2021

Examining the Influence of Perceived Risk on the Selection of Internet Access in the U.S. Intelligence Community

Tyler Michael Pieron

Examining the Influence of Perceived Risk on the Selection of Internet Access in the U.S. Intelligence Community

by

Tyler Michael Pieron

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in Information Assurance

College of Computing and Engineering
Nova Southeastern University

2021

We hereby certify that this dissertation, submitted by Tyler Pieron conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

3/15/21

Ling Wang, Ph.D
Chairperson of Dissertation Committee

Date

3/15/2021

James N. Smith, Ph.D.
Dissertation Committee Member

Date

Martha M. Snyder

3/15/21

Martha M. Snyder, Ph.D.
Dissertation Committee Member

Date

Approved:

3/15/21

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

Date

College of Computing and Engineering
Nova Southeastern University

2021

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Examining the Influence of Perceived Risk on the Selection of Internet Access in the U.S. Intelligence Community

by
Tyler M. Pieron
March 2021

Information technology security policies are designed explicitly to protect IT systems. However, overly restrictive information security policies may be inadvertently creating an unforeseen information risk by encouraging users to bypass protected systems in favor of personal devices, where the potential loss of organizational intellectual property is greater.

Current models regarding the acceptance and use of technology, Technology Acceptance Model Version 3 (TAM3) and the Unified Theory of Acceptance and Use of Technology Version 2 (UTAUT2), address the use of technology in organizations and by consumers, but little research has been done to identify an appropriate model to begin to understand what factors would influence users that can choose between using their own personal device and using organizational IT assets, separate and distinct from “bring your own device” constructs. There are few organizations with radical demarcations between organizational assets and personal devices. One such organization, the United States Intelligence Community (USIC), provides a controlled environment where personal devices are expressly forbidden in workspaces and therefore provides a uniquely situated organizational milieu in that the use of personal devices would have to occur outside of the organizational environment. This research aims to bridge the divide between these choices by identifying the factors that influence users to select their own devices to overcome organizational restrictions in order to conduct open-source research.

The research model was amalgamated from the two primary theoretical frameworks, TAM3 and UTAUT2, and is the first to integrate these theories as they relate to the intention to use personal or organizational systems to address the choices employees make when choosing between personal and organizational assets to accomplish work related tasks. Using survey data collected from a sample of 240 employees of the USIC, Partial Least Squares Structural Equation Modeling (PLS-SEM) statistical techniques were used to evaluate and test the model, estimate the path relationships, and provide reliability and validity checks.

The results indicated that the Perception of Risk in the Enterprise (PoRE) significantly increased the Intention to Use Private Internet and decreased the Intention to Use Enterprise devices, as well as increasing the Perceived Ease of Use of Private Internet (PEUPI). The results of this study provide support to the concept that organizations must

do more to balance threats to information systems with threats to information security. The imposition of safeguards to protect networks and systems, as well as employee misuse of information technology resources, may unwittingly incentivize users to use their own Internet and devices instead, where enterprise safeguards and protections are absent. This incentive is particularly pronounced when organizations increase the perceived threat of risk to users, whether intentional or inadvertent, and when the perception of the ease of use and usefulness of private Internet devices is high.

Acknowledgements

This dissertation, nor any of my endeavors over the past 20 years, would not have been possible without the love and support of my best friend and wife, Claire. She was, perhaps unknowingly, the inspiration and the genesis for this research as we discussed ways of using open-source intel in the face of organizational challenges. She has read, critiqued, and improved so many versions of this research with her wise counsel, deep insights, and extensive intelligence experience. Thank you!

When I first began researching opportunities to complete a doctoral course of study, my leadership at work, Mr. Gregg Crawford and Dr. Coy “Bert” Hawkins, were behind me 100%. They provided me both the time away from work and the pathway for my research to be funded, and for that I am forever grateful. I hope to make you both proud and prove that your investment was a wise one.

To my dissertation committee and advisors, I cannot thank you enough for the support, mentoring, training, and patience. From spending months (years!) teaching me how to master advanced statistical modeling to learning the basics and beyond of academic research, Dr. James Smith, Dr. Ling Wang, Dr. Marti Snyder and Dr. Steven R. Terrell have set the standard for helping doctoral students succeed.

Developing friends and colleagues has been an integral part of the doctoral process and I was extremely lucky to have found so many in Team AIS aka the OG NSU PhD Group – Dr. Vasilka Chergarova, Dr. Molly Cooper, Prof. Javier Coto, Dr. John McConnell, Prof. Kimberly Smith and Prof. Mel Tomeo, and so many others.

To everyone that participated in the research, served on the Delphi panel, found people who wanted to help, shared the data call, and assisted in every other way, thank you!

Table of Contents

Chapters

Appendices

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Insider threats have existed for millennia, acknowledged in the earliest known writings, including in the histories of Herodotus of Halicarnassus where he described Greek spies being spared by Xerxes (Herodotus & Grene, 1987). Sun Tzu also recognized insider threats in his famous treatise *On the Art of War*, where he identified five classes of spies, including “having local spies means employing the services of the inhabitants of a district” and “having inward spies, making use of officials of the enemy” (Sawyer & Sawyer, 1994, p. 67). Insider threats are nothing new, but the vastness of information that can be compromised by one trusted insider have increased exponentially since the advent of the Information Age. Indeed, Bickers (2000) cited the potential loss of company information as a restraining factor in beginning to conduct e-commerce.

Despite the multitude of historical examples, research into insider threats to information systems has long been neglected in favor of the perceived threats posed by external factors, such as viruses, worms, hackers, and others (T. Brown, 2018; Gordon & Loeb, 2002; Wang, 2019). This general trend continues, with recent research by Beckett (2015) indicating that while organizations have doubled their spending to protect themselves against the loss of information and systems, the vast majority of spending has been to harden systems against external threats. One potential reason for this divide is the lack of reliable data concerning insider threats, as organizations aim to minimize the damage caused by malicious insiders and therefore limit their exposure to the secondary and tertiary effects of losses (Bulgurcu et al., 2010; Pfleeger & Stolfo, 2009).

Despite the focus on systems and processes for identifying threats to information systems against external threats, and the recognition of the threats posed by malicious insiders, a comprehensive and systematic review of the literature reveals there has been little study or effort to identify ways in which critical information can be exposed by non-malicious insiders who use personal devices to conduct work related tasks outside of the organizational information systems infrastructure.

Within intelligence agencies, there exists two distinct types of information: closed (or classified) sources and open sources. Closed sources consist of information collected in such a way that the origin, knowledge, or method by which the information is collected must be protected from disclosure (Richelson, 2018). Open sources consist of any other information that is available, such as websites, newspapers, magazines, subscription services, academic journals, Internet websites, and television broadcasts (M. Glassman & Kang, 2012). The Director of National Intelligence provided a formal definition of Open Source Intelligence (OSINT) in 2011 as “intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement” (H. Williams & Blum, 2018, p. ix). Despite the recognition of the value and use of OSINT for over 50 years, the United States government continues to evolve the definition and characterization of OSINT as both an intelligence discipline and what it consists of. Similar to academia and the general population, the Internet is now the primary mechanism by which OSINT is collected and reviewed by intelligence personnel (M. Glassman & Kang, 2012).

Management and organizational restrictions regarding Internet usage within large organizations are common (Coles-Kemp & Theoharidou, 2010; J. Glassman et al., 2015; Schulman, 2001; Symantec, 2016). Management and organizational Internet restrictions within agencies of the U.S. government are managed by policies detailing ethical guidelines (Department of Defense, 2012), however, these restrictions impede the ability of intelligence analysts to conduct Internet based research (M. Glassman & Kang, 2012). These restrictions include prohibitions on "viewing, storage, copying or transmission of materials related to…illegal weapons, terrorist activities or any other illegal activities or activities otherwise prohibited" (Frederick, 2014, para. 8.7). Offensive, prohibited and resource intensive websites, such as video and audio streaming services, are frequently blocked by Web filtering tools (United States Cyber Command, 2020). These restrictions are specifically applicable to the unofficial use of IT systems, allowing for access to these materials and subjects for official purposes, but through practice and design, there are limited methods to differentiate between official and unofficial use except in ex post facto reviews (Frederick, 2014).

There is a gap in the literature to understand the motivations and choices employees make to choose between enterprise systems and personal systems to accomplish work related tasks. Colvin described "non-malicious" information technology misuse as situations in which an "employee improvises, takes short cuts, or works around IT procedures and guidelines in order to perform their assigned tasks"(Colvin, 2016, p. 2). In keeping with Colvin's findings that non-malicious IT use tends to be motivated by internal factors such as performance, intelligence analysts that wish to avoid lengthy review processes in which they have to justify accessing prohibited content, or burdensome processes required for requesting permission in advance, may choose to forego accessing potentially challenging materials while using government systems, opting instead to use personal devices and networks to access information, potentially exposing information unwittingly.

These concerns are not purely speculative or remote. Advanced intelligence collection systems that act as a man in the middle attack on cellular telephones and devices, known colloquially as IMSI catchers and Stingrays, have been discovered near U.S. intelligence and defense facilities, lend credence to the concept that the use of personal devices may unwittingly expose information (Fleischer et al., 2018; Fredericks, 2018; Timberg, 2018). As a result, employees who fully comply with applicable restrictions while operating enterprise IT systems may unknowingly expose critical information by conducting research using personal equipment, such as at home or using mobile devices in order to accomplish work tasks. The use of personal Internet access devices, including such generally benign devices like fitness trackers, have revealed confidential and sensitive information (Ching & Singh, 2016; Lidynia et al., 2017). In 2018, a security flaw in a mobile fitness application revealed "6,400 users believed to be exercising at sensitive locations, including the NSA, the White House, MI6 in London, and the Guantanamo Bay detention center in Cuba, as well as personnel working on foreign military bases" (Whittaker, 2018, para. 10)**.** In another example, the location of U.S. military personnel engaged in combat operations in Syria and Afghanistan were revealed through another fitness tracking device (Sly, 2018). In January 2020, partially as a result of the threats posed by personal device usage, members of the U.S. Army's 82nd Airborne Division were ordered to leave all personal electronic devices in the United States when they were deployed to Kuwait following hostilities with Iran (Rempfer, 2020)**.** While the use of personal devices did not violate organizational policies (Sisk, 2018)**,** nor did they involve organizational information systems, they exposed highly sensitive information to potential adversaries.

Problem Statement

Organizations that impose significant restrictions on Internet use increase the likelihood that employees will use personal devices outside of the organization to conduct work related tasks, which in turn, escalates information security risks (Gundu & Flowerday, 2012; Hovav & Putri, 2016). The use of Web filters and other information technology approaches to limit the accessibility of potentially inflammatory, objectionable, or ostensibly non work-related websites are largely effective in reducing employee misuse of information technology resources (J. Glassman et al., 2015); however, when access to Internet resources that are necessary to accomplishing work related tasks are restricted, these constraints may encourage employees to bypass organizational constraints by using their own devices and networks to access Internet based information. The use of personal devices and Internet resources to conduct work related activities increase the risk of information compromise (Garba et al., 2015; Hovav & Putri, 2016).

Dissertation Goal

The purpose of this dissertation research was to assess the influence the perception of risk has on the behavioral intention and use behavior of personally-owned Internet devices and access to conduct open-source research among members of the United States Intelligence Community. Selected constructs derived from the Unified Theory of Acceptance and Use of Technology (UTAUT) model (Venkatesh et al., 2003), the Technology Acceptance Model (TAM) (Venkatesh et al., 2012) and validated extensions of UTAUT (Dwivedi et al., 2019) were used to establish a proposed structural path model to assess the impact the perception of risk has on user selection of enterprise or personal devices when conducting open-source research for work purposes**.**

There have been extensive studies evaluating how, when, and why users accept and use technology. The two primary competing models reflect the differences between the organizational use of technology and how consumers use technology. The primary models used to understand how technology is used within organizations is known as the Technology Acceptance Model 3 (TAM3) (Venkatesh & Bala, 2008), which includes antecedents such as voluntariness, perceived ease of use, as well as perceptions of external control. Recognizing that models developed to understand how well users accept technology they are required to use for employment and provided to them in an organizational environment is fundamentally different from technology users choose for their personal use, an alternative theory known as the Unified Theory of Acceptance And Use Of Technology (UTAUT) was developed and later extended into UTAUT Version 2 (UTAUT2) (Venkatesh et al., 2003, 2012)**.** UTAUT2 is similar in many ways to TAM3 but reflects the unique influences that individual choice has on using technology, such as incorporating age, gender, and experience as moderating factors. While TAM3 is well suited to evaluating technology acceptance in organizations, UTAUT2 is generally better suited and designed to accomplish this for individual consumers. The UTAUT2 model is generally considered the most well-developed of the technology acceptance models focused on non-organizational use of technology (Venkatesh et al., 2003; M. Williams et al., 2015)

Conceptually, this research attempted to bridge the gap between the various acceptance theories by examining what factors influence users to select personal Internet access devices over organizational systems to accomplish work related tasks. Additionally, this research incorporated the impact that the perception of risk, as a surrogate for security, has on the behavioral intention and use behavior of employees to avoid use restrictions and other barriers to accessing the Internet. This research model incorporated selected constructs as antecedents to behavioral intention and use behavior derived from the TAM3 and UTAUT2 models and well as the inclusion of attitude as codified in a revised UTAUT model (Dwivedi et al., 2019)**.** The research model was used to investigate what effect organizational policies, along with perception of risk, have on users selecting between organizational resources and personal devices to conduct work related activities.

The use of personal devices and systems to accomplish work related information gathering tasks likely does not pose a direct threat to information systems of an organization; however, the use of extra-organizational resources, such as personally owned smart phones or home computers, may introduce unintended risks to sensitive information (Garba et al., 2015)**.** Intelligence professionals provide a unique social milieu in which to examine the factors influencing personal device usage, as they are prohibited by law and policy from possessing or using personal devices within their work spaces (National Counterintelligence and Security Center, 2017). This policy prohibiting the possession and use of personal devices allows for a clear demarcation between organizational IT devices and other situations wherein personal devices are not provided by the organization but are authorized for use, such as is the case with “Bring Your Own Device” (BYOD) situations where users are authorized to use their own devices to conduct work tasks (Hovav & Putri, 2016).

By examining this unique population to determine whether the perception of risk inadvertently influences individuals to conduct work related activities using personally owned Internet access, a broader understanding of the impact of enterprise use policies has on organizations, including potentially exposing confidential information to adversaries, is realized (Fleischer et al., 2018; Fredericks, 2018; Timberg, 2018). Additionally, this research provides insights into user risk perception, allowing organizations to make informed decisions as to what Internet use policies are appropriate and develop remediation strategies to mitigate risks.

Research Questions

Open Source Intelligence, or the collection of information that is publicly available, is a frequent and routine function for intelligence analysts (M. Glassman & Kang, 2012). The most common method for conducting open-source research is through the Internet due to the vast amount of timely and accurate information available on a multitude of topics and issues. Despite the recognition of the value of open-source research, organizational and institutional Internet use policies that habitually prevent access to routine sources of information, often in the form of enterprise-wide restrictions (H. Williams & Blum, 2018). The ubiquity of the Internet and the ease in which intelligence professionals can conduct open-source research using their personal devices, and avoiding enterprise restrictions tempered by the perception of risk, forms the foundation for this research. The following primary research question was derived from the antecedents and moderating variables that comprise UTAUT2, TAM3, and related extensions of these theoretical models:

RQ: What is the relationship between the perception of risk and how members of the US Intelligence Community intend to conduct open-source research?

Relevance and Significance

This study blended the foundational concepts found within TAM and UTAUT and applied them in a unique situation where the influences found in institutional aspects of accepting and using technology combine and contrast against a personal choice in selecting the use of personal Internet access devices to accomplish a work task in the form of conducting open-source research. The study population is highly segmented in terms of isolation from the use of personal devices at work locations, as BYOD is not only unavailable, but prohibited by policy and law. Therefore, the blurring of lines between personal and organization equipment and networks found with most study populations, such as corporate or academic situations, does not exist. The prohibition of personal devices within work spaces allows for a marked delineation between personal and professional equipment and networks, providing the opportunity to isolate uncontrollable variables and more clearly identify the role the perception of risk plays in the selection of personal equipment to conduct open-source research in support of work-related tasks.

Barriers and Issues

Several barriers and issues were addressed while conducting this research. The primary barrier that would have affected this study is the failure to acquire a sufficient number of quantitative samples. This barrier was mitigated by engineering a variety of pathways for survey subjects to respond, with each pathway serving as a potential complete source for responses. The pathways used to collect survey data included a commercial survey application on the Internet known as Typeform, Sharepoint survey tools hosted on a Department of Defense network known as the Secret Internet Protocol Router Network (SIPRnet) as well within an unclassified Department of Defense enclave linked to Typeform, each serving as a method to ensure the correct population is being sampled as well as ensuring the validity of the responses. The use of classified networks, primarily SIPRnet, introduced additional challenges, such as the ability to extract survey responses, but provided a milieu in which only Intelligence Community personnel can reply, ensuring the validity of the sample population. The use of the primary Intelligence Community network, known as the Joint Worldwide Intelligence Communications System (JWICS), was considered but ultimately discarded due to significant challenges in extracting completed survey results. Combining samples to ensure a sufficient number of valid samples was incorporated following statistical analysis to ensure the similarity of the responses.

Another potential barrier was that the results would be unusable stemming from biases and other factors that would make the outputs unusable for analysis. This potential barrier was ameliorated through the use of validated survey questions, thoughtful survey design, pretesting, and conscientious administration of the survey.

Limitations and Delimitations

Limitations

One of the primary limitations is the use of self-reporting as the primary mechanism for data collection. While self-reporting is a frequent and common method for organizational and management research, research has shown that responses can be biased towards socially desirable answers (Podsakoff & Organ, 1986). Additionally, significant variability exists between reported actions and their actual frequency of use (Verplanken & Orbell, 2003).

The study was limited to members of the United States Intelligence Community (USIC), which encompasses personnel physically located around the world (Richelson, 2018). As such, the location of the study was distributed, but through the use of controlled access to common platforms which only USIC members can access, this limitation was managed. The organizational culture of each organization of the USIC varies, and collection of demographic data, including the mission category of respondents, length of time in the IC, pay category, and other population demographics, will serve as useful data for further analysis.

Delimitations

This study was limited to members of the US Intelligence Community. The sample included staff, contractors, as well as military members. The study differentiated between members who use open-source materials in their work and those who do not.

Definition of Terms

Cybersecurity. Computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries" (Burley et al., 2018, p. 919)

*Delphi method. "*An iterative process to collect and distill the anonymous judgments of experts using a series of data collection and analysis techniques interspersed with feedback" (Skulmoski et al., 2007, p. 1)

Information system. A "work system whose processes and activities are devoted to processing information, that is, capturing, transmitting, storing, retrieving, manipulating, and displaying information" (Alter, 2008, p. 453)

Insider threat. "An insider can thus be defined with regard to two primitive actions: 1. violation of a security policy using legitimate access, and 2. violation of an access control policy by obtaining unauthorized access" (Bishop & Gates, 2008, p. 15:2)

Open Source Intelligence. "…intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement" (H. Williams & Blum, 2018, p. ix)

Perceived risk. The assessment of an individual "composed of individual judgments regarding the likelihood that the unfavorable experience will happen, and the impact of that experience were it to happen" (Boss, 2007, p. 27)

Risk. "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would rise if the circumstance or event occurs; and (ii) the likelihood of occurrence" (Barrett, 2018, p. 46)

List of Acronyms

APCO. Antecedents–Privacy Concerns–Outcomes

AVE. Average Variance Extracted

BI. Behavioral Intent

BYOD. Bring Your Own Device

CMB. Common Method Bias

CMV. Common Method Variance

DISL Defense Intelligence Senior Leader

DOD. Department of Defense

EO. Executive Order

GS. Government Service

HTMT. Heterotrait-monotrait (HTMT)

IC. Intelligence Community

IDT. Innovation diffusion theory

IMSI. International Mobile Subscriber Identity

IP. Internet Protocol

IRB. Institutional Review Board

IS. Information System

IT. Information Technology

IUIPC. Internet Users Information Privacy Concerns

JWICS. Joint Worldwide Intelligence Communications System

MI6. Military Intelligence, Section 6

MM. Motivation model

MPCU. *M*odel of PC utilization

NSA. National Security Agency

ODNI. Office of the Director of National Intelligence

OSINT. Open Source Intelligence

PEUEI. Perceived Ease of Use of Enterprise Internet

PEUPI. Perceived Ease of Use of Private Internet

PLSc. Partial Least Squares – Consistent

PLS-SEM. Partial Least Squares Structural Equation Modeling

PoRE. Perception of Risk – Enterprise

PUEI. Perceived Usefulness of Enterprise Internet

PUPI Perceived Usefulness of Private Internet

SCT. Social Cognitive Theory

SES. Senior Executive Service

SIPRnet. Secret Internet Protocol Router Network

TAM. Technology Acceptance Model

TAM2. Technology Acceptance Model Version 2

TAM3. Technology Acceptance Model Version 3

TOR. The Onion Router

TPB. Theory of Planned Behavior

TRA. Theory of Reasoned Action

USIC. United States Intelligence Community

UTAUT. Unified Theory of Acceptance and Use of Technology

UTAUT2. Unified Theory of Acceptance and Use of Technology Version 2

VIF. Variance Inflation Factor

Summary

The purpose of this chapter is to introduce a research question, supported by presenting the background, research goals, relevance and significance, barriers and issues as well as potential limitations and delimitations for this research. The background established the pervasiveness of insider threats and the unwitting nature of potential compromises by users. The research goal identifies what this study aimed to accomplish and the research question focused and shaped the literature review. The relevance and significance section reinforced the problem statement and research goal while the barriers and issues sections identified potential concerns with the successful completion of this research. The limitations and delimitations identified issues that were recognized but were unable to be controlled, as well as the scope of the research population. The definition of terms and acronyms provides clear and unambiguous meanings to terms used in this dissertation report.

