Prospectus

An Analysis of Cybersecurity Behavior in Older Adults Using Protection Motivation Theory and the Theory of Planned Behavior

Chapter 1: Introduction to the Study

Introduction

Research has found that a prevalent cybersecurity paradox exists between privacy needs and actual cybersecurity behaviors (Choi, Levy, & Hovav, 2013; Onarlioglu, Yilmaz, Kirda, & Balzarotti, 2012; Othmane et al., 2013; Pfleeger & Caputo, 2012). Although there is an expansive body of literature on cybersecurity behaviors, the majority of studies lack homogeneous data, consistent results, and adequate solutions for increasing cybersecurity awareness and the adoption of safe practices. The proposed study seeks to examine the nature and extent of perceptions, attitudes, and responses to cybersecurity risk management. The background of the study, research design, theoretical frameworks, limitations, and significance will be discussed in the following sections.

Background of the Study

A systematic review was conducted to identify studies on cybersecurity, cyber risk management behavior, cyberinsurance, and theoretical studies on Protection Motivation Theory and the theory of planned behavior. The database was used to search the terms including: *cybersecurity, cybersecurity risk, online privacy, cyberinsurance, Protection Motivation Theory, theory of planned behavior, cybersecurity and age, cybersecurity and gender, cybersecurity and ethnicity, digital divide, online risk, social media, information sharing, cybersecurity practices, cybersecurity perceptions,* and *mobile security.* Publications were restricted to peer-reviewed journals and only recent publications (since year 2011) were used except for a minority of earlier seminal publications. Reference lists in publications were also used to screen for acceptable

studies. There is a potential for selection bias as the search was limited to published, peer-reviewed studies written in English. However, due to the nature of the study, sources applicable to Internet-use in the United States were of interest.

Inadequate cyber safety measures significantly impact the security of privacy and economic stability individuals (Choi, Levy, & Hovav, 2013; Onarlioglu, Yilmaz, Kirda, & Balzarotti, 2012; Othmane et al., 2013; Pfleeger & Caputo, 2012). Human error accounts for 50% to 75% of data breaches. $20 billion in economic losses are a result of cybersecurity breaches (Choi, Levy, & Hovay, 2013; Lagrule, 2015). Factors such as age, gender, and ethnicity have not adequately been examined in contexts of technology use, accessibility, and safety practices (Chakraborty, Vishik, & Rao, 2013; Maaß, 2011; Sánchez, Kaplan, & Bradley, 2015; Kisekka, Bagchi-Sen, & Rao, 2013; Sofo & Sofo, 2014; Thelwall, 2011; Whitty, Doodson, Creese, & Hodges, 2015). The proposed study will examine cybersecurity practices and perceptions using Protection Motivation Theory and the theory of planned behavior (Crossler & Bélanger, 2014; Saeri et al., 2014; Salleh et al., 2012). This study will contribute to data on human factors in cybersecurity behavior, as research has shown that cybersecurity risks are not always adequately addressed or realized (Claar & Johnson, 2012; Hettema et al., 2014).

Cybersecurity risks. Cybersecurity risks threaten micro-level stability such as individual financial stability and unethical use of personal information as well as macro-level stability including organizational and governmental stability and functionality (Choi, Levy, & Hovav, 2013; Levy, Ramim, & Hackney, 2013; Onarlioglu, Yilmaz, Kirda, & Balzarotti, 2012; Othmane et al., 2013; Pfleeger & Caputo, 2012). Human error and misuse is a substantial factor in cybersecurity breaches (Choi, Levy, & Hovay, 2013;

Lagrule, 2015). There is a gap in consistent data on the impact of human behaviors and perceptions on safe security practices (Choi, Levy, & Hovay, 2013; Crossler & Bélanger, 2014; Onarlioglu et al., 2012; Othmane et al., 2013; Pfleeger & Caputo, 2012; Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014; Salleh et al., 2012). There is also a need to examine perceptions that keep individuals from adopting safe security practices (Claar & Johnson, 2012; Crossler & Bélanger, 2014). In order to examine perceptions on cybersecurity risks, Protection Motivation Theory, a framework often used to analyze behavioral factors that affect security adoption behaviors, will be used in the study.

Protection Motivation Theory. Protection Motivation Theory is frequently used in theoretical works to understand fear and risk motivation (Crossler & Bélanger, 2014; Salleh et al., 2012). Crossler and Bélanger (2014), using Protection Motivation Theory frameworks, found that the literature is not consistent on the effect of perceived severity and vulnerability with safe security practices. Salleh et al. (2012), however, found that cybersecurity behaviors were mediated by all of the tenets of PMT. Furthermore, perceived vulnerabilities, perceived severity, previous incidents, and response efficacy affect the adoption of safe security practices (Anwar et al., 2015; Choo et al., 2015; Crossler & Bélanger, 2014; Salleh et al., 2012). In several studies, it was found that skill is not as much of a factor as perceptions and beliefs in the adoption of safe security practices (Anwar et al., 2015; Choo et al., 2015; Crossler & Bélanger, 2014; Salleh et al., 2012).

