2021

Development of a Social Engineering eXposure Index (SEXI) using Open-Source Personal Information

William Shawn Wilkerson
Nova Southeastern University, drwshawn@shawnwilkerson.com

Development of a Social Engineering eXposure Index (SEXI) using Open-Source Personal Information

by

W. Shawn Wilkerson

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

College of Computing and Engineering
Nova Southeastern University

2021

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

Yair Levy, Ph.D. — **10/5/21**
Chairperson of Dissertation Committee — **Date**

James R. Kiper, Ph.D. — **10/5/21**
Dissertation Committee Member — **Date**

Martha M. Snyder, Ph.D. — **10/5/21**
Dissertation Committee Member — **Date**

Approved:

Meline Kevorkian, Ed.D. — **10/5/21**
Dean, College of Computing and Engineering — **Date**

College of Computing and Engineering
Nova Southeastern University

2021

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

Development of a Social Engineering eXposure Index (SEXI) using Open-Source Personal Information

By
William Shawn Wilkerson
October 2021

Millions of people willingly expose their lives via Internet technologies every day, and even the very few ones who refrain from the use of the Internet find themselves exposed through data breaches. Billions of private information records are exposed through the Internet. Marketers gather personal preferences to influence shopping behavior. Providers gather personal information to deliver enhanced services, and underground hacker networks contain repositories of immense data sets. Few users of Internet technologies have considered where their information is going or who has access to it. Even fewer are aware of how decisions made in their own lives expose significant pieces of information, which can be used by cyber hackers to harm the very organizations with whom they are affiliated. While this threat can affect any person holding any position at an organization, upper management poses a significantly higher risk due to their level of access to critical data and finances targeted by cybercrime.

The goal of this research was to develop and validate a Social Engineering eXposure Index (SEXI)™ using Open-Source Personal Information (OSPI) to assist in identifying and classifying social engineering vulnerabilities. This study combined an expert panel using the Delphi method, developmental research, and quantitative data collection. The expert panel categorized and assessed information privacy components into three identifiability groups, subsequently used to develop an algorithm that formed the basis for a SEXI. Validation of the algorithm used open-source personal information found on the Internet for 50 executives of Fortune 500 organizations and 50 Hollywood celebrities. The exposure of each executive and persona was quantified and the collected data were evaluated, analyzed, and presented in an anonymous aggregated form.

Phase 1 of this study developed and evaluated the SEXI benchmarking instrument via an expert panel using the Delphi expert methodology. During the first round, 3,531 data points were collected with 1,530 having to do with the demographics, qualifications, experience, and working environments of the panel members as well as 2,001 attributing levels of exposure to personal information. The second Delphi round presented the panel members with the feedback of the first-round tasking them with categorizing personal information, resulting in 1,816 data points. Phase 2 of this study used the composition, weights, and categories of personal information from Phase 1 in the development of a preliminary SEXI benchmarking instrument comprised of 105 personal information items. Simulated data was used to validate the instrument prior to the data collection.

Before initiating Phase 3, the preliminary SEXI benchmarking instrument was fully tested to verify the accuracy of recorded data. Phase 3 began with discovering, evaluating, and validating repositories of publicly available data sources of personal information. Approximately two dozen sources were used to collect 11,800 data points with the SEXI benchmarking index. Upon completion of Phase 3, data analysis of the Fortune 500 executives and Hollywood personas used to validate the SEXI benchmarking index.

Data analysis was conducted in Phase 3 by one-way Analysis of Variance (ANOVA). The results of the ANOVA data analysis from Phase 3 revealed that age, gender, marital status, and military/police experience were not significant in showing SEXI differences. Additionally, income, estimated worth, industry, organization position, philanthropic contributions are significant, showing differences in SEXI. The most significant differences in SEXI in this research study were found with writers and chief information officers. A *t*-test was performed to compare the Fortune 500 executives and the Hollywood personas. The results of the *t*-test data analysis showed a significant difference between the two groups in that Hollywood Personas had a higher SEXI than the Fortune 500 Executives suggesting increased exposure due to OSPI.

The results of this research study established, categorized, and validated a quantifiable measurement of personal information. Moreover, the results of this research study validated that the SEXI benchmarking index could be used to assess an individual's exposure to social engineering due to publicly available personal information. As organizations and public figures rely on Internet technologies understanding the level of personal information exposure is critical is protecting against social engineering attacks. Furthermore, assessing personal information exposure could provide an organization insight into exposed personal information facilitating further mitigation of threats or potential social engineering attack vectors. Discussions and implications for future research are provided.

William Shawn Wilkerson

Acknowledgments

This work is dedicated to my wife, soulmate, best friend, Princess, and fellow explorer: Victoria. I love you and thank you for the immense amount of support, occasional redirection, and oft glimpses into your wonderful self. To Jesus Christ, who has always been the voice that guides from one adventure to the next, the hope the future can be obtained, and the dream that keeps me ever pressing on - building and planting.

For every monumental task in one's life many people took part. In my life there have been several. From my 1st and 2nd grade teacher, Mrs. Gallion, who put up with the kid who was a little too smart for his own good, to 6th grade Mr. Broxton who taught me that there was no box. Jack McCabe, my high school Calculus teacher, instilled in me that learning is fun when combined with curiosity and effort. In basic training, Sargent First Class I. Fields demonstrated to me the single best example of leadership I have seen. My fellow student and friend, Dr. Helen Hernandez, and her husband Joe, for the 5-hour carpools, conversation, and lasting friendships. Bishop Ray Willis, you believed in my wife and myself. You loved us. You accepted us. You gave us a home. There were hundreds, if not thousands, of others. I thank each of you named, unnamed, known, and unknown.

My appreciation and gratitude to my adviser, Dr. Levy, who saw a glimmer of potential in my research topic and who nudged me into crafting this work. I would also like to acknowledge the committee members, who each brought very needed skill sets to this effort. Dr. Martha Snyder for having a desire to see the message flow clearly. Dr. James Richard Kiper for expecting a logical and precise presentation. Each respectively catered to the writer and analyst in me. I thank all three of you for the *many* hours of reading, reviewing, and providing feedback.

I must thank my mother, dad, and kids. They have listened to me talk about this project for years. Mom, Monica, you allowed me to work at an early age and purchase that first 1.79 MHz TI-99/4A. You also taught me the fulfillment that comes from exploration. Thank you. Dad, William, you taught me to tinker and be inquisitive. You both also allowed me to make my own mistakes and learn from them. Thank you. Between my wife and I we have 5 children: Christina, Heather, Christopher, Joshua Caleb, Kymberli. We were not perfect, but each of you have everything you need to succeed. You can and will. I also thank my brother, Michael, who has had to put up with my schedule. I thank each of you.

I feel it mandatory to acknowledge the efforts of the Delphi panel members who subjected themselves to two very long surveys. Thank you. I also wish to thank those who will read and build upon this work and continue to further the body of knowledge.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Cybersecurity issues are as ubiquitous as the Internet itself and can be observed in social engineering victims ranging from a child targeted by pedophiles to the Director of the U.S. Central Intelligence Agency (CIA) (Federal Bureau of Investigation, 2015b; Franceschi-Bicchierai, 2015). Cyber attackers can be anyone from teenagers to foreign government actors (Federal Bureau of Investigation, 2016; Kopan, 2015). Objectives are as diverse as embarrassment to murder, but usually takes the form of fraud with the loss for United States (U.S.) organizations averaging over $100,000 per incident in 2013 (Federal Bureau of Investigation, 2015a; Mouton et al., 2016).

Open-source is defined herein as "publicly available print and digital/electronic data from unclassified, non-secret, and 'grey literature' sources," not requiring credentials or special access, including data available through breaches, leaks, etc. (Fleisher, 2008, p. 853). Marketing (Culnan & Bies, 2003; Moon, 2000), personalization (Chellappa & Sin, 2005; Culnan, 1993; Kim & Pan, 2006), e-commerce (Dinev & Hart, 2006; Feijóo et al., 2014), self-surveillance (Kang et al., 2011), surveys, contests, order forms, registrations (Federal Trade Commission, 2000), and social media (Acquisti et al., 2015; Karaduman, 2013; Peer & Acquisti, 2016) are just a few ubiquitous open-source repositories. Additionally, grey literature is typically comprised of less-than-formal publications such as Websites and unpublished papers (Fleisher, 2008).

