male	Over 64	No	No	N/A	No	21 – 25
Male	55 - 64	No	No	Don't Know	Don't Know	36 – 40
Male	Over 64	No	No	N/A	No	Over > 40
Female	45 - 54	No	No	N/A	Don't Know	6 – 10
Male	35 - 44	No	N/A	N/A	No	11 – 15
Male	35 - 44	Yes	Yes	Yes	Yes	16 – 20
Male	45 - 54	No	No	N/A	No	16 – 20
Male	Over 64	No	No	Yes	No	16 – 20
Male	45 - 54	No	No	N/A	No	16 – 20
Male	55 - 64	No	Yes	Yes	Yes	21 – 25
Male	Over 64	No	No	N/A	No	Over > 40
Male	25 - 34	No	Yes	Don't Know	No	6 – 10
Male	45 - 54	No	No	N/A	No	16 – 20
Male	Over 64	Yes	Yes	Yes	Yes	26 – 30
Male	18 - 24	Yes	Yes	Yes	Yes	6 – 10
Male	25 - 34	No	No	Don't Know	No	1 – 5
Male	35 - 44	No	No	Don't Know	No	21 – 25
Male	35 - 44	No	No	No	No	11 – 15
Male	55 - 64	No	No	Don't Know	Don't Know	36 – 40
Male	55 - 64	No	No	No	Don't Know	16 – 20
Male	35 - 44	No	No	Don't Know	No	11 – 15
Female	45 - 54	Yes	Yes	Yes	No	11 – 15
Male	45 - 54	No	N/A	N/A	No	26 – 30
Female	35 - 44	No	No	N/A	No	16 – 20

Male	35 - 44	No	Yes	Yes	No	1 – 5
Male	55 - 64	No	N/A	No	Don't Know	31 – 35
Female	55 - 64	No	No	Don't Know	Yes	1 – 5
Female	35 - 44	No	No	N/A	Yes	1 – 5

Appendix D: Zed Attack Proxy (ZAP©)

ZAP© Business Alerts

Alert Description	Number of Instances
Absence of Anti-CSRF Tokens	20,086
Application Error Disclosure	607
Charset Mismatch	867
Content-Type Header Missing	3
Cookie No HTTPOnly Flag	2,433
Cookie Without SameSite Attribute	3,687
Cookie Without Secure Flag	2,323
Cross Domain Misconfiguration	1,544
Cross-Domain JavaScript Source File inclusion	54,510
CSP Scanner Notices	5,610
CSP Scanner Wildcard Directive	5,675
Incomplete or No Cache-control and Pragma HTTP Header Set	12,356
Information Disclosure - Debug Error Messages	109
Informational Disclosure - Sensitive Information in URL	59
Informational Disclosure - Suspicious Comments	12,139
Loosely Scoped Cookie	48
Old ASP Net Version in Use	1
Private IP Disclosure	6
Secure Pages Include Mixed Content	39
Sever Leaks Information via "X-Powered-By" HTTP Response Header Fields(s)	6,352
Timestamp Disclosure - Unix	98,359
Viewstate Without MAC Signature (Unsure)	2
X-AspNet-Version Response Header Scanner	13,775
X-Content-Type-Options Header Missing	16,985
X-Frame-Options Header Not Set	3,570

Appendix E: ZAP© Alerts

ZAP© Passive Scan Alerts

Alert Risk	Description
Low	**Absence of Anti-CSRF Tokens (CSRF Countermeasures)**
	This scanner identifies “potential” vulnerabilities with the lack of known CSRF countermeasures in pages with forms.
Medium/Low	**Application Error Disclosure**
	Check server responses for HTTP 500 - Internal Server Error type responses or those that contain a known error string. Note: Matches made within script blocks or files are against the entire content not only comments.
Informational	**Charset Mismatch**
	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set.
Informational	**Content Type Missing**
	Raises an alert if the response is lacking a Content-Type header or if the header exists but the value is empty.
Low	**Cookie No HTTPOnly Flag (Cookie HttpOnly)**
	Ensures that as cookies are set they are flagged HttpOnly. The HttpOnly flag indicates to browsers that the cookie being set should not be acted upon by client side script (such as JavaScript).
Low	**Cookie Without SameSite Attribute**
	This reports any cookies that do not have the SameSite attribute or that do not have a recognized valid value for that attribute.
Low	**Cookie Secure Flag**
	Looks for cookies set during HTTPS sessions, raises an alert for those that are set but do not include the secure flag. A cookie set with the secure flag will not be sent during a plain HTTP session.
Medium	**Cross Domain Misconfiguration**
	Passively scan responses for Cross Domain MisConfigurations, which relax the Same Origin Policy in the web browser, for instance. The current implementation looks at excessively permissive CORS headers.
Low	**Cross-Domain JavaScript Source File inclusion (Cross Domain Script Inclusion)**
	Validates whether or not scripts are included from domains other than the domain hosting the content. By looking at the “src” attributes of “script” tags in HTML responses.
Medium/Low	**CSP Scanner Notices**
	The Content Security Policy (CSP) Scanner adds a passive scan rule which parses and analyzes CSP headers for potential misconfiguration or weakness. This scanner leverages Shape Security's Salvation library to perform its parsing and assessment of CSPs. Note: If multiple CSP headers are encountered they are merged (intersected)

