# EXPLORING SECURITY PROFESSIONALS' PERCEPTIONS ON MOBILE DEVICES PAIRED WITH RENTAL AUTOMOBILES

**A Dissertation Presented in Partial Fulfillment of the Requirements for the Degree of Doctor of Computer Science**

**By**

**Jeffrey Struik**

**Colorado Technical University**

**March 2018**

**Committee**

James O. Webb, Jr, Ph.D., Chair

Steven H. Munkeby, DM, Committee Member

Cynthia M. Calongne, D.CS, Committee Member

February 26, 2018
Date Approved

## Abstract

The exploratory study observed and interviewed 10 security professionals with industry experience, and industry-recognized security certifications. The study identified security, privacy, and trust issues after exploring the attitudes and behaviors of security professionals when pairing a mobile device with an automotive infotainment system. The results of the study developed four themes. The themes suggested that all study participants exhibited an attitude of distrust towards infotainment systems. Many of the participants also demonstrated attitudes that the infotainment system potentially leaked data and that personal information remained on the system after removing the smartphone. Further, there was a contradiction between the behaviors and the attitudes when navigating the pairing process, which was among the younger participants. Future research opportunities include conducting a similar study at a different location, conducting a similar study observing individuals without security training, and conducting a quantitative study to determine differences in behavior between security and non-security professionals.

## Dedication

To my supportive wife, my children, my family, friends, and God for blessing me with the ability to learn.

**Acknowledgements**

I would like to thank my amazing wife; your encouragement, support, and help enabled me to keep my focus, so I could persevere and accomplish my goal. Your relentless encouragement and positive attitude helped me to complete my dissertation and stay motivated during this journey. I would like to thank my children Jaydon, Peyton, Elijah, Dakota, Tomi, and Josiah, for their patience during the long nights researching. Thanks to Dr. James Webb, my research supervisor, who provided valuable advice and was dedicated to seeing me complete my dissertation. Thanks to Dr. Richard Livingood and Dr. Cynthia Calongne for helping me find the path for this dissertation.

## Table of Contents

## List of Tables

## List of Figures

# CHAPTER ONE

Cybersecurity continues to be an important topic and continues to warrant research curiosity. Events such as the Stuxnet virus which proved the hackers' ability to negatively affect a physical system using malware as explained by Chen (2010). This study plans to explore how information technology (IT) security professional's behaviors varied when pairing a smartphone to a rental vehicle depending on the security professionals' experiences and professional certifications.

This chapter introduces the topic, provides a topic overview, problem statement, and purpose statement. Further, it presents the research questions, the hypothesis, and the theoretical framework. It also provides the limitations, delimitations, study significance, and study assumptions and biases. This chapter includes a definitions section to enlighten the reader to various technical terms surrounding the phenomenon of interest. A research design overview describes the high-level aspects of the design used in this study.

## Topic Overview/Background

Pairing smartphones to an automobile via Bluetooth presents an opportunity for increased convenience and safety for drivers. Onishi, Wu, Yoshida, and Kato (2017) shared that onboard Bluetooth capabilities afford the convenience of connecting a mobile phone to the automobile as well as additional functions like streaming music, or car diagnostics monitoring. The use of Bluetooth also adds the capability to download the user's phonebook to the automobile for the convenience of placing calls using the automobile's infotainment system. Cheah, Shaikh, Haas, and Ruddle (2017) discovered that the most common use of Bluetooth in automobiles is for hands-free calling which involves synchronizing the device's phonebook using the Phone Book Access Profile (PBAP) which holds personal information.

During past rental experiences, there was the discovery that multiple phonebooks could pair with the automobile at one time. Each vehicle allowed for access to the other phonebooks without additional authentication requirements, thus exposing the other user's contact information and other information which, when combined, could become personally identifiable information (PII). Rozenberg (2012) posited that PII is any combination or a unique piece of information, which can be used to identify some individual, and malicious actors often use it for identity theft. Further, retrieving this information from a phonebook on an automobile presents the hacker the opportunity to learn more about the individual and pursue acts such as personal information theft or selling of the information to other bad actors, according to Corbett, Schoch, Kargl, and Felix (2016).

Not every individual automobile driver pairs a smartphone to the rental vehicle, however which raises the question of why do the behaviors differ from one renter to another. Security awareness training is an important component used to influence the behaviors of individuals using information technology in both public and private sector organizations since security awareness can affect the behaviors of individuals according to Pahnila, Karjalainen, and Siponen (2013). Siponen (2001) suggested that the general public falls into two categories: computer/information technology professionals, and other users. This segregation poses the question of what effect the security awareness of an individual has on the observed behaviors in everyday interactions with computer systems, to include vehicle-borne systems. This study looks specifically at the subset of computer security professionals, which is in the category of computer/information technology professionals.

## Problem Opportunity Statement

The continued growth of Internet-accessible devices continues to create new attack vectors for malicious actors. Advancements in technology lead to the ability to connect Bluetooth devices, such as smartphones, to automobiles for the convenience of hands-free calling. Although there is added convenience, there is additional risk resulting from the additional connectivity abilities. Onishi et al. (2017) explained that Bluetooth interfaces have vulnerabilities such as not requiring user permissions to pair, limited security mechanisms, and exploitable personal information, such as address books or passwords. Currently, there is a general lack of awareness by consumers regarding the risks of pairing a smartphone to an automobile and the risk increases with rental vehicles. The lack of awareness and tendency of consumers to seek out convenience presented an opportunity for malicious actors to exploit poorly designed automobile infotainment access controls to steal private information from the vehicle user. The objective of this study was to understand if security awareness training affected the behaviors of automobile renters, specifically habits of pairing a smartphone and any actions taken upon return of the vehicle to the rental facility.

## Purpose Statement

The purpose of this exploratory study is to observe the differences in the behavior of automobile users who have formal security training when presented the option to connect a smartphone to an automobile using Bluetooth. This exploratory study hinges on the observed information left on automobiles after an individual connects the device to the automobile. Goyal Chin, Etudo, and Harris (2016) explained as users become more dependent on device manufacturers and software companies there is a propensity for users to subconsciously blindly trust the companies to ensure the security of mobile devices. This study sought to determine the

differences based on the training of 8 to 10 security professional and could present valuable information in educating automobile renters in proper sanitization procedures before returning the automobile. The population of interest was security professionals from the Cedar Rapids, Iowa area who had rented an automobile during the past 6 to 12 months.

Chen, Ramamurthy, and Wen (2015) found that effective security training directly influenced the culture of the organization and can change member attitudes and views towards security awareness. Given that the sample population also has industry-recognized security certifications understanding the behavioral changes from such certifications may add value. Hurst, Shone, El Rhalibi, Happe, Kotze, and Duncan (2017) explained that most security certifications do not focus on hands-on approaches. This study may present potential shortcomings in the traditionally accepted security certification. Understanding if security awareness training affects renters' behaviors when pairing smartphones to rental vehicles could present an opportunity to increase consumer security awareness. Further, the understanding the renters' behaviors and attitudes may discover similarities in behavior, which revealed areas for improvement.

## Research Questions

There were three primary research questions developed to understand the phenomenon of interest. Since this study is qualitative, the answers to these questions were narrative. Additional sub-questions exist to strengthen the research. The questions below are the primary research questions.

Research Question 1. How do the attitudes and behaviors differ among IT security professionals around Cedar Rapids, IA when presented the opportunity to pair a smartphone to an automobile?

Research Question 2. What effect do different professional backgrounds have on the security professionals' attitudes and behaviors?

Research Question 3. What similar behaviors and attitudes exist among the security professionals?

Chapters 4 and 5 provide a detailed explanation of the findings and conclusions and answers to the research questions.

## Propositions

This study sought to understand the effects of security awareness training and the behaviors exhibited when pairing a smartphone with a rental automobile. This study focused on asking respondents open-ended questions regarding actions taken when pairing a smartphone to a rental vehicle to examine what type of relationship existed between the security awareness training of the individual and the propensity to connect a smartphone to a rental vehicle. Further, as part of understanding the relationship, the questions sought to understand what security-conscious behaviors the individual exhibited when removing the smartphone from the rental automobile. Before data collection, this study suggested that the behaviors would exhibit variance depending upon the participant's receipt of security awareness training and the study sought to determine if this assumption was accurate.

## Conceptual Framework

Ellison et al. (2012) shared that connected vehicles convey the benefit of modern convenience but increase the threat of intrusion, which could result in PII data compromise. The PII data is either direct or is derivable from the combination of data that downloads from the user's mobile device at the time of pairing and stored in the automotive system's persistent storage. Engoulou, Bellaiche, Pierre, and Quintero (2014) explained that maintaining driver

privacy is a major concern and challenge with VANETs including vehicle locations, driving behaviors, and the individual's identity. Further, the VANET external connectivity could be an attack vector that a malicious actor could violate in efforts to gain unauthorized access to data stores resident on the target vehicle.

Individuals renting automobiles may not always be aware of the threats when pairing a smartphone with a rental car. SETA is commonplace across various industries intended to protect organizational data and assets but is less copious among consumers. Pfleeger and Caputo (2012) suggested that to address the human-centric security approach there must be an understanding of behavioral science and how to integrate it into all phases of technology. The conceptual framework provides a depiction of the phenomenon of interest and the topics and sub-topics, which surround the phenomenon providing clear boundaries to the scope of this research study.

## Assumptions/Biases

A few assumptions were surrounding this study. It was assumed that there would be individuals with security training that met the participation criteria to participate in the research study. Further, it was believed that the participants of the study would provide a complete and honest response to each of the questions found within the research instrument. General assumptions surrounding this study were that the researcher controlled personal bias, the completeness of interview recordings, and the accuracy of transcribed interviews. The personal biases were the expectation that individuals with security awareness training would exhibit different behaviors than those who did not receive such training, as well as the expectation that the individuals without training would answer the questions differently than those with the

training. To control these biases, the use of a question script for all interviews prevented the unintentional rewording of questions.

## Significance of the Study

This study provided an opportunity to further understand the effects of security awareness training on the behaviors and attitudes of the training recipients. Understanding if the training affected the individuals about security-conscious behaviors when pairing a smartphone to an automobile offered an opportunity to reflect on current security awareness training practices and the overall effectiveness. Further, it allowed the opportunity to view the area of security hygiene with automobile infotainment systems as an area for future security awareness training curriculum and training efforts.

This study could identify potential risks to rental vehicle companies. The realization of the inherent risks of residual personal information left on rental vehicles demonstrated the need for updating rental vehicle return check-in practices and policies. It could present the need for rental companies to verify that automobiles with Bluetooth capabilities received proper sanitization before re-issuance to a new renter, thus protecting the consumer from potential identity theft and the rental company from the liability of such theft.

This study may also find shortcomings in the benefit of security certifications. Industries such as defense and finance require security certifications such as the CompTIA Security+ and the $ISC^2$ Certified Information Systems Security Professional (CISSP). If the study finds behaviors or attitudes incongruent with security best practices, it could present an opportunity for revising such certifications to include more hands-on exercises.

## Delimitations

The research pursued in this study presented several delimiters. These delimiters include both population and geographic limitations. For this study, limiting the population to IT security professionals in the Cedar Rapids, Iowa area allowed for a more accessible population. Limiting the geographical region to Cedar Rapids, Iowa restricted the diversity of viewpoints. Limiting to this geographical subset allowed for gaining a clear view of the level of security awareness and security-related behaviors within the area.

## Limitations

The limitations of this study were the participant definition. The participants for this research study were security professionals with at least 1 year of experience and associated industry-recognized security certification. Further, the participant's definition of security awareness presented limitations to this study and constrained it to the preconceived understanding of the individual participants. Given a more diverse participant definition, a broader definition of security awareness may have emerged.

## Definition of Terms

The definitions of the following terms below aid in understanding the context of this study.

*Bluetooth:* The Bluetooth protocol is a short-range wireless protocol used for personal area networks (PANs) that operates at 2.4 GHz (Omar, 2012).

*Infotainment System:* An infotainment system provides a combination of information and entertainment that allows for user interaction and has common network services (Corbett et al., 2016).

*Mobile Device:* A mobile device is a portable computing device easily carried by an individual that possesses wireless transmission capabilities such as a smartphone (NIST, 2013).

*Personally Identifiable Information*: Personally identifiable information is any combination or singular piece of information which can be used to identify an individual and often used for identity theft (Rozenberg, 2012).

*Risk:* A risk is a measurement of the extent an entity threatened by the loss of confidentiality, integrity, or availability (NIST, 2013).

*Security Awareness Training*: Security awareness training is the process of making individuals aware of security-related objectives to develop a deeper commitment to them (Siponen, 2001).

*Security Control: A security control is* a safeguard applied to an information system to protect the confidentiality, integrity, and availability (NIST, 2013).

*Threat:* A threat is any circumstance that could lead to adverse impact on an information system (NIST, 2013).

*Vehicle Ad-hoc Network:* A vehicle ad-hoc network is a set of smart vehicles providing communications between automobiles and roadside units that utilize wireless network technologies (Engoulou et al., 2014).

*Vulnerability:* A vulnerability is a weakness in an information system or procedure that could be exploited by an adversary. (NIST, 2013)

## General Overview of the Research Design

The research design, which offers the greatest opportunity for exploring the phenomenon around this study, is exploratory research. Exploratory research is not as structured as other research designs. Lofland, Snow, Anderson, and Lofland (2005) shared that exploratory studies

aim at being lower key to allow participants to feel more comfortable which would prevent the participants from exhibiting inhibitions about the study.

Exploratory studies are part of the qualitative research method. Due to limited research surrounding the phenomenon of interest, a qualitative study may be most appropriate. This type of study aligns with a nascent research methodology. Edmondson and Mcmanus (2007) explained that in nascent research questions that produce a better understanding of how a process or set of actions occurs are key to developing the theory. Creswell (2013) explained that quantitative research seeks to test theories through the relationship between variables, and since this study seeks to explore the attitudes and behaviors of IT security professionals renting automobiles, quantitative or mixed methods would not be an appropriate fit.

For this study, the target population was IT security professionals from the Cedar Rapids, Iowa area. The target population is IT security professionals with a minimum of 1 year of professional experience and an industry relevant security certification. This study used a convenience sampling method to ensure that the target population received adequate representation to aid in finding the validity of the research questions. Chapter 3 of this study provides in-depth details of the research methodology and design.

## Summary of Chapter One

This chapter offered a synopsis of the proposed study sharing the topic overview, problem opportunity statement, purpose statement, and the research questions. This chapter also discussed the delimitations, limitations, research propositions, a summary of the theoretical framework, and study assumptions and biases relating to this study. Further, Chapter 1 defined relevant terms relating to this study, a high-level overview of the research design, and a summarization of the chapter.

## Organization of Dissertation

Chapter 1 provided introductory information into the proposed research study. Following Chapter 1, Chapter 2 detailed the review of existing literature and demonstrated the gap in the body of knowledge surrounding the topic of interest. Chapter 3 examined details of the of the research design. Chapter 3 explained the research methodology, research traditions and methods, detailed information about the population and sample, and the research instrumentation. Chapter 3 also included discussion explaining the data validity and reliability, as well as collection procedures, analysis procedures, and chapter summary. Chapter 4 shared the results of the study, presented the collected data, and a chapter summary. Chapter 5 presented the conclusions and findings, reflections, study implications, opportunities for further research, and the conclusion of the study. The following chapter examined the topics and concepts of attitude, behavior, security awareness training, personally identifiable information, Bluetooth security, Bluetooth vulnerabilities, and Vehicle Ad-hoc Networks to identify the gap in existing literature and the body of knowledge that generated the need for the proposed study.

# CHAPTER TWO

The topic of cyber security is extensive and significant research exists for many facets of cybersecurity. New reports of data breaches occur regularly, and Astani and Ready (2016) suggested that this trend is the result of security holes in the hardware and software currently developed. The following chapter discusses the current literature about the areas of Bluetooth security, Bluetooth vulnerabilities, Personally Identifiable Information (PII), Vehicle Ad-hoc Networks (VANETs), attitude and behavior theories, and Security Education Training and Awareness (SETA). The chapter also reviews the technology acceptance model (TAM). The discussion delivers clarity about a gap in the literature surrounding the question of how security awareness training affects the attitudes and behaviors of individuals in the Cedar Rapids, Iowa area when pairing a smartphone to a rental vehicle.