The exponential growth of personal information available online via open-source technologies has exposed unsuspecting users for social engineers to attack relentlessly (Acquisti et al., 2015; Mitnick & Simon, 2002). The Open-Source Personal Information (OSPI) provided by social media and other platforms facilitate many successful SE attacks on potential victims (Krishnamurthy & Wills, 2009; Maynard et al., 2015). E-mail is another tool used to gain OSPI by disguising its origin and purpose, usually to appear as a trusted entity known by the intended victim (Almomani et al., 2013; Federal Bureau of Investigation, 2015a; Mouton et al., 2016). The increased availability of OSPI furnishes social engineers with a larger number of victims, with no end in sight (Acquisti et al., 2015; Mitnick & Simon, 2002).

Problem Statement

The research problem that this study addressed was the proliferation of Social Engineering (SE) attacks due to publicly available OSPI (Heartfield & Loukas, 2015; Maynard et al., 2015; Mitnick & Simon, 2002). SE "is a combination of techniques used to manipulate victims into divulging confidential information or performing actions that compromise security" (Luo et al., 2013, p. 2; Mitnick & Simon, 2002). Social engineers use deception and often use roleplaying to represent someone to whom their intended targets are more susceptible (Orgill et al., 2004). Additionally, the use of pretense and persuasion is often noted in successful SE attacks (Heartfield & Loukas, 2015; Mitnick & Simon, 2002). This behavior is consistent with the Theory of Mind (TOM) where an actor attempts to persuade another individual through pretense and deception, while remaining within the confines of the representation held by the other individual. TOM is defined as

"the individual imputes mental states to himself and to others" (Premack & Woodruff, 1978, p. 515). A help desk may hold a representation of aiding those who request it. Several employees may hold a representation that an auditor is part of the Information Technology (IT) department, if they are observing someone dressed in a manner acceptable for the role and who is appearing to perform functions that represent the expected activity (Krombholz et al., 2013; Orgill et al., 2004). Social engineers are able to pretend and persuade even experts into behaving favorably for the attacker, even when they suspect something is wrong and are mandated as well as trained to take appropriate defensive action (Allen, 2006; Heartfield & Loukas, 2015).

Prior research has shown the information being used to execute SE attacks typically originates at the target or those closely associated with them (Heartfield & Loukas, 2015; Junger et al., 2017; Luo et al., 2013). Studies have also shown a significant increase of personal information exposed on social networking sites and the overall willingness to provide personal content by Americans (Acquisti et al., 2015; Boyd & Ellison, 2007; Hong & Thong, 2013). Olmstead and Smith (2017) stated that 64% of Americans had been exposed via a data breach.

According to Solove (2006), "Exposure involves the exposing to others of certain physical and emotional attributes about a person" (p. 533). Some studies suggested that people willingly expose private information in exchange for content gratification, even after adjusting their settings for what they perceived as increased privacy (Sutanto et al., 2013). Ku et al. (2013) found that a positive association exists between the gratification of using social networking sites and the intention for continued usage. The availability of OSPI has grown substantially over recent years and looks to have exponential growth as

more people gain access to the Web and service providers continually introduce innovative, and arguably predatory, mechanisms for self-disclosure (Acquisti et al., 2015).

When Facebook, a social network site, first went public, it targeted the needs of business users to facilitate professional relationships and was later expanded to provide any user the ability to share far more personal information (Acquisti et al., 2015). Initially, the majority of information posted by Facebook users was related to business efforts providing very few self-identifying descriptive items, while also restricting the scope of people having access to the shared information (Acquisti et al., 2015; Pew Research Center, 2019). By 2014, the basic and extended profiles of a user's Personally Identifiable Information (PII) were potentially shareable to anyone on the Internet with access to the original Facebook postings (Acquisti et al., 2015). Examples of PII may include name, email, postal address, phone or fax number (Federal Trade Commission, 2000). This availability of OSPI allows potential hackers to glean necessary information to successfully social engineer an exposed target via a myriad of attack vectors (Heartfield & Loukas, 2015; Luo et al., 2013). Acquisti et al. (2015) found that the number of Facebook categories of exposure increased from three (networks, genders, & names) to eight (networks, genders, names, friends, basic profile, extended profile, likes, & pictures) between 2005 and 2014 beginning with text and progressively expanding to including live video content. Twitter microdata is another source of OSPI allowing indirect access to a user's identity (Singh et al., 2014).

The literature typically describes PII as including any content that has the potential to identify an individual (McCallister et al., 2010). Schwartz and Solove (2011) suggested

another category of information, named herein as Personally Distinguishable Information (PDI). They argue that PDI will definitively identify someone, whereas most PII only has the potential of identifying a specific individual (Schwartz & Solove, 2011). Additionally, a third category of PII is suggested, named herein as Personally Unidentifiable Information (PUI), which has no chance to identify an individual on its own (McCallister et al., 2010; Schwartz & Solove, 2011). OSPI provides access to PDI, PII, and PUI making up the three primary categories of personal information, with PDI having the highest level of exposure, PII exhibiting the potential of exposure, and PUI offering no exposure by itself, however, combined with the prior two categories can add to the overall exposure of an individual (McCallister et al., 2010; Schwartz & Solove, 2011). PDI is any information which specifically distinguishes the individual on its own, slightly differing from PII in that the potential of exposure is absolute (Chellappa & Sin, 2005; Schwartz & Solove, 2011). PDI may include a digital photograph, video, social security number, Global Positioning System (GPS), passport number, credit card number, security clearance, bank account number, biometric data, date with the place of birth, mother's maiden name, criminal background, medical record, financial record, and educational transcript (42 U.S.C. § 200.82). PUI is any information which cannot solely be used to identify an individual (Chellappa & Sin, 2005; Schwartz & Solove, 2011). PUI may include age, date of birth, gender, education, hobby, income, interest, the name of the software used, occupation, type of hardware in configuration, and Zip Code (Chellappa & Sin, 2005; Federal Trade Commission, 2000).

The threat to organizations with leaders having their PDI, PII, and PUI available via OSPI is easily translated into risk assessments. According to the U.S. Federal Bureau of

Investigation (FBI) (2015a), Business Email Compromise (BEC) affected over 7000 organizations within the U.S. approached $800 million in losses between October 2013 and August 2015. A substantial increase of over 270% in the number of BEC cases occurred during the opening months of 2015 indicating SE attacks are dramatically on the rise (Federal Bureau of Investigation, 2015a).

Phishing is another attack vector of SE, whereby the target is baited with a fake copy of a Web page or Website to solicit sensitive information or to inject malware onto the victim's computer or mobile devices. OSPI provides attackers the information to craft specific bait to spear-phish a group or induvial, whereas whaling attacks attempt to specifically target the most valuable among them (Heartfield & Loukas, 2015). Neupane et al. (2015) conducted phishing research and found that the longer an individual looked at the content on a fake Web page, during each 10-second trial, the more likely they would accept it as being authentic. They also discovered the possibility of a successful phishing event significantly increased if the participant was distracted or sleep-deprived (Neupane et al., 2015). The growing availability of OSPI is providing the content used for successful SE attacks, and in the creation of effective spear-phishing campaigns (Heartfield & Loukas, 2015; Neupane et al., 2015).

In 1994, a French social engineer called the FBI in Washington, D.C. and successfully persuaded someone to expose the information required to make phone calls at the agency's expense (Allen, 2006; Schneier, 2000). In another example, the FBI described how the practices of a company facilitated a $737,000 transfer to an unauthorized recipient in China (Federal Bureau of Investigation, 2015a). In 2016, state-sponsored Iranians performed Distributed Denial of Service (DDoS) attacks on U.S. financial

institutions blocking hundreds of thousands of customers from accessing their bank accounts using IP Address information registered at the domain names (Federal Bureau of Investigation, 2016). In 2018, nine Iranians were indicted for the theft of over "31 terabytes of documents and data from more than 140 American universities, 30 American companies, five American government agencies", as well as "compromised approximately 8,000 professor email accounts across 144 U.S.-based universities" (U.S. Department of Justice, 2018, pp. 1,2). Acquisti and Gross (2009) described the simplicity of predicting Social Security Numbers and the dangers of mass identity theft due to weaknesses in the U.S. identifier system.