Chapter 2

Review of the Literature

Introduction

Within the study of information systems, the basis for why and how users accept technology is an extensively studied concept. These efforts have led to an evolution of various models and theories being developed and expanded over the years, primarily within organizational constructs. Previous studies examining how and when people use technology have largely approached the issue in a bifurcated manner, examining the use of technology in organizations and by consumers as discrete and separate (Venkatesh et al., 2012; Venkatesh & Bala, 2008)

One of the most advanced and developed of these theories is the Unified Theory of Acceptance and Use of Technology (UTAUT), identified by Venkatesh et al. (2003). UTAUT aimed to incorporate the primary operant theory, the Technology Acceptance Model, with other predictive theories of acceptance to produce a "best of breed" amalgamated model that has a greater predictive value than the individual components (M. Williams et al., 2015). Expanding on previous work, this model is well grounded in theory and provides for an understanding of the various concepts that influence acceptance, and includes performance expectation, effort expectancy, social influence and facilitating conditions as the primary factors that influence behavioral intention, leading to actual use. Affecting these primary determinants are key moderators of gender, age, experience and voluntariness of use, which seeks to account for individual variables.

Acceptance and Use Models

While UTAUT has proven to be an excellent predictor of acceptance within organizational structures, its predictive capabilities have proven to be of less value when addressing consumer use contexts. To address these shortcomings, Venkatesh et al. (2012) developed an extension of the UTAUT model, known as UTAUT2. A brief review of the evolution of user acceptance models provides context to how UTAUT2 was developed, as well as how the conceptualization of privacy within the UTAUT2 framework comports to the foundational concepts previously established.

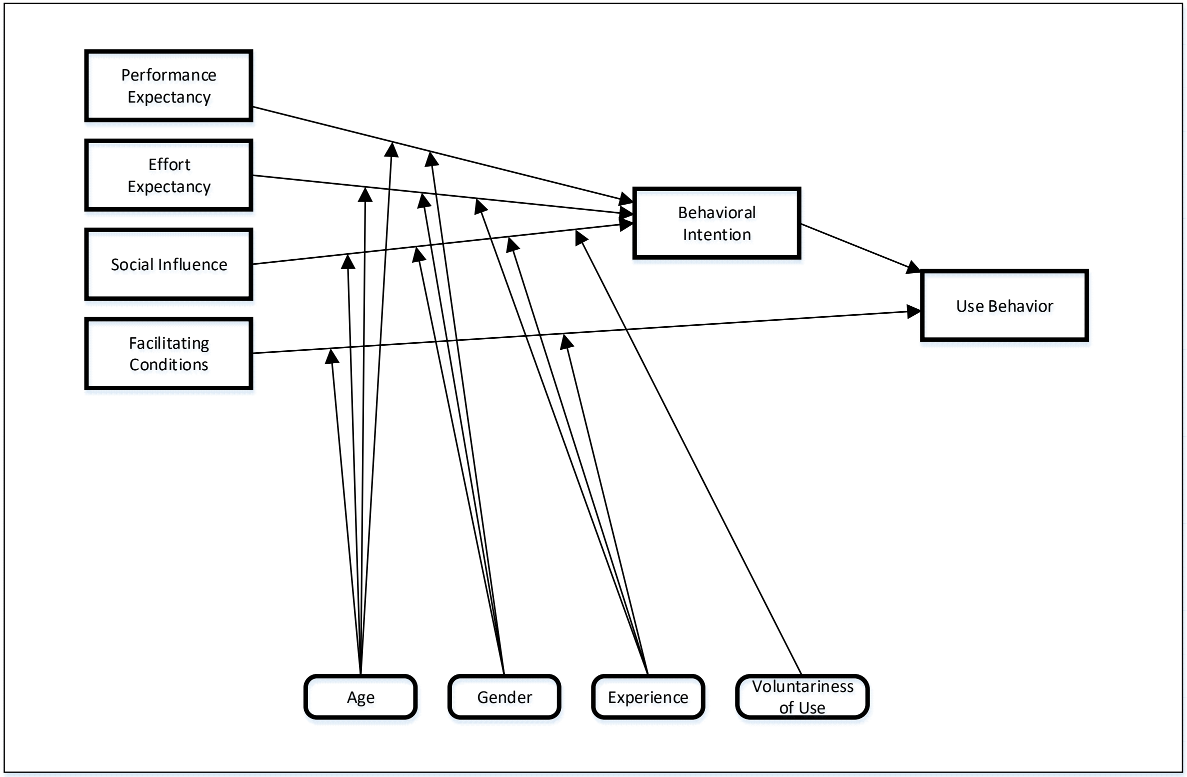
The foundational concepts regarding user acceptance of technology are largely based on a theory from the social psychology discipline called the Theory of Reasoned Action (TRA) which was developed by Ajzen and Fishbein (1973). TRA proposes that a person's behavior, referred to as actual behavior, is largely determined by a construct referred to as behavioral intent (BI) and defined as "a measure of the strength of one's intention to perform a specified behavior" (Davis et al., 1989, p. 984)**.** In 1986, Fred Davis took the theory of reasoned action and developed an adaptation of it specific to information systems, which was later known as the technology acceptance model (TAM) (Davis, 1985, 1989; Davis et al., 1989)**.** His technology acceptance model, and its derivative works, have formed the bedrock of a vast amount of the scholarly research in information systems.

As work with TAM continued through the 1990's and into the 2000's, the focus shifted to the task of better identifying variables by which to operationalize the constructs of TAM and to expanding the scope of TAM, including efforts to test the outer boundaries of the theory's applicability by validating it based on factors such as culture, gender, and nationality (Adams et al., 1992; Y. Lee et al., 2003; Venkatesh & Bala, 2008; Venkatesh & Davis, 2000). In 2000, Venkatesh and Davis published an expanded technology acceptance model, which sought to conceptually expand TAM by theorizing the determinate constructs which drive perceived usefulness and to explore some moderators of those constructs (Venkatesh & Davis, 2000).

In 2003, a group of researchers, including Davis and Venkatesh, embarked on an effort to combine TAM with theories of acceptance originating from other disciplines to create a model that would bring the best predictive capabilities of the various models together into one theory (Venkatesh et al., 2003). The eight theories that were amalgamated were the theory of reasoned action (TRA), from which TAM had been derived; TAM and its TAM2 extension; the motivational model (MM) taken from psychology; the theory of planned behavior (TPB), an extension of TRA; a combined TAM and TPB (C-TAM-TPB); the model of PC utilization (MPCU), a native information systems theory that contrasts with TRA and TPB; social cognitive theory (SCT) taken from psychology; and finally, the innovation diffusion theory (IDT) taken from sociology (Venkatesh et al., 2003). The researchers compared the constructs of each model and derived an amalgamation that had greater predictive value than the eight individual models. The resultant theory is known as the Unified Theory of Acceptance and Use of Technology (UTAUT), which is depicted in Figure 1.

Figure 1

Unified Theory of Acceptance and Use of Technology



Note. From “User acceptance of information technology: Toward a unified view” by V. Venkatesh, M. Morris, G. Davis, and F. Davis, 2003, *MIS Quarterly*, *27*(3), p. 447. Copyright 2003 by MIS Quarterly.

Each of the constructs included as antecedents to behavioral intention and use behavior is actually a combination of constructs derived from the eight extant theories that were combined into UTAUT. Each of these sub-constructs has its own scale items and brings predictive value to the constructs as a whole. Performance expectancy is defined as “the degree to which an individual believes that using the system will help him or her to attain gains in job performance” (Venkatesh et al., 2003, p. 447). Performance expectancy is derived from perceived usefulness, taken from TAM/TAM2 and C-TAM-TPB; extrinsic motivation, taken from MM; job-fit, taken from MPCU; relative advantage, taken from IDT; and outcome expectations from SCT. Effort expectancy is defined as “the degree of ease associated with the use of the system” (Venkatesh et al., 2003, p. 450). Effort expectancy is composed of perceived ease of use from TAM/TAM2, complexity from MPCU, and ease of use from IDT. Social influence is defined as “the degree to which an individual perceives that important others believe that he or she should use the new system” (Venkatesh et al., 2003, p. 451). Social influence consists of the subjective norm from TRA, TAM2, TPB, and C-TAM-TPB; social factors from MPCU and image from IDT. Facilitating conditions is defined as “the degree to which an individual believes that an organizational and technical infrastructure exists to support the use of the system” (Venkatesh et al., 2003, p. 453). Facilitating conditions consists of perceived behavioral control from TPB and C-TAM-TPB, facilitating conditions from MPCU, and compatibility from IDT (Venkatesh et al., 2003). In addition, UTAUT includes a complement of moderating variables including gender, age, and the moderating constructs of experience and voluntariness of use that were derived from TAM/TAM2. These moderators are hypothesized to moderate various antecedents (Venkatesh et al., 2003). In 2012, recognizing that UTAUT possessed limitations in modeling technology adoption and use by consumers, the aspects of consumer affect, financial cost and automaticity were incorporated into a second version known as UTAUT2 (Venkatesh et al., 2012). Three additional constructs (hedonic motivation, price value and habit) were incorporated into UTAUT2 to more fully capture the variations between organizational and individual influences affecting technology adoption and use (Venkatesh et al., 2012). The UTAUT and UTAUT2 models comprised a step forward in the study of user acceptance in the IS discipline in both organizational and individual settings.

In 2008, Venkatesh and Bala introduced the Technology Acceptance Model 3 (TAM3) (Venkatesh & Bala, 2008). TAM3 introduces the new determinant constructs in two groups known as “the anchoring and adjustment framing of human decision making” (Venkatesh & Bala, 2008, p. 278). The anchors represent individual differences in “general beliefs associated with computers and computer use” (Venkatesh & Bala, 2008, p. 278). TAM3, in particular, provides a fully developed structure of the determinants left vague in the original TAM model, as shown in Figure 2. The TAM3 and UTAUT2 models represent the current state of acceptance theory in information systems.

Figure 2

Technology Acceptance Model 3

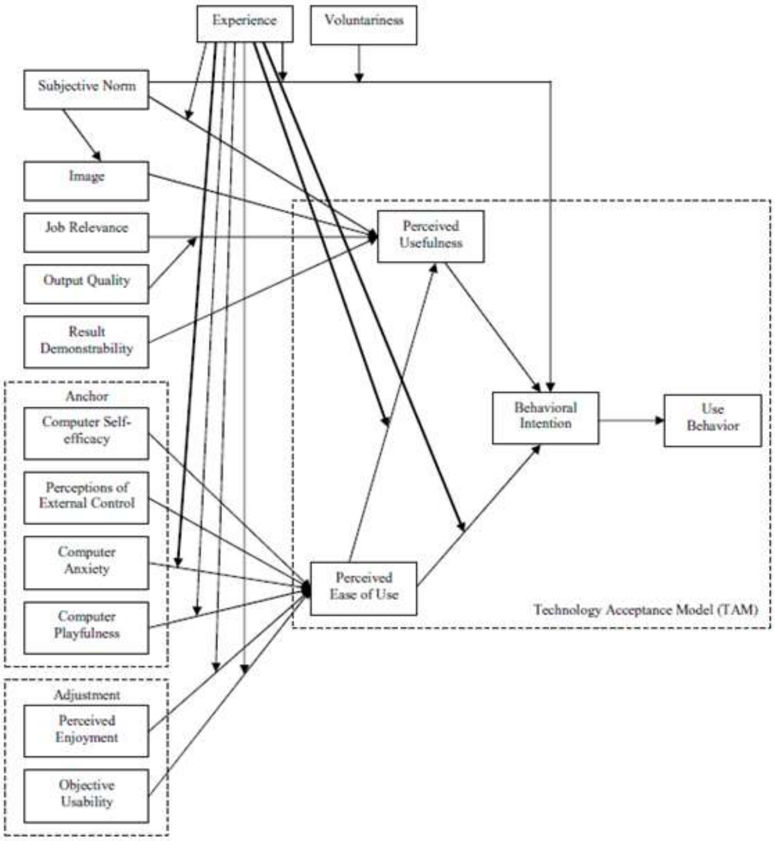


Figure 2

Note. From "Technology acceptance model 3 and a research agenda on interventions." By V. Venkatesh, and H. Bala, 2008, *Decision Sciences*, *39*(2), 273–315. Copyright 2003 by Decision Sciences, by permission.

Insider Threat

Significant research has been conducted regarding the implementation and effectiveness of Internet use policies (Herath & Rao, 2009), Web filtering and other formal and informal control mechanisms and sanctions (J. Glassman et al., 2015), and behavioral and motivational pressures (Willison & Lowry, 2018), all which have undoubtably decreased misuse of information technology systems (D'Arcy & Devaraj, 2012). However, there is limited research as to what effect these policies have on users avoiding using provided enterprise information systems in order to more efficiently access information, leading to what might be referred to as a non-malicious extra-organizational insider threat.

While a seemingly simple term to describe, the term "insider threat" has met with numerous definitions over the years aiming to categorize and better convey what is meant by the phrase. At its core, an insider threat consists of two components: access and intent, but as intent is generally not observable until some action has been taken, the definition has evolved over the years (Willison & Lowry, 2018). Initially, the term derived its context from physical protection measures taken by a number of industries, including banking, accounting, and sales that were more focused on protecting money and property than less tangible intellectual assets (Brackney & Anderson, 2004). In contrast, governments have always had an interest in protecting intellectual property from being lost, stolen, or otherwise exposed. As a result, it is not surprising that the earliest studies relating to insider threats, including how to bound the definition, were primarily a result of government-funded research (Baram et al., 2017).

Bishop (2005) proposed the term insider threat be defined as "a trusted entity that is given the power to violate one or more rules in a given security policy... the insider threat occurs when a trusted entity abuses that power" (pp.77-78). While this addresses both access and intent, and is certainly a usable definition, Bishop quickly superseded this definition with more expansive language that aimed to differentiate between the specific actions taken by users with authorized access (Bishop, 2005).

In 2008, Bishop, working with Gates, again addressed the definition of insider threat in an effort to standardize the terminology to provide increased accuracy and reliability when evaluating research towards the detection of threats from insiders (Bishop & Gates, 2008). They note that without a consistent definition of the term, each researcher implicitly expects the reader to comport to a common understanding of the term, but that these definitions are often influenced by unique experiences, knowledge, assumptions, and data. Consequently, Bishop and Gates proposed that insider threats are best defined by the constraints imposed by both access control rules and a security policy: "An insider can thus be defined with regard to two primitive actions: 1. violation of a security policy using legitimate access, and 2. violation of an access control policy by obtaining unauthorized access" (Bishop & Gates, 2008, p. 15:2). Additional studies reinforce the concept that insider threats are the result of trusted insiders violating access control rules and policies (Greitzer et al., 2008), whether maliciously or not (Colvin, 2016).

Continuing the theme that access and policy are guiding elements when determining how to define insider threats, as well as the potentiality of the loss of data, the United States Department of Defense (DoD) categorizes insider information security incidents as either infractions or violations (Department of Defense, 2013). DoD Manual 5200.01 defines infractions as "a security incident involving failure to comply with requirements which cannot reasonably be expected to, and does not, result in the loss, suspected compromise, or compromise of classified information. An infraction may be unintentional or inadvertent" (Department of Defense, 2013, p. 86). Security violations are more serious and are defined as “security incidents that indicate knowing, willful, and negligent disregard for security regulations, and result in, or could be expected to result in, the loss or compromise of classified information” (Department of Defense, 2013, p. 86).

Despite these various definitions, the use of personal information systems to access publicly available information does not meet the current definitions generally applied to insider threats, since no explicit policies would be violated nor would access to the organizations information systems be compromised. One early definition for insider threats of “malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information” may be appropriate (Brackney & Anderson, 2004, p. xi). However, the combination of two factors, namely the association of the individual with a specific organization, such as the U.S. Intelligence Community and specific search terms, topics or focus used while conducting extra-organizational research could provide adversaries indications and warning regarding information of interest as well as more specific actionable information.

Privacy, Trust, and Risk

An employee conducting extra-organizational research is largely relying on a common, and generally considered unwise, approach to privacy by depending on being able to hide in the noise and volume of information, also known as “security through obscurity” (Hartzog & Stutzman, 2013, p. 21). In isolated cases, this approach may make sense, especially when available identifiers, such as Internet Protocol (IP) addresses, are relatively common or change frequently. However, when enough uniquely identifiable information elements are present and able to be associated with an individual or an organization, such as mobile telephone international mobile subscriber identity (IMSI) numbers, hardware addresses, email and physical addresses, phone numbers, and other identifiers, the scant protections offered by security through obscurity are lost (Hartzog & Stutzman, 2013; Kehr et al., 2015).

While the concept of privacy has been extensively studied, a universally accepted understanding of what constitutes privacy has proven to be an elusive quarry (Culnan & Armstrong, 1999; Solove, 2008). The concept of privacy encompasses many dimensions and elements, including “the right to be left alone” (Warren & Brandeis, 1890, p. 193), as an element of human dignity (Bloustein, 1964)**,** or as Westin described information privacy, the ability for entities to “determine for themselves when, how, and to what extent information about them is communicated to others” (Westin, 1967, p. 7). Despite the lack of a common definition or even a single coherent understanding of the concept, privacy can be described, in a simplified manner, as the absence of intrusion. Similar to how Justice Potter of the United Supreme Court defined pornography as “I know it when I see it” (Jacobellis v. Ohio 378 U.S. 184, 1964, p. 197), an invasion of privacy is readily apparent to those affected when they are aware it has occurred (Dinev et al., 2013). Information privacy, as it relates to privacy and the use of technology, is well grounded by Dinev et al.’s (2013) definition: “an individual’s self-assessed state in which external [parties] have limited access to information about him or her” (p. 299).

The concept of privacy, sometimes also referred to as trust, has been approached in a number of ways within the literature, including as a contextual relationship within the existing UTAUT and TAM models, specifically as part of adoption beliefs such as effort expectancy and facilitating conditions (Venkatesh et al., 2011), but generally not as an independent moderating factor. Other works, such as Dinev et al's (2015) expanded Antecedents–Privacy Concerns–Outcomes (APCO) approach recognizes the impact privacy plays in individuals' choices, which is not reflected in current technology acceptance models. There have been a number of studies that focus on incorporating privacy as a factor within the UTAUT models, generally focusing on the intention to use specific technologies, such as near-field communication (Morosan & DeFranco, 2016), social media messaging (Lai & Shi, 2015), and the sharing of user generated content within social media platforms (Herrero et al., 2017), among others. These studies generally focus on privacy as a barrier or impediment to the use of existing technology.