## Security Awareness Training

The purpose of Security Education Training and Awareness (SETA) is to change user behavior through various training methods and internalize security-aware actions. Siponen (2001) advocated that there are five dimensions of security awareness consisting of organizational, public, socio-political, institutional, and computer all of which need addressing to internalize security aware behaviors. The ensuing paragraphs discuss literature regarding current SETA research, driving factors for SETA, and gaps in the consumer dimension.

An individual's behaviors receive significant influence from the possessed training and awareness, and this is evident with information security as well. Alexandrou (2015) shared when medical professionals better understood the security risks of bringing your own device; there was a greater intention to adhere to organizational security controls. The study by Safa et al. (2015) discovered that an individual's security awareness had a notable effect on the security-related

behavior and attitude. Further, the study conducted by Mitra (2016) found that higher user response success resulted in greater behavioral intention to use mobile technology to alleviate security threats to personal data stored on mobile devices. The literature, however, does not adequately address the issues of security awareness training's effect on the behaviors of individuals renting automobiles and pairing smartphones and warrants additional research on the specific topic of interest.

SETA is a fundamental component in reducing cybersecurity risks, which involve addressing the human side of cybersecurity. Von Solms and van Niekerk (2013) suggested that humans are a significant threat, as well as a significant vulnerability to information systems. Given the explained risk that humans add to information systems, systematically modifying behavior to advocate security is at the core of proper security awareness training. Pfleeger and Caputo (2012) added to address a human-centric security approach an understanding of behavioral science and how to integrate it into all phases of the technology must be established, but can be difficult to identify. Further, information system users often lack an understanding of the consequences of poor security habits and risky behavior. Aubeterre, Iyer, and Singh (2009) expounded to include perceiving the security elements, and violations of the security elements is an important aspect of security awareness. The increased use of networked devices suggests a greater need for cybersecurity training. Tyagi (2016) stated that due to the connected nature of society, and the continuous use of the internet for personal and professional purposes, there is a greater need for cybersecurity education and training. Boyce et al. (2011) added that intentional or unintentional undermining of security of an information system is often the weakest link in securing information systems. The same unintentional security-undermining behaviors need further exploration in the area of pairing smartphones in rental automobiles.

SETA is often a requirement for employees but could benefit consumers also. Greene (2014) explicated that implementation of SETA can increase stewardship of information systems and aid policy acceptance. Strickland and Hunt (2005) explained that there is an overarching fear of information technologies, which collect information that suggests SETA could provide a better understanding. Siponen (2001) shared the purpose of addressing the general public concerning security related issues is to increase awareness of central issues like viruses and malware. Stanciu and Tinca (2016) suggested that users may have a certain level of technical knowledge, but there is a gap of knowledge regarding information security resulting in the manifest necessity for increased security awareness and behavior training such as a formal information security awareness program.

The continued increase of dependency on mobile technology warrants the need for more robust security awareness and training. Hines (2015) shared that individual have a propensity to discard compliance and best practices for ease of use that can increase opportunity for security incidents. Mensch (2015) added that the need for proper physical and digital security has not matched the continued increased dependence on mobile devices. As part of the means to bridge the training and dependency gap, McCormac et al. (2016) explicated that security awareness training should be individualized to match learning styles as a mechanism to raise internalization of security training. Furthermore, investment needs to be made in awareness because adding this competence will increase overall security awareness (Asplund & Nadjm-Tehrani, 2016). Goyal Chin, Etudo, and Harris (2016) found in their study that the provision of general security training based on the self-determination theory proved to be unsuccessful among the testing population. McCormac et al. (2016) added that factors such as personality, risk proclivity, emotional well-being and diligence resulted in significant variance in participants' information security

awareness. Further, Liu (2015) found that employees at the studied organization, although receiving similar training, each observed a specific area of information security as the most important.

Significant research exists in understanding the areas of training influence and comprehension regarding current security awareness training practices. Hayani Abd Rahim, Hamid, Mat Kiah, Shamshirband, and Furnell (2015) suggested that proper categorization of users ensures appropriate security training delivery to the individuals. Chen et al., (2015) suggested a model centering around changing attitudes, perceptions, and beliefs of security as a key component of employee security awareness training while Bada and Sasse (2014) presented the need for both implicit and explicit knowledge in the development of security awareness training. Also, McCrohan, Engel, and Harvey (2010) found that providing highly informational training influenced the password habits of the study participants. Further, Choi and Lee (2015) proposed a training methodology that detects policy violations and uses the violations to change the security awareness of individuals positively. The lack of clear consumer training methodologies further exposes the gap in the literature regarding SETA and consumers who are renting automobiles and connecting smartphones to the rental vehicle.

## Attitude and Behavior

Attitude and behavior are two closely related theories. Allport (1935) explained there is a myriad of attitudes relating to social values and several potential values for a given attitude. The following sections and paragraphs discuss literature surrounding attitudes and behavior theories. The theories discussed include the theory of reasoned action, the theory of planned behavior, and protection motivation theory and the relationship to security-related behaviors.

## Attitude

Attitude contributes to the security behaviors individuals carry out and provide meaningful data about an individual's underlying perceptions. Allport (1935) stated that attitude is the operation of the mind by which individuals dictate possible and veritable responses that the individual directs at a recipient object. As attitude theory matured, Ajzen and Fishbein (1969) shared that the expected behavior to execute a defined behavioral act is predictable by observing an individual's attitude and beliefs about the act. Further, Ajzen and Fishbein (1977) posited that attitude predictions are identical to the behavior criteria based on the elements of the action to be carried out, the time of performance, the context of the act, and the target of the deed. Attitudes are integral to perceptions of all aspects of life, and information security is just one of those areas. Further understanding users' attitudes and perceptions surrounding the potential security impacts of connecting mobile devices via Bluetooth to rental vehicles is just one area warranting additional research.

There exists a significant amount of prior research regarding the effects of attitude on information security behavior. The attitudes of users' demonstrate positive changes resulting from the inclusion of security awareness training. Anzaldua (2016) demonstrated a positive change in security attitude and perception of risk among the test subjects after receiving security awareness training. Further, research by Da Veiga (2016) explained understanding security specific policies is necessary because if it is not understood, there is no effect on the individual's security-related attitudes and behaviors. Existing models of understanding security related attitudes demonstrated deviations in the overall attitudinal changes of people. Egelman and Peer (2016) suggested that predicting a person's attitudes towards privacy preferences based on the five-factor model is inadequate, contrary to prior literature.

The attitudes of individuals provide tremendous influence on the decided behaviors and actions taken by the individuals. Fishbein and Ajzen (1972) suggested an individual's intentions and behaviors determine attitude, and there is strong evidence for a significant relationship between a set of intentions and attitude. The relationship between intentions and attitude manifests itself in the field of information security. Pattinson, Parsons, Butavicius, McCormac, and Calic (2016) demonstrated that there are significant complexities in the measurement of information security related attitudes and a continued need for attitude research to reduce risk-inclined behaviors among individuals. An example of such complexity exists in the study conducted by Shropshire, Warkentin, and Sharma (2015) showed there was the significant intention of adoption which predicted initial use while fewer than 25% of the measured population carried out their intentions. Further, Dang-Pham, Pittayachawan, and Bruno (2016) suggested that depending on the type of interpersonal networks a person is involved in will drive the most efficient mechanism to present security training and modify the individual's attitude.

Other research suggests that using different inputs to influence an individual's behavior can affect the person's attitude such as a fear appeal. Johnston and Warkentin (2015) suggested a departure from conventional fear appeals mechanisms such as protection motivation theory (PMT) for informal sanctions approach providing reminders to users to change behavior. Also, Boss, Galletta, Lowry, Moody, and Polak (2015) suggested that by measuring both information security intentions and behaviors, increased clarity illuminates the path from one's intentions to behavior relating to situations of high fear appeal. Further, Yoon, Hwang, and Kim (2012) demonstrated that students attitudes and behaviors were not impacted by regular information security training but would benefit more from a PMT approach of exposure to the severity of losses resultant from security negligence to influence behavior. The current research regarding

fear appeal applies to organizational information security but does not extend to consumer information security awareness.

**Behavior**

Behavioral theories provide valuable insights into the driving forces behind individual actions and the variations seen between different entities. Ajzen and Fishbein (1973) suggested an individual's attitude towards the act and the product of the motivation to obey and normative ideologies determines an individual's behavioral intent. One imperative behavioral theory is the Theory of Planned Behavior. Ajzen (1985) explained that according to the theory of planned behavior an individual will venture to execute a specific behavior if the perceived advantages of success are greater than the benefits of failing. Further, Foltz, Newkirk, and Schwager (2016) found that behavior regarding individuals' social networking privacy and security settings positively changed in the majority of the constructs used in the experiment which relied on the theory of planned behavior as the fundamental framework. Such theory has produced alternative theories such as the Protection Motivation Theory (PMT).

The premise of the protection motivation theory suggests that if an event is likely to occur and is considered harmful and the mitigating action is effective at preventing the event the behavior will change as stated by Rogers (1975). Several researchers have applied the theory to information security. Posey, Roberts, and Lowry (2015) explained that an individual receives information about security threats using PMT, but PMT can also explain how to mitigate such threats. Further, Sommestad, Karlzén, and Hallberg (2017) concluded that the use of variables in the threat appraisal process of the PMT could enhance information security policy compliance when using the theory of planned behavior as the primary theory. Warkentin, Walden, Johnston, and William Straub (2016) suggested that providing security training focusing on the desired

behavior instead of threats or fear tactics produced better protection behavior due to the recipients' perceptions of self-adequacy.

Information security is one area in which behavioral theory explains the actions of system users. Das and Khan (2016) found that the recognized effectiveness of security responses and the financial burden of adoption were consistent predictors of smartphone security behavior. Understanding drivers influencing the security behaviors of users' possesses the potential to better influence user behavior to align with security best practices. Further, Simpson (2016) explained that self-sufficiency has a likely consequence on individuals using smartphones and the associated security attitudes and conduct. Additional research by Ngoqo and Flowerday (2015) established that a student's knowledge of information security produced no significant changes in the student's attitude towards information security and security appropriate behavior. Findings made by Humaidi and Balakrishnan (2015) suggested that an individual's behavior regarding security is directly related to how they perceive the security threat or risk. Accurately communicating the severity of security risks and potential consequences of compromise may affect change in user behavior. Sohrabi Safa, von Solms, and Futcher (2016) added that conscious care behavior, meaning that individuals consider the ramifications of the security-related behaviors, is an efficient means of minimizing careless or risky information security behaviors. Changing the users' behavior based on positive reinforcement poses the potential for positive behavioral change. Kegel and Wieringa (2015) added that a behavior change support system could benefit user security and privacy by observing the user's actions over time and adjust the preferences based on their risk acceptance levels. Throughout the literature, however, no discussion occurs regarding behaviors of consumers pairing smartphones to rental automobiles.

## Personally Identifiable Information

Personally Identifiable Information (PII) was previously considered to be items such as tax identification, health records or financial records. Recently, malicious individuals and groups achieved re-identifying data from secondary sources such as phone numbers. Rubinstein and Hartzog (2016) postulated that ensuring continuity in the protection of PII is challenging, but guaranteeing that the individuals handling the data sanitize such data properly results from combining administrative tools and policies. Further, Wall, Lowry, and Barlow (2016) found that increased use of technology across industries like healthcare and payment card along with scandals in the financial services sector bring clarity to the need to comply with privacy and security rules. The following paragraphs discuss current research surrounding PII, security challenges, and the varying definitions.

PII is considered to be information that can be used to identify an individual uniquely. Chellappa and Sin (2005) explained a major difference between offline, and online privacy is the concern that any transaction completed electronically leaves trace data behind which can then be used to create a somewhat accurate understanding of the individual. Cooper (2014) described PII as including names, phone numbers, social security numbers, and addresses. Rozenberg (2012) adds that PII is any combination or a unique piece of information that can be used to identify an individual and malicious actors often use it for identity theft. Griffin (2014) included that biometrics can be used to verify an individual's identity by comparing it to the user provided biometric reference data. Krishnan and Vorobyov (2015) further clarified that many consumer businesses do not define what is considered to be personally identifiable information.

The theft of PII continues to be a growing cybersecurity threat. Rozenberg (2012) shared that breaches of individual's PII have become a costly action over the past few years and has had

a widespread negative impact on organizations and individuals. Knight and Saxby (2014) added that identity theft-related crimes have become a significant problem on the global scale since the turn of the millennium. Rental automobiles present the possibility of storing substantial amounts of PII, which would be valuable to cybercriminals. Cates (2015) shared that malicious actors continuously look to steal PII, credit card information, and other types of legally protected information and seek to sell the data to other criminals. Understanding how attitudes of automobile renters affect the propensity to attach mobile devices to automobiles and how they handle returning the vehicle provides an opportunity to contribute to current literature regarding the security of PII in the mobile environment.

Increased data gathering continues to cause greater exposure of PII, further increasing the opportunities for PII theft. Weber (2015) explained that PII gathering occurs through the use of different internet of things devices; included in this is behavioral patterns collected through the activities in our daily lives. Ellison et al. (2012) added that personally identifiable and privacy-related information is being gathered via networked vehicles, and consumers have no control over the collection and have no idea who consumes this information and what the intent of the usage is. Lacking awareness of such data gathering techniques presents the need for further exploring the effects of security awareness training on the behaviors of vehicle renters on pairing smartphones.

Securing PII becomes the challenge. Li et al. (2015) conducted a study suggesting that incorporating virtualization technology provides better security, and the result presents themselves in the automobile industry. Another suggestion is implementing additional cryptographic methods in adding security and maintaining the confidentiality of personally identifiable information on motor vehicles. Nguyen, Laurent, and Oualha (2015) suggested the

use of a zero-knowledge proof system where the provider must demonstrate knowledge of the secret to the verifier, without exposing any part of the secret to the verifier. Koscher (2014) developed a virtualized system to conduct dynamic analysis to secure embedded systems, further demonstrating the utility of virtualization as a component of securing PII.

Maintaining the privacy of PII is a task, which receives significant research and organizational backing in business. Krishnan and Vorobyov (2015) developed a privacy maintaining protocol, which combined the analysis of system behavior and access control restrictions to maintain the privacy of PII of healthcare-related information. Further, Nguyen, Laurent, and Oualha (2015) explained that protecting private data in transit in a network of things uses lightweight protocols to compensate for lessened processing power but does not speak to the issue of securing the data at rest such as in an automobile. Knight and Saxby (2014) added that the increased amount of data available online combined with the growing capabilities to access such data makes it possible to connect formerly discrete elements of identity in new methods, further threatening the protection of PII. Von Solms and van Niekerk (2013) further suggested that increases in technology such as home automation and the Internet of Things (IoT) increase the risks to cybersecurity, which includes unauthorized exposure or compromise of PII.

Mobility increases the inherent risks of compromising an individual's PII when compared to the standard forms of holding such data. Fisher and Allen (2015) explicated that the compromise of sensitive data often occurs unintentionally by traveling individuals through misplaced tablets or lost cell phones. There is no discussion about the potential for PII leakage via pairing a smartphone to a rental automobile in current research, however. Another facet of mobility discussing PII protection is big data. Allen (2016) explained that although protecting PII is the individual's responsibility, the proliferation of big data needs a collective approach to

PII protection. The use of vehicle ad-hoc networks presents an avenue through which big data collection gathers large amounts of information, some of which could be PII or other sensitive driver information.

## Vehicle Area Networks

Vehicle Ad-hoc Networks (VANETs) consists of multiple functions ranging from traffic reporting and automatic toll payment to improving navigation and location services. Karumanchi, Squicciarini, and Lin (2015) explained that VANETs allow automobiles to communicate with each other, roadside units, and act as network nodes to publish messages between the roadside units and other vehicles. The next paragraphs review the literature relating to VANETs, security issues surrounding VANETS, and current security controls.