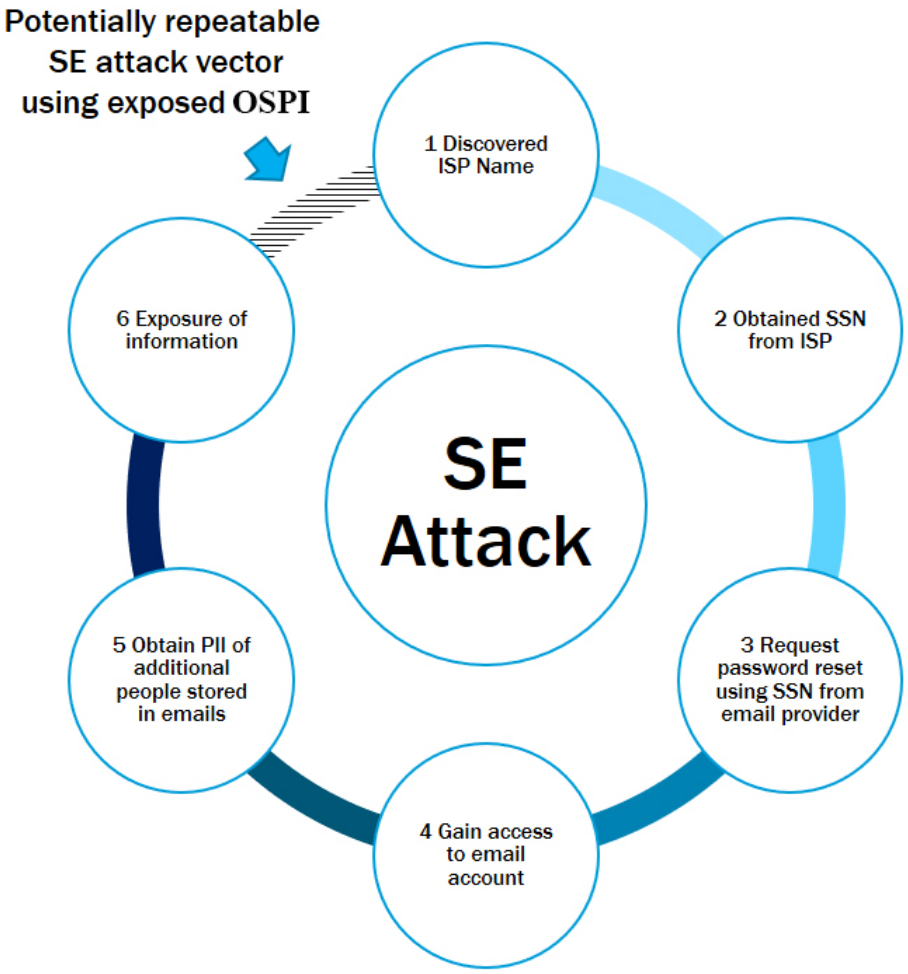
To illustrate the effectiveness of SE against organizations, Orgill et al. (2004) described an unannounced security audit where 19 out of 32 people gave their password to an unknown person walking through the facility with a name badge retrieved from a desk where an employee left it. While seven people supplied the username and password for another person's account with access elevated beyond their own, only four of the 32 employees asked for the auditor's identification (Orgill et al., 2004). Two days later the auditor returned and was able to find multiple company credit cards and a master key to the building within 30 seconds of beginning a general search near an executive's office (Orgill et al., 2004). Orgill et al. (2004) found that even organizations with a high awareness of data security and requirements to follow privacy standards are vulnerable to SE due to exposure.

The October 2015 BEC attack on the Director of the CIA provides an example where OSPI was used to gain access to a private email account. Teenagers were able to gather data from OSPI located across multiple online accounts belonging to the CIA Director,

and use the information to pretext, another SE attack vector, customer service representatives via telephonic communication into exposing additional personal details (Franceschi-Bicchierai, 2015). Figure 1 represents the SE attack used on the CIA Director that may have been repeatable as the perpetrators had possession of the personal information of agents, contractors, and government personnel stored within the compromised e-mail account. The collected information could also be used in any number of other SE attacks as well.

Figure 1

SE attack used against the CIA Director in 2015



Using the combined data, the attackers obtained the necessary information to access the personal email account of the CIA Director. Subsequently, the attackers released the PII of many of the CIA Director's associates and subordinates to WikiLeaks (Franceschi-Bicchierai, 2015; Kopan, 2015). The availability of OSPI allowed the successful targeting of the CIA Director by a group of high school students having no formal information security training (Franceschi-Bicchierai, 2015).

Heartfield and Loukas (2015) found that familiarity with content, such as a logo, provides a substantial increase in employees mistaking a SE attack for an official request. Additionally, Acquisti et al. (2015) found that OSPI is readily accessible and increasingly available. According to the FBI, BEC attacks and the financial loss associated with them have significantly increased (Federal Bureau of Investigation, 2015a). The growth of BEC, SE, and OSPI indicate the current cybersecurity defense methodologies may not be sufficient to protect individuals or organizations from SE attacks (Tetri & Vuorinen, 2013). Thus, it appears additional research is warranted to assess and classify social engineering exposure of individuals, especially top executives of large organizations and key strategic personnel.

Dissertation Goal

The goal of this research was to develop and validate a Social Engineering eXposure Index (SEXI) using Open-source Personal Information (OSPI) to assist in identifying and classifying SE vulnerabilities. The index was validated on 50 executives of Fortune 500 companies and 50 Hollywood personas. SEXI provided a rating of the exposure to SE due to OSPI. The need for this research was demonstrated by the work of Mitnick and Simon (2002), Tetri and Vuorinen (2013), Heartfield and Loukas (2015), as well as

Mouton et al. (2016) that acknowledged the progressive expansion of SE attack vectors, the lack of a predictive threat system, the availability of OSPI which circumvent organizational cybersecurity technologies, and the dearth of data on information gathering techniques for the successful execution of prior SE attacks.

Mouton et al. (2016) described the difficulty in performing SE research due to the lack of information provided in news articles, especially the method of attack and where the information was gathered to prosecute the intended target. Despite proposed SE attack templates, the effect of OSPI on target exposure is not a well-understood phenomenon, making it a viable and challenging research problem (Mouton et al., 2016). Mouton et al. (2016) reinforced the sentiment found by Mitnick and Simon (2002) that the human component is the weakest link for organizational security, as it serves both as a bypass to security technologies and as the fountain of information by which SE attacks occur. Additionally, Mouton et al. (2016) suggested that SE research is still in its infancy despite the rapid growth of information security research.

Heartfield and Loukas (2015) described the ineffectiveness of studying "semantic attacks" as it occurs after the damage is done and may be limited by a lens focused on a singular attack vector (p. 31). Of significance, for this dissertation study, is the call for a prediction mechanism by Heartfield and Loukas (2015) for determining exposure in real time that is automatically updated with a rapid response window. The availability of OSPI used for SE attacks can also serve to determine SE exposure (Heartfield & Loukas, 2015; Tetri & Vuorinen, 2013). Armed with a SE prediction mechanism, executives can take an offensive stance in organizational security risk mitigation and likewise monitor

the overall exposure of the organization in real-time by evaluating the availability of OSPI of key personnel – including themselves (Mouton et al., 2016).

This study built on previous research by Bélanger and Crossler (2011), Tetri and Vuorinen (2013), Acquisti et al. (2015), as well as Heartfield and Loukas (2015). Bélanger and Crossler (2011) called for "the development of more (and easier to use) privacy protection tools for individuals, groups, organizations, and society" (p. 1035). Acquisti et al. (2015) described the exponential increase of OSPI via social networking sites while Tetri and Vuorinen (2013) found that its availability enabled as well as facilitated SE attackers across a broad spectrum of attack vectors. Current research and defense mechanisms tend to focus on a single attack vector or technique, thereby drastically limiting their actual benefit or significance to the security strategy (Tetri & Vuorinen, 2013). Specifically, Tetri and Vuorinen (2013) suggested that research might include an evaluation of where the information was obtained by attackers as well as how the SE attack vectors were possible in the first place (p. 1020). Heartfield and Loukas (2015) called for the development of a formal framework that could profile the exposure of users to SE attacks. Schwartz and Solove (2011) argued that privacy must move beyond an ineffective legal system split between standard and rule towards an understanding of "identification in terms of risk level (p. 1979)" and realize "a standards-based approach can be made operational and predictable" (p. 1884). Ohm (2010) views the entire PII concept as broken and believes almost any information can be traced as well as used to identify an individual. This study developed and validated, using Subject Matter Experts (SMEs), an instrument tool to aid organizations in SE mitigation and an

index of exposure to SE due to the availability of OSPI for 100 individuals and corporate executives.

While there have been many discussions in the literature concerning personal information, there is very little in the quantification and grouping of the components. The first specific goal of this research study was to gather the SME-approved components for an index of SE exposure by eliciting quantitative feedback on personal information. The second specific goal of this research study was to assign categories to personal information components based on exposure. The third specific goal of this research study was to develop and validate, using SMEs, the components and hierarchical weights for SEXI via a Delphi method. The fourth specific goal of this research study was to apply the SEXI method to measure the OSPI exposure of 50 executives of Fortune 500 organizations and 50 Hollywood celebrities. The fifth specific goal of this research study was to assess and statistically test for significant mean differences of the SEXI of 100 individuals based on demographical indicators of age, gender, income, marital status, estimated worth, industry, organizational position, philanthropic contributions, and prior military/police experience. The sixth specific goal of this research study was to compare the SEXI results from the set of US executives to those of Hollywood personas in an effort to uncover which group is more vulnerable to SE attack from an OSPI exposure perspective.