Another specific factor that impacts user acceptance of technology as well as privacy that is generally unique among intelligence professionals is compliance with information collection processes regarding the collection and use of information created by or about United States citizens, residents and corporations as codified in United States Presidential Executive Order 12333 (*Executive Orders*, 2016). This order directs intelligence activities of the United States to avoid collecting, retaining or disseminating any information regarding or identifying any United States person if collected through intelligence channels. The largest organization that collects intelligence information in the United States is the Department of Defense, which implements EO 12333 through Department of Defense Manual 5240.01, which provides procedures governing the conduct of DOD intelligence activities (Carter, 2016). Within DOD Manual 5240.01, it specifically states that if information is publicly available regarding United States Persons, there are no restrictions (Carter, 2016). However, this broad exemption is frequently limited by subordinate organizations (H. Williams & Blum, 2018), and may affect the perception of risk experienced by members of the study population.

Privacy and risk are increasingly important aspects in understanding the causal and indirect factors affecting the selection, use, and discontinuation of technology in all its forms, including hardware, operating systems and applications (Harborth & Pape, 2019; Ho et al., 2017). A study undertaken by Harborth and Pape (2019) examined what "…influence have privacy concerns and associated trust and risk beliefs on the behavioral intention and actual use of Tor?" and "What influence does trust in Tor itself have on the behavioral intention and the actual use?" (p. 4852), finding that only the degree of trust in privacy enhancing technologies, in this case the anonymizing network known as Tor, affected the behavior intention to use the technology. While this study based its research on the Internet Users Information Privacy Concerns (IUIPC) model by Malhotra et al. (2004) as opposed to the TAM3/UTAUT2 models, it used a structural model containing numerous relationships between exogenous and endogenous variables to analyze the cause and effect relationship between unobserved latent variables with Partial Least Squares Structural Equation Modeling (PLS-SEM) in an effort to estimate behavioral intention (Harborth & Pape, 2019). A study by Karwatzki et al. (2018) also examined the concept of risk and the impact on behavior intention, developing a nomological network model focusing on the antecedents of privacy experience and familiarity affecting privacy risks, which is represented by a seven-dimensional construct of the various ways privacy invasions affect individuals, such as physical, social or psychological effects. This study used PLS-SEM to empirically assess "how privacy risks influence individuals' information disclosure and usage intentions" (Karwatzki et al., 2018, p. 12), finding the conceptualization of privacy risks as a multidimensional construct incorporating the various ways an individual could be affected by an invasion of privacy and the impact on use intention to be well grounded. Other work researching the impact of the awareness of information security threats on privacy protective behaviors, such as password strength and non-disclosure of information, which is a suitable proxy for the behavior intention to use technology, found that while awareness of threats significantly affected both disclosure and protective measures such as password complexity, privacy self-efficacy was not positively associated moderating the impact of security threat awareness (Mamonov & Benbunan-Fich, 2018). Mamonov and Benbunan-Fich's (2018) study used PLS-SEM to assess the structural path and relationships between the reflective construct of the awareness of information security threats and the moderating impact of privacy self-efficacy on disclosure behavior and password strength selection.

Cloud computing, where data is physically and logically stored in locations not under the individual (or an organizations) immediate control, introduce further opportunities to examine the causal effect of perceived risk on both trust and intention to use technology (Ho et al., 2017). Ho et al. (2017) examined perceived risk and subjective norms within cloud computing adoption and established a research framework based on the theoretical foundations found in TAM, but with the modification of intention to use towards intention to trust as the dependent variable, with the independent variables of knowledge, attitude and perceived behavioral control with subjective norms and perceived risk as both independent and moderating variables. This study on the impact of perceived risk and subjective norms on cloud adoption used PLS-SEM to "identify and explain the causal relationships between and among the variables" (Ho et al., 2017, p. 32), finding that both perceived risk and subjective normal have a significant effect on cloud computing adoption

The research model for the current study is presented in Figure 3. It is holistically comprised of constructs derived from Venkatesh et al's (2003, 2012) Unified Theory of Acceptance and Use of Technology Versions 1 and 2 and Venkatech and Bala's (2008) Technology Acceptance Model Version 3, research on information privacy by Culnan and Armstrong (1999), Dinev et al. (2013), Kehr (2015), as well as recent work by Dwivedi et al. (2019) to validate and extend UTAUT's primary constructs to include the impact they have on behavioral intention and use behavior. The perception of risk, and its association with privacy, is a significant factor regarding the use of technology (Dinev et al., 2013), and impacts the performance expectancy, perceived ease of use and behavioral intention to use information systems. By incorporating the perception of risk into the proposed theoretical model, the antecedents found within TAM3 are appropriately included.

Figure 3

The Research Model

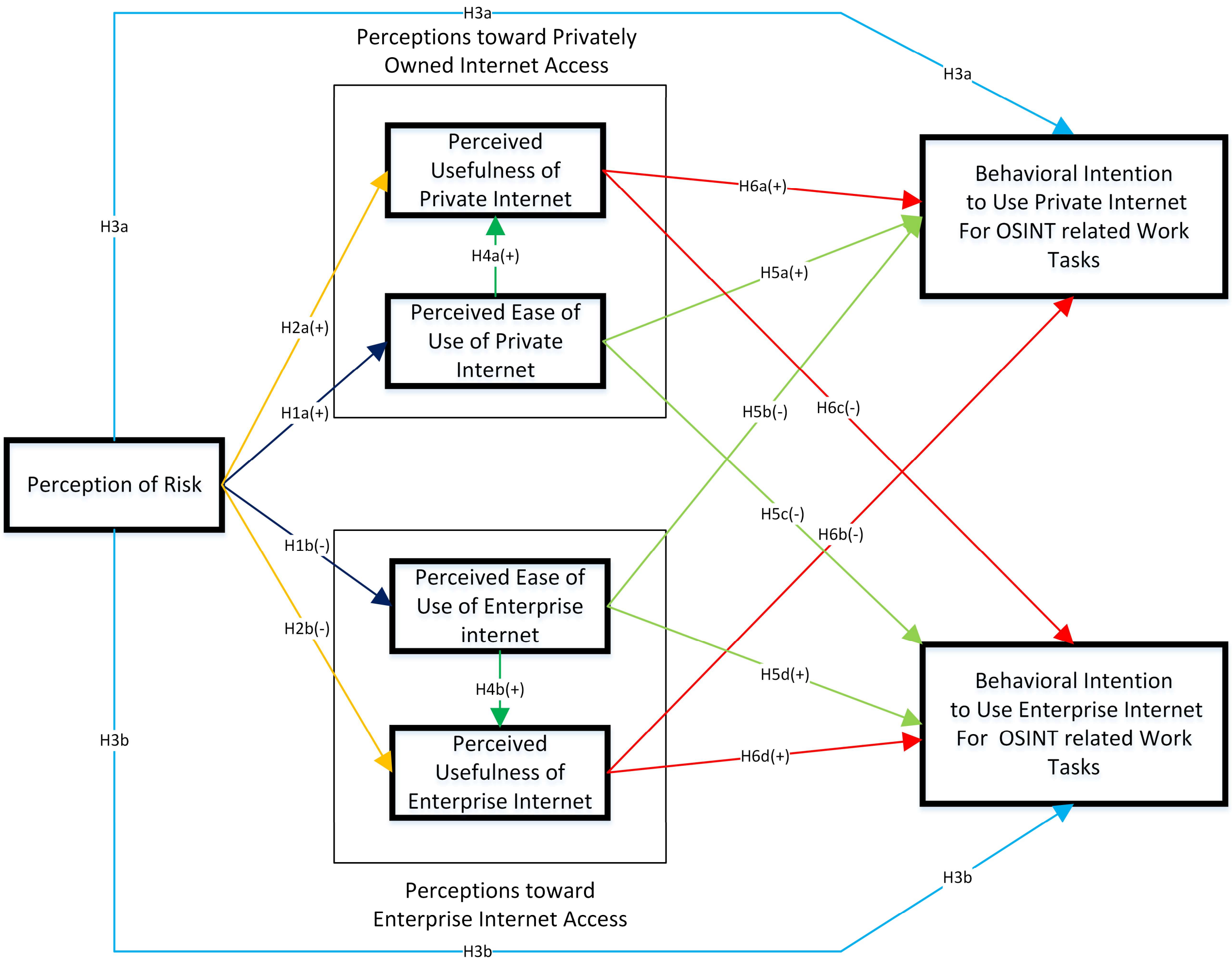

H3a
Perceptions toward Privately Owned Internet Access
H3a
Perceived Usefulness of Private Internet
H6a(+)
Behavioral Intention to Use Private Internet For OSINT related Work Tasks
H3a
H4a(+)
H5a(+)
H2a(+)
Perceived Ease of Use of Private Internet
H1a(+)
H5b(-)
H6c(-)
Perception of Risk
H5c(-)
H6b(-)
H1b(-)
Perceived Ease of Use of Enterprise internet
H2b(-)
H4b(+)
H5d(+)
Behavioral Intention to Use Enterprise Internet For OSINT related Work Tasks
H3b
Perceived Usefulness of Enterprise Internet
H6d(+)
H3b
Perceptions toward Enterprise Internet Access
H3b

Figure 3

Hypotheses

The following hypothesis were formulated for this study:

H1a: Perception of risk will have a positive effect on the perceived ease of use of private Internet access.

H1b: Perception of risk will have a negative effect on the perceived ease of use of enterprise Internet access.

H2a: Perception of risk will have a positive effect on the perceived usefulness of private Internet access.

H2b: Perception of risk will have a negative effect on the perceived usefulness of enterprise Internet access.

H3a: The perception of enterprise risk will have a direct relationship with the intention to conduct Internet based research using Private Internet access for OSINT related work activities.

H3b: The perception of enterprise risk will have a direct relationship with the intention to conduct Internet based research using Enterprise Internet access for OSINT related work activities.

H4a: Perceived ease of use of private Internet access positively influences the perceived usefulness of private Internet access.

H4b: Perceived ease of use of enterprise Internet access positively influences the perceived usefulness of enterprise Internet access.

H5a: Perceived ease of use of private Internet access positively influences employees' intention to use private Internet access for OSINT related work activities.

H5b: Perceived ease of use of enterprise Internet access negatively influences employees' intention to use private Internet access for OSINT related work activities.

H5c: Perceived ease of use of private Internet access negatively influences employees' intention to use Enterprise Internet access for OSINT related work activities.

H5d: Perceived ease of use of enterprise Internet access positively influences employees' intention to use Enterprise Internet access for OSINT related work activities.

H6a: Perceived usefulness of private Internet access positively influences employees' intention to use private Internet access for OSINT related work activities.

H6b: Perceived usefulness of enterprise Internet access negatively influences employees' intention to use private Internet access for OSINT related work activities.

H6c: Perceived usefulness of private Internet access negatively influences employees' intention to use Enterprise Internet access for OSINT related work activities.

H6d: Perceived usefulness of enterprise Internet access positively influences employees' intention to use Enterprise Internet access for OSINT related work activities.

Summary

A comprehensive review of the literature was performed to provide the baseline of extant knowledge of user acceptance of technology theory, the evolution of those theories over time, an understanding of how these theories were developed and shaped by shifting usage patterns of information technology over time, the role insiders have as a threat vector and the impact trust and risk has on the adoption and use of technology. The literature provides numerous examples of the various methods developed over time to assess both the adoption of technology within organizations and well as by individuals. The literature establishes that organizational and individual acceptance and use constructs vary significantly due to both the obligatory nature of institutional requirements as well as the vagaries of the human condition affecting individual choices. The primary construct which will be under evaluation in this study, the perception of risk, is incorporated obliquely in both TAM3 and UTAUT2 through the effort expectancy and facilitating conditions constructs, but as risk perception becomes increasingly relevant to the acceptance and use of technology by individual consumers, more research is required to understand the factors by which these decisions are made. A review of contemporaneous studies examining the impact of privacy and perceptions of risk on behavior and use intentions of technology reveals that due to the latent variables inherent in reflective constructs, the use of Partial Least Squares Structural Equation Modeling (PLS-SEM) statistical techniques to examine this phenomenon is well grounded in theory and practice.

Chapter 3

Methodology

This chapter details the research methodology designed to answer the primary research question: “What is the relationship between the perception of enterprise risk and how members of the US Intelligence Community intend to conduct open-source research?”. This chapter includes a detailed description of the research design, data collection techniques, instrument development and validation, and data analysis processes used. A summary is provided to synthesize the overall methodological approach.

Overview of Research Design

In order to develop empirical support within a modified UTAUT/TAM framework, this study employed an exploratory research design using survey instruments to collect quantitative data to examine the impact of the perception of enterprise risk on the selection and use of private or organizational assets to conduct Open Source Intelligence research. A quantitative approach allowed this study to minimize the effects of bias that may affect the hypotheses through statistical analysis techniques (Plonsky & Gass, 2011). The use of a structural path model based on fundamental theory and described in Figure 3, which specify how the latent variables are related to one another as well as the impact on the dependent variable, will provide the opportunity to estimate complex cause and effect relationships (Hair et al., 2017).

The research was conducted in three phases. During the first phase, the survey instrument was developed following a comprehensive review of literature and construct validity and reliability validated against a panel of nine experts recruited from academia, industry and government agencies specializing in information security, cybersecurity and related disciples. The titles, professional associations, areas of concentration, years of experience, and the gender of the Delphi panel members are listed in Table 1.

Table 1

Delphi Panel Characteristics

Title	Professional Area	Area of Concentration	Years of Experience	Gender
Professor	Academia	Information Systems	15+	Male
Professor	Academia	Information Systems	20+	Male
Director	Industry	Open-Source Research/Training	20+	Male
Professor	Academia	Information Systems	10+	Female
Intel Officer	Government	Cyber Threat Analysis	20+	Male
Researcher	Academia	Information Security	20+	Male
Professor	Academia	Information Systems	15+	Male
Professor	Academia	Information Security	15+	Female
Director	Industry	Cybersecurity	30+	Male

The survey instrument was refined based on feedback from the Delphi panel and validated scales from previous studies, which according to Hair et al.(2010) is consistent with established best practices. A pre-test was used to increase confidence and ensure respondents understand the survey questions (Oksenberg & Kalton, 1991) and were examined to minimize issues related to instrument validity, including content and construct validity as well as reliability as identified by Straub (1989). Ex ante power analysis was conducted prior to the data collection to ensure adequate statistical power (Aguirre-Urreta & Rönkkö, 2015). In the final phase, following the development of the survey instrument and validation, an online survey was provided to members of the United States Intelligence Community through a variety of platforms, receiving 240 valid responses. This survey and invitations to participate were approved for posting on US government systems, which increased the quality and quantity of responses.

The study population, the United States Intelligence Community that conducts analysis and uses Open Source Intelligence, is small enough (IC EEO, 2019) that the population is likely to not be normally distributed and it is unlikely that obtaining sample sizes necessary for confirmatory analysis processes used in covariance based statistical analysis would have been possible. Based on the size of the samples from the study population, the character of the structural path model and the exploratory nature of this proposed research, analysis was conducted through the use of Partial Least Squares Structured Equation Modeling (PLS-SEM) (Hair et al., 2010, 2017; Mamonov & Benbunan-Fich, 2018). The use of PLS-SEM is widely recognized as a valid method in both the information systems and business disciplines and is best used on small sample sizes when developing and evaluating theories (Hair et al., 2010, 2019; Khan et al., 2019).

Instrument Development

For the dependent variables of the intention to use privately or enterprise owned Internet access to conduct open-source research, the measure introduced by Brown and Venkatesh (2005) was adopted. Davis's (1989) measures regarding ease of use and usefulness were adjusted to the context of private Internet access devices and enterprise provided Internet access, with the constructs referring to completing Open Source Intelligence (OSINT) work tasks involving the use of the Internet, allowing for comparison. The perception of risk measures were adapted from Lee's (2009) measures of performance and security risks and the facilitating conditions measures were adapted from Hong et al.'s (2011) measures facilitating conditions in the acceptance of agile information systems. The measures for facilitating conditions and perception of risk for privately owned devices and Internet were not incorporated into the research model. The instrument also collected Diener et al.'s (1985) "Satisfaction With Life Scale" as a marker variable to implement the partial correlation procedure in the event common method bias was indicated (Podsakoff et al., 2003). All measures were assessed using a 7-point Likert scale ranging from completely agree to completely disagree, except one excluded indicator which included a binary choice between the intention to use enterprise or private Internet. Table 2 shows an overview of the measurement instruments that were used.

Table 2

Overview of the Measurement Instruments

Perception of Risk (Enterprise) (PoRE)	POR1: I would not feel safe using my work provided devices and Internet to do open source research. POR2: I'm worried that using my work provided devices and Internet to research work topics could cause me problems. POR3: I would not feel secure using my work provided devices and Internet to research publicly available websites from other countries.	(M.-C. Lee, 2009)
Perceived Ease of Use [of private Internet / enterprise Internet] (PEUPI/PEUEI)	If I used [enterprise provided Internet access / my own Internet access at home] for work related Internet research… PE [E/P] 1:…learning how to operate the Internet browser would be easy for me. PE [E/P] 2:…I would find it easy to find the information I was looking for. PE [E/P] 3:…my interaction with the applications would be clear, effective and flexible. PE [E/P] 4:…it would be easy for me to become skilled at open source research. PE [E/P] 5:…I would find that the tools I need are easy to use.	(Davis et al., 1989)

Perceived Usefulness **[of private Internet / enterprise Internet]** **(PUPI/PUEI)**	**Using [enterprise provided Internet access / my own Internet access at home] for work related Internet research…** **PU [E/P] 1:…would enable me to accomplish Internet research more quickly.** **PU [E/P] 2:…would improve my job performance.** **PU [E/P] 3:…would increase my productivity.** **PU [E/P] 4:…would enhance my effectiveness.** **PU [E/P] 5:…would make it easier to do my job.** **PU [E/P] 6: I would find using my own Internet access at home /at work useful to do work related Internet research.**	(Davis et al., 1989)
Intention to Use [of private Internet / enterprise Internet] for Work Activities.	**PIAW1: I intend to use my [enterprise/personal] Internet access to do Open Source research within the next two months.** **PIAW2: I predict that I will use my [enterprise/personal] Internet access for Open Source research in the next two months.** **PIAW3: I expect that I will use my [enterprise/personal] Internet access for work in the next two months.** **PIAW4: Within the next two months, I am likely to use my [enterprise/personal] Internet access to do work.**	(S. A. Brown & Venkatesh, 2005)
Facilitating Conditions	**FC1: I have the technical resources to use [enterprise provided/personal] open source Internet research tools on the Internet.** **FC2: I have the knowledge necessary to use [enterprise provided/personal] open source Internet research tools on the Internet.**	(Hong et al., 2011)

Validity and Reliability

The measurement items have been selected from previously validated studies, with most slightly modified to suit the information assurance nature of this inquiry, which provides fidelity of measurement (Mowbray et al., 2003). The survey instrument was tested to ensure it meets acceptable levels of validity and reliability, as well as comparisons to previously validated measurements. The model was evaluated using convergent validity, collinearity between indicators and the significance and relevance of outer weights (Hair et al., 2017). Additionally, the structural model was evaluated using the coefficients of determination (R^2), predictive relevance (Q^2), the size and significance of path coefficients, as well as f^2 effect sizes (Hair et al., 2017, 2019).

Validity

Salkind (2011) described internal validity as “the quality of an experimental design such that the results obtained can be attributed to the manipulation of the independent variable, whereas external validity is the quality of an experimental design such that the results can be generalized from the original sample and by extension, to the population from which the sample originated" (p. 148-149), while Gay and Airasian (2003) described validity as "the degree to which a survey measures what it is supposed to measure" (p. 23). Instrument validation is defined by Straub (1989) as the "prior and primary process in confirmatory empirical research" (p. 162). Together, these efforts describe the effect of validity on the quality of research and the generalizability of the results.