VANETs continue to expand as new technology incorporates into vehicles regularly. Engoulou et al., (2014) explained that VANETs provide benefits to automobile users through adding features to incorporate safety, convenience, and entertainment. The added convenience and safety does not come without risks to the privacy of the automobile users, however. Mastakar (2012) added that automobiles are no longer mechanical devices but have become highly technological devices containing many computers, each doing a role in the vehicle.

The introduction of VANETs and other mobile-to-mobile communications has introduced security gaps. Kumar et al. (2016) stated that the use of different devices in mobile-to-mobile communications introduces challenges due to the incorporation of various technologies, which compounds challenges of enabling secure communications and identification of individual appliances. As such, providing the confidentiality of personal data on vehicles becomes an increased challenge and further presents the vulnerabilities and threats to properly securing vehicle-borne PII and sensitive information. Ellison et al. (2012) added that

there is an alarming risk of attack or disruption to the network communications with the networked devices without a built-in trusted infrastructure for networked devices. Sicari, Rizzardi, Grieco, and Coen-Porisini (2014) shared that common security mechanism, and enforcement methods are not applicable to the internet of things devices, to include VANETs, because of the limitations in computational power. Security gaps such as mentioned above lead to additional concerns with individual privacy and security, further presenting the opportunity to determine impacts from security awareness training on the user behaviors in the IoT or VANET environments.

Security and privacy concerns are a key issue with consumers and automobile users. Ying, Makrakis, and Mouftah (2012) shared security and confidentiality are important points to address in-vehicle networks because automobile users wish to preserve their privacy of information such as location, identity, and direction of travel. Ellison et al. (2012) added that gathering of personally identifiable and privacy-related information via networked vehicles occurs regularly, and consumers have no control over the collection and have no idea who receives the information and what the intent of the usage is. The implications of VANET data breaches is greater than the local incident. Hiller and Russell (2013) explicated that on the larger scale, attacks on an individual sector or product can have global implications because of the interconnected network, which connects these devices. Such security concerns aggregate a need to develop a model specific for the internet of things devices.

Security models have been developed to address the security needs of VANETs and mobile-to-mobile networks. Ying, Makrakis, and Mouftah (2012) explained enabling sufficient message authentication and maintaining privacy is a necessity for enabling security on automobile applications. A component of the privacy maintenance is the proper security around

the data stored on the infotainment systems that contain the data downloaded from the mobile device connected to the vehicle. Engoulou et al. (2014) stated maintaining driver privacy is a major concern and challenge with VANETs. Driver privacy includes vehicle locations, driving behaviors, and the individual's identity, which may be direct or indirect, derived from a combination of data such as phone numbers, phone information, or other available data. Kumar and Vaid (2015) described an architecture where message digests verify authenticity while reducing the size of packets on the network to prevent unnecessary network congestion. Including additional research about maintaining the confidentiality of the PII on VANETs presents the opportunity for the proposed research.

The advent of more advanced mobile malware creates a potential for increased VANET susceptibility. Lu, Wang, and Wang (2015) demonstrated that malware could propagate via mobile devices on Wi-Fi and Bluetooth networks, exponentially increasing the potential for Denial of Service (DoS) attacks because of the mobile botnet. Further, Fernandez Ruiz, Hidalgo, Nieto Guerra, and Gomez Skarmeta (2015) recommended the use of WiMAX and Wi-Fi as the backbone for VANET base stations. This further increases the ability for mobile malware to propagate across such networks and potentially compromise PII on automotive systems, which received no discussion within current literature.

## Bluetooth

Sengupta and Sarkar (2015) explained that over the course of the past several years Bluetooth had become widely accepted as the protocol for connecting auxiliary devices to smartphones, connecting home entertainment systems, and conducting ad-hoc file sharing. Onishi, Wu, Yoshida, and Kato (2017) explained that since the Bluetooth interface enables connectivity between carry-on devices and automobile systems creates a potential exposure of

personal data such as vehicle health monitoring, personal calendars, and address books, and vehicle diagnostic systems. Cheah et al., (2017) discovered that the most common use of Bluetooth in automobiles is for hands-free calling which involves synchronizing the device's phonebook using the Phone Book Access Profile (PBAP), which holds personal information. Further, with some manipulation, a rogue connection could manipulate the PBAP to extract personal information about other devices' profiles, Cheah et al. (2017) explained. The following section reviews the literature relating to Bluetooth security and vulnerabilities. It looks at current security research around Bluetooth connectivity, and the Internet of Things (IoT) as well as smartphones and how the different vulnerabilities threaten user privacy and data.

**Bluetooth Security**

Bluetooth connected devices provide a convenient way of providing short-range connectivity between Bluetooth enabled devices. Hines (2015) posited that connecting devices via Bluetooth is becoming an increasingly popular way to connect devices. The ease of Bluetooth connectivity reveals potential security problems. Cooper (2014) explained that smartphones, having become part of an individual, does not come preset with security in mind and requires the intervention of the individual to apply the appropriate security settings, which often is not realized by the individual. Further, Zhou (2015) suggested that smartphone privacy and security become increasingly important as this technology is further augmented into every facet of life and the vulnerabilities present on smartphones make the technology susceptible to sensitive and personal information theft by malicious actors. Dardanelli et al. (2013) shared incorporating external device communications with vehicles increases the attack surface of vehicles and can result in greater risk of attack.

Embedded systems often include the ability to connect via Bluetooth due to the limitations in computing power. Fournaris and Sklavos (2014) explained embedded systems have different specifications that result in a more restrictive system when compared to a full computer system. Securing Bluetooth connections have distinct challenges relating to the mobility of the devices. Bhabad and Bagade (2015) suggested that the ease of connecting and disconnecting devices, often with no authentication, increases the risks of malicious code injection into the network. Kaur and Jain (2013) shared that current Bluetooth architectures require a trust relationship between Bluetooth devices to allow for the exchange of data without being prompted for permission, which contradicts the previous statement of Bhabad and Bagade. Further, Coney (2015) suggested the establishment of a common architecture for privacy and security-related controls which would support the end users' ability to use the controls while supporting the capability to recognize different types of devices and technologies.

The security of Bluetooth connections is important in efforts to maintain the confidentiality of mobile device users. Onishi, Wu, Yoshida, and Kato (2017) explained that Bluetooth connections between mobile devices and automobiles create potential pathways for malware injection into automotive systems. Evaluating the existing security controls of Bluetooth reveals the susceptibility to various attacks. Mozzaquatro, Jardim-Goncalves, Melo, and Agostinho (2016) added that networks of this type are particularly susceptible to cybersecurity threats and proper security strategies are necessary. Further, Yadav, Bose, Bhange, and Kapoor (2016) explained intercepting the phone's MAC address is a method of an attacker gaining access to the vehicle network. Vulnerabilities, such as intercepting the MAC address receive a further explanation in the following section.

**Bluetooth Vulnerabilities**

Bluetooth, although a cheap and popular networking technology, allows for several vulnerabilities. Ibn Minar and Tarique (2012) explained despite its popularity; Bluetooth contains security gaps that make the protocol vulnerable to attacks. Lee and Kang (2015) explained that the majority of the threats to mobile devices target the individual's data and pairing a smartphone to the automobile provides an additional attack surface, which contains some of the personal data. Vulnerabilities can result in an attacker gaining access to connected devices. Yadav, Bose, Bhange, and Kapoor (2016) explained that intercepting the phone's Bluetooth MAC address is a method of an attacker gaining access to the vehicle network. By intercepting the Bluetooth MAC, the attacker gains the ability to spoof the MAC and automatically reconnect via Bluetooth to the automobile, thus gaining unauthorized access to the data stores on the motor vehicle's infotainment systems. Similarly, Sengupta and Sarkar (2015) described a denial of service (DoS) attack where the malicious Bluetooth device spoofs as the desired connection point preventing a legitimate connection and denying the user connectivity. Achieving this false connection Andrejevic and Burdon (2014) explained could allow for extraction of personal information which could be used maliciously by an adversarial actor.

The vulnerabilities exposed by Bluetooth connections bear the potential for amplification when in the context of automobiles. Hoppe, Kiltz, and Dittmann (2011) explained that security related issues and possible attacks have a greater impact on automotive information technology because it can not only breach sensitive data but can also result in a compromise of passenger safety if the system compromise occurs. Mastakar (2012) added the combination of the various interconnected vehicle computer systems provide the platform for access to the external network which further exemplifies the need to reevaluate the computer security requirements of vehicles.

Gaining a better understanding of the potential security and confidentiality impacts regarding data stored on automotive systems resulting from connecting mobile devices through Bluetooth advocates the current research surrounding the renters' attitudes towards connecting the devices and the effects of appropriate security awareness training.

Bluetooth vulnerabilities often result from the unpatched firmware. Kaur and Jain (2013) explained an attacker could exploit a vulnerability in older Bluetooth firmware, which is known as Bluesnarfing. Additional attacks exist for the Bluetooth protocol, each exploiting different vulnerabilities and requiring various levels of experience. Qu and Chan (2016) added that other well-known Bluetooth attacks include Bluebugging, Blueprinting, Bluejacking, and Bluesniffing. To further the impact of such vulnerabilities are threats of mobile malware capable of hijacking mobile devices. Wibowo and Ali (2016) suggested that the relentlessly increased dependence on mobile technologies such as smartphones and tablets is driving malicious actors to target mobile devices more often for exploiting via malicious code. The increases in mobile device dependence present the need for better security awareness of mobile users and the possible consequences of connecting devices to automobiles, or other devices present in the user's environment. Further, Popescul and Radu (2016) suggested that in scenarios such as smart cities which use multiple wireless protocols, including Bluetooth, a compromise of the security of one device quickly propagates across the entire system due to the constant interconnections further showing potential vulnerabilities within Bluetooth networks. There is a lack of studies incorporating the risks to automobile-borne personally identifiable information resulting from Bluetooth vulnerabilities, however.

## Technology Acceptance Model

The technology acceptance model (TAM) intended to determine user motivation factors leading to the actual system use. Davis, (1985) explained that the TAM consisted of the inputs of design features which led to cognitive responses, followed by affective responses, and concluded with the behavioral response of system use. Davis (1985) added that the perceived ease of use would significantly affect the perceived usefulness that occurred during the cognitive response. Further, Davis (1993) explained that the actual system usefulness is more important than only the perceived ease.

Past researchers applied the TAM to various different scenarios, such as with students or gender mobile shopping behaviors, to determine usefulness and user acceptance of technology. Nikou and Economides (2017) found that students exhibited a greater willingness to participate in mobile device-based assessments when the system was perceived to be easy to use and seemed useful. Faqih and Jaradat (2015) shared similar findings relating to mobile commerce suggesting that individuals would only use m-commerce if it were convenient and perceived as useful. Further, Fathema, Shannon, and Ross (2015) found that system quality positively affected perceived usefulness and perceived ease of use for learning management systems. Another study focused on education systems showed similar results. Wu and Chen (2017) found that individuals would be more likely to view a Massive Open Online Course (MOOC) as useful if the MOOC is viewed as easy to use. Many studies discussed the application of TAM to education and commerce, but no recent studies applied TAM to the behaviors of security professionals and pairing smartphones with automobiles.

## Conceptual Framework

Personally Identifiable Information (PII) is a key target for hackers because of the value associated with the information. Increased computing capabilities and reduced component sizes have led to technological revolutions such as the Internet of Things (IoT) which has enabled the proliferation of PII across many devices such as automobiles. Ellison et al. (2012) shared that connected vehicles convey the benefit of modern convenience but increase the threat of intrusion, which could result in PII data compromise. The PII data is either direct or is derivable from the combination of data that downloads from the user's mobile device at the time of pairing and stored in the automotive system's persistent storage. Securing the PII on the persistent storage is paramount in maintaining the confidentiality of the users' data and prevention of misuse by unauthorized individuals.

Specific challenges arise in protecting PII when such information is vehicle-borne. Engoulou et al., (2014) explained that maintaining driver privacy is a major concern and challenge with VANETs including vehicle locations, driving behaviors, and the individual's identity. The increased vulnerability exists from the VANET connection, providing an exfiltration path through external connectivity, and the use of the automobile Bluetooth, which may have weak security controls or unmitigated vulnerabilities unknown to the unaware consumer using the connection for convenience. Further, the VANET external connectivity could be an attack vector that a malicious actor could violate in efforts to gain unauthorized access to data stores resident on the target vehicle.

Individuals renting automobiles may not always be aware of the threats when pairing a smartphone with a rental car. The process of pairing the smartphone allows for the consumer's personal information to download into the automobile's storage increasing the chances of leaving

PII on the motor vehicle. The TAM provides a means of determining the likelihood of a renter to connect a smartphone to a rental automobile based on the perceived usefulness and ease of use of the infotainment system. Davis (1993) suggested that the perceived usefulness of the system hinges on the increased performance gain and associated rewards; in the case of this study, it would be the benefits gained from using the embedded features of pairing the device to the vehicle. SETA is commonplace across various industries intended to protect organizational data and assets but is less abundant with consumers. Pfleeger and Caputo (2012) suggested that to address the human-centric security approach there must be an understanding of behavioral science and how to integrate it into all phases of technology. Understanding the differences in behavior of individuals who have received SETA compared to those who have not could provide vital insights into the need for more consumer-based SETA in the area of renting automobiles. Further, the gained understanding provides an opportunity to address current business practices of automobile rental companies and the associated return policies to ensure proper data erasure upon reinstatement of the car. The conceptual framework below provides a depiction of the phenomenon of interest and the topics and sub-topics, which surround the phenomenon.

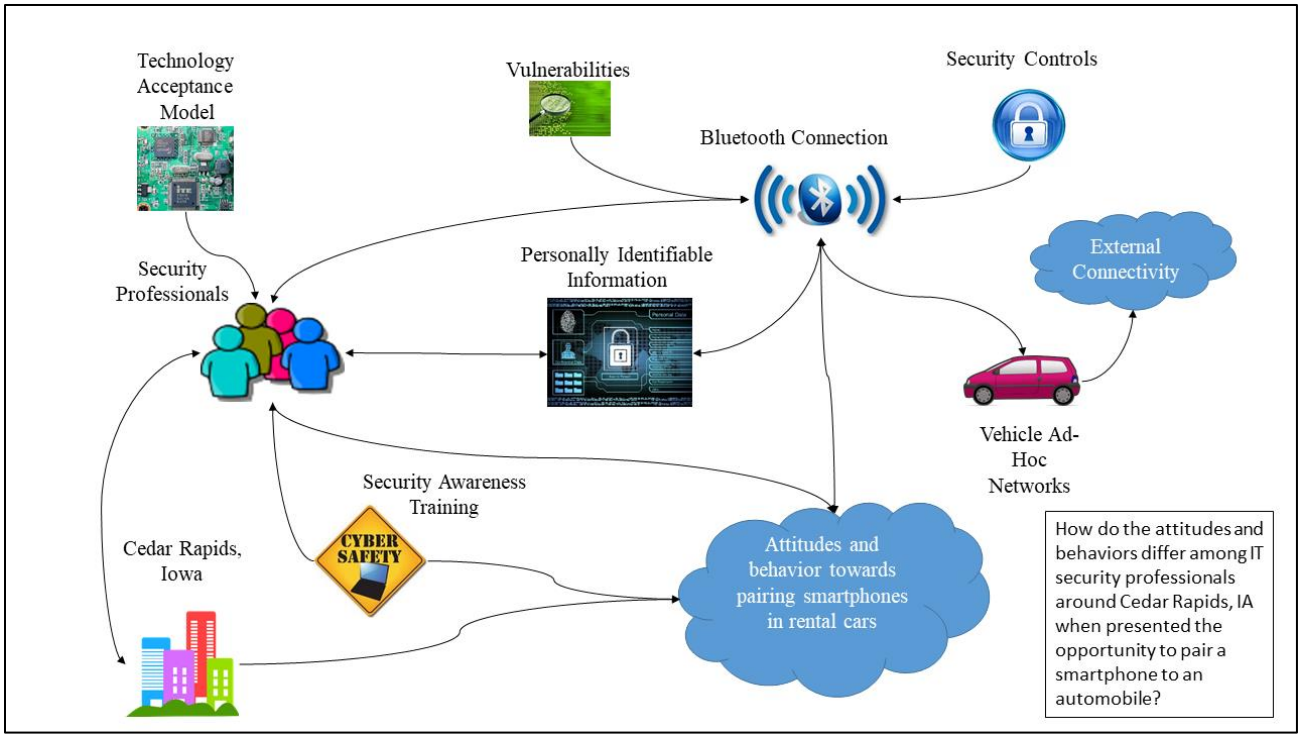


*Figure 1.* Conceptual framework

## Summary of Literature Review

There are many areas of cybersecurity previously researched by multiple individuals across a profusion of subtopics. The previous sections discussed the current literature regarding Bluetooth, PII, VANETs, attitude and behavior theory, TAM, and SETA. Review of the literature provided insights into the present state of research from both the theoretical and application perspectives. These sections also identified the gaps in the contemporary literature regarding how SETA affects the attitudes of renter's and if they pair a smartphone to the rental vehicle. Further, this section identified the gap surrounding the behaviors of renter's dependent upon the level of security awareness further presenting the opportunity for research and expanding the existing body of knowledge. In Chapter 3, the proposed qualitative research method develops the process for conducting the study that examines renters' behaviors regarding

pairing a smartphone to a rental vehicle dependent upon the renter's level of security awareness training.