Research Questions

The main Research Question (RQ) that this study addressed was: What are the expert-approved required components comprising an index of exposure to SE attacks due to OSPI? The specific research questions that this study addressed were:

RQ1: What are the specific SME-panel approved set of personal information components for an index of SE exposure?

RQ2: What are the specific SME-panel approved categories for the identified set of personal information components?

RQ3: What are the specific SME-panel identified weights of the personal information components and categories that enable a validated hierarchical aggregation to the Social Engineering eXposure Index (SEXI) benchmarking index?

RQ4: How are 100 individuals assessed and classified by SEXI using OSPI?

RQ5: Are there any statistically significant mean differences of SEXI based on demographical indicators of age, gender, income, marital status, estimated worth, industry, organizational position, philanthropic contributions, and prior military/police experience?

RQ6: Do SEXI results from the set of US executives and Hollywood personas indicate one group being more vulnerable to SE attack from their OSPI exposure perspective?

SE attacks are on the rise, and the OSPI used to perpetrate these crimes is far too readily available (Acquisti et al., 2015; Federal Bureau of Investigation, 2015a). Tetri and Vuorinen (2013) conducted a literature review of 40 journal articles and found them primarily explorative and descriptive with very few SE studies being empirical, thereby validating a knowledge gap in the literature.

The merit of developing an exposure index is that it can assist in the prediction of the SE exposure of targets, the content of potential attacks, and possible attack vectors which

current security structures may fail to detect or provide (Heartfield & Loukas, 2015; Mouton et al., 2016). Prior research indicated that people readily expose themselves online (Acquisti et al., 2015; Pew Research Center, 2019; Smith, 2015) and that organizations can end up paying for their executives' OSPI exposure in a myriad of ways (Federal Bureau of Investigation, 2015a; Mouton et al., 2016).

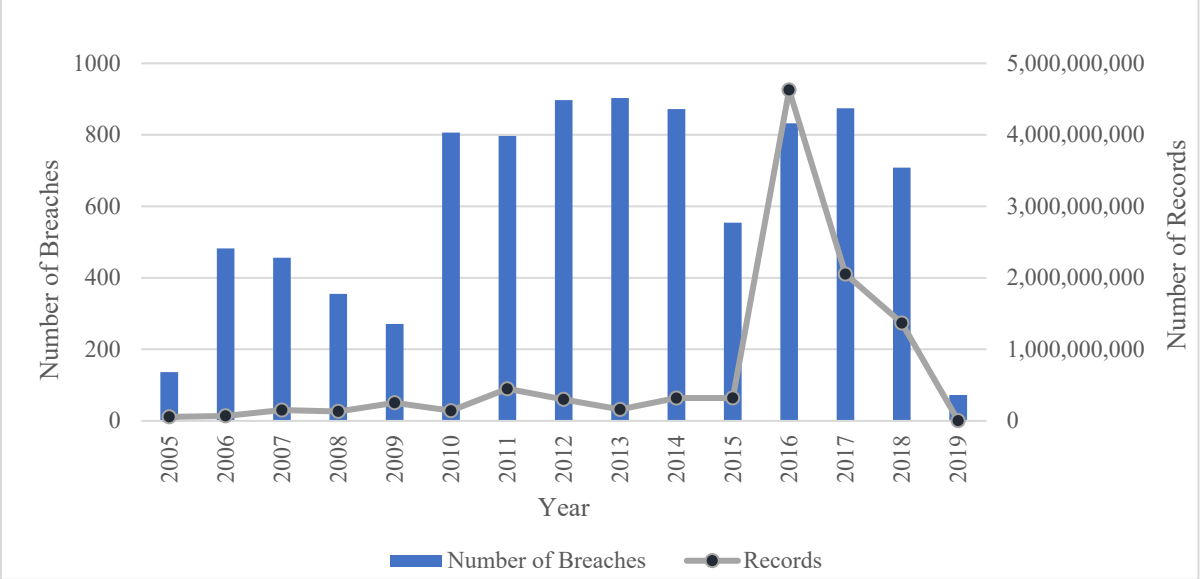
Relevance and Significance

Relevance

The privacy chain, defined as the flow of PII communication between two endpoints (Wilkerson et al., 2017), appears to have no lack of supply (Mitnick & Simon, 2002; Tetri & Vuorinen, 2013) or demand (Federal Bureau of Investigation, 2012; Jasper, 2017). People continue to freely share PII even though they are aware of the consequences of doing so (Acquisti et al., 2015; Olmstead & Smith, 2017). Figure 2 provides the number of breaches and the number of records from 2005-2017.

Figure 2

Reported data breaches from 2005-2019



The literature provides troubling insight into the primary creator of PII, the subjects themselves. People continue self-disclosure even though 64% of Americans have experienced data breaches (Olmstead & Smith, 2017). Since 2015, the number of Facebook users has increased by 7%, bringing the total to 79% of Internet users using the service – 68% of American adults (Greenwood et al., 2016).

Note: Adapted from "Data Breaches," by the Privacy Rights Clearing House, 2021. Used with the permission of the Privacy Rights Clearinghouse, under a Creative Commons Attribution NonCommercial-ShareAlike 4.0 (CC BY-NC-SA 4.0).

The alarming rate of PII released and subsequently available via OSPI is a continual threat to organizations (Mouton et al., 2016). Case in point, the successful attack on the Director of the CIA demonstrates how OSPI provided attackers access to a private email account of a key figure, which contained and provided PII of many CIA agents (Franceschi-Bicchierai, 2015; Kopan, 2015). It should be noted that no correlation exists as to the number of data breaches and the number of records. A single data breach can exceed billions of records (Green, 2017), while others may contain no records at all (Privacy Rights Clearinghouse, 2018).

The literature indicated that SE success often depends on the availability of PII (Junger et al., 2017). Combined with the exponential growth of PII available via open-source technologies, an onslaught of effective SE attacks continues to plague organizations with a snowballing relentlessness (Acquisti et al., 2015; Bélanger & Crossler, 2011). In response, prior literature has assuaged the demand for security policies, training, and awareness efforts, but has shown limited effectiveness in curbing the crushing weight of potential PII-related threats (Mitnick & Simon, 2002; Mouton et

al., 2016; Tetri & Vuorinen, 2013). Junger et al. (2017) found that people are typically ill prepared to make PII-related decisions, even with training and warnings. Additionally, research has shown that a direct connection and potential threat exists with the way people perceive the significance of PII between virtual and physical worlds (Junger et al., 2017).

SE attacks on organizations occur without the benefit of knowing what PII is available or from where the attack will come (Tetri & Vuorinen, 2013). In effect, organizations are largely ineffective in staving off SE attacks due to current security structures failing to predict PII exposure of organizational targets, the content of potential attacks, or possible attack vectors (Heartfield & Loukas, 2015). Given the documented exponential increase of the availability of PII, the relevance of this study is considerable.