Reliability

Reliability relates to the degree in which the results of a study can be replicated, i.e. different researchers are able to reach the same or similar result (Carmines & Zeller, 1979). One measure of reliability found in the literature and widely used is Cronbach's α, which is used to determine the internal consistency and provides a summary measure based on the correlation of a given scale (Cronbach, 1951). As a result of Cronbach's α being readily discernable, and easily understood, it has been adopted as the prevailing method to determine reliability. More recent studies have called for the abandonment of this measure in favor of more dynamic analysis such as convergent reliability (Bonett & Wright, 2015; Hair et al., 2017), with studies indicating that "Cronbach's alpha is both unrelated to a scale's internal consistency and a fatally flawed estimate of its reliability" (Peters, 2018, p. 56). In addition to Cronbach's α, this study examined content validity before collecting data, and following data collection, convergent validity, the significance and relevance of indicator weights, and the presence of collinearity amongst indicators to measure and assess the measurement model.

Data Collection

Initial data collection focused on a Delphi panel of nine experts recruited from academia, industry and government agencies specializing in information security, cybersecurity and related disciplines, with the intent to form a consensus of the study's content, face validity, and reliability, with multiple iterative rounds necessary to achieve consensus. When there is a clear basis in literature from which to establish the survey instrument, a two round Delphi is often suitable, but additional iterations were necessary to resolve concerns (Dalkey et al., 1970). According to Akins et al. (2005), a Delphi panel consisting of a relatively small number of experts achieves reliable outcomes when strict inclusion methods are employed. The Delphi method is generally considered a quick, inexpensive, and relatively efficient method to ensure consensus regarding a topic or process that require individual judgements (Powell, 2003).

The Delphi group was provided the proposed survey instrument through the online Google Forms tool, which provided the opportunity to solicit qualitative responses, allowing for anonymous but secure participation and discussion within the Delphi group, both between the researcher and other participants, which is an established best practice (Akins et al., 2005). The Delphi panel identified several questions relating to perception of risk which were inadvertently reverse coded, e.g. "I would feel safe..." as opposed to "I would not feel safe…" and were subsequently corrected. The Delphi panel discussed the potential for social desirability to influence to the results, but ultimately decided that the anonymity protections provided sufficient mitigation of these concerns. Several survey and demographic questions were reworded to add clarity, remove ambiguity or were identified as being unnecessary as was the case in several demographic questions adopted from other survey instruments, including respondent’s sexual preference.

Upon completion of the Delphi panel, the survey was provided through secure government information system enclaves to members of the United States Intelligence Community who use open-source intelligence as part of their work functions. Due to the nature of the secure government information system enclaves, the study population is isolated, ensuring population integrity. Survey responses, along with appropriate demographic information, was collected through the use of Typeform, an online survey tool which provides a secure, customizable, and easily accessible data collection process, as well as a mirror of the survey hosted by Sharepoint available with each government enclave (*Security at Typeform*, 2020). All data collected were anonymized, password protected and secured with multi-factor authentication to ensure the confidentiality and integrity of the responses and to ensure only study personnel had access.

Population and Sample

This study population was limited to members of the US intelligence community. The sample included staff, contractors, as well as military members. For the purposes of this study, members of the United States Intelligence Community are defined as individuals employed, assigned, attached or working on behalf of any of the 17 separate United States government intelligence agencies that conduct intelligence activities in support of the national security of the United States (Richelson, 2018). The United States Intelligence Community consists of entities that encompass a broad range of specializations and missions, broadly categorized into national intelligence (Central Intelligence Agency, National Security Agency, National Reconnaissance Office, National Geospatial-Intelligence Agency), defense and military intelligence (Defense Intelligence Agency, and the service specific intelligence elements of the Army, Navy, Air Force, Marines and Coast Guard) and civilian intelligence agencies (Department of State, Department of Energy, Department of Treasury, Department of Homeland Security, Federal Bureau of Investigation and the Drug Enforcement Agency) (Richelson, 2018).

Sample Size

According to Hair et al. (2017), a recommended sample size of 26 observations would be needed to arrive at a statistical power of 80% for observing R^2 value of at least 0.50, accounting for a 1% error probability, based on 5 independent variables. The R^2 values reported in the studies used to develop the instrument were identified to determine the minimum values for endogenous constructs to calculate the appropriate sample size. Brown and Venkatesh (2005) reported an adjusted R^2 value of .74, Davis (1989) reported an adjusted R^2 value of .79, Lee (2009) reported an adjusted R^2 value of .80 and Hong et al. Hong (2011) reported an R^2 value of .51.

Another method for determining sample size within PLS-SEM is known as the 10 times rule, which indicates that the sample should be the larger of 10 times the largest number of formative indicators used to measure a single construct or 10 times the largest number of structural paths directed towards a particular construct in the structural model (Barclay et al., 1995; Chin & Newsted, 1999). Applying this rule of thumb to the research model results in 50 (10 x 5 reflective indicators) samples needed to adequately provide statistical power and confidence.

Data Analysis

Data analysis of the Delphi panel consisted of an examination of the responses to the initial round of semi-open questions regarding the proposed structural and measurement model as well as the survey instrument and three rounds of structured questions to verify previous consensus and finalize the model and survey instrument (Brady, 2015). Data analysis of the survey instrument was initially used to ensure the suitability of the data collected, with an emphasis on non-response bias and common method bias (Chin et al., 2012; MacKenzie et al., 2011) as well as obvious data integrity issues such as patterning, straight lining and missing data. Partial Least Squares Structured Equation Modeling (PLS-SEM) is an accepted method within IS research and is an appropriate method to be used for the analysis due to the theoretical nature of the study as well as the conceptual model (Hair et al., 2010; Khan et al., 2019). Analysis consisted of an examination of the measurement models to ensure suitability of the constructs and an evaluation of the structural model as proposed by the hypothesis of this study (Gefen et al., 2011; Hair et al., 2010).

Resources

This research study required the following resources:

- Expert panel for Delphi Method: Phase 1 of the research required an expert panel of nine cybersecurity and information systems Subject Matter Experts with diverse backgrounds and expertise within the field, as well as varying in age and education.
- Google Forms: A Web-based tool was used to gather expert panel input.

- Access to employee population: Approval from the IRB at Nova Southeastern University was obtained and is shown in Appendix A.
- Typeform: This is a multiplatform and versatile online data collection tool, which will be used to collect surveys.
- Microsoft Sharepoint: A web-based collaborative platform that was used to host a mirror of the survey on U.S. government systems.
- Microsoft Excel: A spreadsheet application used to compile and present sample demographics.
- Statistical analysis tool: Following data collection, SmartPLS Version 3.3.3, was used to conduct PLS-SEM analysis of the data and GNU PSPP Version 1.4.1-g79ad47 was used to conduct factor analysis.

Summary

This chapter consists of an overview of the quantitative research design and methodology. The research design is an exploratory model developing theory, based on established literature. The population is described as members of the United States Intelligence Community that uses Open Source Intelligence as part of their work, located throughout the world. The size of the study population is not publicly disclosed, but the response rate of 240 valid responses exceeds the minimum of 50 valid survey responses needed to provide sufficient statistical power (Hair et al., 2017) for analysis. Data were collected was obtained through the use of online tools and Web-based survey instruments. Collected data were analyzed through the use of SmartPLS Version 3.3.3, a statistical analysis toolset used to conduct PLS-SEM, and GNU PSPP Version 1.4.1 for factor analysis.

Chapter 4

Results

Overview

This chapter provides the results of a quantitative analysis of the data, as well as the demographics of the responses and the sample population. Analysis was performed on a sample of 240 cases from the data, reduced from 243 cases due to missed attention check indicators. The first section provides a demographic overview of the respondents. The subsequent sections detail the quantitative analysis of the data, consistent with the process for assessing PLS-SEM data identified by Hair et al. (2017). Beginning with the assessment of the measurement model, reflective constructs were assessed for convergent and discriminant validity as well as internal consistency. The measurement model was also assessed for common method bias. The structural model was then assessed for effect size and significance, followed by an assessment of the explanatory power and predictive relevance of the model. These analytical results are presented, followed by the results of the hypotheses of this study.

The quantitative results of the study were developed using SmartPLS version 3.3.3 (Ringle et al., 2015) for PLS-SEM analysis, and GNU PSPP Version 1.4.1 (GNU Project, 2020) was used to conduct the Harmon one-factor test for common method variance. The consistent PLS (PLSc) algorithm, with all latent variables connected to ensure consistent results, was used for PLS-SEM analysis as well as PLS bootstrapping, as recommend when the research model contains all reflective constructs (Dijkstra & Henseler, 2015; Hair et al., 2017; Ringle et al., 2015). The PLSc algorithm ensures consistent results with a factor-model by making corrections of reflective constructs' correlations (Dijkstra, 2014; Dijkstra & Henseler, 2015; Dijkstra & Schermelleh-Engel, 2014). The sample demographics were assembled using Microsoft Excel (*Microsoft Excel*, 2020)

Sample Demographics

The details of the survey responses are listed in Table 3, including the number of surveys started, the number of surveys in which the participant declined to continue or did not meet the inclusion criteria, as well as those rejected due to a missed attention check question. Due to the design of the survey software, missing or incomplete data were included in the dropout/declined numbers. The remainder of the usable responses were examined for data integrity issues such as patterning or straight lining, with no issues found.

Table 3

Response Rate Details

	Count	Percentage
Surveys Started	272	100%
Dropouts/Declined	29	10.66%
Completed responses	243	89.34%
Rejected due to missed attention check	3	1.10%
Usable responses	240	88.24%

Table 4 identifies number and percentage of the respondents' self-identified gender. The responses indicate a fairly equitable distribution of both the IC population and the population at large.

Table 4

Participant Gender (N=240)

Gender	Count	Percentage
Female	105	43.8%
Male	134	55.8%
Other	1	0.4%

Table 5 identifies number and percentage of the respondents' self-identified age category. The responses indicate a normal distribution of participants.

Table 5

Participant Age (N=240)

Age	Count	Percentage
18-24	16	6.7%
25-34	49	20.4%
35-44	83	34.6%
45-54	61	25.4%
55-64	20	8.3%
65+	11	4.6%

Table 6 identifies number and percentage of the respondents' self-identified ethnicity. The responses indicate a moderate bias towards those identifying as White or Caucasian, comprising of 72.5% of respondents, followed by those identifying as Black or African American with 9.2%.

Table 6

Participant Ethnicity (N=240)

Ethnicity	Count	Percentage
Asian or Pacific Islander	14	5.8%
Black or African American	22	9.2%
Hispanic or Latino	15	6.3%
Native American or American Indian	4	1.7%
Other	11	4.6%
White or Caucasian	174	72.5%

Table 7 identifies number and percentage of the respondents' self-identified length of service in the Intelligence Community. Approximately half (48.8%) of the respondents have served in the IC for 1-10 years, about one-third (27.9%) have served 11-20 years and 23.3% have served for more than 20 years.

Table 7

Participant Length of Service (N=240)

Length of IC Service	Count	Percentage
1 to 3 years	28	11.7%
4 to 5 years	46	19.2%
6 to 10 years	43	17.9%
11 to 20 years	67	27.9%
More than 20 years	56	23.3%

Table 8 identifies number and percentage of the respondents' self-identified levels of education attainment. It should be noted that the majority of civilian positions within the IC require a minimum education level, usually a Bachelor's degree (*Career Fields | Intelligence Careers*, 2020). Some military and contractor positions do not have these requirements.

Table 8

Participant Education (N=240)

Education	Count	Percentage
High School Diploma/GED or equivalent	9	3.8%
Associate Degree (e.g., AA, AS)	5	2.1%
Bachelor's Degree (e.g., BA, BS)	102	42.5%
Master's Degree (e.g., MA, MS, MBA)	117	48.8%
Professional Degree (e.g., MD, DDS, JD)	1	0.4%
Doctorate Degree (e.g., PhD, EdD)	6	2.5%

Table 9 identifies number and percentage of the respondents' self-identified seniority, as identified by categorized pay grade or rank, within the IC. Government Service (GS) grades range between 1 and 15, with higher grades indicating increased responsibility and pay, followed by executive level positions including Senior Executive Service (SES) and Defense Intelligence Senior Leader (DISL) (US Office of Personnel Management, 2009). Military grades range from E-1 to E-9 for enlisted personnel and O-1 to O-10 for officer personnel. Contractor personnel do not have assigned grades, but work under the supervision of government employees, with a de facto grade one less than the supervising employee.

Table 9

Participant Seniority (N=240)

Pay Grade or Rank	Count	Percentage
GS 1-5 or E1 to E4 (MIL)	3	1.3%
GS 6-9 or E5 to E7 (MIL)	25	10.4%
GS 10-12 or E8-O2 (MIL)	51	21.3%
GS 13-14 or O3 - O4 (MIL)	130	54.2%
GS 15 or O5-O6 (MIL)	28	11.7%
SES/DISL/General Officer	3	1.3%

Measurement Model Analysis

Internal Consistency and Convergent Validity of Reflective Constructs

This study reports both Cronbach's α and composite reliability score in the evaluation of the internal consistency for the reflective constructs. Cronbach's α has been traditionally used as the primary method of assessing internal consistency and reliability, with scores greater than 0.7 indicating reliability of the measured construct (Bonett & Wright, 2015; Hair et al., 2017) but as discussed in Chapter 3, the relevance of Cronbach's α has been questioned (Peters, 2018). Composite reliability is a preferred measure for internal consistency when using PLS-SEM analysis, wherein scores above 0.7 indicate reliability and scores above 0.9 indicate possible multicollinearity within the construct (Hair et al., 2017). The requirement that the dimensions of reflective constructs be related, or convergent validity, are assessed in this study through average variance extracted (AVE), with scores greater than 0.5 indicating support. All of the scores for Cronbach's α, composite reliability and AVE indicate internal consistency and convergent validity, respectively, of the reflective constructs and are shown in Table 10.

Table 10

Composite and Convergent Validity (N=240)

Construct	Cronbach's α	Composite Reliability	Average Variance Extracted (AVE)
Intention to Use Enterprise	0.770	0.769	0.528
Intention to Use Private	0.801	0.803	0.577
PEUEI	0.864	0.868	0.580
PEUPI	0.863	0.865	0.567
PUEI	0.865	0.864	0.516
PUPI	0.887	0.886	0.566
PoRE	0.832	0.839	0.642

Discriminant Validity of Reflective Constructs

Heterotrait-monotrait (HTMT) ratio is a measure of discriminant validity to determine if the constructs of a reflective model are empirically distinct from each other, and is recommended as a robust measure of discriminant validity (Ab Hamid et al., 2017), especially when conducting PLS-SEM analysis (Hair et al., 2017). Generally, HTMT ratios should not exceed 0.85, or 0.9 if the reflective constructs are closely related (Hair et al., 2017; Henseler et al., 2015). None of the HTMT ratios reported in Table 11 exceed the recommended cutoff of 0.85.

Table 11

Hetrotrait-Monotrait Ratio (HTMT) (N=240)

	Intention to Use Enterprise	Intention to Use Private	PEUEI	PEUPI	PUEI	PUPI	PoRE
Intention to Use Private	0.498						
PEUEI	0.106	0.116					
PEUPI	0.466	0.567	0.158				
PUEI	0.164	0.107	0.560	0.275			
PUPI	0.390	0.699	0.208	0.658	0.330		
PoRE	0.641	0.445	0.120	0.379	0.125	0.326	

Common Method Variance

Common method variance (CMV) is defined by Richardson et al. (2009, p. 763) as the “systematic error variance shared among variables measured with and introduced as a function of the same method and/or source”, and is a potential source of bias when the same respondent provides both independent and dependent data collected on the same instrument, a common trait of survey based research (Eichhorn, 2014). In significant levels, this variance can lead to common method bias (CMB), indicating the design of the survey instrument unduly affects the responses and which would call into question the validity of the study. One useful measure to identify disproportionate CMV is Harman's One-Factor Test, also known as Harmon's Single-Factor Test, which identifies the variance explained by a single factor, including all indicators within the model and if the variance is <50%, excessive CMV does not exist (Tehseen et al., 2017). As shown in Table 12, 27.50% of the variance is explained by one factor, well below the threshold of >50% which would indicate CMB and threaten the validity of the study.

Table 12

Harmon's One-Factor Test

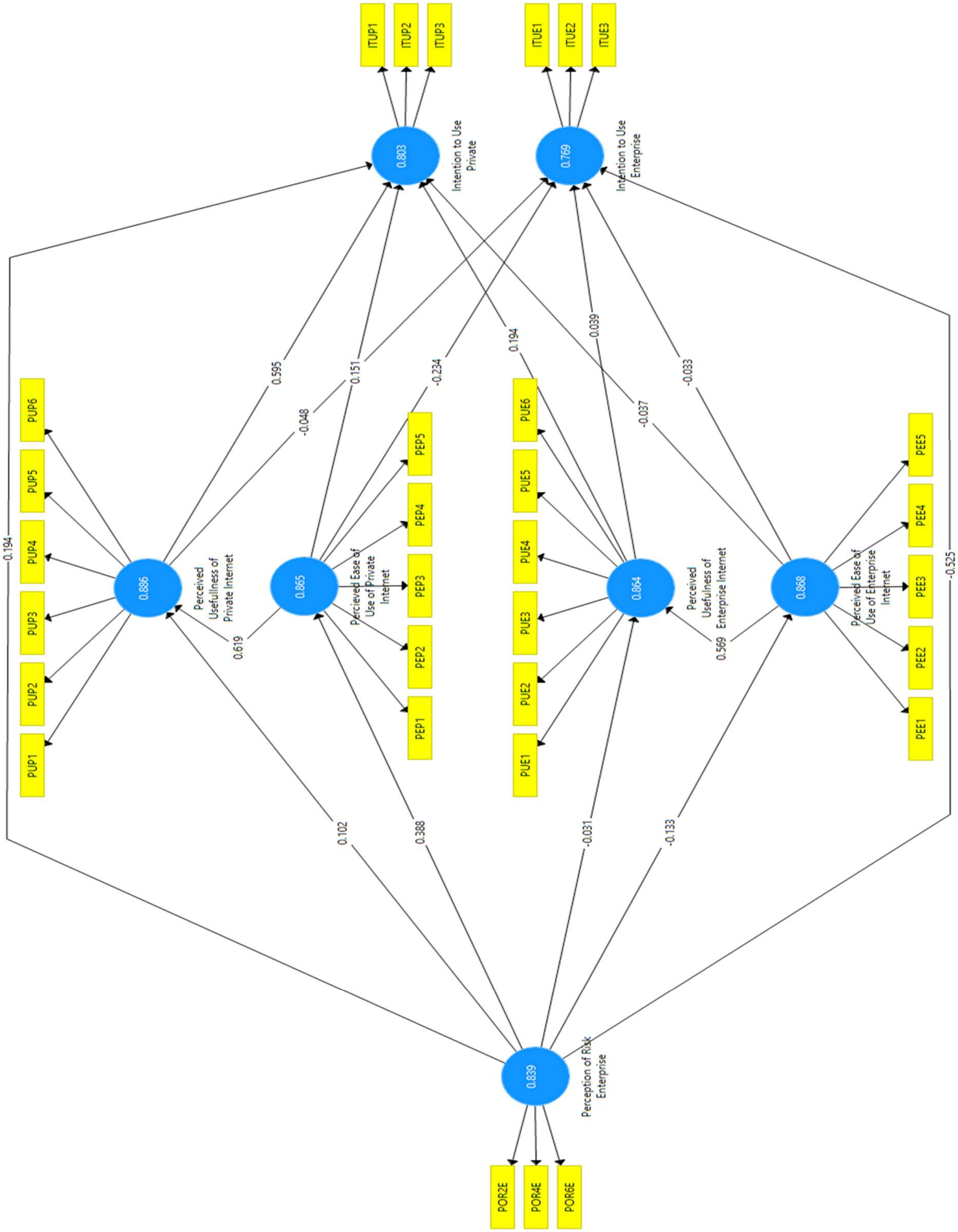
Component	Total	% of Variance	Cumulative Variance %
1.00	28.27	27.50%	27.50%

Structural Model Analysis

Following the validation of the measurement model, the structural model is assessed, beginning with the evaluation of the statistical significance of the diverse paths of the model. The effect size of each path coefficient, which estimates how one construct contributes to the explanatory power of other constructs, represented using the f^2 measure, is then reported (Cohen, 1992; Hair et al., 2017). Next, the size and significance of each endogenous construct is evaluated using the R^2 coefficient of determination and the predictive relevance of the endogenous constructs evaluated using the Q^2 measure. The final section evaluates the theorized hypotheses of this study and accepts or rejects the hypotheses based on the analysis of the structural model. The results of the PLS-SEM analysis are displayed in Figure 4, which shows the composite reliability of the constructs and the path coefficients.