Some research suggests perception of responsibility and personal and work boundaries also affect the adoption of safe security practices (Ifinedo, 2012; McBride, Carter, & Warkentin, 2012; Safa et al., 2015; Warkentin, Malimage, & Malimage, 2012).

Individuals that do not feel continuity in organizational cybersecurity policies and their role in the organization are less likely to consistently adopt and use safe security practices (Ifinedo, 2012; McBride, Carter, & Warkentin, 2012; Safa et al., 2015; Warkentin, Malimage, & Malimage, 2012). Cultural differences in risk perceptions also affect security habits (Bada, Sasse, & Nurse, 2014; Crossler et al., 2013; Whitty et al., 2015).

Cybersecurity solutions to improving awareness have varied in consistency. Threat appraisals may be more successful in promoting safe security practices than coping appeals (Boss et al., 2015; Lee, 2011). However, it is unknown how effective threat appraisals are in longitudinal studies on cybersecurity practices, and factors that mediate security behaviors are not widely understood. More research is needed to separate insider deviant behavior and misbehavior, understand hackers, and improve security compliance (Crossler et al., 2013). When examining cybersecurity behaviors, the theory of planned behavior is also used to analyze behavior by linking beliefs to behaviors.

Theory of planned behavior. The theory of planned behavior posits that subjective norms mediate behavior intentions (Ajzen, 1991; Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014). Tenets of the theory of planned behavior, including security experience and involvement, attitude, subjective norms, threat appraisal, and self-efficacy, positively affect user behavior (Claar & Johnson, 2012; Ifinedo, 2012; Safa et al., 2015; Sommestad & Hallberg, 2013). Online behaviors, attitudes, and normative beliefs are mediated through intentions (Burns & Roberts, 2013). Perceived behavioral control affects security behaviors (Burns & Roberts). Technical knowledge, organizational impact, and attacker assessment are correlated with cybersecurity

awareness (Mejias, 2012). Additionally, cultural differences have been found to affect sharing behavior (Hassandoust, Kazerouni, & Perumal, 2012). Security incidents also affect safe security practice adoption (Lee & Lee, 2012). Online habits, social media practices, and information disclosure results in a privacy paradox between social interaction and cybersecurity practices (Lewis, 2011; Taddicken & Jers, 2011; Trepte & Reineke, 2011; Ziegele & Quiring, 2011).

Information disclosure and privacy. Cybersecurity misconceptions, smart device use, lack of awareness, and information disclosure behavior affect security risks (Geneiatakis, Kounelis, Loeschner, Fovino, & Stirparo, 2013; Henshel, Cains, Hoffman, & Kelley, 2015; Manson & Pike, 2014; McClain et al., 2015; Onarlioglu et al., 2012, Othmane et al., 2013; Pfleeger & Caputo, 2012; Salem & Stolfo, 2011; Wang, 2013). Social capital theory has been used to explain information sharing behavior. Lack of sharing leads to reduced user experience and may be seen as anti-normative in some contexts (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011; Joinson, Houghton, Vasalou, & Marder, 2011; Papacharissi & Gibson, 2011). Privacy can be seen as a way to control personal information or to control outside perceptions (Debatin, 2011; Yao, 2011). Privacy is dynamic and defined by users (Hartmann, 2011). While privacy is defined by user perceptions, social networking provides avenues for self-presentation and new avenues for presenting the self (Krämer & Haferkamp, 2011; Papacharissi & Gibson, 2011). Social networking and the ability to present the self may conflict with privacy maintenance (Krämer & Haferkamp, 2011). Cybersecurity practices are further affected by access, technological exposure, and perceptions mediated by age, ethnicity, and sex.

Cybersecurity practices and the digital divide. Research has shown older individuals and women are greatly impacted by cybersecurity threats (Sánchez, Kaplan, & Bradley, 2015). Social media use in older individuals has doubled from 2009 to 2010 (Maaß, 2011). Email and Internet searches are the most commonly used Internet functions in older individuals (Maaß, 2011). Individuals over the age of 55 are also more vulnerable to cybersecurity threats (Sánchez, Kaplan, & Bradley, 2015). For instance, older individuals are more likely to disclose private information online (Chakraborty, Vishik, & Rao, 2013; Kisekka, Bagchi-Sen, & Rao, 2013). Older adults are more likely to be influenced by friends on social media and may feel more comfortable with sharing information when they observe their friends sharing information (Chakraborty, Vishik, & Rao, 2013). Older individuals also face barriers, such as medical issues, to acquiring technological skill (Sofo & Sofo, 2014). Gender is also a significant factor when analyzing cybersecurity behavior. Specific cybersecurity concerns, such as cyberbullying and stalking, affect women more frequently (Thelwall, 2011). Some women are more likely to use Internet websites due to the perceived safety of communicating online verses in person, where the threat of physical violence is a possibility (Thelwall, 2011). Though risks may affect individuals disproportionately, cybersecurity measures can be taken to aid in providing technological security.