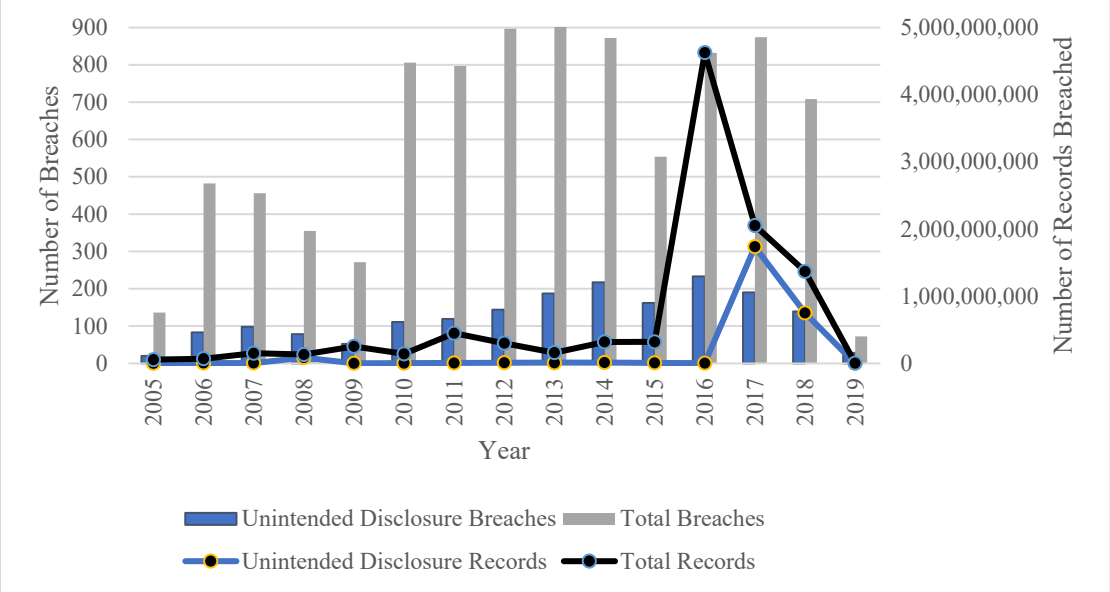
Significance

The significance of this study is highlighted by the dramatic increase in the availability of OSPI due to the willingness of people to share on social networks and other media as well as billions of records compromised via data breaches. The existence of hacker undergrounds where personal information and SE attack vectors are shared increases the exposure. Prior literature has documented the existence of OSPI as the precursor for many successful social engineering attacks (Heartfield & Loukas, 2015). The significant problem identified in this study is addressed by the development and validation of a SEXI using OSPI to assist in identifying and classifying SE exposure. Since privacy is highly subjective (Acquisti et al., 2015; Acquisti et al., 2016; Moon, 2000) and traditionally understood through context (Heurix et al., 2015; Hong & Thong, 2013) prior literature has called for a tool to serve as a predictor and determinant for

potential SE attacks (Heartfield & Loukas, 2015; Mohaisen et al., 2017) seeking the specificity of available information (Tetri & Vuorinen, 2013). The security training and policies implemented by organizations rely heavily on people (Mouton et al., 2016; Tetri & Vuorinen, 2013), which the literature indicates is the weakest defense point (Mitnick & Simon, 2002), the easiest to compromise (Neupane et al., 2015), and who superimpose their virtual openness to the current environment as evidenced by a willingness to share information (Junger et al., 2017).

Figure 3

Unintended exposures contrasted with all reported data breaches 2005-2019



Note: Unintended disclosures accounted for nearly half of 2017's data breaches and most of the exposed records. Adapted from "Data Breaches," by the Privacy Rights Clearing House, 2021. Used with the permission of the Privacy Rights Clearinghouse, under a Creative Commons Attribution NonCommercial-ShareAlike 4.0 (CC BY-NC-SA 4.0).

While organizations implement security policies and training (Mouton et al., 2016), research has found that warnings issued to users may actually increase exposure of personal information (Junger et al., 2017). Zhang et al. (2014) found that even though users perceived a heightened online security threat, they tended to expose even more personal information. Figure 3 provides the significance of unintended disclosures of datasets, which has grown during recent years.

Research indicates that the majority of users do not read or understand privacy policies in their lives, because they appear unwilling to put forth any significant effort in managing the privacy they value (Acquisti et al., 2015; Hong & Thong, 2013). These same people make up the cyber defense of the organizations (Mouton et al., 2016). During late 2016, Yahoo announced one billion customer records had been stolen (Green, 2017). The Privacy Rights Clearinghouse (2018) has logged almost 10 billion breached data records since 2005, with 18% (1.8 billion) occurring in the first 10 months of 2017. According to Jasper (2017), often data from breaches are shared on the hacker underground marketplace (i.e. Dark Web) within 72 hours, facilitating further successful attacks using the information. Public releases of stolen information are not uncommon, as is the case with the WikiLeaks release of CIA personnel PII instantly transforming the PII into OSPI (Franceschi-Bicchierai, 2015; Kopan, 2015). Public release of protected information serves as the foundation for SE attackers to mount attacks through unknown vectors using a massive amount of accurate data to orchestrate a cacophony of SE attacks (Mouton et al., 2016; Tetri & Vuorinen, 2013). Given the documented increase in PII exposed via data breaches and the continual avalanche of successful SE attacks using

OSPI, the significance of this study was substantial. Armed with a SE prediction mechanism, executives can take an offensive stance in organizational security risk mitigation and likewise monitor the overall exposure of the organization in real-time by evaluating the availability of OSPI of key personnel – including themselves (Mouton et al., 2016).

Barriers and Issues

Limited discernable empirical literature appears to exist regarding exposure, personal information, and social engineering. In addition, it appears that there is limited literature with regards to exposure related to open-source personal information. Hence, limited predictive literature indicates how to measure the exposure of individuals due to the availability of open-source personal information. To resolve this, a new instrument is to be developed using Schwartz and Solove (2011)'s privacy categories as well as McCallister et al. (2010)'s privacy-related descriptions and definitions used to protect the confidentiality of PII. Reliability for the internal consistency of intercorrelated items of the SEXI instrument is one of the barriers that requires overcoming.

One potential barrier for this study was obtaining permission to measure TOM of the SMEs. IRB approval was needed to use the SMEs as participants. Additionally, the SEXI instrument derived from the SMEs indicated the existence of personal information and inadvertently created PII or PDI of the 50 executives of Fortune 500 organizations and 50 Hollywood celebrities. This study did not collect or retain any personal information. IRB approval was obtained prior to the formation of the SMEs and data collection.

Exposure of the executives and their respective organizations was an issue in this study. This issue was addressed by randomizing the list of fortune 500 companies and

subsequently assigning each organization a nondescript identifier (F001, F002, etc.). Additionally, the executive position titles (e.g. CEO, CIO, CFO, etc.) were randomized and given a title designation (e.g. C01, C02, C03, etc.), which did not directly indicate the position nor the executive. Efforts were made to maintain the confidentiality of all Fortune 500 organizations and associated executives. A unique identifier was applied to each executive, i.e. F023-C06, thereby obfuscating the organization and executives. The original designations were be stored in a separate system.

Exposure of the Hollywood personas is also an issue in this study. This was addressed by randomizing a list of the 500 top grossing films of all time, filtered to exclude titles released before 1980, and assigning each movie a nondescript identifier (e.g. M001, M002, etc.). Hollywood personas were randomly selected from the top 10 cast positions from each feature presentation according to the IMDB. Each persona was obfuscated via a nondescript identifier (e.g. H01, H02, etc.). A unique identifier was applied to each Hollywood persona, i.e. M081-H03 to maintain their confidentiality. The original designations were stored in a separate system.

Another barrier that this research study had to overcome was the requirement of validity. To address this barrier, a close-ended Delphi was used with a pre-defined stop criterion. Content validity was addressed by providing the findings of each Delphi round to the SMEs in aggregate form for them to evaluate (Linstone & Turoff, 1975). The responses of the SMEs solicited for participation in this study required consensus or constructiveness, thereby posing another issue. Therefore, to address this concern, each item was individually assessed through multiple rounds. Items that did not reach

consensus were presented to the SEMs in a subsequent round for re-evaluation (von der Gracht, 2012).

TOM, the imputation of mental states to oneself and to others (Premack & Woodruff, 1978), within the SMEs is expected to be an issue due to their respective understanding of privacy. Mitnick and Simon (2002), McCallister et al. (2010), Schwartz and Solove (2011), Pavlou (2011), Junger et al. (2017) discussed the issue of privacy being contextual and thereby idiosyncratic. Therefore, to address this concern, the SMEs were asked to answer a survey to understand better their respective experiences and conceptualization associated with privacy to provide a richer understanding of the panel composition and to ensure they met the requirements. The survey also presented questions on organizational privacy policy and practices, as these may not necessarily be synonymous.

Using the Delphi method is a potential barrier vis-à-vis over-simplification, suppression of uncertainty, and bias (Linstone & Turoff, 1975). This issue was addressed by seeking SMEs from multiple industries having extensive professional privacy experience. Additionally, items of consensus and those discarded were made available and discussed.

Assumptions, Limitations, and Delimitations

Assumptions

It was assumed that SMEs were able to provide the required components and hierarchical weights as well as reach consensus required to develop the SEXI instrument. Additionally, it was assumed that the SMEs would provide honest and truthful responses

as to their experience and expert opinion. An assumption was made as to the availability and accessibility of personal information via open-source.