Figure 4

PLS-SEM Analysis Results



Path Model Coefficient Significance and Effect Size

The initial evaluation of the statistical significance of the diverse paths of the model was conducted using an analysis of the variance inflation factors (VIF), which assesses collinearity (Hair et al., 2017). Constructs with high collinearity, as shown by VIF values exceeding five, indicate significant correlation between multiple predictor variables as well as redundancy (Hair et al., 2017). As shown in Table 13, the path model VIF values fall well below the threshold of 5, indicating a lack of collinearity between constructs.

Table 13

Path Model Variance Inflation Factor (VIF)

	Intention to Use Enterprise	Intention to Use Private	PEUEI	PEUPI	PUEI	PUPI	PoRE
PEUEI	1.635	1.635			1.018		
PEUPI	2.045	2.045				1.177	
PUEI	1.690	1.690					
PUPI	1.929	1.929					
PoRE	1.225	1.225	1.000	1.000	1.018	1.177	

Path model coefficients (β) were evaluated, which represent the hypothesized relationships between and among the constructs and range from -1 to 1 (Hair et al., 2017). Effect sizes (f^2) are also assessed, as they provide a method of determining the impact an exogenous construct has on endogenous constructs. According to Cohen (1992), assessing effect sizes (f^2) should follow these guidelines: values <0.02 indicate no effect; values between 0.02 and <0.15 represent a small effect; values between 0.15 and <0.35 represent a medium effect and values of 0.35 of greater indicate a large effect on the exogenous latent variables.

Statistical significance was further evaluated following the PLS-SEM bootstrapping process. Bootstrapping is a process where subsamples of the data are analyzed to determine significance as PLS-SEM is a non-parametric statistical method wherein there is no assumption that the underlying data are statistically distributed (Hair et al., 2017). Bootstrapping was calculated using the SmartPLS consistent PLS (PLSc) method with maximum iterations, complete bootstrapping complexity, Bias-Corrected and Accelerated (BCa) bootstrap as the confidence interval method, using 5000 samples with a two tailed test type at a 0.05 significance level, consistent with recommendations by Hair et al. (2017). The bootstrapping process provided a calculation of the *t* values, which were assessed using a two-tailed basis due to the non-directional nature of hypotheses within this study, allowing for an evaluation of the significance levels. Critical values for two-tailed *t* values at a 90% significance level are 1.645, 95% significance level is 1.96 and at a 99% significance level, 2.57 (Hair et al., 2017). Path model coefficients (β), two-tailed *t* values, effect sizes (f^2) and the corresponding p values are displayed in Table 14.

Table 14

Path Model Coefficients (N=240)

Inner Path Model	β	*t* Values	f^2	p Values
PEUEI -> Intention to Use Enterprise	-0.033	0.362	0.001	0.718
PEUEI -> Intention to Use Private	-0.037	0.457	0.002	0.648
PEUEI -> PUEI	0.569	10.319	0.474+++	<0.001***
PEUPI -> Intention to Use Enterprise	-0.234	2.204	0.050+	0.028*
PEUPI -> Intention to Use Private	0.151	1.494	0.027+	0.135
PEUPI -> PUPI	0.619	9.309	0.584+++	<0.001***
PUEI -> Intention to Use Enterprise	0.039	0.312	0.002	0.755
PUEI -> Intention to Use Private	0.194	2.156	0.053+	0.031**
PUPI -> Intention to Use Enterprise	-0.048	0.418	0.002	0.676
PUPI -> Intention to Use Private	0.595	6.780	0.435+++	<0.001***
PoRE -> Intention to Use Enterprise	-0.525	6.338	0.423+++	<0.001***
PoRE -> Intention to Use Private	0.194	2.849	0.073+	0.004***
PoRE -> PEUEI	-0.133	1.731	0.018	0.084
PoRE -> PEUPI	0.388	5.546	0.177++	<0.001***
PoRE -> PUEI	-0.031	0.477	0.001	0.634
PoRE -> PUPI	0.102	1.545	0.016	0.123

Note. *p<.10 **p<.05 ***p<.01 f^2 effect size +Small ++Medium +++Large

Path model coefficients (β), representing the path effect of linked constructs, provides an estimation of the relationship between a dependent and independent variable, wherein for every standard deviation change in the independent variable, the dependent variable will change by the path coefficient (β) standard deviations (Hair et al., 2017). The relationships between constructs with the highest positive β were PEUPI-PUPI (0.619), PUPI-Intention to Use Private (0.595), PEUEI-PUEI (0.569), PoRE-PEUPI (0.388) and PUEI-Intention to Use Private (0.194). The path relationships with the largest negative β were PoRE-Intention to Use Enterprise (-0.525) and PEUPI-Intention to Use Enterprise (-0.234). The path models of PEUPI-PUPI, PUPI-Intention to Use Private, PEUEI-PUEI and PoRE-Intention to Use Enterprise each have a large effect size and a p value <0.001.

PoRE-PEUPI has a medium effect size and a p value <0.001 while PEUPI-Intention to Use Enterprise has a small effect size and a p value <.10.

Specific indirect effects, which evaluate the β on constructs through at least one additional mediating construct and estimate the relevance of significant relationships (Hair et al., 2017), were analyzed using SmartPLS software and is shown in Table 15. The most significant effect paths were PEUPI-PUPI-Intention to Use Private (0.368), PoRE-PEUPI-PUPI (0.240), PoRE-PEUPI-PUPI-Intention to Use Private (0.143) and PEUEI-PUEI-Intention to Use Private (0.111).

Table 15

Path Model Specific Indirect Effects (N=240)

Path	Specific Indirect Effects
PEUPI -> PUPI -> Intention to Use Private	0.368
PoRE -> PEUPI -> PUPI	0.240
PoRE -> PEUPI -> PUPI -> Intention to Use Private	0.143
PEUEI -> PUEI -> Intention to Use Private	0.111
PoRE -> PUPI -> Intention to Use Private	0.061
PoRE -> PEUPI -> Intention to Use Private	0.059
PEUEI -> PUEI -> Intention to Use Enterprise	0.022
PoRE -> PEUEI -> Intention to Use Private	0.005
PoRE -> PEUEI -> Intention to Use Enterprise	0.004
PoRE -> PUEI -> Intention to Use Enterprise	-0.001
PoRE -> PEUEI -> PUEI -> Intention to Use Enterprise	-0.003
PoRE -> PUPI -> Intention to Use Enterprise	-0.005
PoRE -> PUEI -> Intention to Use Private	-0.006
PoRE -> PEUPI -> PUPI -> Intention to Use Enterprise	-0.011
PoRE -> PEUEI -> PUEI -> Intention to Use Private	-0.015
PEUPI -> PUPI -> Intention to Use Enterprise	-0.030
PoRE -> PEUEI -> PUEI	-0.076
PoRE -> PEUPI -> Intention to Use Enterprise	-0.091

Total effects, the sum of direct and indirect effects, represent both the direct effect of one construct on another as well as the indirect effects of mediating constructs (Hair et al., 2017; Sarstedt et al., 2019) and is shown in Table 16.

Table 16

Path Model Total Effects

	Intention to Use Enterprise	Intention to Use Private	PEUEI	PEUPI	PUEI	PUPI	PoRE
PEUEI	-0.011	0.073			0.569		
PEUPI	-0.264	0.520				0.619	
PUEI	0.039	0.194					
PUPI	-0.048	0.595					
PoRE	-0.632	0.441	-0.133	0.388	-0.107	0.342	

Explanatory Power and Predictive Relevance

Within this study, two endogenous constructs existed: Intention to Use Private [Internet] and Intention to Use Enterprise [Internet]. The quality of the structural model was assessed to identify the explanatory power and predictive relevance of these endogenous constructs and is detailed in Table 17. Predictive power is calculated as the coefficient of determination (R^2), which is the “squared correlation between a specific endogenous construct’s actual and predicted values” (Hair et al., 2017, p. 198), which is an in-sample prediction. To avoid bias towards more complex models, an adjusted coefficient of determination is used, where the exogenous constructs relative to the sample size are adjusted, systematically compensating for nonsignificant exogenous constructs which would otherwise increase explained variance (Hair et al., 2017). For both R^2 and Adjusted R^2, values range from 0 to 1, with increasing values indicating increasing predictive relevance. R^2 values for endogenous constructs are generally identified as substantial with values of 0.75, moderate with values of 0.5 and weak with values of 0.25 (Hair et al., 2017, 2019).

Out-of-sample predictive power, or predictive relevance, is assessed through Stone-Geisser's Q^2 value, which predicts data not found within the model estimation (Geisser, 1974; Hair et al., 2017; Stone, 1974). Q^2 values are developed using a blindfolding technique where data points in the endogenous constructs are systematically and iteratively removed and the remaining data are used to predict the missing data; the true values are then compared to the predicted values to develop the Q^2 measure (Hair et al., 2017). Q^2 values that exceed 0 are considered to have some predictive relevance, with values of 0.02, 0.15, and 0.35 representing small, medium and large predictive relevance for reflective endogenous constructs (Hair et al., 2017).

Table 17

Explanatory Power and Predictive Relevance

	R^2	Adjusted R^2	Q^2
Intention to Use Enterprise	0.467***	0.498***	0.207
Intention to Use Private	0.578***	0.598***	0.295

Note. *p<.10 **p<.05 ***p<.01

The structural model in this study provides a weak coefficient of determination (R^2) for the endogenous construct Intention to Use Enterprise (0.467) and a moderate coefficient of determination for Intention to Use Private (0.578), both of which are statistically significant at $p<0.01$. Both constructs have medium predictive value with Q^2 scores of 0.207 and 0.295, respectively.

Hypothesized Relationships

The results of the hypothesized relationships of the research model are presented in this section. The hypotheses, associated predictor paths, path coefficient (β), significance (*t* value and associated p values) and the result of the hypotheses are show in Table 18. Structural paths not associated with hypotheses are not displayed and will be discussed in Chapter 5.

Table 18

Hypotheses Results (N=240)

Label	Predictor	β	*t* Values	p Values	Result
H1a	PoRE -> PEUPI	0.388	5.546	<0.001***	**Supported**
H1b	PoRE -> PEUEI	-0.133	1.731	0.084	Not Supported
H2a	PoRE -> PUPI	0.102	1.545	0.123	Not Supported
H2b	PoRE -> PUEI	-0.031	0.477	0.634	Not Supported
H3a	PoRE -> Intention to Use Private	0.194	2.849	0.004***	**Supported**
H3b	PoRE -> Intention to Use Enterprise	-0.525	6.338	<0.001***	**Supported**
H4a	PEUPI -> PUPI	0.619	9.309	<0.001***	**Supported**
H4b	PEUEI -> PUEI	0.569	10.319	<0.001***	**Supported**
H5a	PEUPI -> Intention to Use Private	0.151	1.494	0.135	Not Supported
H5b	PEUEI -> Intention to Use Private	-0.037	0.457	0.648	Not Supported
H5c	PEUPI -> Intention to Use Enterprise	-0.234	2.204	0.028**	**Supported**
H5d	PEUEI -> Intention to Use Enterprise	-0.033	0.362	0.718	Not Supported
H6a	PUPI -> Intention to Use Private	0.595	6.780	<0.001***	**Supported**
H6b	PUEI -> Intention to Use Private	0.194	2.156	0.031**	Not Supported
H6c	PUPI -> Intention to Use Enterprise	-0.048	0.418	0.676	Not Supported
H6d	PUEI -> Intention to Use Enterprise	0.039	0.312	0.755	Not Supported

Note. *p<.10 **p<.05 ***p<.01

The majority of theorized hypotheses were not supported for lack of statistical significance, including: H1b, H2a, H3b, H5a, H5b, H5d, H6c and H6d. Hypothesis 6b: “Perceived usefulness of enterprise Internet access negatively influences employees’ intention to use private Internet access for OSINT related work activities” is not supported because while it is statistically significant, the path coefficient indicates a positive effect, contrary to the hypothesis.

The following seven hypotheses were supported and are displayed in Figure 5:

H1a: Perception of risk will have a positive effect on the perceived ease of use of private Internet access.

H3a: The perception of enterprise risk will have a direct relationship with the intention to conduct Internet based research using Private Internet access for OSINT related work activities.

H3b: The perception of enterprise risk will have a direct relationship with the intention to conduct Internet based research using Enterprise Internet access for OSINT related work activities.

H4a: Perceived ease of use of private Internet access positively influences the perceived usefulness of private Internet access.

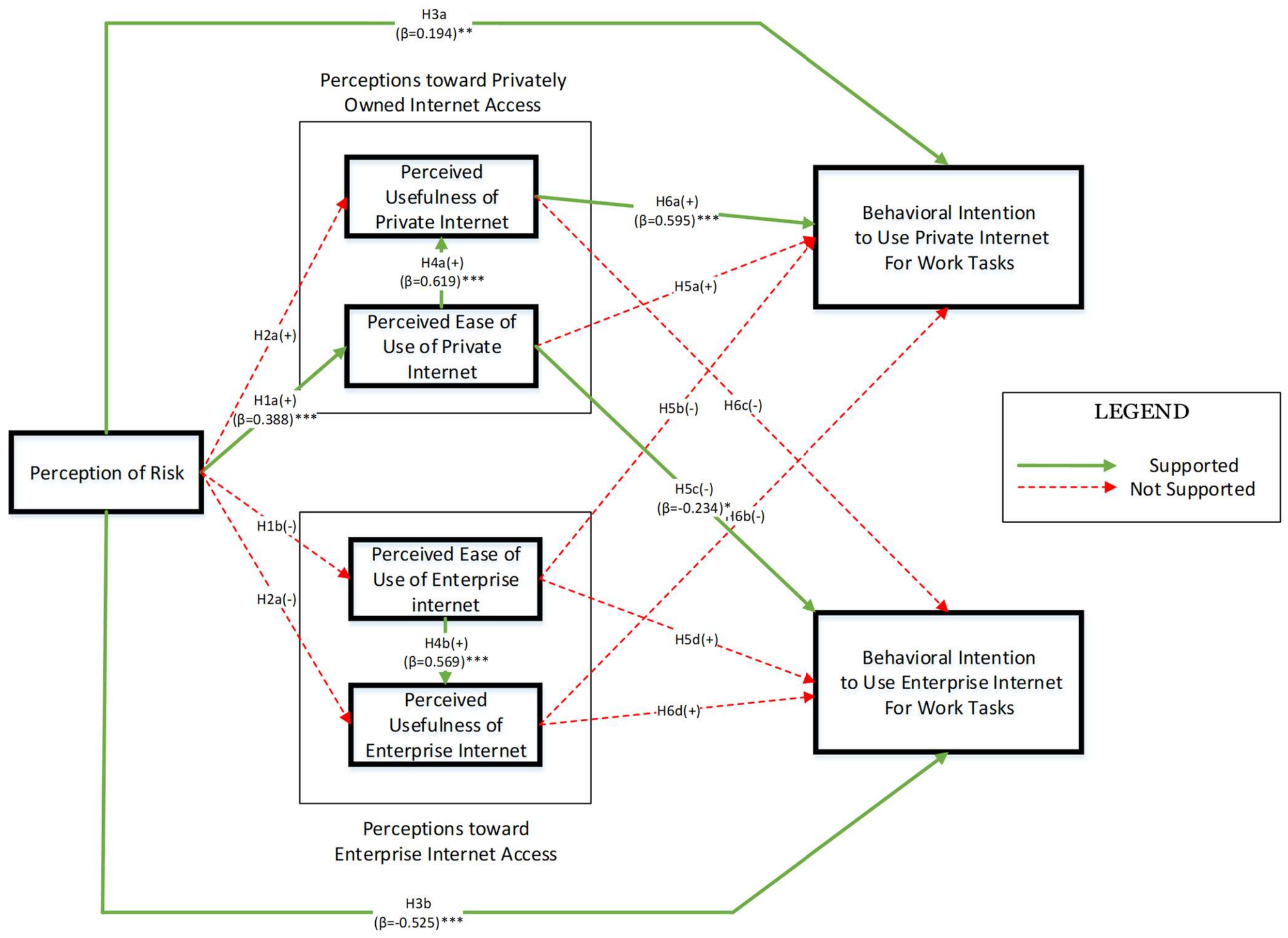
H4b: Perceived ease of use of enterprise Internet access positively influences the perceived usefulness of enterprise Internet access.

H5c: Perceived ease of use of private Internet access negatively influences employees' intention to use Enterprise Internet access for OSINT related work activities.

H6a: Perceived usefulness of private Internet access positively influences employees' intention to use private Internet access for OSINT related work activities.

Figure 5

Hypothesis Results



Note. *p<.10 **p<.05 ***p<.01

Summary

The goal of this study was to empirically assess the effects perception of risk of using enterprise provided Internet access has on the ease of use and usefulness of both private and enterprise Internet access, and the intention to use private or enterprise systems for OSINT related work activities. To accomplish this, participants completed a survey. This chapter provides the results of the quantitative analysis of the demographics of the responses and the study population, the measurement and structural models, and the results of the hypotheses. The data were analyzed using SmartPLS software to conduct PLS-SEM analysis and GNU PSPP software to assess for the presence of common method bias, which provided measures that confirmed the validity and reliability of the measurement and structural model, as well as the significance and effects of path coefficients in the model. Based on these analyses, seven hypotheses were supported and nine were not supported.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Overview

This chapter includes conclusions drawn from the findings of the analytical results provided in Chapter 4, in light of the literature reviewed, followed by discussion of the study's limitations, strengths and weaknesses. Next, implications of the research on organizational Internet restrictions and usage are discussed. The final sections of this chapter focus on recommendations for future research opportunities and a summary.

Conclusions

The goal of this research was to assess the influence the perception of risk has on the behavioral intention and use behavior of personally-owned Internet devices and access to conduct open-source research among members of the United States Intelligence Community. Based on the results of this study, the perception of risk when using enterprise provided Internet devices and access has a significant negative impact on the intention of using enterprise provided devices (H3b: β=-0.525, p<0.001, f^2 >0.35). Inversely, the perception of risk when using enterprise provided Internet devices and access on the intention to use private devices was less robust, but with a positive effect (H3a: β=0.194, p<0.01, f^2 >0.02). These results comport well to Lee's (2009) prior work evaluating the impact of risk on intention to use and support the proposition of the study that as risk increases with the use of enterprise resources, individuals are more likely to use their own Internet and devices to conduct work related tasks, which increases the risk of information compromise (Garba et al., 2015; Hovav & Putri, 2016).

The perceived ease of use of both private and enterprise Internet devices and access largely had no statistical effect on the intention to use (H5a, H5b, H5d), with one exception. The perceived ease of use of private Internet had a negative effect on the intention to use enterprise Internet (H5c: $\beta=-0.234$, $p<0.05$, $f^2>0.02$). These results may have been influenced by the relatively well educated and professionally experienced nature of the sample population; a population that has used both enterprise and personal information systems for significant lengths of time and in a variety of settings. The perception of risk on the perceived ease of use and usefulness of both private and enterprise Internet (H1b, H2a, H2b) provides a similar result – with the exception of perception of risk on perceived ease of use of private Internet (H1a: $\beta=0.388$, $p<0.001$, $f^2>0.15$). The fact that perceived risk only influenced the perceived ease of use of private Internet may be the manifestation of burdensome or difficult policies or procedures when using enterprise provided Internet.

The perceived usability of both private and enterprise Internet on the intention to use (H6b, H6c, H6d) follows the same pattern, with the exception that the perceived usability of private Internet strongly affects the intention to use private Internet positively (H6a: $\beta=0.595$, $p<0.001$, $f^2>0.35$). These results represent that a preference is shown towards using private Internet because it is perceived as being easier to use, more useful, and less risky than using enterprise provided Internet and devices. The positive relationship between perceived ease of use and perceived usefulness of both private and enterprise

Internet and devices represented in hypotheses H4a and H4b are well supported by the literature.