Cyberinsurance. Cyberinsurance and safety measures, including decoy information fogging, can provide individuals and network providers with solutions to dealing with cybersecurity threats (Bowen, Devarajan, & Stolfo, 2011; Pal & Hui, 2012; Pal, Golubchik, Psounis, & Hui, 2014; Silva et al., 2014; Stolfo, Salem, & Keromytis, 2012; Toregas, C., & Zahn, 2014; Zang and Lui, 2014). Risk estimation can be

calculated using connection network information, user behavior, health insurance models, and prediction markets (Bandyopadhyay, 2012; Barracchini & Addessi, 2014; Bonner, 2012; Garrie & Mann, 2014; Herath & Herath, 2011; Lazka, 2014; Pal & Hui, 2012; Pal et al., 2014; Pandey & Snekkenes, 2014; Stolfo, Salem, & Keromytis, 2012; Toregas, C., & Zahn, 2014; Zang and Lui, 2014). Some research, however, suggests that cyberinsurance is impractical because security is interdependent on an individual's own security and network security (Schwartz, Shetty, & Walrand, 2013). Biener, Eling, & Wirfs (2015) argue that because cyber systems are designed in similar ways, they are vulnerable to the same risks; therefore, cyberinsurance can be designed based on risk estimation.

Problem Statement

Cybersecurity vulnerabilities pose a significant threat to the financial stability of organizations and individuals, and cybersecurity threats have significantly increased with the use of social media and smart devices (Choi, Levy, & Hovav, 2013; Onarlioglu, Yilmaz, Kirda, & Balzarotti, 2012; Othmane et al., 2013; Pfleeger & Caputo, 2012). Information systems misuse accounts for 50% to 75% of cybersecurity threats (Choi, Levy, & Hovay, 2013). Cybersecurity improvements have been attempted, but there is a gap in consistent, heterogeneous studies analyzing the impact of behavior on cybersecurity (Choi, Levy, & Hovay, 2013; Crossler & Bélanger, 2014; Onarlioglu et al., 2012; Othmane et al., 2013; Pfleeger & Caputo, 2012; Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014; Salleh et al., 2012). The problem to be studied addresses behaviors such as perceived trust, information disclosure, and lack of use of security software that create cybersecurity vulnerabilities. The study will draw from Protection Motivation Theory

(PMT), involving the examination of the processes undertaken when making decisions about security, and the theory of planned behavior, a framework involving the prediction of behavior using attitudes, subjective norms, and perceived behavioral control to understand intention (Crossler & Bélanger, 2014; Saeri et al., 2014; Salleh et al., 2012). Using PMT and the theory of planned behavior, behaviors and user beliefs on cybersecurity will be investigated to increase awareness and identify solutions. Several studies have examined specific misuse and risk management tactics, finding that misconceptions on safe Internet use, strong interconnectedness with smart devices, misinformation, and information disclosure behavior affect security risks (Geneiatakis, Kounelis, Loeschner, Fovino, & Stirparo, 2013; Onarlioglu et al., 2012, Othmane et al., 2013; Pfleeger & Caputo, 2012; Salem & Stolfo, 2011; Wang, 2013). Other studies have examined possible solutions, including decoy information fogging and cyber-insurance (Pal & Hui, 2012; Pal, Golubchik, Psounis, & Hui, 2014; Stolfo, Salem, & Keromytis, 2012; Toregas, C., & Zahn, 2014; Zang & Lui, 2014). In the proposed study, cybersecurity behaviors and beliefs will be examined in relation to the perceived effectiveness of solutions, such as cyber-insurance, adding to the theoretical knowledge of human factors in security management.

Purpose of the Study

The purpose of this cognitive ethnographic study is to understand cybersecurity decision-making processes, and the attitudes, subjective norms, and perceived behavioral control factors that affect the intention to adopt safe security practices. The proposed study will examine cognitive processes and social contexts of a diverse sample of 15 individuals age 55 and older in Maryland. Research has shown that a "digital divide"

persists between older and younger Internet users (Whitty, Doodson, Creese, & Hodges, 2015). At this stage in research, "digital divide" will be defined as a gap between demographic or regional groups that have little to no access to modern technology and groups that do not have restricted access to technology. In this particular study, the "digital divide" will be focused on accessibility and understanding of technology in older adults. The theories guiding this study are Protection Motivation Theory and the theory of planned behavior as they examine how social contexts and behavioral factors relate to security intention and motivation.