Limitations

This research study developed a new benchmarking instrument, the SEXI benchmarking index, based on the foundational literature, as well as the feedback, validation, and adjustments needed from the SMEs via the Delphi method. SMEs were asked to provide feedback on the SE exposure candidate components found in the literature and provide additional relevant components that were not previously in the literature. The second limitation was the set of measures combined to form SEXI. Given that cyber attacks and SE attacks, in particular, are changing over time, the SEXI benchmarking index was based on the current SE threat vectors, techniques, or approaches. The SEXI instrument was envisioned to require more adjustments in the future in response to trends in SE, changes in social media security and privacy settings, as well as innovations that evolve the means by which identity theft occurs. The third limitation was the reliance on an American group of experts for the SME panel to establish the instrument. International participation of SMEs may represent broader population of SMEs, while providing more generalizability to the relative weights, criteria, and measures (Wilkerson et al., 2017). The fourth limitation was the group of executives from Fortune 500 companies as well as the Hollywood personas. Therefore, the results may not be generalizable to other populations.

The potential sixth limitation of this study was response bias. The SMEs were asked to describe their privacy experiences and organizational practices. A potential exists for response bias, acquiescence bias, or social desirability bias. To mitigate this limitation,

the SMEs were informed that their responses will not be attributable and will be reported anonymously (with quotes sanitized, if necessary) or else reported in the aggregate.

The sample represented a random selection of executives from U.S. organizations and Hollywood personas. The results were not representative of all similar positions within U.S. organizations, entertainment industries, or those found in other countries. This research study was performed on a fixed set of U.S. executives and Hollywood personas. To get a cross-section of executives, the sample included individuals spread across randomly selected U.S. based organizations and positions from the list of Fortune 500 companies as of 2018. To get a cross-section of Hollywood personas, the sample included individuals spread across the top 500 grossing films of all time, filtered to exclude titles before 1980.

Delimitations

First, a delimitation of this research study was the convenience sampling of the experts recruited for the panel. Sekaran and Bougie (2013) defined convenience sampling as "the collection of information from members of the population who are conveniently available to provide it" (p. 252). The experts were solicited from multiple professional associations.

The second delimitation was that each source was validated to ensure that it correctly associates with the executive or Hollywood persona. A possibility exists for the returned data to be associated with another individual having the same identifier, such as name. Specific details were not collected.

Data collection in this study comprised a third delimitation, as it depended on the existence of information at the point of the survey. The availability of personal

information was unpredictable as well as subject to technology implementation and limitations. The information may or may not exist when queried or on subsequent queries. The source of data may also change. To address this issue, each query was timestamped, logged, and archived for analysis. A fourth delimitation was that data were collected during a specific period for the study. A fifth delimitation was that all information items were coded as either located (1) or not found (0), while the actual data was not captured as it is not required for analysis or construction of the SEXI score. The sixth delimitation of this study was the restriction of the scope of this study to validate the SEXI instrument on only 50 executives of Fortune 500 companies and 50 Hollywood personas.

Definition of Terms

The following represent terms and definitions.

Anonymous – "implies that the data cannot be manipulated or linked to identify an individual" (Sweeney, 1997, p. 100).

Anonymous information – "is defined as previously identifiable information that has been de-identified and for which a code or other association for re-identification no longer exists" (McCallister et al., 2010 p. 4-5).

Biometric – "A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris image samples are all examples of biometrics" (Ferraiolo et al., 2013, p. 64).

Business email compromise – "the scammer skillfully impersonates a trusted entity, typically a colleague or vendor, asking the would-be victim to help perform a task… sending information or money" (Jakobsson, 2016, p. xiv).

Cognitive privacy link - the surmised private connection between an actor and a provider (Acquisti & Grossklags, 2005; Bandura, 2001).

Confidentiality – "preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information" (44 U.S.C. § 3552, p. 1).

Content validity – "the extent to which the questions on the instrument and the scores from the questions are representative of all the possible questions that could be asked about the content or skills" (Creswell, 2012, p. 618).

Convenience sampling –"the collection of information from members of the population who are conveniently available to provide it" (Sekaran & Bougie, 2013, p. 252).

Deception – "manipulation of another person's thoughts—making someone believe something false" (Baron-Cohen, 1992, p. 1142).

Deidentified data – "all explicit identifiers, such as SSN, name, address, and telephone number, are removed, generalized, or replaced with a made-up alternative … does not guarantee that the result is anonymous" (Sweeney, 1997, p. 100).

Deidentified information – "is used to describe records that have had enough PII removed or obscured, also referred to as masked or obfuscated, such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual, [which] can be reidentified" (McCallister et al., 2010 p. 4-4).

Delphi method – " a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem" (Linstone & Turoff, 1975, p. 3).

Descriptive study – "often designed to collect data that describe the characteristics of persons, events, or situations (Sekaran & Bougie, 2013, p. 97).

Developmental research – "(i) supporting the development of prototypical products (including providing empirical evidence for their effectiveness), and (ii) generating methodological directions for the design and evaluation of such products" (Van den Akker et al., 2012, p. 4).

Distinguish – "is to identify an individual" (McCallister et al., 2010, p. 2-1).

Exploratory study – "used when not much is known about the situation at hand, or no information is available on how similar problems or research issues have been solved in the past" (Sekaran & Bougie, 2013, p. 96)

Exposure – "a measure of how well an object … can be observed … over a period of time" (Meguerdichian et al., 2001, p. 139).

Grey literature – "is published material that is not indexed and often lacks data about the publisher" (Fleisher, 2008, p. 853).

Harm – "any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII" (McCallister et al., 2010, p. ES-1).

Highly restricted personal information – "means an individual's photograph or image, social security number, medical or disability information" (18 U.S.C. § 2725, p. 601).

Information – “Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual” (Ross et al., 2016, p. 22).

Information privacy – “the ability of the individual to personally control information about one's self” (Stone et al., 1983, p. 460).

Information security – “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction”(44 U.S.C. § 3552, p. 1).

Information type – “A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation” (FIPS 199, 2004).

Intimate self-disclosure – “are … those that contain high-risk (as opposed to low-risk) information that makes the discloser feel vulnerable in some way” (Moon, 2000, p. 323).

Intimate information exchanges – “as those involving risky, evaluative disclosures – tend to lead to resilient long-term relationships in which both parties experience strong feelings of commitment and loyalty” (Moon, 2000, p. 331).

Linkable information – “is information about or related to an individual for which there is a possibility of logical association with other information about the individual” (McCallister et al., 2010, p. 2-1).

Linked information – “is information about or related to an individual that is logically associated with other information about the individual” (McCallister et al., 2010, p. 2-1).

Measurement of the self – "a recording of an observation about the self, which may include the environment to which the self is exposed" (Kang et al., 2011, p. 814).

Mental states – "purpose or intention, as well as knowledge, belief, thinking, doubt, guessing, pretending, liking, and so forth" (Premack & Woodruff, 1978, p. 515).

Monetization – "often means parsing … data for behavioral targeting and advertising, in ways that the average user is unaware" (Kang et al., 2011, p. 824).

Obscured Data – "Data that has been distorted by cryptographic or other means to hide information. It is also referred to as being masked or obfuscated" (McCallister et al., 2010 p. E-1).

Open-source – "publicly available print and digital/electronic data from unclassified, non-secret, and 'grey literature' sources," not requiring credentials or special access, including data available through breaches, leaks, etc. (Fleisher, 2008, p. 853).

Open-source personal information – personal information that is available openly to everyone who has access to the Internet (Fleisher, 2008)

Personal branding – "the process whereby people and their careers are marked as brands and it differs from reputation management and impression management with its purpose" (Karaduman, 2013, p. 465).

Personal information – "means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information…" (18 U.S.C. § 2725, p. 601).

Personally distinguishable information – "any information about an individual maintained by an agency … that can be used to distinguish or trace an individual's

identity … and is linked or linkable to an individual" (McCallister et al., 2010, Section 2.1).

Personally identifiable information – "refers to information that can be used to identify or locate an individual" (Chellappa & Sin, 2005, p. 188).

Personally unidentifiable information – "information that, taken alone, cannot be used to identify or locate an individual" (Federal Trade Commission, 2000, p. 46).

Persuasion – "changing persons' mental states, usually as precursors to behavioral change" (O'keefe, 2002, p. 32).

Phishing – "is a criminal trick of stealing victims' personal information by sending them spoofed emails urging them to visit a forged webpage that looks like a true one" (Wenyin et al., 2005, p. 1060).

Pretending – "of 'acting as if' something is the case when it is not" (Leslie, 1987, p. 413).

Pretense – "deliberately distort reality" (Leslie, 1987, p. 412).

Pretext – "an imposter creates a setting designed to influence an intended victim to release sensitive information, pay money, or perform actions that compromise the confidentiality of information" (Workman, 2008, p. 3).

Privacy – "the degree to which an individual can control the collection, disclosure, and use of personal data" (Kang et al., 2011, p. 820).