One of the most significant challenges facing this study was that it relies on reported behavior vice actual behavior. As discussed previously, responses can be biased towards socially desirable answers (Podsakoff & Organ, 1986), and significant variability exists between reported actions and their actual frequency of use (Verplanken & Orbell, 2003). Additionally, self-selection response bias may be present due to the fact respondents chose whether to participate or not. While this study supported the central research idea that as the perception of risk increases when using enterprise Internet and devices individuals may choose to forgo using these devices in favor of their own private Internet and devices, the scope and scale of these relationships may be exaggerated or minimized due to the reliance on survey data. Another challenge was the number of participants and the inability to validate, beyond the use of qualification questions and disseminating requests to complete the survey within Intelligence Community enclaves, that the participants were in fact members of the IC due to the anonymized method of data collection. The number of participants (N=240) exceeds the minimum threshold of 50 for statistical power and confidence (Barclay et al., 1995; Chin & Newsted, 1999), but additional samples could provide more robust generalizability. One of the strengths of this study was the high degree of internal consistency and reliability, with every construct indicating Cronbach's α and Composite Reliability scores exceeding 0.750, representing a lack of multicollinearity. Another strength was the diversity of gender, age, and experience among the IC population sample, providing a broad cross-section of responses.

Implications

This study provides insights into the intention of employees to use private Internet and devices to conduct work related tasks when enterprise provided Internet and devices are considered risky, cumbersome or difficult to use. The demarcation of private devices and Internet from enterprise Internet and devices within the milieu of the sample population, as well as the likelihood of pernicious and persistent attempts to obtain insights into Internet usage by adversaries is likely to be an unusual circumstance for most organizations. However, the threat posed by the incidental or accidental release of information when users avoid using provided enterprise information systems in order to more efficiently access information applies to organizations of all sizes and types.

The results of this study provide support to the concept that organizations must do more to balance threats to information systems with threats to information security. The imposition of safeguards to protect networks and systems, as well as employee misuse of information technology resources, may unwittingly incentivize users to use their own Internet and devices instead, where enterprise safeguards and protections are absent. This incentive is particularly pronounced when organizations increase the perceived threat of risk to users, whether intentional or inadvertent, and when the perception of the ease of use and usefulness of private Internet devices is high. This study also provides insights into user risk perception, allowing organizations to make informed decisions as to what Internet use policies are appropriate and which policies induce risk that enterprise provided systems will be avoided.

Recommendations

This study, examining what effect the perception of risk has on the intention of individuals to choose between enterprise or personal Internet and devices to do work related tasks, provides an incremental advancement in the literature of information systems. Based on the analysis of this study, as well as the study's exploratory nature, several recommendations are provided to further this line of research.

The first recommendation is to conduct appropriately tailored versions of this study across a broad array of organizations, including government entities at the federal, state, and local levels, within academic institutions, and private organizations to assess whether the risk effects are broadly generalizable. Further empirical studies would provide additional support to the theoretical concepts of risk developed in this study and its impact on individual choices selecting between an enterprise and private environment. The second recommendation is to incorporate the perception of risk of using private Internet and devices as an additional exogenous construct into the research model, which would facilitate cross comparison of the effect risk has on intention to use behaviors as well as ease of use and usefulness measures. The third recommendation is to assess whether moderating variables derived from the UTAUT model, such as age, gender, and experience (Venkatesh et al., 2003; M. Williams et al., 2015), have a significant effect. The fourth recommendation is to assess whether measures of facilitating conditions for both enterprise and personally owned Internet access have a significant effect on intention to use behaviors, especially when selecting between organizational and private Internet and devices as influenced by perceived risk.

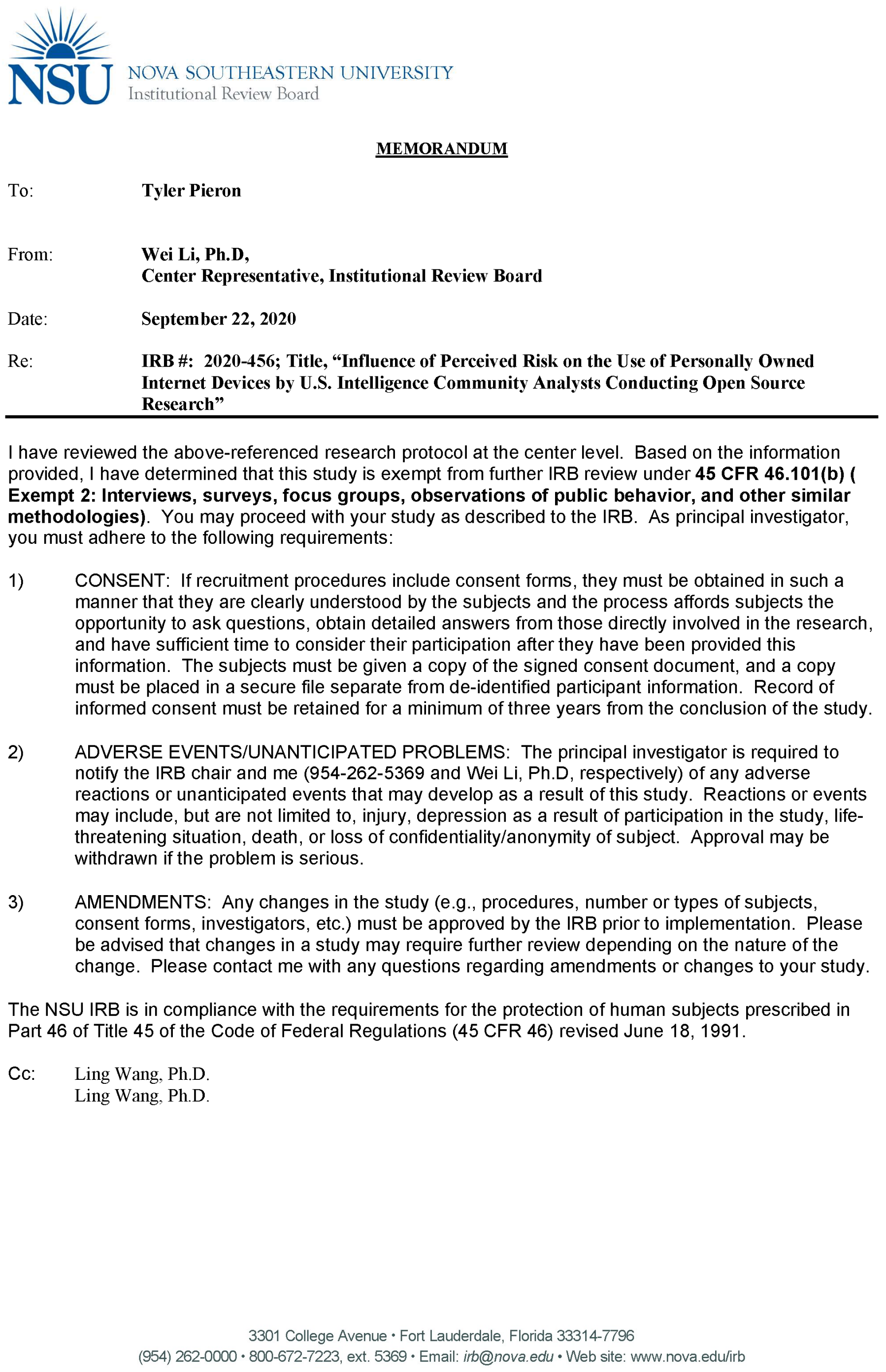
Summary

Securing information systems against external threats is often the primary motivation of information security professionals (T. Brown, 2018; Gordon & Loeb, 2002; Wang, 2019), but protecting critical information, as well as systems, is a necessary and essential component of a holistic organizational security effort. When critical information is potentially exposed by non-malicious insiders who use personal devices to conduct work related tasks outside of the organizational information systems infrastructure, the organization loses both visibility of the potential loss and is unable to provide appropriate safeguards to prevent information compromise. When organizations increase the perception of risk when using enterprise systems and networks to conduct work related activities, or impose restrictions that impede the usefulness or ease of use of information systems (Gundu & Flowerday, 2012; Hovav & Putri, 2016), they are inadvertently incentivizing users to bypass these limitations and use personally owned devices and Internet (Colvin, 2016), potentially increasing the risk of information compromise.

This study demonstrated that increases in the perception of risk when using enterprise provided devices and Internet significantly affects the intention to use personally owned devices and Internet to conduct work related tasks. It also demonstrated that the perceived usefulness of personally owned devices, compared to the usefulness of enterprise provided devices, plays a significant role in intention to use behaviors.

The study's limitations, strengths and weaknesses were identified and discussed. The study's implications, including the recognition that organizations must carefully balance threats to information systems with threats to information security and imposing restrictions which increase the perception of risk or impede user's ability to perform their work introduce the possibility that outside resources may be used, such as personally owned devices. Finally, several recommendations for future research opportunities were provided. As a result of this study, the extant gap in the literature to understand the motivations and choices employees make to choose between enterprise systems and personal systems to accomplish work related tasks has been partially filled.

Appendix A: Institutional Review Board Approval



NSU NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Tyler Pieron**

From: **Wei Li, Ph.D,**
Center Representative, Institutional Review Board

Date: **September 22, 2020**

Re: **IRB #: 2020-456; Title, "Influence of Perceived Risk on the Use of Personally Owned Internet Devices by U.S. Intelligence Community Analysts Conducting Open Source Research"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Wei Li, Ph.D, respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Ling Wang, Ph.D.
Ling Wang, Ph.D.

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-0000 • 800-672-7223, ext. 5369 • Email: *irb@nova.edu* • Web site: www.nova.edu/irb

Appendix B: Delphi Survey Questionnaire

Dear Panel Members,

Thank you for agreeing to participate in the review of my survey! Your views, thoughts, opinions, and suggestions are very appreciated. I know each of you are very busy and I thank you for your time and attention.

Some background:

My dissertation research is incorporating a survey looking at how members of the Intelligence Community obtain open source information from the Internet, and how the perception of risk influences these choices. The theoretical framework is derived from the two primary "technology acceptance use" theories and is attached to this email to help provide context.

The survey questions are also derived from other validated studies and are related to each of the constructs being reviewed. The survey includes some additional features to help ensure validity and consistency, such as attention check questions as well as a few questions completely unrelated to the study to help identify and minimize common method bias, which is when the way the survey is administered affects the results. Several demographic questions complete the survey, which should take on average about 20 minutes to finish.

Instructions:

I have attached a document that contains the survey as well as annotations and background for each set of questions. You can also preview the survey as it will be presented here: https://tp877.typeform.com/to/fOqHuzUe

Please review the wording, phrasing and sequence of the questions, the style of the survey, and any other factor that could be misinterpreted, cause confusion, or cause respondents to answer the survey in ways other than which is intended. The goal is the ensure that the survey questions are clear, unambiguous, and easily answered by the study population with clarity.

As you identify any issues or areas needing clarification, please identify the question number (and sub-question as applicable) as this will help me ensure that the issue is addressed. You can also use the document and make your comments there (Please use another color font for text)

In order to ensure your confidentiality and to encourage open communication, each participant is receiving a blind copy of this email. Please reply to this email with your responses, questions, or anything else you may require.

Please provide any feedback you may have by 9 October 2020.

Thank you for participating and let me know if you have any questions.

Tyler Pieron
PhD Candidate
Nova Southeastern University

The survey questions are examining the influence of perceived risk on the use of personally owned Internet devices by U.S. Intelligence Community analysts conducting Open Source research and are derived from previous validates studies. The study questions are listed below and are numbered for easy reference. Text that appears in the survey is indicated by **BOLD** text.

Annotations will be italicized and are not present in the survey itself and are provided to assist you in reviewing the survey. All questions are mandatory, including demographic questions. An attention check question is located within the survey as is a series of questions to assess and control for common method bias, which helps to ensure that the format of the survey itself doesn't influence the responses.

0. Welcome Screen
1. **Before we begin, we want you to be informed about the nature of the study, who is conducting it, and any risks. A full printable version of this consent form can be downloaded here: http://ow.ly/o45Y50BqoWO**

   If you choose not to participate, please close your browser.

   Do you agree to participate in this study?

   Respondents can choose between I Agree and I Disagree. If they choose Disagree, the survey will exit.

2. **First, we need to make sure you are part of the population we are trying to reach with this survey.** *These two questions are YES/NO and serve to verify the sample population. If either question is responded to with a NO, the survey will exit. If both are yes, the survey will continue.*

   a. **Are you a member of the United States Intelligence Community?**
   b. **Do you use Open Source Intelligence as part of your work in the Intelligence Community? (Open Source Intelligence is defined as "…intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an**

appropriate audience for the purpose of addressing a specific intelligence requirement")

Excellent! You have been qualified as a member of the study population. This study uses scales to measure your opinion on various questions. Please select the response that most accurately captures how much you agree or disagree with a particular statement.

The survey will now begin.

As a reminder, all answers are confidential and your participation is completely voluntary.

3. **The first section focuses on your thoughts on Information Security.** *(All responses are collected via a 7-point Likert Scale ranging from Strongly Disagree to Strongly Agree. In each question, the source of the Internet is bolded to call attention to the difference between questions.)*
   a. **I would feel safe using my personal device/Internet to do research on the same topics I research for work**
   b. **I would feel safe using my work provided devices/Internet to do Internet research**
   c. **I'm worried that using my private devices and Internet to research work topics could cause me problems.**
   d. **I'm worried that using work provided devices and Internet to research work topics could cause me problems.**
   e. **I feel secure using my personal Internet to research publicly available websites from other countries.**
   f. **I feel secure using work provided Internet to research publicly available websites from other countries.**
   g. **I am more like to use my ____________ Internet access for Open Source research in the next two months.** *(This question has two options)*
      i. **Personal**
      ii. **Work Provided**

4. **Great, now let's focus how easy (or hard) it is to use your personally owned devices/Internet or work provided devices/Internet for Internet research. We will begin with your own Internet access and devices you use at home.** *(All responses are collected via a 7-point Likert Scale ranging from Strongly Disagree to Strongly Agree. In each question, the source of the Internet is bolded to call attention to the difference between questions.)*

a. **If I used my own Internet access and devices at home for work related Internet research, learning how to operate the Internet browser would be easy for me.**
b. **If I used my own Internet access and devices at home for work related Internet research, I would find it easy to find the information I was looking for.**
c. **If I used my own Internet access and devices at home for work related Internet research, my interaction with the applications I need to use would be clear, effective and flexible.**
d. **If I used my own Internet access and devices at home for work related Internet research, it would be easy for me to become skilled at open source research.**
e. **If I used my own Internet access and devices at home for work related Internet research, I would find that the tools I need are easy to use.**
f. **Within the next two months, I am likely to use my own Internet access and devices at home to do Open Source work.**

The following questions are asking about enterprise (work) provided Internet access and devices:

g. **If I used enterprise (work) provided Internet access and devices for work related Internet research, learning how to operate the Internet browser would be easy for me.**
h. **If I used enterprise (work) provided Internet access and devices for work related Internet research, I would find it easy to find the information I was looking for.**
i. **If I used enterprise (work) provided Internet access and devices for work related Internet research, my interaction with the applications I need to use would be clear, effective and flexible.**
j. **If I used enterprise (work) provided Internet access and devices for work related Internet research, it would be easy for me to become skilled at open source research.**
k. **If I used enterprise (work) provided Internet access and devices for work related Internet research, I would find that the tools I need are easy to use.**
l. **Within the next two months, I am likely to use enterprise (work) provided Internet access and devices to do Open Source work.**

5. **Now, we want to know how useful you find using your own devices and Internet is compared to how useful your find work provided devices and Internet is when doing Open Source research.** *(All responses are collected via a 7-point Likert Scale ranging from Strongly Disagree to Strongly Agree. In each question, the source of the Internet is bolded to call attention to the difference*

between questions.)

Over halfway there now, keep it up!

a. **Using enterprise (work) provided Internet access and devices for work related Internet research enables me to accomplish Internet research more quickly.**
b. **Using enterprise (work) provided Internet access and devices for work related Internet research improves my job performance.**
c. **Using enterprise (work) provided Internet access and devices for work related Internet research increases my productivity.**
d. **Using enterprise (work) provided Internet access and devices for work related Internet research enhances my effectiveness.**
e. **Using enterprise (work) provided Internet access and devices for work related Internet research makes it easier to do my job.**
f. **I find using enterprise (work) provided Internet access and devices useful to do work related Internet research.**
g. **We know there are a bunch of questions. Please select Strongly Agree for this question. *(This question is designed to ensure the participant is paying attention to the questions).***
h. **I intend to use my enterprise (work) provided Internet access to do Open Source research within the next two months**
i. **Using my own Internet access at home for work related Internet research enables me to accomplish Internet research more quickly.**
j. **Using my own Internet access at home for work related Internet research improves my job performance.**
k. **Using my own Internet access at home for work related Internet research increases my productivity**
l. **Using my own Internet access at home for work related Internet research enhances my effectiveness.**
m. **Using my own Internet access at home for work related Internet research makes it easier to do my job.**
n. **Using my own Internet access at home is useful to do work related Internet research.**
o. **I intend to use my personal Internet access to do Open Source research within the next two months**

6. **This section is asking how likely you are to conduct Open Source research in the near future.** *(These two questions are included to ensure internal consistency and validity of the survey. All responses are collected via a 7-point Likert Scale ranging from Strongly Disagree to Strongly Agree. In each question, the source of the Internet is bolded to call attention to the difference between questions.)*

   a. **I expect that I will use my work provided Internet access for Open Source research in the next two months.**
   b. **I expect that I will use my personal Internet access for Open Source research in the next two months.**

7. **This section is asking about how you are doing and your satisfaction with life.** *(This section helps to address Common Method Bias and are completely unrelated to the study. Responses are collected via a 7-point Likert Scale)*
   a. **In most ways, my life is close to my ideal.**
   b. **So far, I have gotten the important things I want in life.**
   c. **If I could live my life over, I would change almost nothing.**

8. **This short section is asking whether you have to the tools and resources to do Open Source research.** *All responses are collected via a 7-point Likert Scale ranging from Strongly Disagree to Strongly Agree. In each question, the source of the Internet is bolded to call attention to the difference between questions.)*
   a. **My enterprise (work) provides the technical resources and tools I need to obtain Open Source information from the Internet myself.**
   b. **I have the knowledge necessary to use enterprise provided open source research tools on the Internet.**
   c. **I have the technical resources and tools I need to obtain Open Source information from the Internet using my own devices and Internet access.**
   d. **I have the knowledge necessary to use my own (not work provided) open source research tools on the Internet.**

9. **OK, we are almost done!**
   Just a few demographic questions to help us analyze the data.
   Don't worry - your responses are completely anonymous and will be aggregated by category to protect your privacy.
   a. **Select the category that you belong to.**
      If you are in more than one category, please identify what role you serve in the most.
      a. **Government Employee (Civilian)**
      b. **Military**
      c. **Contractor**

   b. **Are you:**
      a. **Male**
      b. **Female**
      c. **Other**

c. **How old are you?**
   a. **18-24**
   b. **25-34**
   c. **35-44**
   d. **45-54**
   e. **55-64**
   f. **65+**

d. **Which of the following do you consider yourself to be?**
   a. **Straight, this not gay or lesbian**
   b. **Gay or Lesbian**
   c. **Bisexual**
   d. **Something else**

e. **What ethnic origin do you most closely identify with?**
   a. **Hispanic or Latino**
   b. **White or Caucasian**
   c. **Black or African American**
   d. **Native American or American Indian**
   e. **Asian or Pacific Islander**
   f. **Other**

f. **How long have you been in the Intelligence Community?**
   a. **Less than 1 year**
   b. **1 to 3 years**
   c. **4 to 5 years**
   d. **6 to 10 years**
   e. **11 to 20 years**
   f. **More than 20 years**

g. **What is your pay category/grade?**
   Please choose one of the following answers. If you belong to another scale system, i.e. contractor, pay banding, or military, please select the grouping that best reflects your equivalent pay/grade category

(Members of the IC are assigned equivalent pay grades based on position and function and respondents will have no issues responding accurately)

a. **GS 1-5**
b. **GS 6-9**
c. **GS 10-12**
d. **GS 13-14**
e. **GS 15**
f. **Senior Executive Service or DISL**

h. **What is the highest degree or level of education you have completed?**
   a. **Less than High School**
   b. **High School Diploma/GED or equivalent**
   c. **Trade or Technical Certificate**
   d. **Some College (no degree)**
   e. **Associate Degree (e.g., AA, AS)**
   f. **Bachelor's Degree (e.g., BA, BS)**
   g. **Master's Degree (e.g., MA, MS, MBA)**
   h. **Professional Degree (e.g., MD, DDS, JD)**
   i. **Doctorate Degree (e.g., PhD, Ed.D)**

i. **Indicate the mission category that best fits your position.** *(The primary function of members of the IC determines what authorities and requirements they are expected to comply with and what their day to day job functions are. This is a standard demographic question within IC based surveys)*
   a. **COLLECTION AND OPERATIONS - Positions that involve the collection and reporting of information obtained from sources by various means, including human and technical means, as well as occupations involved in intelligence operations.**
   b. **PROCESSING AND EXPLOITATION - Occupations or positions that involve the conversion of information collected from various intelligence sources into a form that can be analyzed to produce an intelligence product.**
   c. **ANALYSIS AND PRODUCTION - Occupations or positions that involve the preparation of a finished intelligence product from information obtained and processed from one or more intelligence sources in support of customer requirements.**
   d. **RESEARCH AND TECHNOLOGY - Occupations or positions that involve basic, applied, and advanced scientific and engineering research and development.**
   e. **ENTERPRISE INFORMATION TECHNOLOGY - Positions that support the organization's information systems. This category includes telecommunications, network operations, operation and maintenance of common user systems, and computing infrastructure.**
   f. **ENTERPRISE MANAGEMENT AND SUPPORT- Occupations or positions that involve support for the organization's human, financial, physical, and other resources, such as financial management, human resources management, and acquisition.**
   g. **MISSION MANAGEMENT- Occupations or positions that involve the coordination and integration of IC-wide intelligence requirements, resources, and activities.**

10. Exit Screen

You have completed the survey!