Research Questions

To understand the implications of cybersecurity perceptions on user behavior, several questions must be addressed. These questions center on perceptions of cybersecurity threats, attitudes on cybersecurity, observation of practices, and lived experiences with technology. The research questions are addressed below:

RQ1. Do impulsivity, self-monitoring, locus of control, and knowledge factors affect the adoption of safe cybersecurity practices?

RQ2. How do older adults perceive cybersecurity threats?

RQ3. How do older adults describe their experiences with using technology?

Theoretical Framework

Protection Motivation Theory (PMT) and the theory of planned behavior are proposed to understand security and risk behaviors. PMT was proposed by R.W. Rodgers in 1975 to understand fear coping behavior. PMT has been extended to understand fear and risk thought processes, including perceived cybersecurity risks (Crossler & Bélanger, 2014; Salleh et al., 2012). In PMT, the process begins with

receiving and evaluating information, described as the cognitive mediating process. Information can be received from the external environment or interpersonal beliefs. Finally, the information is used to take action, known as the coping mode (Crossler & Bélanger, 2014; Salleh et al., 2012). In the cognitive mediating process, the threat appraisal process and the coping appraisal process mediate the application of a response (Crossler & Bélanger, 2014; Salleh et al., 2012).

In the threat appraisal process, the individual perceives the vulnerability and severity of a threat (Crossler & Bélanger, 2014; Salleh et al., 2012). During the coping appraisal phase, threat solutions or actions, the ability to perform actions (self-efficacy), and action-worth (perceived cost) are examined (Crossler & Bélanger, 2014; Salleh et al., 2012). In studies on PMT and cybersecurity, interpretations of security behaviors indicate a range of beliefs and embodied perceptions of risk (Crossler & Bélanger, 2014; Salleh et al., 2012). Crossler and Bélanger (2014) found that the effect of perceived severity and vulnerability on the adoption of cybersecurity practices is not consistent in the literature, while Salleh et al. (2012), found that all of the tenets of PMT were applicable to cybersecurity behaviors. However, most research has focused on singular rather than holistic or generalizable aspects of behavior.

The theory of planned behavior, created by Icek Ajzen in 1985, also examines processes that produce behavioral change by linking beliefs to behaviors (Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014). Recently, researchers have investigated the utility of online behavior and privacy applications to the theory. Research has found the theory of planned behavior can predict behavior based on attitudes and intentions, however, other factors, such as fear of crime and trust, can also predict behavior (Saeri et al., 2014). One

significant component of the theory is the subjective norm component. Subjective norms are comprised of injunctive norms, what individuals approve or disprove of, and descriptive norms, what individuals actually do (Saeri et al., 2014). Theoretically, these norms are seen as predictors of behavior (Saeri et al., 2014). In terms of online behavior and security, anecdotal evidence suggests that analyzing the distinction between subjective norms can shed light on misalignments of online privacy norms (Saeri et al., 2014). Still, information on behavioral influence has not been consistently conducted, and there is a need for research guided by theoretical frameworks.

Nature of the Study

The purpose of this cognitive ethnographic study is to understand cybersecurity decision-making processes, and the attitudes, subjective norms, and perceived behavioral control factors that affect the intention to adopt safe security practices in a diverse sample of 15 computer users with various levels of technological self-efficacy over the age of 55 in Maryland. The research design, proposed methodology, data collection and analysis methods, and ethical considerations will be discussed below.

Methodology. This study will employ a qualitative ethnographic analysis to examine cognitive thought processes and behaviors that mediate the adoption of safe cybersecurity practices. Cognitive ethnography will be specifically used to study the cognitive processes that affect social contexts and meanings (Wolf, 2012). Cognitive ethnography specifically focuses on the meanings of social practices, how people acquire information about the world, how information is processed and culturally transmitted, and how individuals act on their decisions (Wolf, 2012). This type of ethnography is appropriate because many factors and cultural beliefs have been shown to affect

cybersecurity practices and awareness during decision-making processes (Crossler & Bélanger, 2014; Saeri et al., 2014; Salleh et al., 2012). A qualitative approach, in this context, is more appropriate for understanding the extent of social experiences that have deep-rooted sociocultural influences. Quantitative analysis will not be used because the research questions of this study center on the in-depth analysis of perceptions and behavior within a particular group of people.