Privacy Chain – **"**the flow of PUI/PII/PDI [personal information] communication between two endpoints" (Wilkerson et al., 2017, p. 3).

Privacy Web – the extent PUI/PII/PDI [personal information] is gathered and transferred in relation to an individual to heterogeneous systems (Acquisti et al., 2015; Braun et al., 2001; McCallister et al., 2010).

Publicly available information – "Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could lawfully be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any vent that is open to the public" (Defense Intelligence Agency, 2011 p. GL-144).

Record – "means any item, collection, or grouping of information about an individual that is maintained by an agency [of the U.S. Federal Government], including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph" (5 U.S.C. § 552a, p. 317).

Reidentification – "combines datasets that were meant to be kept apart, and in doing so, gains power through accretion: Every successful reidentification, even one that reveals seemingly nonsensitive data like movie ratings, abets future reidentification" (Ohm, 2010, p. 1705).

Representation – "to represent aspects of the world in an accurate, faithful, and literal way, in so far as this is possible for a given organism" (Leslie, 1987, p. 414).

Risk – "refers to uncertainty about and severity of the events and consequences (or

outcomes) of an activity with respect to something that humans value" (Aven & Renn, 2009, p. 6).

Sanitization – "Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs" (Ross et al., 2006, p. 8).

Self –"a list of terms or features that have been derived from a lifetime of experience with personal data" (Rogers et al., 1977, p. 677).

Self-disclosure – "the act of revealing personal and sensitive information about oneself" (Moon, 2000; Peer & Acquisti, 2016, p. 429).

Self-surveillance – "a practice that measures, collects, and stores self-surveillance data" (Kang et al., 2011, p. 814).

Self-surveillance data – "are measurements of the individual self, initiated by the self, using sensors that are in one's control, for the primary purpose of measuring the self" (Kang et al., 2011, p. 814).

Semantic attack – "The manipulation of user-computer interfacing with the purpose to breach a computer system's information security through user deception" (Heartfield & Loukas, 2015, p. 0:1).

Semantics – "the study of meaning and symbolization" (Heartfield & Loukas, 2015, p. 0:1).

SEXI – The social engineering exposure index is a logical and repeatable quantitative measure that indicates the level of personal exposure for an individual. It is also a data aggregation that provides a means for classifying personal information.

Social network sites – "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system" (Boyd & Ellison, 2007, p. 211).

Social engineering – "is a combination of techniques used to manipulate victims into divulging confidential information or performing actions that compromise security" (Luo et al., 2013, p. 2).

Spear-Phishing – "is the targeted version of phishing, where a carefully crafted phishing email is directed to a specific individual or organization" (Heartfield & Loukas, 2015).

Subject matter experts – "define the curriculum universe which we then designate as the "content domain"" (Lawshe, 1975, p. 565).

Theory of mind – "the individual imputes mental states to himself and to others (either to conspecifics or to other species as well)" (Premack & Woodruff, 1978, p. 515).

Trace – "is to process sufficient information to make a determination about a specific aspect of an individual's activities or status" (McCallister et al., 2010, p. 2-1).

Whaling – "spear phishing (especially valuable targets)" (Orman, 2013).

List of Acronyms

API – Application Program Interface

BEC – Business Email Compromise

CEO – Chief Executive Officer

CFO – Chief Finance Officer

CIA – Central Intelligence Agency

CIO – Chief Information Officer

CSO – Chief Security Officer

CVR -- Content Validity Ratio

DDoS-- Distributed Denial of Service

DNA – Does Not Apply

FBI – Federal Bureau of Investigation

FIPs – Fair Information Practices

GPS – Global Positioning System

IRB – Institutional Review Board

IS – Information Systems

IT – Information Technology

OSPI – Open-source Personal Information

PDI – Personally Distinguishable Information

PDIM – The measurement of personally distinguishable information

PICC – Personal Information Candidate Component

PII – Personally Identifiable Information

PIIM – The measurement of personally identifiable information

PUI – Personally Unidentifiable Information

PUIM – The measurement of personally unidentifiable information

SE – Social Engineering

SEXI – Social Engineering eXposure Index

TOM – Theory of Mind

U.S. – United States

UNF – Unfamiliar (used during phase 1 of Delphi method)

Summary

The purpose of this section was to introduce the research study as well as to identify the research problem, barriers and issues, assumptions, limitations, and delimitations. A theoretical justification for the research study was also presented. The research problem that this study addressed was the proliferation of SE attacks due to OSPI, which is increasing despite warnings, media exposure, laws, and data breaches. Supporting literature corroborates the research problem and the need for this study.

The literature demonstrates the exponential growth of personal information via open-source repositories (Acquisti et al., 2015). Cybercrimes are also on the increase with little information as to where the SE attacks will come from or the composition used (Federal Bureau of Investigation, 2012; Mouton et al., 2016; Tetri & Vuorinen, 2013). Consequently, the need to determine the availability of personal information as well as predicting potential SE attack vectors is significant to personal and organizational security (Mouton et al., 2016). The need for this work was demonstrated by the literature that acknowledged the progressive expansion of SE attack vectors (Mitnick & Simon, 2002), the lack of a predictive threat system (Tetri & Vuorinen, 2013), the availability of OSPI which circumvent organizational cybersecurity technologies (Heartfield & Loukas, 2015), and the dearth of data on information gathering techniques for the successful execution of prior SE attacks (Mouton et al., 2016).

The goal of this research was to develop and validate a SEXI using OSPI to assist in identifying and classifying SE vulnerabilities. The literature provided grounding for this research with the concept of categories of PII introduced by Schwartz and Solove (2011)

and described by McCallister et al. (2010). The newly developed benchmarking index was validated by measuring the SEXI of 50 Fortune 500 executives and 50 Hollywood personas. The collected data were analyzed to assess and statistically test for significant mean differences of the SEXI of 100 individuals and reported.

Multiple barriers were overcome and met the requirements of this dissertation research. Given that limited discernible empirical literature appears to exist regarding how exposure of personal information to social engineering should be measured, rated, or summarized, an expert panel was tasked with this purpose. The IRB process addressed two associated issues in this study: the use of the SMEs to measure TOM, and the collection of publicly available personal information of 50 executives of Fortune 500 companies and 50 Hollywood personas. The SMEs were informed that their responses were not attributable and were reported anonymously (with quotes sanitized, if necessary) or else reported in the aggregate. The specific OSPI of the executives and Hollywood personas were codified in a “found” / “not found” dichotomous scale to maintain confidentiality. IRB approval was obtained before the Delphi method and data collection began. Each Hollywood persona as well as executive and their respective organization were coded into a concatenated identification label consisting of two strings – the first denoted the organization or feature film with the remaining portion made up of a random identifier.

Another barrier that this research study overcame is the requirement of validity in the weights, groupings, and rankings of the exposure of OSPI. To address this barrier, the SMEs must reach a consensus based on the literature. The resulting SEXI instrument was used to assess the exposure of 50 Fortune 500 executives and 50 Hollywood personas.

The data were analyzed and subsequently reported. The literature served as the foundation for the benchmarking index development. The use of open-ended questions, Likert scales, and binary response were used to facilitate the successful development of the SEXI benchmarking instrument. While the literature discussed taxonomies of SE attacks (Heartfield & Loukas, 2015), described SE (Mitnick & Simon, 2002), established privacy standards (McCallister et al., 2010), discussed privacy (Schwartz & Solove, 2011; Solove, 2006), and critiqued security policies (Wolff, 2016), the effort thus far appears to have fallen short. Mouton et al. (2016), Tetri and Vuorinen (2013), as well as Bélanger and Crossler (2011) called for a predictive tool that can potentially facilitate organizational cybersecurity by providing insight into possible SE attack vectors as well as potential personal information used in their execution. Therefore, this research developed and validated the SEXI benchmarking index to measure the level of exposure of executives to SE due to OSPI.

Chapter 2

Review of Literature

Introduction

In this chapter, an overview of relevant literature is offered. Bhattacherjee (2012) described a three-fold purpose for literature review: survey, grounding, and gap identification. Hart (1998) described the obligation for researchers to have an exhaustive grasp of the literature in their area of interest, to provide a foundation for contribution. Ellis and Levy (2006) correlated significance and quality with the accuracy of the review of the literature. This interdisciplinary study involves an overview of the information systems (IS) literature using several databases from multiple fields: IS, psychology, law, and business.