# CHAPTER THREE

The proposed study seeks to answer the question of how attitudes and behaviors differ between automobile renters from Cedar Rapids when pairing a smartphone via Bluetooth depending if the renter received prior security awareness training. The purpose of the proposed study qualitatively examines effects of the security awareness training to determine if it changes security relevant behaviors with pairing smartphones and the associated personal information that transfers to the rental vehicle. Understanding the influences of security awareness on the behaviors of security professionals presents the opportunity to advise rental car companies on updating return procedures to include the sanitization of the infotainment system, as well as develop a means of making consumers aware of the security risks involved with connecting a smartphone to a rental automobile. The following sections further explore the research tradition, research method, target population, sample size, sampling procedure, permission requirements, proposed research instrument, and trustworthiness and credibility.

## Research Tradition

The research topic of how security awareness training influences IT security professionals who use rental vehicles attitudes and behaviors is a topic for which there is little or no earlier research. Such research aligns with applying a nascent methodology for research tradition determination. Edmondson and Mcmanus (2007) explained that in nascent research questions that produce a better understanding of how a process or set of actions occurs are key to developing the theory. Creswell (2013) explained that quantitative research seeks to test theories through the relationship between variables, and since this study seeks to explore the attitudes and behaviors of IT security professionals renting automobiles, quantitative or mixed methods would not be an appropriate fit. Further, since there is no formal hypothesis testing as is common with

a mature research paradigm, quantitative methods or mixed methods would not be appropriate, according to Edmondson and Mcmanus (2007).

The research tradition that offers the greatest opportunity for exploration of this study is exploratory research. Nelson and Martin (2013) explained that exploratory research reviews a single case and seeks to provide insights into a particular issue, and by doing so further understand a larger issue. Creswell and Poth (2017) explained that bounding the scope of a study is consistent with exploratory design. It demonstrates how the proposed study is a suitable selection for an exploratory research study as it seeks to explore the behaviors of security professionals when presented with the opportunity to connect a smartphone to an automobile for the first time.

A qualitative approach is the best methodological fit to aid in the exploration of attitudes and behaviors of IT security professionals when presented the opportunity of pairing smartphones to rental vehicles. The use of qualitative methods allows for better understanding the security behaviors of IT security professionals in a natural setting. Pope and Mays (1995) posited that using qualitative methods allows the researcher to acquire the understanding of the phenomenon of interest by focusing on the experiences, viewpoints and perceived meanings of the research participants. Further, King, Keohane, and Verba (1994) explained that qualitative research allows for many different approaches, often uses intensive interviews focusing on specific topics, and seeks to provide an all-inclusive interpretation of the specific topic. In the case of this research study, the ideal method of data collection is through the use of intensive interviews to gain a thorough understanding of the renters' behaviors when pairing smartphones to the rental automobile. Lofland, Snow, Anderson, and Lofland (2005) defined intensive interviewing as the process of both listening to the ordinary conversation as it occurs under

normal circumstances and using semi-structured interviews where the research asks open-ended questions to allow the participant to deliver a detailed answer instead of a simple yes or no or other pre-defined response.

## Research Questions

There are three primary research questions developed to understand the phenomenon of interest. Since this study is qualitative, the answers to these questions were narrative. The following research questions will be the focus of the proposed study.

Research Question 1. How do the attitudes and behaviors differ among IT security professionals around Cedar Rapids, IA when presented the opportunity to pair a smartphone to an automobile?

Research Question 2. What effect do different professional backgrounds have on the security professionals' attitudes and behaviors?

Research Question 3. What similar behaviors and attitudes exist among the security professionals?

Chapters 4 and 5 provide a detailed explanation of the findings and conclusions and answers to the research questions.

## Research Design

Automotive information system security is an area that will take many years to fully develop, according to Yadav et al. (2016). This study seeks to explore the attitudes and behaviors of security professionals when presented the opportunity to pair a smartphone with an automobile. Using direct observation and semi-structured interviews allow for the opportunity to witness the behaviors when pairing a smartphone and gather qualitative information from the interviews. The research process starts with the observation of the participant when pairing a

smartphone with an automotive infotainment system. The observations utilized the same automobile for all participants to ensure that all participants experienced similar interactions from the perspective of the user interface. Further, the participants had the option of using the same Android smartphone loaded with fake contacts to prevent the need for the participant to connect a personal device. Immediately following the observation was the participant interview.

An audio recorder captured the interactions during the observations and interviews. The interview and observation data were placed in the centralized location on the laptop to allow for further analysis. IBM Watson provided an initial transcription of the audio files. After the initial transcription, the files received further verification to ensure accurate transcription. The data was then coded to allow for further analysis. Further, the codes provided a means of determining the themes present in the research.

**Population and Sample**

For this study, the target population will be security professionals from the Cedar Rapids, IA area. The target population of security professionals will have a minimum of 3 years of professional experience and professional certification to demonstrate their security understanding. This study seeks to use a purposive sampling method to ensure that both sub-groups of the target population received adequate representation to aid in finding the validity of the research questions.

The population of Cedar Rapids is estimated to be 130,405 as of 2015 according to U.S. Census Bureau (n.d.). According to U.S. Census Bureau (n.d.) 15% or 19,500 individuals of the population of Cedar Rapids works in professional or management occupations. For this study, sampling occurs among the security professionals in the Cedar Rapids area, to include Iowa City, which is less than 20 miles away.

The sample size for the proposed study is 10 - 12 security professionals that meet the criteria previously described. The sample size is adequate due to the subpopulation being from the same professional background, and likely show similar behaviors. According to Boddy (2016), the small sample sizes work when the target population have a common method of doing things and can lead to the proper representation of the behaviors or actions of the larger group.

**Sampling Procedure**

The specific type of convenience sampling used is a purposive sampling method. Tongco (2007) explained that purposive sampling is applicable for the study of aspects of knowledge that are not known by all individuals since there are individuals within every culture which know more than the average member of that culture. In the case of this study, the knowledge aspects are automobile renters and the renters with greater security awareness training and knowledge.

Selection of 10-12 participants from the two categories within the population occurs using the convenience sampling method. Choosing the participants for the two categories results from inquiring with the individuals about the amount of business travel and frequencies of renting motor vehicles during the periods of business travel. Further, the selected participant level of security awareness training influenced the acceptance and use of the participants for this study, thus aligning with a purposive sampling method.

**Instrumentation**

The research instrument used for this study is a semi-structured interview process consisting of several open-ended questions surrounding the phenomena of interest, and some basic demographic questions to allow for further categorization. The questions presented in Appendix A contains the questions asked to each participant during the interview process.

The use of the questions in Appendix A shows the interview protocol used in this study. Depending upon the answers offered during the interviews, asking more probing questions may occur ad-hoc. In the instance of more questions, offering prior interviewees the opportunity to answer the questions ensured uniformity across the participants and the added questions noted in the findings section of Chapter 4.

**Validity**

Validity is an important aspect of qualitative studies. This study addresses the dependability, credibility, transferability, and confirmability of the results and study design to confirm the study's validity. The following paragraph outlines how each of this study handled the previously mentioned items.

The methods outlined in this chapter offer proficient detail for an external party to conduct the study on a similar sample group. Ensuring dependability and credibility results from keeping an adequate audit trail of the activities of the research study, including the events of the interviews and the steps of the data analysis. Similarly, the confirmability and transferability result from the detailed data collection and analysis procedures outlined in this chapter, which give other researchers a means of repeating the study in different populations, and the theory that supplements the results is pertinent to other populations for conducting follow-on studies.

**Reliability**

The trustworthiness and credibility of the study rely on proper data analysis techniques used by the researcher after data collection. Depending on the type of research method, there exist various techniques for use. The following paragraphs show the techniques used in this study to confirm the trustworthiness and credibility of this study.

Since this study is a qualitative study, to ensure the trustworthiness and credibility of the study, evaluating validity offers this assurance. Creswell and Miller (2000) explained the technique of triangulation in which the researcher searches for common themes among the interview transcripts gathered during the interviewing and categorizing them appropriately. Triangulating the data offers research validity because it relies on multiple accounts of an occurrence instead of allowing for a single instance to define a theme.

This study used the technique of bracketing to strengthen the reliability of this exploratory study. Hycner (1985) explained that bracketing requires that the researcher approach the analysis of the interview recordings or transcriptions with openness in which disregarding prior beliefs or elucidations allowing the researcher to discover whatever meaning emerges from the analysis. Using bracketing prevents the earlier security beliefs from interfering with the analysis of the data allowing for the correct discovery of meaning from the data gathered in this study.

Member checking is another method to ensure study reliability. The use of member checking relies on the participants instead of the researcher as Creswell and Miller (2000) explained that in member checking the researcher returns to participants with the derived themes to decide if they are sensible and if the overall account of the interview is correct.

Using the methods mentioned above deliver adequate assurance of research reliability. The combination of triangulation, bracketing, and member checking offers depth and strength to the validity of the study by not relying on a single validation method. As stated by Creswell and Miller (2000), it is of utmost importance that the credibility of the account is depicted accurately in the study.

**Data Collection**

Data collection will occur using a semi-structured interview scenario. Polkinghorne (2005) explained that to collect the data necessary for understanding the participant's experience, researchers must engage in rigorous evaluation with the participant. The interview location will be mutually agreed upon to ensure adequate comfort level of participants. All interviews will occur in person to better capture the nonverbal responses of the participants. The following steps detail the data collection process to be used uniformly across all interviews.

1. Each interview will elapse over a 30 to 60-minute timeframe depending upon the descriptiveness of answers provided by the participants.
2. The interviews will occur in person to allow for the audio recording of the interview session.
3. Before conducting the interviews, participants will sign an informed consent saying that the researcher ensured maintaining the confidentiality of any gathered data.
4. The opening part of the interview will consist of gathering basic demographic information and determining the level of security awareness training.
5. The intensive interview will consist of the questions defined in the sampling procedure and followed the initial questions.
6. The questions will stimulate the participants to reveal in-depth details about the experiences surrounding renting an automobile and pairing a smartphone.
7. After completing the interview, the recordings will be transferred and transcribed to the computer for analysis.

## Data Analysis

Data analysis will use a combination of manual techniques and automated tools to code the data efficiently. The method of data analysis used in this study is constant comparative analysis. Leech and Onwuegbuzie (2007) explained that constant comparison analysis is the most common method, sometimes known as coding, where the researcher creates specific codes and places portions of the transcripts within the different codes. The following steps detail the data analysis process to use for this study.

1. Relabeling the transcripts offers a level of anonymity to the data sets to prevent identification of participants by readers.
2. Using qualitative analysis software assists in code development and refinement. The software to be used in the analysis was MaxQDA 12.
3. Continued review of the transcripts will result in code refinement and better grouping of the data.
4. Reviewing the codes will produce common themes among the data to allow for discovery of trends among the responses.
5. Reporting of the themes and a more in-depth analysis occurs in chapter four of this study.

## Ethical Considerations

Ensuring proper permissions for conducting this study is important to ensure that there are no violations of the privacy of the participants. The following paragraph expands on the permission requirements of this study.

The primary permissions requirement for participants is the release of basic, non-identifiable demographics information. The individual participants specified basic explanation of career field, years of experience, amount of earlier security awareness training, and frequency

of automobile rental activities. This data, being generic, needed only the permissions to use the data in developing the scenario to discover if the security awareness training factored into security behaviors when renting automobiles. Additionally, participants granted permission to use the recorded interviews to develop the added narrative in the discussion of the research findings. The recordings offered the detailed information surrounding the individual behaviors and attitudes of each participant.

Protection of privacy and human rights protection is an important aspect of the research process. Part of the ethical considerations is keeping anonymity of research participants. Making consideration of other ethical and human rights requirements is also necessary. The following describes the ethical considerations and methods to protect human rights during this study.

A major ethical consideration is ensuring proper consent. Before conducting interviews, each participant signed an informed consent form. The informed consent covered aspects of the data collection process, the intent of the study, and the methods used to protect the privacy of the participants.

The anonymity guarantee considered several different aspects surrounding the privacy of the individuals who took part in the study. The original interview recordings stayed locked in a safe to prevent unauthorized access to the recordings. Encrypting the transcribed interviews prevented unauthorized access to the transcribed files. Further, the files needed a password before viewing the file.

To benefit the participants lacking adequate security awareness training, brief training after the interview shared the inherent risks with the pairing smartphones to rental vehicles. This action is to maintain the principle of beneficence. Murphy (1993) explained that the principle of

beneficence needs the promotion of the common good, meaning that since the participant's unawareness of the security risks was unmitigated, professional responsibility required educating the participants of the risks.

## Summary of Chapter Three

This study used a qualitative research tradition as the basis for conducting the applicable research. To show the overall experiences of the participants, a qualitative research method is most fitting. The population derived from financial services organizations within Cedar Rapids, Iowa and sought to sample individuals who engaged in business travel over the past twelve months and rented a motor vehicle during the travel. Making a correct comparison necessitated the use of purposive sampling as the sampling procedure. Given that the study is qualitative, the proper research instrument is an interview protocol developed specifically for this study. Finally, showing the trustworthiness and credibility of the study occurs through using triangulation, bracketing, and member checking, and describing the ethical considerations applicable to this study. In Chapter 4, discussion occurs regarding the findings from the study outlined in this chapter.

# CHAPTER FOUR

The purpose of this study was to explore the behaviors and attitudes of security professionals when pairing a smartphone to an automobile using Bluetooth. This study used a qualitative method with an exploratory research design. Conducting an exploratory study allowed for both the observation of the participants when connecting the device, as well as a series of questions upon completion of the pairing activity. The exploratory observation, followed by the interviews, stimulated expressive responses from the participants. The observation of participants allowed for a holistic view of the pairing experience while focusing on only the specific sample population. The data collection process utilized a small handheld digital voice recorder to capture all interactions with the participants quickly. The recordings contained no PII of the participants to safeguard maximum participant privacy and anonymity. The transcription of the audio to text used a combined approach, which leveraged automated tools to perform a rough transcription. Upon completion, a thorough manual transcription verification allowed for confirming the accuracy and adding any missed audio inputs, or incorrectly transcribed inputs by the automated tool. The transcriptions were then added to MaxQDA 12 to enhance the data analysis, coding, and theme development process.

There were 10 participants involved in the study. This chapter provides information about the participant demographics, it presents the findings, discusses the data analysis process, and relates the findings of the study to the research question. Further, it will provide specific themes derived from the coding process and demonstrate how the participants' responses fit into those themes accordingly.

## Participant Demographics

Participants for this study were recruited using both LinkedIn and networking with fellow security professionals. Both methods allowed for the quick identification of participants using a convenience sampling method, and facilitated a means of verifying current security credentials before conducting the observation and interview. Given the nature of many of the participants' professional lives, anonymity was of the utmost importance for both preservations of professional merit and also to protect the identity of the employer. The initial selection resulted in 11 participants but later realized that one did not possess the requisite security skills and certification to participate in the study.