Research design. Ethnography is often used in qualitative research to analyze how cultural and social processes affect perceptions and behaviors. Cognitive ethnographic analysis was chosen due to its usefulness in understanding sociocultural problems by analyzing thought processes. A case study design would not be appropriate for this study because case studies more often focus on the group-effect of a phenomenon rather than how individuals perceive problems and make decisions (Johansson, 2003; LeCompte & Schensul, 2010; 2013). When using a phenomenological methodology, a broad, universal understanding of a particular phenomenon is formulated, however, the proposed study seeks to understand how several sociocultural phenomena affect beliefs on cybersecurity on an individual level (Moustakas, 1994). Because the proposed study focuses on tenets of Protection Motivation Theory and the theory of planned behavior, Grounded theory and content analysis are not preferred methods (Glaser, 1977; LeCompte & Schensul, 2010; 2013). The study also involves the analysis of direct user experiences, therefore Delphi methods are also unfavorable since they utilize expert testimonies that provide information from an indirect source (Cuhls, 2015). Finally, action research, while beneficial to both researchers and research subjects by eliciting involvement in participatory research, was not chosen as participants will have varying

levels of experience and exposure to technology, and action research produces better results with a homogenous group of stakeholders (LeCompte & Schensul, 2010). In this particular study, cognitive ethnographic methods will provide the most detailed information on experiences and thought processes as well as gender, age, and cultural influences on perspectives.

Sampling. This study focuses on the experiences of older adults (age 55 and over) because older individuals have a wide range of security practices and are more vulnerable to security risks (Whitty, Doodson, Creese, & Hodges, 2015). The sample will depend upon screening for 15 participants based on particular criteria. Sampling criteria will be broad and include individuals age 55 and over and include multiple genders, and ethnicities. The study will focus on Black, White, Asian, and Latino ethnic groups. The study will include participants with varying levels of technological efficacy, but all participants must have some familiarity with computer technology.

The sample size of 15 subjects was chosen to provide a large enough size to obtain high quality data without exhausting time and resources. If the sample size is not obtainable given the current research conditions, more in-depth research will be conducted with the number of participants available for the study. This study requires a large enough sample for generalizability but a small enough size for effective, in-depth analysis. The use of 15 subjects is ideal because it would allow for the researcher to collect more in-depth data about multiple concepts and themes.

Measurement. Since the experiences of the participants cannot be easily measured quantitatively, open-ended interviews will be conducted with participants and coded for significant themes. Confidentiality will be ensured, and participant data will

only be used with signed consent. Participants will be informed of their ability to end research at any time. Information will be gathered using systematic observations, and written and taped field notes and interviews (LeCompte & Schensul, 2010). Interview data will be transcribed, recorded, and coded for common and outlying themes.

Data Collection. Open-ended interviews will be conducted individually. In addition, field notes and observational data will be recorded to observe how participants behave when confronted with virtual processes. In-depth, open-ended interviews do not involve asking interviewees to select from a group of answers, but rather involves the exploration of all relevant responses (LeCompte and Schensul, 2013). Therefore, open-ended interviews will be conducted will all 15 participants. Open-ended interviews were chosen to effectively understand individual behavior and how individuals make decisions on cybersecurity. Open-ended interviews also have the advantage of being able to orient the study to the context of the study site (LeCompte and Schensul, 2013). Another benefit of using open-ended interviews is the building of trust and positive relationships between interviewees and the interviewer. In addition, using maps, organizational charts, photographs, and virtual process demonstrations can be effective in eliciting information about specific concepts. Open-ended interviews will be used to gain a sense of the types of experiences and concerns participants have with cybersecurity processes. Participants will also be observed or asked to demonstrate how security precautions are taken.

After data collection, data will be analyzed using inductive, bottom-up ethnographic methods. Information will be grouped into large conceptual categories derived from Protection Motivation Theory and theory of planned behavior frameworks. Data will be contextualized and sorted into other categories within the broader categories.

Key words, patterns, conceptual models, concepts, social processes, and descriptive theories will be coded for during analysis. Data will be grouped into clusters, or major themes, and compared in terms of similarities, characteristics, and patterns. Tables will be created using "indicators," "themes," and "interpretive statements" and analyzed as either low-levels of inference, including as surface, descriptive, and explicit structures, or high-levels of inference, including deep, symbolic, or latent structures (Wolf, 2012). Relationships between themes and categories will also be analyzed.

The process of crystallization, a result of reflection and interpretation, will be used to cohesively analyze themes into patterns or categories based on beliefs, values, and normative concepts (Wolf, 2012). Interpretations of data will be balanced with theoretical frameworks, research questions, and findings of other studies. To be effective, this study must involve the consideration of people and their cultural contexts. Concepts and themes that emerge during data collection will be defined and described by the participants in order to minimize researcher bias and assumptions. Participant-defined terms will be analyzed within larger thematic concepts. The focus of the research will involve observations of what is actually happening, how certain processes differ from other processes, how individuals behave and interact, and what is considered important (LeCompte & Schensul, 2010; 2013).

Definition of Terms

Cognitive mediating process. The cognitive mediating process is the process of evaluation information using external or interpersonal beliefs and factors (Crossler & Bélanger, 2014; Salleh et al., 2012).