If you know other members of the IC that might want to help this research, please share the link.

(Please close your browser to exit the survey)

Appendix C: Pre-Screening Questions

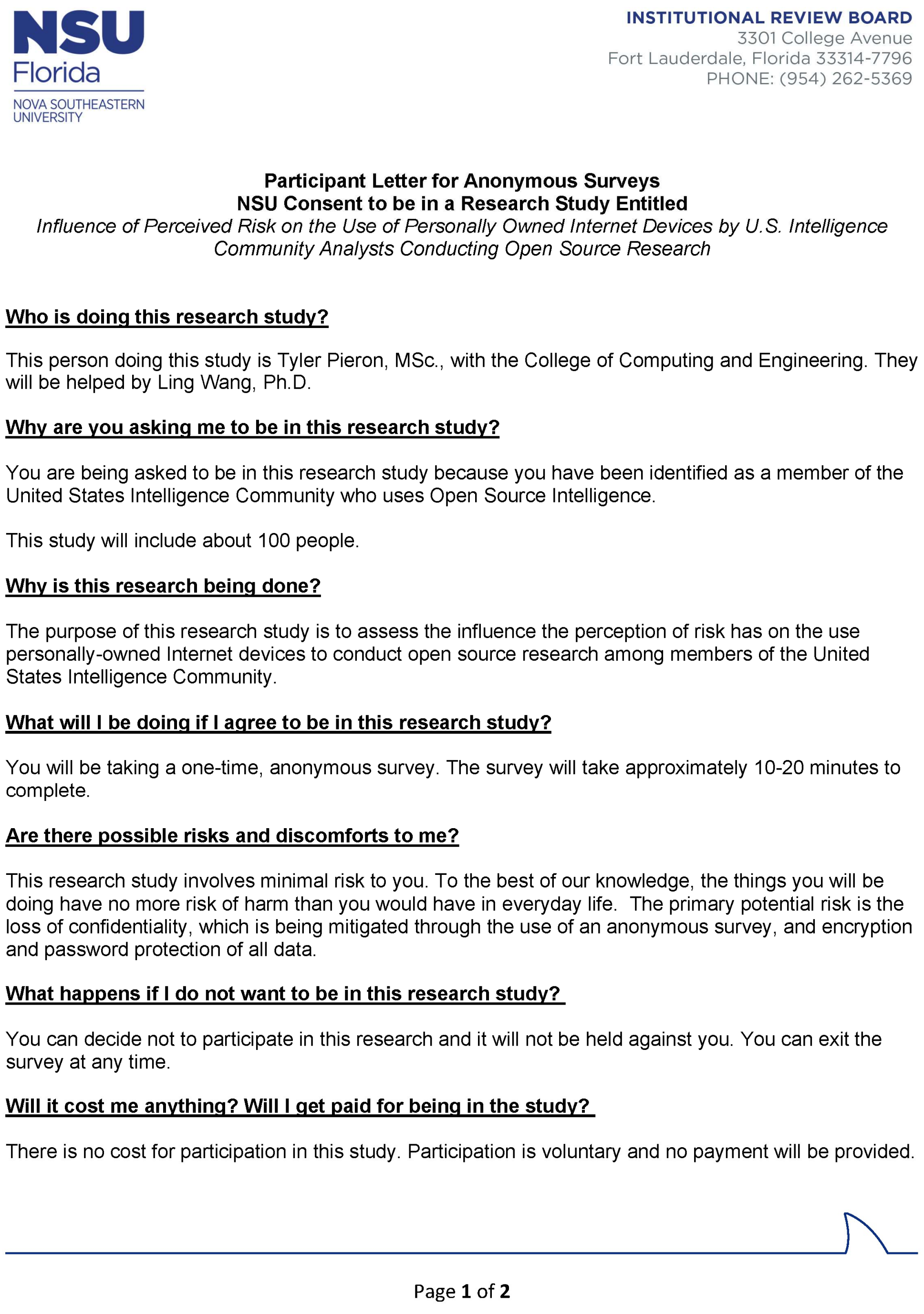
Are you a member of the United States Intelligence Community? YES OR NO

Note: This includes staff, contractors, as well as military members employed, assigned, attached or working on behalf of any of the 17 separate United States government intelligence agencies that conduct intelligence activities in support of the national security of the United States

Do you use Open Source Intelligence as part of your work in the Intelligence Community? YES OR NO

A "NO" answer to either or both of these questions would preclude participation in this study.

Appendix D: Informed Consent Wavier



NSU
Florida
NOVA SOUTHEASTERN
UNIVERSITY

INSTITUTIONAL REVIEW BOARD
3301 College Avenue
Fort Lauderdale, Florida 33314-7796
PHONE: (954) 262-5369

Participant Letter for Anonymous Surveys
NSU Consent to be in a Research Study Entitled
Influence of Perceived Risk on the Use of Personally Owned Internet Devices by U.S. Intelligence Community Analysts Conducting Open Source Research

Who is doing this research study?

This person doing this study is Tyler Pieron, MSc., with the College of Computing and Engineering. They will be helped by Ling Wang, Ph.D.

Why are you asking me to be in this research study?

You are being asked to be in this research study because you have been identified as a member of the United States Intelligence Community who uses Open Source Intelligence.

This study will include about 100 people.

Why is this research being done?

The purpose of this research study is to assess the influence the perception of risk has on the use personally-owned Internet devices to conduct open source research among members of the United States Intelligence Community.

What will I be doing if I agree to be in this research study?

You will be taking a one-time, anonymous survey. The survey will take approximately 10-20 minutes to complete.

Are there possible risks and discomforts to me?

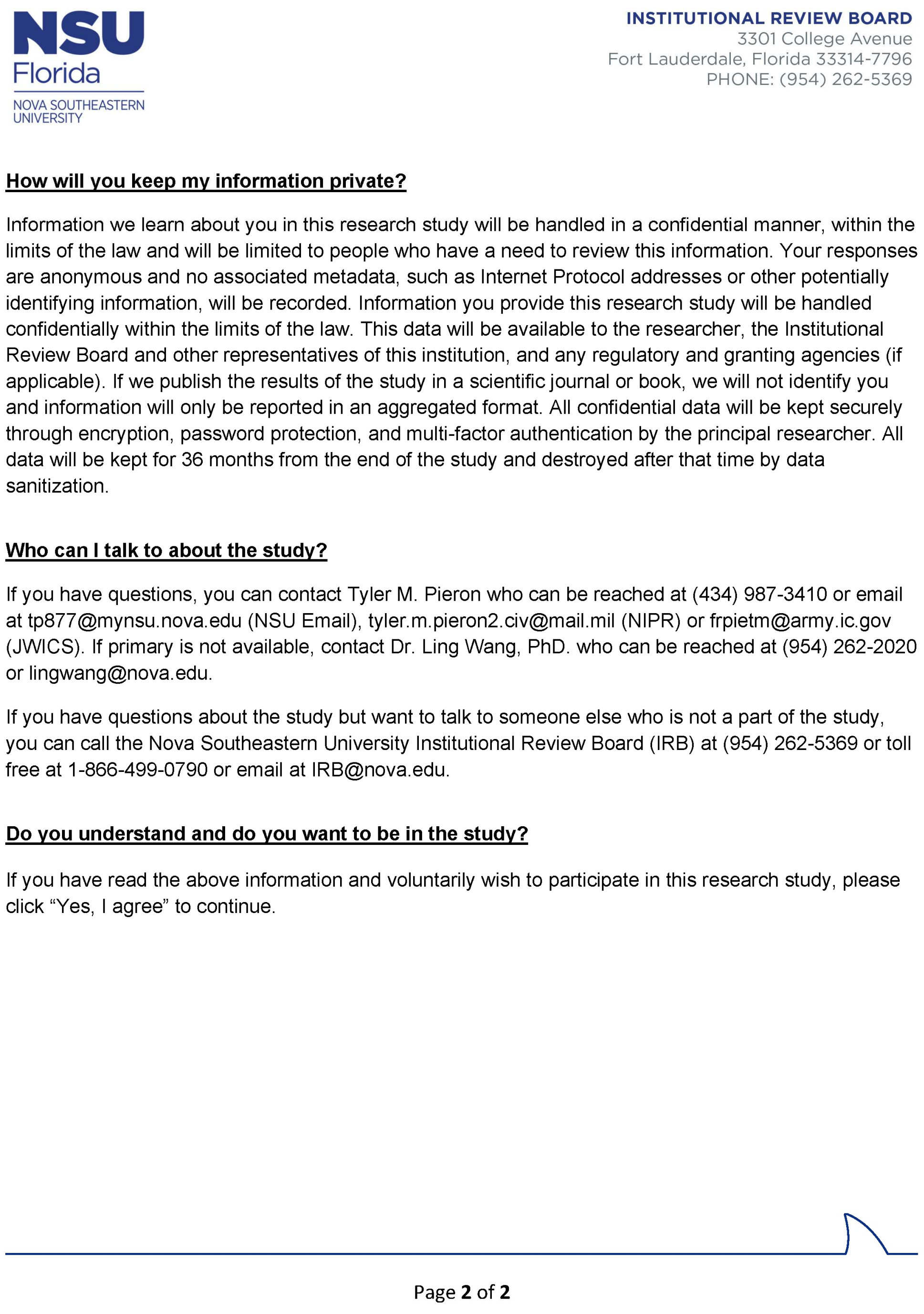
This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life. The primary potential risk is the loss of confidentiality, which is being mitigated through the use of an anonymous survey, and encryption and password protection of all data.

What happens if I do not want to be in this research study?

You can decide not to participate in this research and it will not be held against you. You can exit the survey at any time.

Will it cost me anything? Will I get paid for being in the study?

There is no cost for participation in this study. Participation is voluntary and no payment will be provided.



How will you keep my information private?

Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law and will be limited to people who have a need to review this information. Your responses are anonymous and no associated metadata, such as Internet Protocol addresses or other potentially identifying information, will be recorded. Information you provide this research study will be handled confidentially within the limits of the law. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any regulatory and granting agencies (if applicable). If we publish the results of the study in a scientific journal or book, we will not identify you and information will only be reported in an aggregated format. All confidential data will be kept securely through encryption, password protection, and multi-factor authentication by the principal researcher. All data will be kept for 36 months from the end of the study and destroyed after that time by data sanitization.

Who can I talk to about the study?

If you have questions, you can contact Tyler M. Pieron who can be reached at (434) 987-3410 or email at tp877@mynsu.nova.edu (NSU Email), tyler.m.pieron2.civ@mail.mil (NIPR) or frpietm@army.ic.gov (JWICS). If primary is not available, contact Dr. Ling Wang, PhD. who can be reached at (954) 262-2020 or lingwang@nova.edu.

If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at IRB@nova.edu.

Do you understand and do you want to be in the study?

If you have read the above information and voluntarily wish to participate in this research study, please click "Yes, I agree" to continue.

Appendix E: Sample Recruitment Letter or Email

Sample Recruitment Letter or Email

Dear [*insert name*],

My name is Tyler Pieron and I am a student from the College of Computing and Engineering at Nova Southeastern University. I am writing to invite you to participate in my research study about the influence of perceived risk on the use of personally owned internet devices by U.S. Intelligence Community (IC) analysts conducting open source research. You're eligible to participate in this study if you are a member of the IC and use open source information, such as information found on the Internet.

If you decide to participate in this study, you will complete a short online survey, which will take approximately 20 minutes, asking about your use of both personal and enterprise systems when researching open source information. There is no cost to participate and no payments will be provided to participants.

Remember, this is completely voluntary. You can choose to be in the study or not. You can also choose to participate in the survey but not the interview. If you'd like to participate complete the survey located here: https://www.typeform.com/abc123

If you have any questions about the study, please contact me at (434) 987-3410 or email at tp877@mynsu.nova.edu (NSU Email), tyler.m.pieron2.civ@mail.mil (NIPR) or frpietm@army.ic.gov (JWICS).

Thank you very much.

Sincerely,

Tyler Pieron

Appendix F: Survey Questionnaire

0. Welcome Screen
1. **Before we begin, we want you to be informed about the nature of the study, who is conducting it, and any risks. A full printable version of this consent form can be downloaded here: http://ow.ly/o45Y50BqoWO**

   If you choose not to participate, please close your browser.

   Do you agree to participate in this study?

2. **First, we need to make sure you are part of the population we are trying to reach with this survey.** *These two questions are YES/NO and serve to verify the sample population. If either question is responded to with a NO, the survey will exit. If both are yes, the survey will continue.*

   a. **Are you a member of the United States Intelligence Community?**
   b. **Do you use Open Source Intelligence as part of your work in the Intelligence Community? (Open Source Intelligence is defined as "…intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement")**

   Excellent! You have been qualified as a member of the study population. This study uses scales to measure your opinion on various questions. Please select the response that most accurately captures how much you agree or disagree with a particular statement.

   The survey will now begin.

   As a reminder, all answers are confidential and your participation is completely voluntary.

   (All responses are collected via a 7-point Likert Scale ranging from Strongly Disagree to Strongly Agree.)

3. **The first section focuses on your thoughts on Information Security.**
   a. **I would not feel safe using my personal device/Internet to do research on the same topics I research for work**
   b. **I would not feel safe using my work provided devices/Internet to do Internet research**
   c. **I'm worried that using my private devices and Internet to research work topics could cause me problems.**
   d. **I'm worried that using work provided devices and Internet to research work topics could cause me problems.**

   e. **I would not feel secure using my personal Internet to research publicly available websites from other countries.**
   f. **I would not feel secure using work provided Internet to research publicly available websites from other countries.**
   g. **I am more like to use my ____________ Internet access for Open Source research in the next two months.** *(This question has two options)*
      i. **Personal**
      ii. **Work Provided**

4. **Great, now let's focus how easy (or hard) it is to use your personally owned devices/Internet or work provided devices/Internet for Internet research. We will begin with your own Internet access and devices you use at home.**
   a. **If I used my own Internet access and devices at home for work related Internet research, learning how to operate the Internet browser would be easy for me.**
   b. **If I used my own Internet access and devices at home for work related Internet research, I would find it easy to find the information I was looking for.**
   c. **If I used my own Internet access and devices at home for work related Internet research, my interaction with the applications I need to use would be clear, effective and flexible.**
   d. **If I used my own Internet access and devices at home for work related Internet research, it would be easy for me to become skilled at open source research.**
   e. **If I used my own Internet access and devices at home for work related Internet research, I would find that the tools I need are easy to use.**
   f. **Within the next two months, I am likely to use my own Internet access and devices at home to do Open Source work.**

   The following questions are asking about enterprise (work) provided Internet access and devices:

   g. **If I used enterprise (work) provided Internet access and devices for work related Internet research, learning how to operate the Internet browser would be easy for me.**
   h. **If I used enterprise (work) provided Internet access and devices for work related Internet research, I would find it easy to find the information I was looking for.**
   i. **If I used enterprise (work) provided Internet access and devices for work related Internet research, my interaction with the applications I need to use would be clear, effective and flexible.**

j. **If I used enterprise (work) provided Internet access and devices for work related Internet research, it would be easy for me to become skilled at open source research.**
k. **If I used enterprise (work) provided Internet access and devices for work related Internet research, I would find that the tools I need are easy to use.**
l. **Within the next two months, I am likely to use enterprise (work) provided Internet access and devices to do Open Source work.**

5. **Now, we want to know how useful you find using your own devices and Internet is compared to how useful your find work provided devices and Internet is when doing Open Source research.**

    a. **Using enterprise (work) provided Internet access and devices for work related Internet research enables me to accomplish Internet research more quickly.**
    b. **Using enterprise (work) provided Internet access and devices for work related Internet research improves my job performance.**
    c. **Using enterprise (work) provided Internet access and devices for work related Internet research increases my productivity.**
    d. **Using enterprise (work) provided Internet access and devices for work related Internet research enhances my effectiveness.**
    e. **Using enterprise (work) provided Internet access and devices for work related Internet research makes it easier to do my job.**
    f. **I find using enterprise (work) provided Internet access and devices useful to do work related Internet research.**
    g. **We know there are a bunch of questions. Please select Strongly Agree for this question.** ***(This question is designed to ensure the participant is paying attention to the questions).***
    h. **I intend to use my enterprise (work) provided Internet access to do Open Source research within the next two months**
    i. **Using my own Internet access at home for work related Internet research enables me to accomplish Internet research more quickly.**
    j. **Using my own Internet access at home for work related Internet research improves my job performance.**
    k. **Using my own Internet access at home for work related Internet research increases my productivity**
    l. **Using my own Internet access at home for work related Internet research enhances my effectiveness.**
    m. **Using my own Internet access at home for work related Internet research makes it easier to do my job.**
    n. **Using my own Internet access at home is useful to do work related Internet research.**

o. **I intend to use my personal Internet access to do Open Source research within the next two months**

6. **This section is asking how likely you are to conduct Open Source research in the near future.**
    a. **I expect that I will use my work provided Internet access for Open Source research in the next two months.**
    b. **I expect that I will use my personal Internet access for Open Source research in the next two months.**

7. **This section is asking about how you are doing and your satisfaction with life.**
    a. **In most ways, my life is close to my ideal.**
    b. **So far, I have gotten the important things I want in life.**
    c. **If I could live my life over, I would change almost nothing.**

8. **This short section is asking whether you have to the tools and resources to do Open Source research.**
    a. **My enterprise (work) provides the technical resources and tools I need to obtain Open Source information from the Internet myself.**
    b. **I have the knowledge necessary to use enterprise provided open source research tools on the Internet.**
    c. **I have the technical resources and tools I need to obtain Open Source information from the Internet using my own devices and Internet access.**
    d. **I have the knowledge necessary to use my own (not work provided) open source research tools on the Internet.**

9. **Just a few demographic questions to help us analyze the data.**
   Don't worry - your responses are completely anonymous and will be aggregated by category to protect your privacy.