Study participants met the requirements of at least 3 years of security experience and held a security specific industry certification, such as the CompTIA Security+ or the International Information System Security Certification Consortium ($ISC^2$) Certified Information Systems Security Professional (CISSP). Out of the 11 participants, only one became disqualified due to not meeting the minimum requirements of study participation. Each of the 10 remaining participants came from a variety of professional backgrounds that added depth to the various perspectives explored through the behaviors of security professionals. Table 1 presents the gender and the age range of the participants. Further exploration of the demographics reveals that there were nine males and one female who participated in the observations and interviews. The age ranges were decomposed into 10-year intervals starting at 30 and extending to 69. A closer examination of the ages reveals that 40% of the participants were age 30 to 39, only 10% were age 40-49, and 50% were between the ages of 50 and 69 (20% contained in 50 to 59 and 30% within 60-69). The diversity among the four different age categories gave an opportunity to see if any participant beliefs varied based on the age group. Further, correlating the results to the

age group allowed for an additional vantage point for the participants' behaviors while observing the process of connecting a smartphone to the automobile.

Table 1

*Participant Demographics*

| Gender | Count | Percentage |
|---|---|---|
| Male | 9 | 90% |
| Female | 1 | 10% |
| **Age Range** | **Count** | **Percentage** |
| 30 to 39 | 4 | 40% |
| 40 to 49 | 1 | 10% |
| 50 to 59 | 2 | 20% |
| 60 to 69 | 3 | 30% |

## Presentation of the Data

The exploratory research entailed the observation of the ten participants along with semi-structured interviews following the observation. The interviews used the interview questions found in Appendix A. Based upon the compilation and analysis of the interview transcripts, using MaxQDA 12 to assist in the coding and organization of the data, four primary themes emerged from the research. Table 2, Research Themes provides a summarization of the four themes.

Table 2

*Research Themes*

| Theme | Experienced (E) or Not Experienced (NE) | Percentage of E vs. NE |
|---|---|---|

| | | |
|---|---|---|
| System Distrust | E = 10 | E = 100% |
| Data Leakage | E = 9 | E = 90% |
| | NE = 1 | NE = 10% |
| Loss of | E = 9 | E = 90% |
| Personal | NE = 1 | NE = 10% |
| Information | | |
| Interface | E = 5 | E = 50% |
| Differences | NE = 5 | NE = 50% |

During the initial coding process, review of the interview transcripts allowed for the selection of specific key words to be used as codes. Using MaxQDA to perform lexical searches on the selected words and words with the same meanings presented the ability of finding specific areas in each of the transcripts. These searches required additional refinement to determine that the context around the word added value to the analysis process, and resulted in several search results dismissal or refinement to better support the analysis of the data.

The four themes outlined in Table 2 are System Distrust, Data Leakage, Loss of Personal Information, and Interface Differences. Each of these themes had several codes associated with the theme. System distrust codes included personal identification number (PIN) code, encryption, nervous, and distrust. Data Leakage codes were delete, privacy, and leakage/disclosure. Loss of Personal Information codes consisted of text message, machine access code (MAC) address, contact information, and call history. Interface Differences codes

were difficult, interface, and different. Figure 2 below presents the dissection of the associated codes. Further code explanation follows Figure 2.

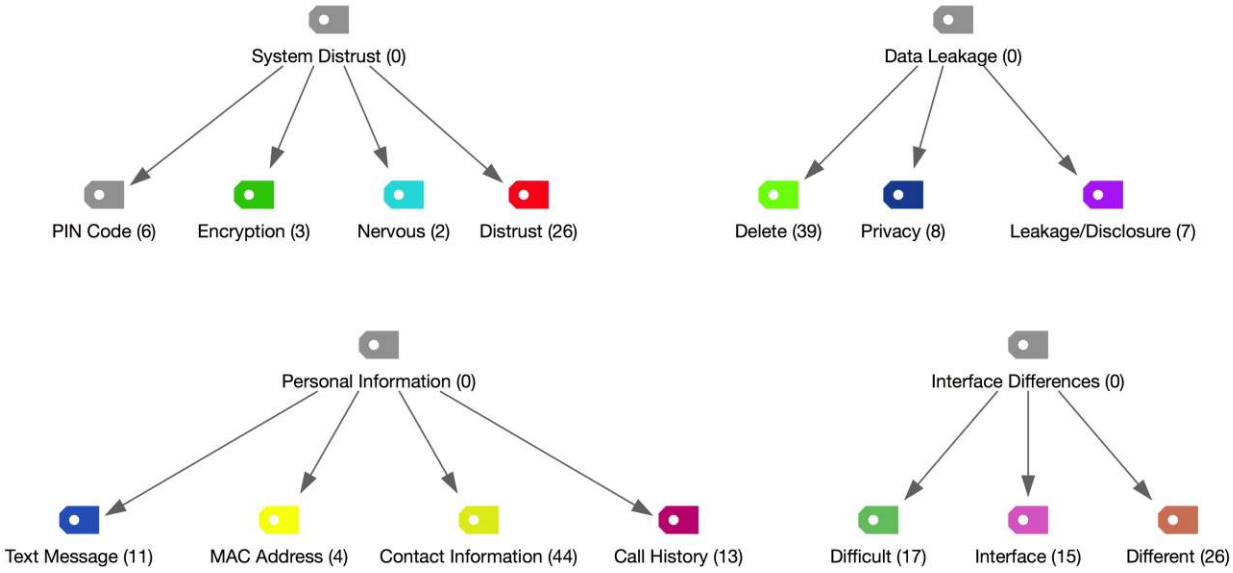


*Figure 2.* Themes and codes.

System distrust was the prominent theme among participants. Reviewing the transcripts presented a significant occurrence of distrust among the participants. The distrust code included both interview data and the observations of participant behavior and body language. Additional modification of coded data relating to distrust was not necessary due to the accuracy of MaxQDA in finding instances of distrust in the transcripts and further review revealed the accuracy of the MaxQDA identification. Another important code for system distrust was encryption. The code of encryption related specifically to the concern of participants about data communications between the smartphone and infotainment system, and data storage of onboard data not applying proper encryption to protect the data. Nervous was a code that related to the expressed and observed feelings of participants. The majority of the data relating to nervousness was from the observations due to the concern participants expressed through behavior. The final code relating to system distrust was PIN code. The interviews revealed concern about the

security of the PIN code exchange and the guarantee of protection of the pairing process. The concern with the PIN code resulted from the PIN code automatically pushing from the automobile to the mobile device.

Data leakage consisted of codes delete, privacy, and leakage/disclosure. The code delete referred to expressed concerns over the thoroughness of the data being deleted by the system when a device is deleted from the automobile. The privacy code related to concerns about the surety of data protection from external connections via cellular connections or additional mobile devices within range of Bluetooth connectivity. The leakage/disclosure code resulted from the expressed feelings of the participants related to the unintentional or intentional exfiltration of personal data from the automotive system via Bluetooth or cellular connections.

Text messages, call history, personal information, and MAC address were codes for the theme of loss of personal information. Interview transcript analysis found that the common areas of concern among participants were call history, text messages, and other personal information. The concern related to another renter or malicious actor gaining access to such information if the data was not deleted or not deleted properly during the device removal process. Another commonality among participants was the ability to gain access to the smartphone's MAC address.

The final set of codes were different, interface, and difficult. These codes related to the user interface component of the infotainment system. The codes of difficult, different, and interface surfaced from participants sharing the difficulty in the deletion process due to the different user interface of the various infotainment systems. Interface also related to the underlying protocol differences between infotainment systems causing additional concerns about the ability to delete data from the system.

Table 2 presents whether or not the participants, through the interview responses, felt like they experienced feelings of system distrust, feared potential data leakage, thought that personal information transferred from the phone to the vehicle, and experienced challenges with deleting the device due to user interface differences. Figure 3 depicts the relationships between the research question and the themes. Figure 3 also presents a representation of the relationship between the themes extracted from the data analysis process.

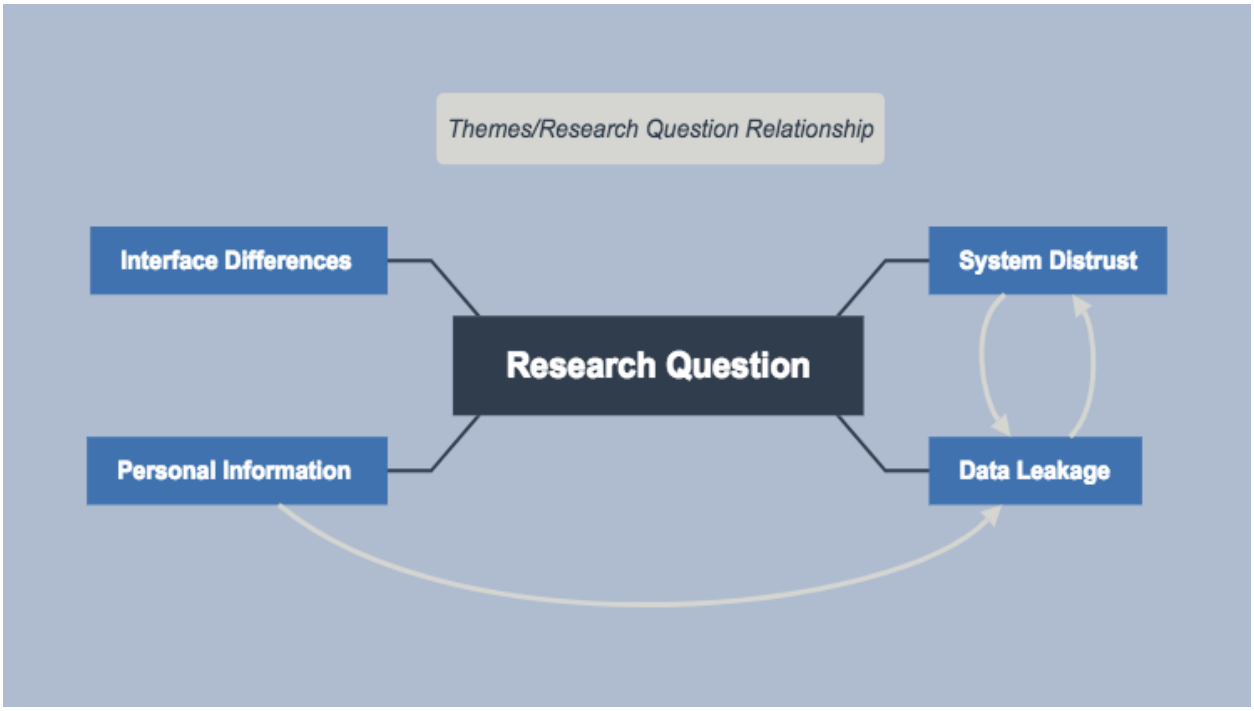


*Figure 3.* Theme and research question relationship.

The results displayed in Table 2 receive additional, in-depth explanation in the following subsections where each theme gets dissected further.

**Theme 1: System Distrust**

Every participant experienced feelings of system distrust when it came to the pairing of the smartphone to the infotainment system. All of the participants stated in their interview some form of distrust of the system, and this was accompanied by a behavioral reaction during the exploratory exercise when the participants paired the smartphones with the automobile. This

theme of system distrust further reflected the various areas of expertise of the different security professionals that participated. Participant 1 focused on the area of encryption, which is an area of expertise. Participant 1 shared the automobile's connection with the smartphone:

> I do not know of any encryption key did not ask me if it was a secure connection. Since I am cyber centric, I am very much in tune with that sort of thing without that kind of feedback you do not know if you got a secure connection or not the average person would probably not worry about it not think about it for me given you know my point of reference. I would say is this connection secure and has not asked me for any kind of a key or told me it is secure therefore it is probably not so I would have to be very careful about how it was used.

A different area of focus stuck out in the response of Participant 3. Participant 3 was more concerned with the design rigor compared to the aviation industry. Participant 3 stated:

> They [external connections] are very insecure, and I would not trust any of them. It just showed me that the car manufacturers have not put the same rigor into their systems that aviation has, and so I trust none of it.

This participant's focus of system distrust resulted from the perception of poor design and implementation practices by the majority of auto manufacturers.

Participants 4, 5, 7, and 9 shared a commonality that the distrust surrounded the security of the data, which transferred from the phone to the automobile. The areas of concern for these participants was related to what happens to the data when it transferred to the vehicle and how the system deletes the data from the persistent storage. The apprehension surrounding the data transfer related to the potential for the data removed from the automobile via external connectivity. These participants also shared trepidation about the method of data removal and

confirmation that the data was deleted. Recently some researchers out of Europe realized this concern. Constantin (2017, November 16) shared that Gabriel Cirlig and Stephan Tanase recently discovered data related to individuals' contact information, call and text messaging histories, email messages, and other personal information on an automobile's infotainment system and the data unencrypted allowing anyone access to read the data, thus violating the privacy of individuals using that specific infotainment system. Although this was a blog post, presentation of these findings took place at DefCamp security conference, and the official reports corresponding with Constantin's article are not yet available.

Another perspective of system distrust presented itself in the response of Participant 6. Similar to 4, 5, 7, and 9, participant 6 was concerned with external connectivity. Participant 6, however, viewed the potential of unauthorized automobile tracking as a source of the system distrust. Although not directly related to the smartphone, the observation of Participant 6 revealed additional security concerns that may be held by security professionals. Participant 6 detailed:

> Many cars have Navstar, and that has a cellular connection, and they are tracking your location all the time. So, this is good and bad right? If you get in an accident and it is very helpful. You know it is basically kind of a 911 thing where if your airbags go off. The other half is that they are tracking your position anytime you drive.

Further, Participant 10 noted system distrust due to the connection between the automobile's Controller Area Network (CAN) bus and the infotainment system. Participant 10 expressed the feelings of distrust due to the potential of a kinetic attack against a moving vehicle that could result from gaining access to the infotainment system through an external connection

such as a smartphone. Unlike the other reasons for distrust, Participant 10 experienced distrust due to the potential impact on human life.

**Theme 2: Data Leakage**

Data leakage was another theme that resulted from participants' concerns with the deleting process. Of the participants, eight males and one female suggested feelings of the potential for data leakage resulting from connecting the smartphone. The one participant who did not express concerns towards data leakage was in the 60-69 age group.

Participants 3, 4, 5, 6, 7, 8, 9, and 10 shared significant concerns regarding the potential for data not being deleted from the persistent storage of the automotive infotainment system. These eight participants shared a similar concern surrounding the underlying mechanisms used to delete the contact information, text messages, and call history from the system. The participants expressed concern that there was no sort of certification to ensure that the design of the system provided a secure means of deleting the data rather than just removing immediate access to the data in the infotainment system's graphical user interface (GUI). The GUI provided confirmation when deleting the phone from the vehicle, but did not state the method of deletion used which raised data leakage concerns for the participants.

Participant 4 stated,

> When I deleted, you know I had no way of knowing that it was actually deleted. It is quite a bit of trust going on there that that stuff is still not in there. That there is not a backdoor or something that somebody could extract that data.

This statement reflects the participant's concerns with data leakage and also demonstrated the correlation with Theme 1: System distrust.

Participant 7 shared,

> In the option to disable or delete the phone I deleted it and it said it erased the contacts and everything that we initially downloaded. So, on the surface it appeared it downloaded everything whether it really did are what it truly obtained gathered from my phone I guess I have no idea. Can only assume that it deleted everything that it gathered.

The statements made by participant 7 shared significant similarities to that of participant 4 further amplifying the participants' concerns about data leakage.

Participant 2 rendered a different perspective regarding the data leakage. Participant 2 viewed the issue of data leakage from the perspective that the automotive manufacturers should design the system in such a way to provide full disclosure of the information that transfers to the system. Participant 2's view demonstrated an attitude more of accepting the data transfers on the current system and exhibiting concern for future development to ensure total consumer awareness. Similarly, Participant 10, although concerned about data leakage, presented an attitude of greater concern on the implications on the kinetic impact of the infiltration via external connectivity and the potential to control portions of the CAN bus remotely.