Coping appraisal process. The coping appraisal process involves the examination of the ability to perform actions to prevent the perceived threat as well as the determination of the perceived worth of the action (Crossler & Bélanger, 2014; Salleh et al., 2012).

Coping mode. The coping mode is when information is used to take action to respond to a perceived threat (Crossler & Bélanger, 2014; Salleh et al., 2012).

Descriptive norms. Descriptive norms are defined as observed behaviors (Saeri et al., 2014).

Injunctive norms. Injunctive norms are behaviors that individuals approve or disprove of (Saeri et al., 2014).

Threat appraisal process. The threat appraisal process occurs when individuals perceive a risk and examine their vulnerability (Crossler & Bélanger, 2014; Salleh et al., 2012).

Assumptions, Limitations, Delimitations

Due to the nature of the study, limitations may be present during research. Because the proposed study is not longitudinal, sampling and maturity bias may have an effect on the perceptions of participants. However, despite changes in perceptions that may occur over time, recording such perceptions will still provide valuable information on the experiences of users. Furthermore, the sample may not be representative or generalizable. The proposed study is seeking to investigate potential differences among individuals in a diverse sample, but there is a possibility that individual perceptions will not vary across age, gender, and ethnicity. Regardless, such information will be of value in designing and improving cybersecurity.

Self-reporting may be a limiting factor in the quantitative studies that assessed cybersecurity behaviors. There is a lack in consistency in qualitative studies on cybersecurity behaviors (Boss et al., 2015; Choi, Levy, & Hovay, 2013; Crossler & Bélanger, 2014; Onarlioglu et al., 2012; Othmane et al., 2013; Pfleeger & Caputo, 2012; Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014; Salleh et al., 2012). Cyberinsurance has been theoretically examined, but user perceptions on cyberinsurance have not been addressed (Bandyopadhyay, 2012; Barracchini & Addessi, 2014; Lazka, 2014; Pal & Hui, 2012; Pal et al., 2014; Pandey & Snekkenes, 2014; Stolfo, Salem, & Keromytis, 2012; Toregas, C., & Zahn, 2014; Zang and Lui, 2014).

Ethical considerations. Voluntary participation, informed consent, full disclosure of the study's purpose, restriction to access of data, and the recognition of protections for individual confidentiality will be ensured. Written consent forms will be provided, and explanations of the study's purpose will be fully discussed with participants. Confidentiality will be protected and no identifying information will be disclosed to keep the participants anonymous. Participants will choose a code name in order to maintain confidentiality. Participant data from the study will be stored in locked file cabinets and shredded after five years and deleted from the secure database, following the study. Furthermore, participants will have the ability to drop out of the study at any time. In the case of participant drop out, data will be dropped from the study and research will then focus on the remaining participants.

Significance of the Study

The dangers and vulnerabilities of cybersecurity threats can be devastating to individuals and organizations. It is necessary to ensure cybersecurity protection and

instill preventative practices in users. Qualitative studies on cybersecurity perceptions and behaviors are crucial to understanding user behavior and improving security awareness and safe practice adoption. This study is significant in that it will fill gaps in research on risk management and external behavioral factors that are not adequately studied while also contributing to knowledge on cybersecurity practices in older adults – a population of people that are especially vulnerable to cybersecurity threats.

Conclusion

In order to improve cybersecurity awareness and safe security practice adoption, research needs to analyze decision-making processes, attitudes and beliefs, subjective norms, and perceived behavioral control factors that mediate cybersecurity behaviors. Future research should focus on analyzing the effect size, the heterogeneity of samples, digital divide effects, cyberinsurance perceptions, sensitivity analyses, robustness of results, the accuracy of self-reported and questionnaire data, and the ability of Protection Motivation Theory and the theory of planned behavior to accurately describe cybersecurity practices.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Anwar, M., Ash, I., He, W., Li, L., Xu, L., & Yuan, X. (2015). A security behavior model of employees in cyberspace. *Information Systems Security, Assurance, and Privacy.*

Bada, M., Sasse, A., & Nurse, J. R. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour? *Global Cyber Security Capacity Centre*, 1-38.

Bandyopadhyay, T. (2012). Organizational adoption of cyber insurance instruments in IT security risk management–A modeling approach. *Organizational Adoption of Cyber Insurance Instruments in IT Security Risk Management*, 23-29.

Barracchini, C., & Addessi, M. E. (2014). Cyber risk and insurance coverage: An actuarial multistate approach. *Review of Economics & Finance*, *4*(1), 57-69.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*(1), 131-158.

Bonner, L. (2012). Cyber risk: How the 2011 Sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches. *Washington University Journal of Law and Policy*, *40*, 257-277.

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 behaviors. *MIS Quarterly*, 1-70.