	into a single policy for analysis, check the 'Other Info' field of alerts for further details.
Medium	**Content Security Policy (CSP) Scanner Wildcard Directive**
	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestor
Low	**Incomplete or No Cache-control and Pragma HTTP Header Set**
	Checks "Cache-Control" and "Pragma" response headers against general industry best practice settings for protection of sensitive content.
Low	**Information Disclosure: Debug Errors Messages**
	This passive scanner checks the content of web responses for known Debug Error message fragments. Access to such details may provide a malicious individual with means by which to further abuse the web site. They may also leak data not specifically meant for end user consumption. Note: Javascript responses are only assessed at LOW threshold.
Informational	**Informational Disclosure - Sensitive Information in URL**
	Attempts to identify the existence of sensitive details within the visited URIs themselves (this may include parameters, document names, directory names, etc.).
Informational	**Informational Disclosure - Suspicious Comments**
	Analyzes web content to identify comments which contain potentially sensitive details. Which may lead to further attack or exposure of unintended data.
Informational	**Cookie - Loosely Scoped**
	Cookies can be scoped by domain or path. This check is only concerned with domain scope. The domain scope applied to a cookie determines which domains can access it. For example, a cookie can be scoped strictly to a subdomain e.g. www.nottrusted.com, or loosely scoped to a parent domain e.g. nottrusted.com. In the latter case, any subdomain of nottrusted.com can access the cookie. Loosely scoped cookies are common in mega-applications like google.com and live. com.
Low	**Old ASP Net Version in Use (X-AspNet-Version Response Header Scanner)**
	This checks response headers for the presence of X-AspNet-Version/X-AspNetMvc-Version details.
Low	**Private IP Disclosure**
	Checks the response content for inclusion of RFC 1918 IPv4 addresses as well as Amazon EC2 private hostnames (for example, ip-10-0-56-78). This information can give an attacker useful information about the IP address scheme of the internal network, and might be helpful for further attacks targeting internal systems.
Low	**Secure Pages Include Mixed Content (Insecure JSF ViewState Mixed Content)**
	For content served via HTTPS analyse all the src attributes in the response looking for those sourced via plain HTTP.
Low	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
	This checks response headers for the presence of X-Powered-By details.
Informational	**Timestamp Disclosure - Unix**
	A timestamp was disclosed by the application/web server.
High	**Viewstate Without MAC Signature (Unsure)**

	Attempts to identify VIEWSTATE parameters and analyze said parameters for various best practices or protective measures such as: • Those based on ASP. NET 1. 0 and 1. 1. • VIEWSTATE Lacking signature. • Split VIEWSTATE. • VIEWSTATE containing email or IP patterns.
Low	**X-AspNet-Version Response Header Scanner**
	This checks response headers for the presence of X-AspNet-Version/X-AspNetMvc-Version details.
Medium	**X-Content-Type-Options Header Missing (Header Not Set)**
	This scanner check for the Anti-MIME-Sniffing header X-Content-Type-Options and ensures it is set to ‘nosniff’.
Low	**X-Frame-Options Header Scanner**
	This scanner checks for the existence and validity of the X-Frame-Options header. At MEDIUM and HIGH thresholds this only looks at non-error or non-redirect HTML responses.

Data in column 2 Adapted from “Documentation >The OWASP ZAP Desktop User Guide>Add-Ons> Passive Scan Rules,” by Zap Dev Team, 2020 (https://www.zaproxy. org/docs/desktop/addons/passive-scan-rules/).