**Theme 3: Loss of Personal Information**

The theme of personal information related to the overall attitudes the participating security professionals had towards pairing a smartphone with a vehicle. For the purposes of this study, the term personal information correlated to contact information (contact names, phone numbers, addresses), and any other data that belongs to the phone book access profile (PBAP), call history information, text messages, phone-based location information, Bluetooth MAC address, and information linking the smart device to the individual. Similar to the data leakage, nine participants experienced concerns regarding the potential personal information on the infotainment system.

Participants 2 through 10 expressed a belief that personal information transferred from the phone to the vehicle's persistent storage. These nine participants expressed a belief that contact information transferred to the automobile. Participant 1 did not mention any belief that information, such as contact information or any other personal information, transferred between the smartphone and the system. Not all nine participants felt that other aspects of personal information transferred. Of the nine participants, participant 10 presented a nonchalant attitude about the transfer of contact information due to the viewpoint that the compromise of such information was merely an inconvenience and not a breach of PII. The other eight participants, in contrast, maintained an attitude that such contact information was PII and shared concerns about the appropriate protection and disposal of such information.

Participants 2, 3, 4, 5, 6, 7, and 9 expressed beliefs that call history information transferred to the vehicle. These participants recognized that the call history transferred and expressed that the dialog for deleting the device provided visual confirmation that the system removed such data. Participant 6 noted that not all systems transfer the same information. Participant 6 elaborated,

> Yeah so, I think that the contacts and call history were synchronized. On other phones and other systems, I have seen your media is also synchronized if you have songs and stuff. Although it [infotainment system] usually asks, but I did not see it in this particular case. So, yeah you never really sure what is transferred right.

Participants 2, 3, 7, and 9 shared feelings that along with call history and contact information, the system transferred text message data. Participant 3 did not observe text message data during the experiment but shared such experience with other automobiles. Participant 3 stated, "My phone in my car will display messages you can read them, or it will read them to you

I should say. So, your message history; texting history is on there." Similarly, the other three participants did not note any text message data transferred during the interaction with the automobile, but rather shared the different data transferred to the device, which included text message data.

During the experiment, observations focused on the key interactions between the users and the infotainment system. These observations revealed that only four of the participants fully read the prompt during pairing and did not allow for any personal information to transfer from the smartphone. These 4 participants included the two individuals of the 50-59 age group and two from the 60-69 age group. Observation of the other six participants revealed an attitude of trust in the process because they did not verify what the prompt on the infotainment system or phone stated regarding the transfer of such personal information.

**Theme 4: Interface Differences**

The interface differences theme resulted from the expressed concerns about the user interface differences along with internal system interfaces. Participants 2, 7, 8, 9, and 10 expressed an attitude of apprehension about the interfaces of the infotainment system. The primary concern among these five participants was the variation in the user interfaces among different vehicles. Participant 2 shared, "The biggest challenge is getting used to the interfaces. The interfaces change from system to system. I am familiar with Uconnect and less familiar with this system's interface."

The root of the apprehension among these participants resulted from the different interface regarding deleting the phone. Each of the participants expressed feelings of anxiety and uneasiness about the smartphone removal process due to the different interfaces and the difficulty experienced in selecting the right menu. Observation of the participants revealed that 7

of the 10 participants were not sure of how to delete the phone from the system. The five participants that experienced concerns about the interface differences were among the seven, which experienced difficulty finding how to delete the phone from the infotainment system.

## Presentation and Discussion of Findings

The four themes presented in Table 2 resulted from an iterative approach towards the analysis of the data. Figure 3 illustrates the analysis process. The analysis process portrayed represents a cyclical process. Further explanation of the process follows Figure 3. Subsequently, interpretation of the findings provides insight into the relationship between the analyzed data and the research question.

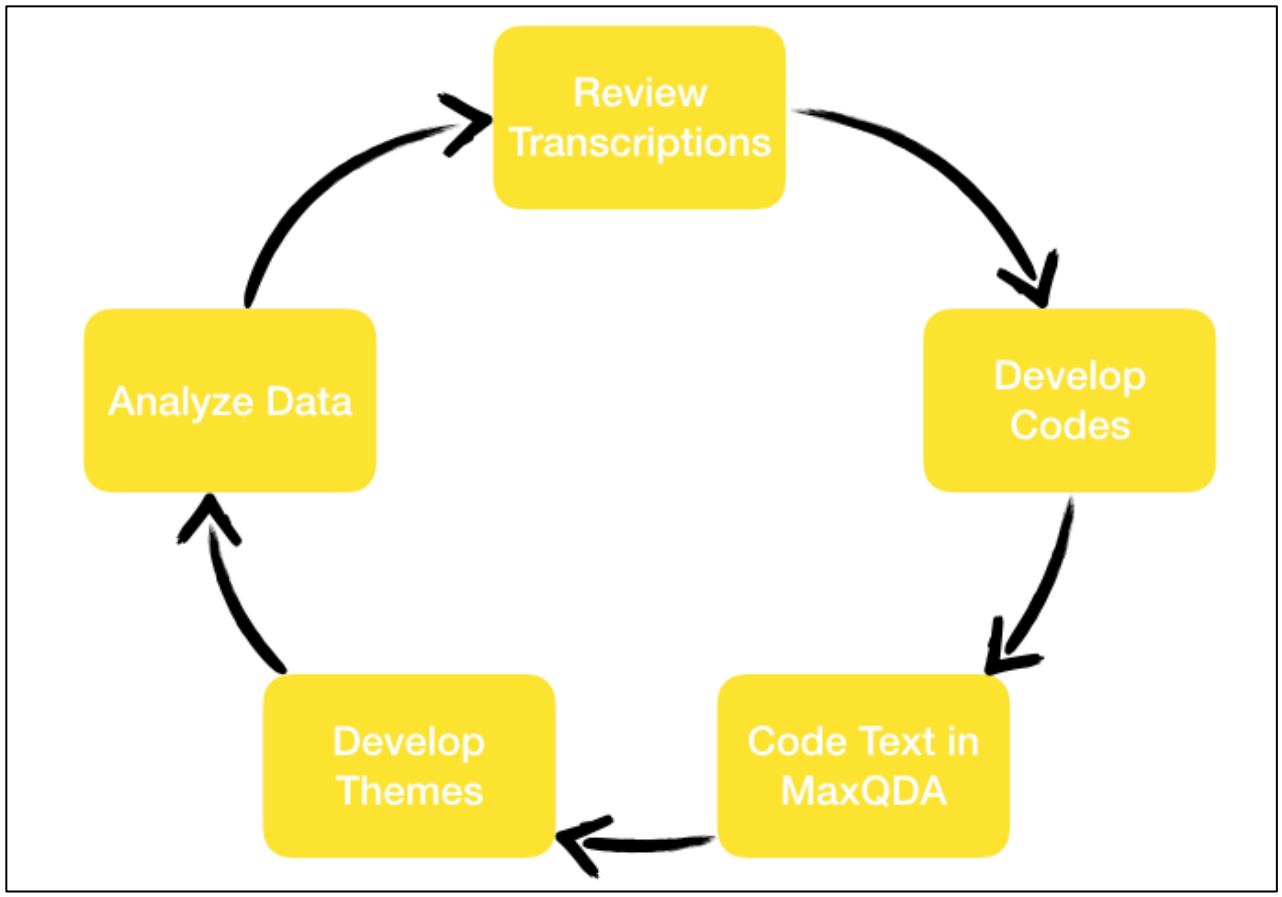


*Figure 4.* Analysis process.

The process depicted in Figure 3 allowed for a continuous approach to revising the data analysis as additional codes appeared. MaxQDA allowed for applying the new codes to the interview transcriptions. The new codes required alignment with one of the four themes. This alignment allowed for a more accurate grouping of the data to demonstrate the themes that protruded from the analysis process. Following is further discussion of the analysis process and the associated findings, which materialized during the process.

**Review Transcriptions**

The first step of the analysis process involved reviewing the transcripts based on the interview recordings. Comparing the transcripts to the recordings ensured that the transcripts provided a complete and accurate representation of each of the interviews and observations. The

transcripts received additional comments to address the observations made both during the observation activity of connecting the smartphone to the automobile and also the observations of the interviewees during the interview process.

**Develop Codes**

Development of an initial code set resulted from the review of the transcripts. These codes provided a starting point for the coding of the transcripts. Grouping of similar codes enabled a means to facilitate theme development later in the analysis process. Definition of additional codes resulted from the cyclical process portrayed in Figure 2 and enhanced the overall analysis and theme development process.

**Code Transcripts**

Applying codes to the documents using some of the lexical search tools provided in MaxQDA 12 aided the overall transcription coding process. Using the lexical search tools allowed for searching of terms and synonymous terms to accurately extract the key areas within the transcripts that related to the specific codes. The initial effort resulted in large amounts of data falling into the various codes and the additional codes developed during the second pass of the data. Further review of each code permitted the opportunity to prune the results and remove codes from the areas of the transcript that did not align with the specific codes. Following these iterations was the grouping of the codes into specific themes.

**Extract Themes**

The four themes described in the Presentation of the Data resulted from the grouping of similar codes. These themes provided an accurate representation of the participants' responses regarding the beliefs, attitudes, and behaviors encapsulated in the transcripts and observations. These four themes presented a correlation to the research question: How do the attitudes and

behaviors differ among IT security professionals around Cedar Rapids, IA when presented the opportunity to pair a smartphone to an automobile?

**Analyze Data**

After creating the themes, it was time to analyze the data. Data analysis occurred by reviewing the data captured within the themes and the codes associated with those themes and determining the relationship to the research question. The analysis of data also included the review of the observation process for the exploratory activity. The development of additional codes allowed for additional analysis of the data. Overall, the analysis process design intended to facilitate a cyclical process to allow for continuous refinement of the data and the findings from the data.

**Interpretation of Findings**

The four themes developed during the analysis process were system distrust, data leakage, personal information, and interface differences. Review of the analyzed data revealed that all of the participants exhibited an attitude of distrust towards the infotainment system. This distrust primarily resulted from the participants' inability to view all of the data transferred to the vehicle and the lack of assurance of data deletion upon deletion of the smartphone from the system. Although there was an attitude of distrust, 60% of the participants still exhibited a contrary behavior. This behavior was allowing the personal information to transfer to the automobile during the pairing process. Further, the demographics the exhibited behavior of distrust were those participants in the 50-59 and 60-69 age groups. From each of these age groups, two individuals exhibited behavior that aligned with the attitudes of system distrust stated during the post-observation interviews.

Findings surrounding the data leakage presented a correlation between the behaviors of the participants and the attitudes presented during the interview. The nine participants sharing the attitude that there is possible data leakage all took time after deleting the smartphone to ensure that the data was not present on the system. Although the only method of confirmation was through the GUI on the infotainment system, each of the participants checked all the locations they thought would possibly be retaining data in the system. All nine participants sharing the attitude of concern towards data leakage found no user-visible remnants of data remained on the system after deleting the phone profile from the vehicle.

The theme of personal information related closely to system distrust and data leakage. The perceptions and attitudes towards personal information varied among the nine participants that experienced concerns with personal information. All nine of the participants felt that contact information was personal information and perceived that such information transferred between the phone and the automobile. The attitude towards such information was the same for eight of the participants. The 9th participant shared an acknowledgment of contact information transference between the devices but presented an attitude that losing such information was a nuisance and not a significant concern. Only four of the participants categorized call history and text message history as personal information. This suggests that the definition of personal information among groups of security professionals is not clear and reflects the viewpoints resulting from personal experiences or beliefs about system behaviors.

The theme of interface differences related to the variance in user experience (UX) differences between automotive manufacturers. This theme surfaced among the lower age categories of participants. The participants in the 30-39 and 40-49 age groups expressed feelings regarding the challenges experienced due to the different user interfaces. The participants

expressed a feeling of anxiety about situations such as renting an automobile with a different interface and the ability to find the system controls to delete the profile from the device.

Beyond the theme related findings, the observation of the participants revealed a common behavior among the security professionals. In seven of the 10 participants, the behaviors during the experiment of connecting the phone to the vehicle, exploring the system, and deleting the device did not match the communicated attitudes towards the security concerns of the infotainment system. This variance resulted from the participants not reading through the access control prompts presented on the phone. Seven of the participants clicked okay on the prompt without reading it and after clicking presented obvious feelings of concern when the infotainment system made the audible statement that contact information, call history, text messages, and other data began downloading to the vehicle. Chapter 5 further explores the findings and the relationship between the findings and conclusions about the research question.

## Summary of Chapter

This chapter presented the results of the exploratory observation and the data collected during the interviews for this research study. It provided introductory information about the data collection process, the time frame, and an overview of the research study. There was an explanation of the participant demographics providing information about the gender and age groups of the participants. The research study involved 10 participants. The resulting interviews required transcription to text to allow for data analysis. The data analysis process produced four themes and several codes aligned with each of the themes. Each of the themes related to the research question based on the described experiences, attitudes, and observed behaviors of the participants. Following the explanation of the themes was the interpretation of findings. The

interpretation of findings added further clarity to the analysis of the data and the relationship to the research question.

Chapter 5 presents the findings and the conclusion of the study. It will also provide recommendations for future work, limitations of the study, and possible implications for practice. Further, it will discuss the implications of this research study to the field of information security, automotive manufacturing, and rental vehicle industry along with the overarching conclusions resulting from the completion of this study.

# CHAPTER FIVE

This chapter presents the findings, recommendations, and conclusions of the study. The findings and conclusions section explores the themes presented in the previous chapter and draws conclusions based on the findings. Following the findings and conclusions are the descriptions of the limitations of the study, the implications for practitioners, implications of the study, and explanation of future research opportunities. The final section of this chapter summarizes the study.

## Findings and Conclusions

The findings indicated four main themes. The themes were system distrust, data leakage, personal information, and interface differences. The findings associated with these themes include several commonalities between all participants, but also demonstrate differences in the participants' beliefs, attitudes, and behaviors. Each of the following sections provides additional details about the various findings.

### Professional Perspective

Each of the participants originated from the same overarching industry. However, within this industry, each participant had different roles ranging from focuses on encryption, intellectual property, or enterprise-level security. This presented itself in the answering of the questions. Although not all participants answered the questions differently, there was an underlying perspective held by the participants that caused focus on the different areas of expertise. This was most evident in the themes of system distrust and data leakage where the participants' responses closely aligned with professional focal areas. For instance, Participant 1 focused heavily on encryption and the lack of guarantees that encryption protected any of the data on the

infotainment system. This pulling towards encryption resulted from the many years working with encryption products.

The perspectives of Participant 1 varied in comparison to Participant 2. Participant 2's professional background related more towards enterprise environments and maintaining security for enterprise systems. This resulted in Participant 2 presenting more of a concern about the authentication mechanism used or not used for preventing other automobile users from being able to access the personal contact information of another smartphone phonebook resident on the infotainment system.

Further, multiple participants' professional expertise is in embedded systems for the aviation industry. Despite their security expertise, they focused on vehicle operations and safety. They expressed less concern regarding the transfer of sensitive data between the smartphone and the infotainment system. A concern expressed by the participants revolved around the ability to remotely access the automobile using the infotainment system as a pivot point to gain further access to the physical controls of the automobile and potentially executing a kinetic attack against an automobile.

**Participant Mindsets**

Another finding was the different mindsets exhibited among the various year groups of the participants. In general, much of the interpretation within the themes revealed an underlying level of similarity in response. The mindsets varied most among responses surrounding interface differences and personal information. The older generations (age groups 50-59 and 60-69) showed less concern with the interface differences and a greater reluctance to accept the risk of connecting the phone to an unknown device [infotainment system]. In contrast, the younger age groups noted the differences in user interface and the possible impact on being able to delete the

devices. The younger age groups also demonstrated less concern with connecting the smartphone to the infotainment system and several did not view the data that is visible to the system user as being private or classified as PII. These differences in the participant mindsets suggest that the older age groups acted in a risk avoidant manner, while the younger age groups demonstrated more of a risk acceptance behavior.