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). International Conference on Technologies for Homeland Security (HST): *Measuring the human factor of cyber security*.

Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, *15*(1), 48-64.

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems*, *55*(4), 948-956.

Choi, M., Levy, Y., & Hovav, A. (2013). Proceedings of the pre-ICIS workshop on information security and privacy (WISP 2013): *The Role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse.* Milan, Italy.

Choo, K. K. R., Heravi, A., Mani, D., & Mubarak, S. (2015). Employees' intended information security behaviour in real estate organisations: A protection motivation perspective. *Information Security Behaviour in Real Estate Organizations,* 1-11.

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems*, *52*(4), 20-29.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, *32*, 90-101.

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection Motivation Theory and a unified security practices (USP) instrument. *ACM SIGMIS Database*, *45*(4), 51-71.

Cuhls, K. (2015). Delphi method [PDF]. Retrieved from http://www.unido.org/fileadmin/import/16959_DelphiMethod.pdf

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. *Privacy Online*, 47-60.

Ellison, N.B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. *Privacy Online*, 19-32.

Garrie, D., & Mann, M. (2014). Cyber-security insurance: Navigating the landscape of a growing field. *John Marshall Journal of Information Technology and Privacy Law*, *31*(3), 379-392.

Geneiatakis, D., Kounelis, I., Loeschner, J., Fovino, I. N., & Stirparo, P. (2013). Security and privacy in mobile cloud under a citizen's perspective. *Cyber Security and Privacy*, 16-27.

Glaser, B.G. & Strauss, A.L. (1977). *The discovery of grounded theory: Strategies for qualitative research.* Chicago: Aldine.

Hartmann, M. (2011). Mobile privacy: Contexts. *Privacy Online*, 191-204.

Hassandoust, F., Kazerouni, M. F., & Perumal, V. (2012). Socio-behavioral factors in virtual knowledge sharing: Theory of reasoned action and theory of planned behavior perspective. *International Journal of Knowledge-Based Organizations (IJKBO)*, *2*(2), 40-53.

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, *3*, 1117-1124.

Herath, H., & Herath, T. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations*, *2*(1), 7-20.

Hettema, H., Watters, P., Sarrafzadeh, H., Fourie, L., Kingston, T., & Pang, S. (2014). Global Business and Technology Association Conference. *The global cyber security workforce: An ongoing human capital crisis.*

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83-95.

Johansson, R. (2003). Proceedings from the International Conference '03: *Case Study Methodology*. Methodologies in Housing Research: Stockholm.

Joinson, A.N., Houghton, D.J., Vasalou, A., & Marder, B.L. (2011). Digital crowding: Privacy, self-disclosure, and technology. *Privacy Online*, 33-46.

Kisekka, V., Bagchi-Sen, S., & Rao, H. R. (2013). Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users. *Computers in Human Behavior*, *29*(6), 2722-2729.

Krämer, N.C. & Haferkamp, N. (2011). Online self-presentation: Balancing privacy concerns and impression construction on social networking sites. *Privacy Online*, 127-143.

Lagrule, C. M. (2015). *The association and probability of a predictive relationship between cyber security incidents and type of Internet connectivity: A quantitative study* (Doctoral dissertation).

Laszka, A., Johnson, B., Grossklags, J., & Felegyhazi, M. (2014). Estimating systematic risk in real-world networks. *Financial Cryptography and Data Security*, 417-435.

Laszka, A., & Grossklags, J. (2015). Should cyber-insurance providers invest in software security? *Computer Security*, 483-502.

LeCompte, M.D. & Schensul, J.J. (2010). *Designing and conducting ethnographic research: An introduction*. Boulder, Colorado: Altamira Press.

LeCompte, M.D. & Schensul, J.J. (2013). *Essential ethnographic methods: A mixed methods approach.* Boulder, Colorado: Altamira Press.

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, *50*(2), 361-369.

Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the Internet. *Information Systems Frontiers*, *14*(2), 375-393.

Lewis, K. (2011). The co-evolution of social network ties and online privacy behavior. *Privacy Online*, 91-110.

Levy, Y., Ramim, M. M., & Hackney, R. A. (2013). Assessing ethical severity of e-learning systems security attacks. *The Journal of Computer Information Systems*, *53*(3), 75-84.

Maaß, W. (2011). The elderly and the Internet: How senior citizens deal with online privacy. *Privacy Online*, 235-249.

Manson, D., & Pike, R. (2014). The case for depth in cybersecurity education. *ACM Inroads*, *5*(1), 47-52.

McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *Institute for Homeland Security Solutions*, 1-36.

McClain, J., Silva, A., Emmanuel, G., Anderson, B., Nauer, K., Abbott, R., & Forsythe, C. (2015). Human performance factors in cyber security forensic analysis. *Procedia Manufacturing*, *3*, 5301-5307.