   Select the category that you belong to. If you are in more than one category, please identify what role you serve in the most.
    a. **Government Employee (Civilian)**
    b. **Military**
    c. **Contractor**

   b. **Are you:**
    a. **Male**
    b. **Female**
    c. **Other**

c. How old are you?

a. 18-24
b. 25-34
c. 35-44
d. 45-54
e. 55-64
f. 65+

d. What ethnic origin do you most closely identify with?

a. Hispanic or Latino
b. White or Caucasian
c. Black or African American
d. Native American or American Indian
e. Asian or Pacific Islander
f. Other

e. How long have you been in the Intelligence Community?

a. 1 to 3 years
b. 4 to 5 years
c. 6 to 10 years
d. 11 to 20 years
e. More than 20 years

f. What is your pay category/grade?
Please choose one of the following answers. If you belong to another scale system, i.e., contractor or pay banding, please select the grouping that best reflects your equivalent pay/grade category

a. GS 1-5 or E1 to E4 (MIL)
b. GS 6-9 or E5 to E7 (MIL)
c. GS 10-12 or E8 to O2 (MIL)
d. GS 13-14 or O3-O4 (MIL)
e. GS 15 or O5-O6 (MIL)
f. Senior Executive Service, DISL, or General Officer

g. What is the highest degree or level of education you have completed?

a. High School Diploma/GED or equivalent
b. Associate Degree (e.g., AA, AS)
c. Bachelor's Degree (e.g., BA, BS)
d. Master's Degree (e.g., MA, MS, MBA)
e. Professional Degree (e.g., MD, DDS, JD)
f. Doctorate Degree (e.g., PhD, Ed.D)

h. Indicate the mission category that best fits your position.

a. COLLECTION AND OPERATIONS - **Positions that involve the collection and reporting of information obtained from sources by various means, including human and technical means, as well as occupations involved in intelligence operations.**
b. PROCESSING AND EXPLOITATION - **Occupations or positions that involve the conversion of information collected from various intelligence sources into a form that can be analyzed to produce an intelligence product.**
c. ANALYSIS AND PRODUCTION - **Occupations or positions that involve the preparation of a finished intelligence product from information obtained and processed from one or more intelligence sources in support of customer requirements.**
d. RESEARCH AND TECHNOLOGY - **Occupations or positions that involve basic, applied, and advanced scientific and engineering research and development.**
e. ENTERPRISE INFORMATION TECHNOLOGY - **Positions that support the organization's information systems. This category includes telecommunications, network operations, operation and maintenance of common user systems, and computing infrastructure.**
f. ENTERPRISE MANAGEMENT AND SUPPORT- **Occupations or positions that involve support for the organization's human, financial, physical, and other resources, such as financial management, human resources management, and acquisition.**
g. MISSION MANAGEMENT- **Occupations or positions that involve the coordination and integration of IC-wide intelligence requirements, resources, and activities.**

10. Exit Screen

You have completed the survey!

If you know other members of the IC that might want to help this research, please share the link.

(Please close your browser to exit the survey)

References

Ab Hamid, M. R., Sami, W., & Sidek, M. M. (2017). Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. *Journal of Physics: Conference Series*, *890*(1), 012163.

Adams, D., Nelson, R., & Todd, P. (1992). Perceived usefulness, ease of use, and usage of information technology: A replication. *Management Information Systems Quarterly*, *16*(2). http://aisel.aisnet.org/misq/vol16/iss2/5

Aguirre-Urreta, M., & Rönkkö, M. (2015). Sample size determination and statistical power analysis in PLS using R: An annotated tutorial. *Communications of the Association for Information Systems*, *36*(1), 3.

Ajzen, I., & Fishbein, M. (1973). Attitudinal and normative variables as predictors of specific behavior. *Journal of Personality and Social Psychology*, *27*(1), 41.

Akins, R. B., Tolson, H., & Cole, B. R. (2005). Stability of response characteristics of a Delphi panel: Application of bootstrap data expansion. *BMC Medical Research Methodology*, *5*(1), 37. https://doi.org/10.1186/1471-2288-5-37

Alter, S. (2008). Defining information systems as work systems: Implications for the IS field. *European Journal of Information Systems*, *17*(5), 448–469.

Baram, G., Paikowsky, D., Pavel, T., & Ben-Israel, I. (2017). *Trends in Government Cyber Security Activities in 2016* (SSRN Scholarly Paper ID 3113106). Social Science Research Network. https://papers.ssrn.com/abstract=3113106

Barclay, D., Higgins, C., & Thompson, R. (1995). The partial least squares (PLS) approach to casual modeling: Personal computer adoption and use as an illustration. *Technology Studies*, *2*(2).

Barrett, M. P. (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. National Institute of Standards and Technology. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

Beckett, P. (2015). An intelligent approach to security. *Network Security*, *2015*(2), 18–20. https://doi.org/10.1016/S1353-4858(15)30009-X

Bickers, C. (2000). Playing it safe. *Far Eastern Economic Review*, *163*(23), 56. buh.

Bishop, M. (2005). Position: Insider is relative. *Proceedings of the 2005 Workshop on New Security Paradigms*, 77–78. http://dl.acm.org/citation.cfm?id=1146288

Bishop, M., & Gates, C. (2008). Defining the Insider Threat. *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*, 15:1-15:3. https://doi.org/10.1145/1413140.1413158

Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *NYUL Rev.*, *39*, 962.

Bonett, D. G., & Wright, T. A. (2015). Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning. *Journal of Organizational Behavior*, *36*(1), 3–15. https://doi.org/10.1002/job.1960

Boss, S. R. (2007). *Control, perceived risk, and information security precautions: External and internal motivations for security behavior* [PhD Thesis]. University of Pittsburgh.

Brackney, R. C., & Anderson, R. H. (2004). *Understanding the Insider Threat. Proceedings of a March 2004 Workshop*. DTIC Document.

Brady, S. R. (2015). Utilizing and Adapting the Delphi Method for Use in Qualitative Research: *International Journal of Qualitative Methods*. https://doi.org/10.1177/1609406915621381

Brown, S. A., & Venkatesh, V. (2005). Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle. *MIS Quarterly*, *29*(3).

Brown, T. (2018). Are miserly budgets putting businesses at risk of cyber-attack? *Computer Fraud & Security*, *2018*(8), 9–11. https://doi.org/10.1016/S1361-3723(18)30074-5

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-A7.

Burley, D., Bishop, M., Kaza, S., Gibson, D. S., Buck, S., Parrish, A., & Mattord, H. (2018). Special Session: Joint Task Force on Cybersecurity Education. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 918–919. https://doi.org/10.1145/3159450.3159635

Career Fields | Intelligence Careers. (2020). U.S. Intelligence Careers. https://www.intelligencecareers.gov/iccareers.html

Carmines, E. G., & Zeller, R. A. (1979). *Reliability and validity assessment* (Vol. 17). Sage publications.

Carter, A. (2016). *Procedures governing the conduct of DOD intelligence activities (DOD Manual 5240.01)*. Department of Defense.

Chin, W. W., & Newsted, P. R. (1999). Structural equation modeling analysis with small samples using partial least squares. *Statistical Strategies for Small Sample Research*, *1*(1), 307–341.

Chin, W. W., Thatcher, J. B., & Wright, R. T. (2012). Assessing common method bias: Problems with the ULMC technique. *MIS Quarterly*, 1003–1019.

Ching, K. W., & Singh, M. M. (2016). Wearable technology devices security and privacy vulnerability analysis. *International Journal of Network Security & Its Applications*, *8*(3), 19–30.

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155.

Coles-Kemp, L., & Theoharidou, M. (2010). Insider threat and information security management. In C. W. Probst, J. Hunker, D. Gollmann, & M. Bishop (Eds.), *Insider Threats in Cyber Security* (pp. 45–71). Springer US. http://dx.doi.org/10.1007/978-1-4419-7133-3_3

Colvin, R. G. (2016). Management and organizational influences on the compliance behavior of employees to reduce non-malicious it misuse intention. *ProQuest Dissertations and Theses*.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297–334. https://doi.org/10.1007/BF02310555

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Dalkey, N. C., Brown, B. B., & Cochran, S. W. (1970). *The Delphi Method, IV: Effect of Percentile Feedback and Feed-In of Relevant Facts*. RAND Corporation. https://www.rand.org/pubs/research_memoranda/RM6118.html

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, *43*(6), 1091–1124. https://doi.org/10.1111/j.1540-5915.2012.00383.x

Davis, F. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* [PhD Thesis]. Massachusetts Institute of Technology.

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319–340.

Davis, F., Bagozzi, R., & Warshaw, P. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003.

Department of Defense. (2012). *Joint Ethics Regulations (DOD 5500.7-R)*. Government Printing Office. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/550007r.pdf

Department of Defense. (2013). *DoD Information Security Program: Protection of Classified Information (DOD Manual 5200.01-3* (Vol. 3). Government Printing Office.

Diener, E. D., Emmons, R. A., Larsen, R. J., & Griffin, S. (1985). The satisfaction with life scale. *Journal of Personality Assessment*, *49*(1), 71–75.

Dijkstra, T. K. (2014). PLS' Janus Face – Response to Professor Rigdon's 'Rethinking Partial Least Squares Modeling: In Praise of Simple Methods.' *Long Range Planning*, *47*(3), 146–153. https://doi.org/10.1016/j.lrp.2014.02.004

Dijkstra, T. K., & Henseler, J. (2015). Consistent partial least squares path modeling. *MIS Quarterly*, *39*(2), 297–316.

Dijkstra, T. K., & Schermelleh-Engel, K. (2014). Consistent Partial Least Squares for Nonlinear Structural Equation Models. *Psychometrika*, *79*(4), 585–604. https://doi.org/10.1007/s11336-013-9370-0

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research*, *26*(4), 639–655. https://doi.org/10.1287/isre.2015.0600

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316. https://doi.org/10.1057/ejis.2012.23

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

Eichhorn, B. R. (2014). Common method variance techniques. *Cleveland State University, Department of Operations & Supply Chain Management. Cleveland, OH: SAS Institute Inc*, 1–11.

Executive Orders. (2016, August 15). National Archives. https://www.archives.gov/federal-register/codification/executive-order/12333.html

Fleischer, J., Yarborough, R., & Piper, J. (2018, May 17). *Potential spy devices which track phones found all over DMV*. NBC4 Washington. http://www.nbcwashington.com/investigations/Potential-Spy-Devices-Which-Track-Cellphones-Intercept-Calls-Found-All-Over-DC-Md-Va-482970231.html

Frederick, H. (2014). *Authorized Unofficial Use of Government-provided Information Technology (DISA Instruction 630-225-15)*. Defense Information Systems Agency.

Fredericks, B. (2018, June 1). Feds reportedly find surveillance tech near White House. *New York Post*. https://nypost.com/2018/06/01/feds-reportedly-find-surveillance-tech-around-white-house/

Garba, A. B., Armarego, J., & Murray, D. (2015). A policy-based framework for managing information security and privacy risks in BYOD environments. *International Journal of Emerging Trends & Technology in Computer Science*, *4*(2), 189–198.

Gay, L., & Airasian, P. (2003). Educational research competencies for analysis and applications. *Harvard Business Review*, *76*(6).

Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's comments: An update and extension to SEM guidelines for administrative and social science research. *Mis Quarterly*, iii–xiv.

Geisser, S. (1974). A predictive approach to the random effect model. *Biometrika*, *61*(1), 101–107.

Glassman, J., Prosch, M., & Shao, B. B. M. (2015). To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure. *Information & Management*, *52*(2), 170–182. https://doi.org/10.1016/j.im.2014.08.001

Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, *28*(2), 673–682.

GNU Project. (2020). *GNU PSPP for Windows* (1.4.1-g79ad47) [Computer software]. Free Software Foundation. Available from: https://www.gnu.org/software/pspp/

Gordon, L. A., & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*. https://dl.acm.org/doi/abs/10.1145/581271.581274

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. *IEEE Security & Privacy*, *6*(1). http://ieeexplore.ieee.org/abstract/document/4446699/

Gundu, T., & Flowerday, S. V. (2012). The enemy within: A behavioural intention model and an information security awareness process. *2012 Information Security for South Africa*, 1–8. https://doi.org/10.1109/ISSA.2012.6320437

Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2010). *Multivariate data analysis* (Vol. 7). Pearson. http://library.wur.nl/WebQuery/clc/1924429

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications. https://books.google.com/books?hl=en&lr=&id=Xn-LCwAAQBAJ&oi=fnd&pg=PA9&dq=A+primer+on+partial+least+squares+structural+equation+modeling+(PLS-SEM)&ots=sl94sXmGSL&sig=WPHPJbDwuDq4YUXCMVJbnE-IhtY

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*.

Harborth, D., & Pape, S. (2019). *How privacy concerns and trust and risk beliefs influence users' intentions to use privacy-enhancing technologies-the case of tor*.

Hartzog, W., & Stutzman, F. (2013). The Case for Online Obscurity. *California Law Review*, *101*(1), 1–49. https://doi.org/10.2307/23409387

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems; Basingstoke*, *18*(2), 106–125. http://dx.doi.org.ezproxylocal.library.nova.edu/10.1057/ejis.2009.6

Herodotus, & Grene, D. (1987). *The history*. University of Chicago Press.

Herrero, Á., San Martín, H., & Salmones, M. del M. (2017). Explaining the adoption of social networks sites for sharing user-generated content: A revision of the UTAUT2. *Computers in Human Behavior*, *71*, 209–217. https://doi.org/10.1016/j.chb.2017.02.007

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

Hong, W., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2011). User Acceptance of Agile Information Systems: A Model and Empirical Test. *Journal of Management Information Systems*, *28*(1), 235–272. https://doi.org/10.2753/MIS0742-1222280108

Hovav, A., & Putri, F. F. (2016). This is my device! Why should i follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing*, *32*, 35–49.

IC EEO. (2019). *Annual demographic report: Fiscal Year 2018*. Office of the Director of National Intelligence (ODNI).

Jacobellis v. Ohio 378 U.S. 184, (1964). https://supreme.justia.com/cases/federal/us/378/184/case.html

Karwatzki, S., Trenz, M., & Veit, D. (2018). *Yes, firms have my data but what does it matter? Measuring privacy risks*.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/isj.12062

Khan, G. F., Sarstedt, M., Shiau, W.-L., Hair, J. F., Ringle, C. M., & Fritze, M. P. (2019). Methodological research on partial least squares structural equation modeling (PLS-SEM). *Internet Research*.

Lai, I. K. W., & Shi, G. (2015). The impact of privacy concerns on the intention for continued use of an integrated mobile instant messaging and social network platform. *International Journal of Mobile Communications*, *13*(6), 641. https://doi.org/10.1504/IJMC.2015.072086

Lee, M.-C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, *8*(3), 130–141. https://doi.org/10.1016/j.elerap.2008.11.006

Lee, Y., Kozar, K., & Larsen, K. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems*, *12*, 752–780.

Lidynia, C., Brauner, P., & Ziefle, M. (2017). A step in the right direction – understanding privacy concerns and perceived sensitivity of fitness trackers. *Advances in Human Factors in Wearable Technologies and Game Design*, 42–53. https://doi.org/10.1007/978-3-319-60639-2_5

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293–334.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32–44.

Microsoft Excel (Version 2101). (2020). [Computer software]. Microsoft Corporation. Available from https://office.microsoft.com/excel

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

Mowbray, C. T., Holter, M. C., Teague, G. B., & Bybee, D. (2003). Fidelity Criteria: Development, Measurement, and Validation. *American Journal of Evaluation*, *24*(3), 315–340. https://doi.org/10.1177/109821400302400303

National Counterintelligence and Security Center. (2017). *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*. Office of the Director of National Security. https://www.dni.gov/files/NCSC/documents/Regulations/Technical-Specifications-SCIF-Construction.pdf

Oksenberg, L., & Kalton, G. (1991). New strategies for pretesting survey questions. *Journal of Official Statistics*, *7*(3), 349.

Peters, G.-J. (2018). The alpha and the omega of scale reliability and validity: Why and how to abandon Cronbach's alpha and the route towards more comprehensive assessment of scale quality. *PsyArXiv*. https://doi.org/10.31234/osf.io/h47fv

Pfleeger, S. L., & Stolfo, S. J. (2009). Addressing the insider threat. *IEEE Security & Privacy Magazine*, *7*(6), 10–13. https://doi.org/10.1109/MSP.2009.146

Plonsky, L., & Gass, S. (2011). Quantitative research methods, study quality, and outcomes: The case of interaction research. *Language Learning*, *61*(2), 325–366.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management*, *12*(4), 531–544. https://doi.org/10.1177/014920638601200408

Powell, C. (2003). The Delphi technique: Myths and realities. *Journal of Advanced Nursing*, *41*(4), 376–382. https://doi.org/10.1046/j.1365-2648.2003.02537.x

Rempfer, K. (2020, January 7). *No cellphones, laptops were allowed to go with Army 82nd paratroopers deploying to Middle East*. Army Times. https://www.armytimes.com/news/your-army/2020/01/06/no-cell-phones-laptops-were-allowed-to-go-with-82nd-paratroopers-deploying-to-middle-east/

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organizational Research Methods*, *12*(4), 762–800.

Richelson, J. T. (2018). *The U.S. Intelligence Community*. Routledge. https://www.taylorfrancis.com/books/9780429494321

Ringle, C., Wende, S., & Becker, J.-M. (2015). *SmartPLS 3* (Version 3) [Computer software]. http://www.smartpls.com

Salkind, N. J. (2011). Internal and External Validity. In *The SAGE Dictionary of Quantitative Management Research* (pp. 148–149). SAGE Publications Ltd. https://doi.org/10.4135/9781446251119

Sarstedt, M., Hair Jr, J. F., Cheah, J.-H., Becker, J.-M., & Ringle, C. M. (2019). How to specify, estimate, and validate higher-order constructs in PLS-SEM. *Australasian Marketing Journal (AMJ)*, *27*(3), 197–211.

Sawyer, R. D., & Sawyer, M. (1994). *The art of war*. Westview Press.

Schulman, A. (2001). The extent of systematic monitoring of employee e-mail and Internet use. *The Privacy Project, July*, *9*.

Security at Typeform. (2020, July 20). Help Center. http://help.typeform.com/hc/en-us/articles/360029259552

Sisk, R. (2018, January 29). *Pentagon reviewing fitness trackers that could expose troop locations*. Military.Com. https://www.military.com/daily-news/2018/01/29/pentagon-reviewing-fitness-trackers-could-expose-troop-locations.html

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education: Research*, *6*(1), 1–21.

Sly, L. (2018, January 29). U.S. soldiers are revealing sensitive and dangerous information by jogging. *Washington Post*.

https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html

Solove, D. J. (2008). *Understanding Privacy* (SSRN Scholarly Paper ID 1127888). Social Science Research Network. https://papers.ssrn.com/abstract=1127888

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society: Series B (Methodological)*, *36*(2), 111–133.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 147–169.

Symantec. (2016). *Internet Security Threat Report 2016*. https://www.symantec.com/security-center/threat-report

Tehseen, S., Ramayah, T., & Sajilan, S. (2017). Testing and controlling for common method variance: A review of available methods. *Journal of Management Sciences*, *4*(2), 142–168.

Timberg, C. (2018, June 1). Signs of sophisticated cellphone spying found near White House, U.S. officials say. *Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2018/06/01/signs-of-sophisticated-cell-phone-spying-found-near-white-house-say-u-s-officials/

United States Cyber Command. (2020). *Effective use of remote work options* (NAVADMIN 068/20). United States Government.

US Office of Personnel Management. (2009). *Introduction to the position classification standards*. OPM.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273–315.

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

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

Venkatesh, V., Thong, J. Y. L., Chan, F. K. Y., Hu, P. J.-H., & Brown, S. A. (2011). Extending the two-stage information systems continuance model: Incorporating UTAUT predictors and the role of context. *Information Systems Journal*, *21*(6), 527–555. https://doi.org/10.1111/j.1365-2575.2011.00373.x

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157–178.

Verplanken, B., & Orbell, S. (2003). Reflections on past behavior: A self-report index of habit strength. *Journal of Applied Social Psychology*, *33*(6), 1313–1330. https://doi.org/10.1111/j.1559-1816.2003.tb01951.x

Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, *57*, 101173. https://doi.org/10.1016/j.pacfin.2019.101173

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 193–220.

Westin, A. F. (1967). *Privacy and freedom* (Vol. 7). Atheneum.

Whittaker, Z. (2018, July 8). *Fitness app Polar exposed locations of spies and military personnel*. ZDNet. https://www.zdnet.com/article/fitness-app-polar-exposed-locations-of-spies-and-military-personnel/

Williams, H., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise* (No. RR1964; pp. 1–62). RAND Corporation. https://www.rand.org/pubs/research_reports/RR1964.html

Williams, M., Rana, N. P., & Dwivedi, Y. K. (2015). The unified theory of acceptance and use of technology (UTAUT): A literature review. *Journal of Enterprise Information Management*, *28*(3), 443–488.

Willison, R., & Lowry, P. B. (2018). Disentangling the motivations for organizational insider computer abuse through the rational choice and life course perspectives. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *49*(1), 81–102. https://doi.org/10.1145/3210530.3210537