The difference in the behaviors and attitudes between the different age groups of security professionals suggests that the older age groups do not perceive the usefulness of providing full connectivity between the phone and automobile. The Technology Acceptance Model (TAM) consists of four distinct areas. Davis (1993) developed the TAM in the four distinct areas of an external stimulus, cognitive response, affective response, and behavioral response. Davis (1993) further explained that within the cognitive response is the determination of perceived usefulness and perceived ease of use, while the affective response presented the attitude toward use and the behavioral response was the actual system use. The results of this study then demonstrate the age groups of 50-69 primarily fell within the cognitive response area while the younger two age groups demonstrated actual system use and thus demonstrated a behavior response, demonstrating the acceptance of the technology.

**System Distrust**

The main area of similarity in the responses was the theme of system distrust. All 10 participants shared an attitude of distrust towards the system. Although the participants all shared unique concerns relating to the infotainment system based on the different areas of professional expertise, each participant shared strong attitudes of distrust towards the automotive system. The system distrust primarily resulted from a lack of proof of the deletion process. In addition, there was a level of distrust presented by participants about the types of data moved

from the smartphone to the vehicle. Further, the potential for undesired external connections increased system distrust due to the increased attack surface and the potential for compromised personal information. Figure 4 presents the word frequency cloud developed from MaxQDA during the analysis of the data.


*Figure 5.* Word frequency cloud.

Figure 4 shows several keywords that correlated closely with the expected attitudes and behaviors of the security professionals. Words like trust, confirm, remove, data, and informed show the areas of concern expressed during the interviews. As presented earlier, the participants shared feelings of distrust about the Bluetooth connection. It also reveals the concern about the deleting mechanism used by the infotainment system. In the center of the word cloud the words secure, delete, and little are larger than the others due to the frequency of use. The high frequency resulted from the participants having little trust that the system would provide a secure delete function.

### Attitude-Behavior Contradiction

Although the attitudes of the participants reflected similarities, the behaviors did not match as closely. During the observation of the participants, six participants quickly clicked through the various prompts that appeared on the cell phone and the infotainment system. The various prompts referenced allowed the infotainment system to download contact and other personal information. The rapid prompt navigation proved contradictory to the attitude about the themes of data leakage, system distrust, and personal information. The contradictory behavior occurred in the younger age groups presented in the demographics section of Chapter 4. This difference in behavior among the younger age groups may suggest desensitization to the regular presence of notifications or alert prompts on the devices. Therefore, even when possessing similar security experience and credentials, the younger age groups demonstrated a willingness to compromise behavior for the sake of overall convenience and thus accepting the associated risks with the activity.

## Limitations of the Study

Study limitations for this study included the participation requirements of holding a security certification and working in the cybersecurity field. For a participant to qualify for participation in the study, the prerequisite of security experience and a security certification limited the potential participants in the sample population. This study focused on participants in Cedar Rapids, IA. The geographic limitation further limited the experiences due to the principal presence of the aerospace industry.

The study constrained the exploration of the attitudes and behaviors to the activities of pairing and unpairing the smartphone in the same session, and on the same day. It did not seek to determine if the behaviors changed over a prolonged experience such as renting a car for a three-week business trip. Further, the study restricted the participants to connecting the

smartphone to a single vehicle. Using a single vehicle limited the ability to discover other potential challenges that the participants may experience if the study involved connecting to multiple vehicles. It further controlled the exposure of the participants to how the automobile handles the data and how the vehicle presents the data on the infotainment system. Part of this limitation includes determining the visibility of another user's data present on the infotainment system. The test vehicle only presented the other phones' names and did not expose additional contact information associated with the devices.

## Implications for Practice

There are a few different implications for practitioners resulting from this study. Each of the inferences for practice will receive a further explanation in the following sections. These suggestions break down between the automotive industry, rental vehicle industry, and general information security guidance.

### Automotive Industry

The findings of this study revealed significant attitudes of distrust among security professionals relating to the infotainment system. The primary recommendation related to auto industries revolved around the design of the deletion mechanism. The automotive manufacturers should seek to create a mechanism to verify the removal of the private information from the device. This type of verification protects the consumer in the case that the infotainment system is removed and sold, compromised using Bluetooth or Ethernet, or unintentional exposure to other infotainment users. Further, providing such verification demonstrates auto manufacturers' commitment toward the security of the technology embedded within the automobile.

Along with the previous implication, it would benefit the automotive industry to demonstrate the security of the infotainment system through an independent certification authority. Relying on an independent certification authority for the secure configuration of the

infotainment system provides consumers with better assurance that the automakers practice secure system design and development practices. This independent assessment could be similar to the Department of Defense the risk management process where a system is assessed and authorized by an independent assessor. Including a third party demonstrates that any potential internal organizational biases do not affect the security posture of the system.

**Rental Industry**

Given that many rental agencies have automobiles in the inventory with infotainment systems, it would benefit the rental industry to demonstrate support for protecting customer privacy. Customer privacy protection includes changing current procedures for employees when processing a returned vehicle. Such changes consist of the manual process of checking for devices that were not previously deleted before returning the car and deleting any smartphones retained by the vehicle. A procedural change that adds the steps above to the return process demonstrates the commitment of the rental agency to safeguard customer information and preventing the potential compromise of such information.

Further, the implication for rental agency contract writers includes modifying verbiage to ensure renters understand the potential risks of pairing a smartphone to the automobile. Security awareness is the key area that modifies attitudes and behaviors of users. Making a renter aware of the risks of connecting the smartphone to the rental vehicle acts as an additional security awareness mechanism, which protects the consumer and the rental company. Improving such security awareness leads to more secure behaviors by the consumers when renting the automobile.

**General Security**

Implications for general information security practitioners revealed itself in the way of increased awareness training. Although connected cars are not new, there is not much security

awareness training provided surrounding the infotainment systems. The lack of awareness among security practitioners reveals a potential gap in the overall security training of which security professionals are recipients. This security awareness also needs dissemination to the broader consumer base. Ensuring that individuals understand the risks of using certain technologies is important in the protection of PII and other sensitive information.

Exploring the differences in user perceptions across the generations may identify influences on technology acceptance. Given the acceptance demonstrated by the younger two age groups, it benefits security practitioners to focus awareness training content on these younger age groups. It also presents the opportunity to customize awareness for the older two age groups and provide increased awareness of the usefulness of the technology, as well as the potential threats to privacy. Many organizations use phishing exercises as a training and awareness mechanism for the security posture of the organization. These exercises often incorporate parts of the protection motivation theory to connect the training to the trainee in a more personal manner. Leveraging similar approaches with educating the general users may result in a better internalization of the security principles relating to the pairing of the smartphone to a vehicle's infotainment system.

## Implications of Study and Recommendations for Future Research

This study included the analysis of the attitudes and behaviors of security professionals towards connecting smartphones to automobiles. During the research process, additional areas of future research emerged. The following paragraphs further explore the recommendations for scholarly research.

### Geographic Location

Understanding the behaviors and attitudes of security professionals in different regions of the United States offers the opportunity to examine if the behaviors and attitudes exhibit similar

themes. Further, it offers the opportunity to discover different themes, which may suggest the different focus of security professionals depending on external factors present in different areas of the United States.

**Non-security Individuals**

There is also an opportunity to research the attitudes and behaviors of individuals without a security background and security certifications. Understanding the attitudes and behaviors of these individuals offers the opportunity to build the case for additional research. Such additional research could be a quantitative study comparing the differences in behaviors and attitudes of the two groups. It also presents the opportunity to find similarities in the themes of attitudes and behaviors such as system distrust.

**Different Industry**

Future research of security professionals in different industries could further build the body of knowledge and reveal trends and differences among security professionals from the different industries. The field of infotainment pairing technology with personal, confidential and sensitive information needs further investigation into the possible different perspectives among different industries. Examining different industries also grants an opportunity to better develop the security workforce based on the trends and differences. For instance, if such research reveals similar results of contradictory behavior among younger age groups it offers the opportunity to modify existing security training to better address the challenges.

**Multiple Vehicles**

Another area of future research opportunity is conducting the same study while observing participant behavior in multiple vehicles. Using multiple vehicles offers the benefit of better understanding how the interface differences increase the challenges of the participants. It also

presents the opportunity for participants to see how each of the different vehicle manufacturers handle the presentation of data and the security of such data differently.

### Safeguarding Personal Data

Building upon the problems emerging from this study surrounding the issues of system distrust and loss of personal information presents an opportunity for future work. Identification of processes or mechanisms that can provide verifiable assurance of the security of personal data would further build upon the body of knowledge. Further, exploration of the necessary security features to develop user trust presents the opportunity for additional research.

## Conclusion

Continuous technological advances enable new mechanisms of convenience for our daily lives. These advancements in technology present both risks and benefits. This study reviewed the attitudes and behaviors of security individuals when pairing a smartphone to an automobile. The study consisted of an observation of the individuals during the pairing and unpairing process. It also used a semi-structured interview process upon completion of the hands-on portion of the study. The observation and interview occurred with 10 participants, and all the participants worked in the aerospace industry.

Among all study participants was the attitude of overall system distrust relating to the vehicle's infotainment system. This distrust stemmed from different aspects that demonstrated a correlation to the different areas of expertise of each of the participants. Most of the participants also presented an attitude of concern about data leakage and the presence of personal information on the infotainment system. Not all participants shared this attitude and showed greater concern towards the potential of a kinetic attack against a vehicle using devices such as smartphones and infotainment systems as pivot points. Further, the study found that participants found difficulty in the process due to the differences in the interfaces between infotainment systems. This

difficulty primarily existed in the participants' ability to delete the smartphone from the infotainment system.

This study identified four themes emerging from the interviews of the 10 participants. The four themes were system distrust, data leakage, personal information, and interface differences. Four key findings developed from the themes. The four findings were the influence of professional perspectives, differences in generational behavior, system distrust, and a contradiction between the attitudes expressed during the interview and the observed behaviors during the hands-on exercise. The overall attitude of all participants was one of system distrust, which resulted in a modified behavior during the interaction with the automobile for most of the study participants.

## REFERENCES


Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control: From cognition to behavior* (pp. 11–39). https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I., & Fishbein, M. (1969). The prediction of behavioral intentions in a choice situation. *Journal of Experimental Social Psychology*, *5*(4), 400–416.

Ajzen, I., & Fishbein, M. (1973). Attitudinal and normative variables as predictors of specific behavior. *Journal of Personality and Social Psychology*, *27*(1), 41–57. https://doi.org/10.1037/h0034440

Ajzen, I., & Fishbein, M. (1977). Attitude-Behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin*, *84*(5), 8–918.

Alexandrou, A. (2015). *The security risk perception model for the adoption of mobile devices in the healthcare industry* (Doctoral dissertation, Pace University). Retrieved from https://digitalcommons.pace.edu/dissertations/AAI10097933/

Allen, A. L. (2016). Protecting one's own privacy in a big data economy. *Harvard Law Review Forum*, *130*, 71–78.

Allport, G. (1935). Attitudes. In *A Handbook of Social Psychology* (pp. 798–844). Worcester, MA, US: Clark University Press.

Andrejevic, M., & Burdon, M. (2014). Defining the sensor society. *Television & New Media*, *16*(1), 19–36. https://doi.org/10.1177/1527476414541552

Anzaldua, R. J. (2016). *Does information security training change Hispanic students' attitudes toward the perception of risk in the management of data security* (Doctoral dissertation, Northcentral University). Available from ProQuest Dissertations and Theses database. (UMI No. 10172955)

Asplund, M., & Nadjm-Tehrani, S. (2016). Attitudes and perceptions of IoT security in critical societal services. *IEEE Access*, *4*, 2130–2138. https://doi.org/10.1109/ACCESS.2016.2560919

Astani, M., & Ready, K. J. (2016). Trends and preventative strategies for mitigating cybersecurity breaches in organizations. *Issues in Information Systems*, *17*(2), 208–214.

Aubeterre, F. D., Iyer, L. S., & Singh, R. (2009). An empirical evaluation of information security awareness levels in designing secure business processes. *DESRIST '09 Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, (16). https://doi.org/10.1145/1555619.1555641

Bada, M., & Sasse, A. (2014). The impact of information security awareness training on information security behaviour: The case for further research. *Information Security*, 309–330.

Bhabad, M. A., & Bagade, S. T. (2015). Internet of Things: Architecture, security issues and countermeasures. *International Journal of Computer Applications*, *125*(14), 1–5.

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

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours. *MIS Quarterly*, *39*(4), 837–864.

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011). Human performance in cybersecurity: A research agenda. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *55*(1), 1115–1119. https://doi.org/10.1177/1071181311551233

Cates, S. (2015). The evolution of security intelligence. *Network Security*, *2015*(3), 8–10. https://doi.org/10.1016/S1353-4858(15)30017-9

Cheah, M., Shaikh, S. A., Haas, O., & Ruddle, A. (2017). Towards a systematic security evaluation of the automotive Bluetooth interface. *Vehicular Communications*, *9*, 8–18. https://doi.org/10.1016/j.vehcom.2017.02.008

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 181–202.

Chen, T. (2010). Stuxnet, the real start of cyber warfare? *IEEE Network*, *24*(6), 2–3. https://doi.org/10.1109/MNET.2010.5634434

Chen, Y., Ramamurthy, K. (Ram), & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems*, *55*(3), 11. https://doi.org/10.1080/08874417.2015.11645767

Choi, K.-H., & Lee, D. (2015). A study on strengthening security awareness programs based on an RFID access control system for inside information leakage prevention. *Multimed Tools Appl*, *74*, 8927–8937. https://doi.org/10.1007/s11042-013-1727-y

Coney, Li. (2015). The IoT and the Ability to Defend Against the Silent Intruder. *Journal of Physical Security*, *8*(2), 42–53.

Constantin, L. (2017). Researchers Hack Car Infotainment System and Find Sensitive User Data Inside. Retrieved December 11, 2017, from https://motherboard.vice.com/en_us/article/3kvw8y/researchers-hack-car-infotainment-system-and-find-sensitive-user-data-inside

Cooper, C. (2014). *Smartphone privacy perceptions and behaviors generaltional influence quantitative analysis: Communications privacy management theory* (Doctoral dissertation,

Colorado Technical University). Available from ProQuest Dissertations and Theses database. (UMI No. 3683360)

Corbett, C., Schoch, E., Kargl, F., & Felix, P. (2016). Automotive ethernet: Security opportunity or challenge? In *Lecture Notes in Informatics (LIN)* (pp. 45–54). Retrieved from http://www.gi.de/service/publikationen/lni/

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. *Research Design qualitative quantitative and mixed methods approaches* (4th ed., Vol. 3rd). Thousand Oaks, CA: SAGE. https://doi.org/10.1016/j.math.2010.09.003

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into Practice*, *39*(3), 124–130.

Creswell, J. W., & Poth, C. N. (2017). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed.). Thousand Oaks, CA: SAGE Publications, Inc.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. *Information and Computer Security*, *24*(2), 139–151. https://doi.org/10.1108/ICS-12-2015-0048

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2016). Exploring behavioral information security networks in an organizational context: an empirical case study. *Journal of Information Security and Applications*. https://doi.org/10.1016/j.jisa.2016.06.002

Dardanelli, A., Maggi, F., Tanelli, M., Zanero, S., Savaresi, S. M., Kochanek, R., & Holz, T. (2013). A security layer for smartphone-to-vehicle communication over bluetooth. *IEEE Embedded Systems Letters*, *5*(3), 34–37. https://doi.org/10.1109/LES.2013.2264594

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information and Computer Security*, *24*(1), 116–134. https://doi.org/10.1108/ICS-04-2015-0018

Davis, F. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. *Massachussetts Institute of technology*. https://doi.org/10.1016/S0378-7206(01)00143-4

Davis, F. D. (1993). User acceptance of information technology: system characteristics, user perceptions and behavioral impact. *International Journal of Man-Machine Studies*, (38), 475–487.

Edmondson, A. C., & Mcmanus, S. E. (2007). Methodological fit in management field research. *Academy of Management Review*, *32*(4), 1155–1179. https://doi.org/10.5465/AMR.2007.26586086

Egelman, S., & Peer, E. (2016). Predicting privacy and security attitudes. *SIGCAS Computers & Society, 45*(1), 22-28.