Mejias, R. J. (2012). 45th Hawaii International Conference on System Science (HICSS): *An integrative model of information security awareness for assessing information systems security risk*, 3258-3267.

Moustakas, C. (1994). *Phenomenological research methods.* London: Sage.

Onarlioglu, K., Yilmaz, U. O., Kirda, E., & Balzarotti, D. (2012). Insights into user behavior in dealing with Internet attacks. *NDSS*. Retrieved from http://mail.seclab.tuwien.ac.at/papers/onarlioglu_ndss12.pdf

Othmane, L. B., Weffers, H., Ranchal, R., Angin, P., Bhargava, B., & Mohamad, M. M. (2013). A case for societal digital security culture. *Security and Privacy Protection in Information Processing Systems*, 391-404.

Pal, R., & Hui, P. (2012). CyberInsurance for cybersecurity: A topological take on modulating insurance premiums. *ACM SIGMETRICS Performance Evaluation Review*, *40*(3), 86-88.

Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2014). Will cyber-insurance improve network security? A market analysis. *INFOCOM, 2014 Proceedings IEEE*, 235-243.

Pandey, P., & Snekkenes, E. A. (2014). Using prediction markets to hedge information security risks. *Security and Trust Management*, 129-145.

Papacharissi, Z. & Gibson, P.L. (2011). Fifteen minutes of privacy: Privacy, sociality, and publicity. *Privacy Online*, 75-90.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597-611.

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of Social Psychology*, *154*(4), 352-369.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65-78.

Salem, M. B., & Stolfo, S. J. (2011). On the design and execution of cyber-security user studies: Methodology, challenges, and lessons learned. *CSET*. Retrieved from https://www.usenix.org/legacy/event/cset11/tech/final_files/Salem.pdf

Salleh, N., Hussein, R., Mohamed, N., Karim, N. S. A., Ahlan, A. R., & Aditiawarman, U. (2012). Examining information disclosure behavior on social network sites using protection motivation theory, trust and risk. *Journal of Internet Social Networking & Virtual Communities*, *2012*, 1-11.

Sánchez, M., Kaplan, M. S., & Bradley, L. (2015). Using technology to connect generations: Some considerations of form and function. *Comunicar, 45*, 1-11.

Schwartz, G., Shetty, N., & Walrand, J. (2013). Why cyber-insurance contracts fail to reflect cyber-risks. *Communication, Control, and Computing*, 781-787.

Silva, A., McClain, J., Reed, T., Anderson, B., Nauer, K., Abbott, R., & Forsythe, C. (2014). Proceedings of the Interservice/Interagency Training, Simulation and Education Conference: *Factors impacting performance in competitive cyber exercises*. Orlando, FL.

Sofo, M., & Sofo, F. (2014). Participatory barriers to the informal learning of older Australians using the Internet and Web 2.0 technologies. *Adult and Continuing Education: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*, 88-110.

Sommestad, T., & Hallberg, J. (2013). A review of the theory of planned behaviour in the context of information security policy compliance. *Security and Privacy Protection in Information Processing Systems*, 257-271.

Stolfo, S. J., Salem, M. B., & Keromytis, A. D. (2012). Fog computing: Mitigating insider data theft attacks in the cloud. *Security and Privacy Workshops (SPW), 2012*, 125-128.

Taddicken, M. & Jers, C. (2011). The uses of privacy online: Trading a loss of privacy for social web gratifications? *Privacy Online*, 143-157.

Thelwall, M. (2011). Privacy and gender in the social web. *Privacy Online*, 251-266.

Trepte, S. & Reinecke, L. (2011). The social web as a shelter for privacy and authentic living. *Privacy Online*, 61-74.

Toregas, C., & Zahn, N. (2014). Insurance for cyber attacks: The issue of setting premiums in context. *George Washington University*. Retrieved from http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/54203258e4b000f16802b810/1411396184449/cyberinsurance_paper_pdf.pdf

Wang, P. A. (2013). International Conference on Internet Monitoring and Protection (ICIMP). *Assessment of cyber security knowledge and behavior: An anti-phishing scenario.*

Warkentin, M., Malimage, N., & Malimage, K. (2012). Proceedings of the Pre-ICIS Workshop on Information Security and Privacy: *Impact of protection motivation and deterrence on IS security policy compliance: A multi-cultural view*. Orlando, FL.

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

Wolf, Z. R. (2012). Ethnography: The method. *Nursing research: A qualitative perspective*, 285-335.

Yang, Z., & Lui, J. C. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, *74*, 1-17.

Yao, M.Z. (2011). Self-protection of online privacy: A behavioral approach. *Privacy Online*, 111-126.

Ziegele, M. & Quiring, O. (2011). Privacy in social network sites. *Privacy Online*, 175-190.