Ellison, G., Lacy, J., Maher, D. P., Nagao, Y., Poonegar, A. D., & Shamoon, T. G. (2012). The

car as an Internet-enabled device, or how to make trusted networked cars. *2012 IEEE International Electric Vehicle Conference, IEVC 2012*. https://doi.org/10.1109/IEVC.2012.6183244

Engoulou, R. G., Bellaiche, M., Pierre, S., & Quintero, A. (2014). VANET security surveys. *Computer Communications*, *44*, 1–13. https://doi.org/10.1016/j.comcom.2014.02.020

Faqih, K. M. S., & Jaradat, M.-I. R. M. (2015). Assessing the moderating effect of gender differences and individualism-collectivism at individual-level on the adoption of mobile commerce technology: TAM3 perspective. *Journal of Retailing and Consumer Services*, *22*, 37–52. Retrieved from https://www.researchgate.net/profile/Khaled_Fagih/publication/268749607_Assessing_the_moderating_effect_of_gender_differences_and_individualism-collectivism_at_individual-level_on_the_adoption_of_mobile_commerce_technology_TAM3_perspective/links/5a3e33ed4

Fathema, N., Shannon, D., & Ross, M. (2015). Expanding the Technology Acceptance Model (TAM) to examine faculty use of Learning Management Systems (LMSs) in higher education institutions. *MERLOT Journal of Online Learning and Teaching*, *11*(2). Retrieved from http://jolt.merlot.org/Vol11no2/Fathema_0615.pdf

Fernandez Ruiz, P. J., Hidalgo, F. B., Nieto Guerra, C. A., & Gomez Skarmeta, A. F. (2015). Mobility and security in a real VANET deployed in a heterogeneous networks. *Security and Communication Networks*, *9*(22), 208–219. https://doi.org/10.1002/sec.518

Fishbein, M., & Ajzen, I. (1972). Attitudes and opinion. *Annual Review of Psychology*, *23*(1), 487–544.

Fisher, W., & Allen, C. (2015). Road warriors and information systems security: Risks and recommendations. *Journal of Management Information and Decision Sciences*, *18*(1), 84–96.

Foltz, C. B., Newkirk, H. E., & Schwager, P. H. (2016). An empirical investigation of factors that influence individual behavior toward changing social networking security settings. *Journal of Theoretical and Applied Electronic Commerce Research*, *11*(2), 2–2. https://doi.org/10.4067/S0718-18762016000200002

Fournaris, A. P., & Sklavos, N. (2014). Secure embedded system hardware design - A flexible security and trust enhanced approach. *Computers and Electrical Engineering*, *40*(1), 121–133. https://doi.org/10.1016/j.compeleceng.2013.11.011

Goyal Chin, A., Etudo, U., & Harris, M. A. (2016). On mobile device security practices and training efficacy: An empirical study. *Informatics in Education*, *15*(2), 235–252. https://doi.org/10.15388/infedu.2016.12

Greene, S. (2014). *Security program and policies: Principles and practices*. Indianapolis, IN: Pearson.

Griffin, P. H. (2014). Telebiometric authentication objects. *Procedia Computer Science*, *36*, 393–400. https://doi.org/10.1016/j.procs.2014.09.011

Hayani Abd Rahim, N., Hamid, S., Mat Kiah, L., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606–622. https://doi.org/10.1108/K-12-2014-0283

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law and Security Review*, *29*(3), 236–245. https://doi.org/10.1016/j.clsr.2013.03.003

Hines, N. (2015). *Barriers to securing data on Bluetooth-enabled mobile devices: A phenomenological study.* (Doctoral dissertation, University of Phoenix). Available from ProQuest Dissertations and Theses database. (UMI No. 10012368)

Hoppe, T., Kiltz, S., & Dittmann, J. (2011). Security threats to automotive CAN networks - Practical examples and selected short-term countermeasures. *Reliability Engineering and System Safety*, *96*(1), 11–25. https://doi.org/10.1016/j.ress.2010.06.026

Humaidi, N., & Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, *5*(4), 311–318. https://doi.org/10.7763/IJIET.2015.V5.522

Hurst, W., Shone, N., El Rhalibi, A., Happe, A., Kotze, B., & Duncan, B. (2017). Advancing the micro-CI testbed for IoT cyber-security research and education. In *The Eighth International Conference on Cloud Computing, GRIDS, and Virtualization* (pp. 129–134).

Hycner, R. H. (1985). Some guidelines for the phenomenological analysis of interview data. *Human Studies*, *8*, 279–303.

Ibn Minar, N. B. N., & Tarique, M. (2012). Bluetooth security threats and solutions: A survey. *International Journal of Distributed and Parallel Systems*, *3*(1), 127–148. https://doi.org/10.5121/ijdps.2012.3110

Johnston, A. C., & Warkentin, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113–134.

Karumanchi, S., Squicciarini, A., & Lin, D. (2015). Privacy-aware access control for message exchange in vehicular ad hoc networks. *Telecommunication Systems*, *58*(4), 349–361. https://doi.org/10.1007/s11235-014-9881-8

Kaur, G., & Jain, B. (2013). Data communication via Bluetooth - A trusted device. *Atharva A Journal of Management Research*, *5*(1), 4–11.

Kegel, R. H. P., & Wieringa, R. J. (2015). Behavior change support systems for privacy and security. Paper presetned at the Third Workshop on Behavior Change Support Systems,

Chicago, IL.

King, G., Keohane, R. O., & Verba, S. (1994). The Science in Social Science. In *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Cambridge: Princeston University Press.

Knight, A., & Saxby, S. (2014). Identity crisis: Global challenges of identity protection in a networked world. *Computer Law & Security Review*, *30*(6), 617–632. https://doi.org/10.1016/j.clsr.2014.09.001

Koscher, K. (2014). *Securing embedded systems: Analyses of modern automotive systems and enabling near-real time dynamic analysis*. (Doctoral dissertation, University of Washington). Available from ProQuest Dissertations and Theses database. (UMI No. 3641563)

Krishnan, P., & Vorobyov, K. (2015). Enforcement of privacy requirements. *Computers & Security*, *52*, 164–177. https://doi.org/10.1016/J.COSE.2015.03.004

Kumar, P., Verma, R., Prakash, A., Agrawal, A., Naik, K., Tripathi, R., … Abogharaf, A. (2016). Journal of network and computer applications Machine-to-Machine ( M2M ) communications : A survey. *Journal of Network and Computer Applications*, *66*, 83–105. https://doi.org/10.1016/j.jnca.2016.02.016

Kumar, V., & Vaid, R. (2015). Secure and authenticated vehicle navigation system. *Indian Journal of Science and Technology*, *8*(28). https://doi.org/10.17485/ijst/2015/v8i28/74872

Lee, S., & Kang, T. (2015). Adaptive multi-layer security approach for cyber defense. *Journal of Internet Computing and Services*, *16*(5), 1–9. https://doi.org/10.7472/jksii.2015.16.5.01

Leech, N. L., & Onwuegbuzie, A. J. (2007). An Array of Qualitative Data Analysis Tools: A Call for Data Analysis Triangulation. *Psychological Association*, *22*(4), 557–584. https://doi.org/10.1037/1045-3830.22.4.557

Li, S.-H., Yen, D. C., Chen, S.-C., Chen, P. S., Lu, W.-H., & Cho, C.-C. (2015). Effects of virtualization on information security. *Computer Standards & Interfaces*, *42*, 1–8. https://doi.org/10.1016/j.csi.2015.03.001

Liu, C.-C. (2015). Types of employee perceptions of information security using Q methodology: An empirical study. *International Journal of Business and Information*, *10*(4), 557–575.

Lofland, J., Snow, D. A., Anderson, L., & Lofland, L. H. (2005). *Analyzing social settings: A guide to qualitative observation and analysis* (4th ed.). Belmont, CA: Wadsworth Cengage Learning. Retrieved from https://bookshelf.vitalsource.com/books/9781305848559

Lu, Z., Wang, W., & Wang, C. (2015). On the evolution and impact of mobile botnets in wireless networks. *IEEE Transactions on Mobile Computing*. https://doi.org/10.1109/TMC.2015.2492545

Mastakar, G. (2012). Experimental security analysis of a modern automobile. *IEEE Symposium on Security and Privacy*, 1–16.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2016). Individual differences and information security awareness. *Computers in Human Behavior*, *69*. https://doi.org/10.1016/j.chb.2016.11.065

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*, 23–41. https://doi.org/10.1080/15332861.2010.487415

Mensch, S. (2015). Cell phone security: Usage trends and awareness of security issues. *Global Education Journal*, 32–39.

Mitra, S. (2016). *A quantitative investigation of the security factors affecting the use of IT systems in public networks*. Trident University International.

Mozzaquatro, B. A., Jardim-Goncalves, R., Melo, R., & Agostinho, C. (2016). The application of security adaptive framework for sensor in industrial systems. *IEEE Instrumentation and Measurement Society*. https://doi.org/10.1109/SAS.2016.7479838

Murphy, L. B. (1993). The demands of beneficence. *Philosophy and Public Affairs*, *22*(4), 267–292.

Nelson, V., & Martin, A. (2013). The Strategic Use of Case Studies in the Monitoring and Evaluation Systems of Sustainability Standards. Retrieved from http://www.nri.org/images/Programmes/EquitableTrade/The-strategic-use-of-case-studies-by-standard-systems.pdf

Ngoqo, B., & Flowerday, S. V. (2015). Exploring the relationship between student mobile information security awareness and behavioural intent. *Information and Computer Security*, *23*(4), 406–420. https://doi.org/10.1108/ICS-10-2014-0072

Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, *32*, 17–31. https://doi.org/10.1016/j.adhoc.2015.01.006

Nikou, S. A., & Economides, A. A. (2017). Mobile-Based Assessment: Integrating acceptance and motivational factors into a combined model of Self-Determination Theory and Technology Acceptance. *Computers in Human Behavior*, *68*, 83–95. https://doi.org/10.1016/j.chb.2016.11.020

NIST. (2013). *Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r4

Omar, M. (2012). *Smartphone Security: Defending Android-based Smartphone Against Emerging Malware Attacks*. (Doctoral dissertation, Colorado Technical University). Available from ProQuest Dissertation and Theses database. (UMI No. 3525516)

Onishi, H., Wu, K., Yoshida, K., & Kato, T. (2017). Approaches for vehicle cyber-security in the US. *International Journal of Automotive Engineering*, *8*, 1–6.

Pahnila, S., Karjalainen, M., & Siponen, M. (2013). Information security behavior: Towards multi-stage models. *PACIS*. Retrieved from https://pdfs.semanticscholar.org/eb88/de4fbece28d90eada9331747b12ee759f810.pdf

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: a comparison of two studies. *Information and Computer Security*, *24*(2), 228–240. https://doi.org/10.1108/ICS-01-2016-0009

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers and Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. *Journal of Counseling Psychology*, *52*(2), 137–145. https://doi.org/10.1037/0022-0167.52.2.137

Pope, C., & Mays, N. (1995). Qualitative Research: Reaching the parts other methods cannot reach: an introduction to qualitative methods in health and health services research. *BMJ*, *311*. https://doi.org/10.1136/bmj.311.6996.42

Popescul, D., & Radu, L. D. (2016). Data Security in Smart Cities: Challenges and Solutions. *Informatica Economică*, *20*(1), 29–39. https://doi.org/10.12948/issn14531305/20.1.2016.03

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Qu, Y., & Chan, P. (2016). Assessing vulnerabilities in Bluetooth Low Energy ( BLE ) wireless network based IoT systems. In *IEEE International Conference on Big Data Security* (pp. 42–48). https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.63

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology: Interdisciplinary and Applied*. https://doi.org/10.1080/00223980.1975.9915803

Rozenberg, Y. (2012). Challenges in PII data protection. *Computer Fraud & Security*, *2012*(6), 5–9. https://doi.org/10.1016/S1361-3723(12)70061-1

Rubinstein, I. S., & Hartzog, W. (2016). Anonymization and risk. *Washington Law Review*, *91*, 703–760.

Safa, N. S., Sookhak, M., Solms, R. Von, Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Sengupta, S., & Sarkar, P. pratim. (2015). An augmented level of security for Bluetooth devices controlled by smart phones and ubiquitous handheld gadgets. *International Journal of*

*Information Engineering and Electronic Business*, *7*(4), 58–75. https://doi.org/10.5815/ijieeb.2015.04.08

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

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2014). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Simpson, J. P. (2016). *Empirical analysis of socio-cognitive factors affecting security behaviors and practices of smartphone users* (Doctoral dissertation, Nova Southeastern University). Available from ProQuest Dissertations and Theses database. (UMI No. 10044129)

Siponen, M. T. (2001). Five dimensions of information security awareness. *Computers and Society*, *31*(2), 24–29. https://doi.org/10.1145/503345.503348

Sohrabi Safa, N., von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, 15–18. https://doi.org/10.1016/S1361-3723(16)30017-3

Sommestad, T., Karlzén, H., & Hallberg, J. (2017). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, *23*(2), 200–217. https://doi.org/10.1108/ICS-04-2014-0025

Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality – an empirical study. *Accounting and Management Information Systems*, *15*(1), 112–130.

Strickland, L. S., & Hunt, L. E. (2005). Technology, security, and individual privacy: New tools, new threats, and new public perceptions. *Journal of the American Society for Information Science and Technology*, *56*(3), 221–234. https://doi.org/10.1002/asi.20122

Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research & Applications*, *5*, 147–158.

Tyagi, A. K. (2016). Cyber Physical Systems ( CPSs ) – Opportunities and challenges for improving cyber security. *International Journal of Computer Applications*, *137*(14), 19–28.

U.S. Census Bureau. (n.d.). Cedar Rapids city, Iowa. Retrieved April 21, 2017, from https://www.census.gov/quickfacts/table/RHI805210/1912000

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

Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under

conditions of strain and excess. *Journal of Association for Information Systems*, *17*(1), 39–76.

Warkentin, M., Walden, E., Johnston, A. C., & William Straub, D. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of Association for Information Systems*, *17*(3), 194–215.

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review*, *31*(5), 618–627. https://doi.org/10.1016/j.clsr.2015.07.002

Wibowo, K., & Ali, A. (2016). Mobile Security: Suggested security practices for malware threats. *Competition Forum; Indiana*, *14*(1), 119–126.

Wu, B., & Chen, X. (2017). Continuance intention to use MOOCs: Integrating the technology acceptance model (TAM) and task technology fit (TTF) model. *Computers in Human Behavior*, *67*, 221–232. https://doi.org/10.1016/j.chb.2016.10.028

Yadav, A., Bose, G., Bhange, R., Kapoor, K., Iyengar, Nc., & Caytiles, R. D. (2016). Security, vulnerability and protection of vehicular on-board diagnostics. *International Journal of Security and Its Applications*, *10*(4), 405–422. https://doi.org/10.14257/ijsia.2016.10.4.36

Ying, B., Makrakis, D., & Mouftah, H. T. (2012). Privacy preserving broadcast message authentication protocol for VANETs. *Journal of Network and Computer Applications*, *36*, 1–13. https://doi.org/10.1016/j.jnca.2012.05.013

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407–416.

Zhou, X. (2015). *The security and privacy of mobile platforms in a rapidly evolving world*. *ProQuest Dissertations and Theses*. Indiana University.

## APPENDIX A

The research instrument used for this study consisted of several questions that the participants were asked. The questions below are the questions each of the participants answered.

1. What are some observations you made when pairing the smartphone to the automobile?
2. When pairing the smartphone, what challenges did you encounter and how did you overcome them?
3. What beliefs do you have about automotive infotainment systems and the external connections?
4. Please describe the overall process of pairing the smartphone.
5. When removing the smart phone, what observations about the un-pairing process are distinct in your memory?
6. What kind of security training have you received within the past twelve months and how has it influenced your behaviors with mobile devices?
7. What topics or learning points were memorable from the security awareness training and why where those specific topics or learning points memorable?
8. What awareness do you have about the information synchronized with an automobile when pairing a smart phone?
9. What information do you think is transferred to an automobile when pairing a smart phone? Why do you think that is the only information?
10. When removing the smartphone from the automobile what feelings did you have that the data was actually removed from the infotainment system?
11. What type of verification mechanism existed to demonstrate the information was removed and how did that influence your feelings about connecting a smartphone?

12. If you could give security advice to the automobile manufacturers regarding infotainment systems, what would that advice be?