Exposure

Meguerdichian et al. (2001) defined exposure as "a measure of how well an object … can be observed … over a period of time" (p. 139). In application, photographers manipulate exposure to control composition and context. Raskar et al. (2006) described how exposure could be manipulated to provide clarity – even to the most obscured subject by adjusting the amount of time it is viewed. The literature has discussed exposure in the areas of big data (Martin, 2015; Rosenbaum, 2015), biology (Kennedy et al., 2001b; Maeterlinck, 1930), bring your own device (Garba et al., 2015), information privacy (Acquisti et al., 2016; Smith et al., 2011), law (Schwartz & Solove, 2011; Solove,

2006), mindfulness (Orlikowski & Baroudi, 1991; Shapiro et al., 2006), persuasion (Johnston et al., 2015; Perloff, 2010), posttraumatic stress disorder (Keane et al., 1989; Youssef et al., 2013), SE (Conteh & Schmick, 2016; Mamonova & Koufaris, 2016), self-disclosure (Bélanger & Crossler, 2011; Culnan & Bies, 2003; Moon, 2000), smartphone (Boyd, 2014; Enck et al., 2014; Xu et al., 2011), and social network sites (Boyd & Ellison, 2007; Choo, 2011; Minkus et al., 2015).

There are many venues where people choose to expose their personal information, including social media, personalization, online forms, and smartphones (Acquisti et al., 2015; Falaki et al., 2010; Lee et al., 2011). Research suggests that people may be giving up on having privacy (Mamonova & Koufaris, 2016). Junger et al. (2017) found that in certain situations a warning may substantially increase disclosure – not always in accordance with assumptions of less personal information disclosed. Similarly, Wolff (2016) introduced a framework which included a measure to understand how and why humans unpredictably interact with technology in the context of information security. Zhang et al. (2014) found that even though users perceived a heightened online security threat, they tended to expose even more personal information.

The literature also indicates that news announcements of government privacy invasion, cyber threat warnings, and the number of Americans personally experiencing a data breach seem to adversely affect how participants control, protect, and even value their PII (Junger et al., 2017; Mamonova & Koufaris, 2016; Olmstead & Smith, 2017). Johnston et al. (2015) indicated that 40% of data breaches are due to organizational insiders. Acquisti et al. (2015) described research that found when people are given enhanced control over their privacy they tend to increase the information shared – despite

assumptions of researchers to the contrary. Chang et al. (2016) found that the views and behaviors of people to share personal information become increasingly favorable after viewing images of scantily clad people. Exposure is of interest as the literature has shown that SE attacks usually comprise personal information originating at the target or from peripheral sources (Heartfield & Loukas, 2015; Junger et al., 2017; Luo et al., 2013). Little is known as to what personal information is available via OSPI or how it is specifically used in various SE attack vectors (Mouton et al., 2016; Tetri & Vuorinen, 2013).

McCallister et al. (2010) viewed exposure from the lens of the harm to individuals and organizations associated with the release of confidential information. Geletkanycz and Hambrick (1997) investigated the relations top executives have with external entities and how they are exposed to information as well as alternative understandings. Executive exposure has been the norm for top-level organizational leaders for many industries as a means to do business (Geletkanycz & Hambrick, 1997). This executive exposure was intended to facilitate daily operations and organizational stability (Coleman, 2000; Geletkanycz & Hambrick, 1997). This exposure has led to multiple SE attacks such as the one enacted by a penetration testing team hired by a company that used the voice and travel itinerary of a Chief Finance Officer (CFO) to access key systems (Granger, 2001). Executive exposure can occur in many forms, from shoulder surfing to dumpster diving (Granger, 2001; Mitnick & Simon, 2002). SE attacks via on-line technologies may intertwine email, postal mail, and other sources of readily available information each providing inroads into the world of the executive via their personal information (Granger, 2001; Heartfield & Loukas, 2015; Luo et al., 2013; Mitnick & Simon, 2002; Mouton et

al., 2016; Peltier, 2006). Just as photographers control the exposure of objects to gain clarity (Raskar et al., 2006), social engineers specialize in the collection of sensitive information and in the refactoring of exposed data into a treatise on potential executives, organizations, or other SE targets (Mitnick & Simon, 2002).

The 2015 BEC attack on the CIA Director illustrated how a single piece of information facilitated the exposure of the personal information of many people. Discovering the ISP of the CIA Director lead to a sequence of SE attacks on multiple organizations, each exposing additional personal information based on the prior discovered data. Eventually, the attackers were able to gain access to a personal email of the CIA Director, which in turn contained the personal information of agents and contractors (Franceschi-Bicchierai, 2015). Orgill et al. (2004) described the hazards of allowing extended exposure to the physical environment and employees of an organization resulting in the collection of usernames, passwords, and corporate credit cards. Tetri and Vuorinen (2013) stated, “Contrary to what the literature suggests, we believe that social engineers should get more credit for spotting organisational [sic] weaknesses from the outside rather than being celebrated as great persuaders” (p. 1019). Allen (2006) described how these outsiders expose weaknesses via SE by “gathering information, developing relationships, exploitation, and execution” – repeating the process with newly discovered information (p. 5). According to Mitnick and Simon (2002), exposure is the craft of SE, while organizations and key personnel form the playground.

Personal information exposure comes in many forms from voluntary disclosure (Bélanger & Crossler, 2011) to big data (Martin, 2015). For photographers, exposure

facilitates composition and context (Raskar et al., 2006). For personal information, its exposure affects composition and context to third-parties, which RQ1 and RQ2 quantitatively assessed (McCallister et al., 2010; Schwartz & Solove, 2011). A summary appears in Table 1 of the literature referenced in this section.

Table 1

Summary of Exposure Literature

Study	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Acquisti et al. (2015)	Review		Literature streams: Context-Dependence Malleability and Influence Uncertainty	"Norms and behaviors regarding private and public realms greatly differ across cultures, within cultures, while varying dramatically for the same individual, and for societies, over time" (p. 513).
Acquisti et al. (2016)	Comprehensive Survey of Literature		Literature Streams: Consumers Unaware of Privacy threats Economic Theory Empirical Analysis of Privacy Exposure in Varying Scenarios Unifying Economic	"One of the themes emerging from this review is that both the sharing and the protecting of personal data can have positive and negative consequences at both the individual and societal levels" (p. 483).

			Theory of Privacy	
Allen (2006)	Descriptive		The Cycle: Information Gathering Developing Relationship Exploitation Execution	"[T]here will always be the possibility of the 'human factor' being influenced by a social, political and/or cultural event" (p. 9).
Bélanger and Crossler (2011)	Review	500 Articles 142 Journal Articles 102 Conference Proceedings	Framework of Theory Classifications Information Privacy Structural View of Information Privacy	Many topics Research focused largely on explaining and predicting Research is largely confined to the U.S. and student contexts
Boyd and Ellison (2007)	Descriptive	Historical overview Serves as introduction of 7 Articles for a special issue	Exposure Signaling Theory	A formal definition of "social network sites" (p. 211). Overview of Social Network Sites and underlying methodology such as "friending".
Boyd (2014)	Survey	166 Formal, semistructured interviews of teens over three years	Audience Media Public	Insight into the minds of youth and their use of privacy-related technologies
Chang et al. (2016)	Experiment	Main study: 387 Turk Workers (105 female / 200 male) Study 2:	Less Provocative Images Provocative Images	"Empirically identifying a key mechanism by which norm-shaping designs can change beliefs

		82 (38 female / 44 male)		and subsequent disclosure behaviors" (p. 587).
Choo (2011)	Descriptive		Routine Activity Theory	The authors "explain how the Routine Activity Theory can help to inform and enhance cyber crime prevention strategies" (p.720).
Coleman (2000)	Longitudinal Study	4000 Students from public schools	Human Capital Social Capital	Demonstrated "the effect of social capital in the family and in the community in aiding the formation of human capital" (p. S118).
Conteh and Schmick (2016)	Review			"[W]hile technology has a role to play in reducing the impact of social engineering attacks, the vulnerability resides with human behaviour [sic], human impulses and psychological predispositions that can be influenced through education" (p. 37).

Culnan and Bies (2003)	Review		Fair Information Practices Justice theory Trust-gap	"[S]uggests new privacy rules are needed" (p. 335). "[S]elf regulation is unlikely to work 100% of the time as there will always be bad actors or organizations who have implemented the formal trappings but not the substance of fair information practices creating a need for baseline privacy legislation" (p. 338).
Enck et al. (2014)	Descriptive		Taintdroid	"We have presented TaintDroid, an efficient, system-wide information-flow tracking tool that can simultaneously track multiple sources of sensitive data" (p. 5:25).
Falaki et al. (2010)	Field Study	Dataset 1: 33 Android users (16 high school students; 17 knowledge workers) Dataset 2: 222 Windows Mobile users (116 U.S.;	Business Power User Life Power User Organizer Practical Social Communicator	"[W]e comprehensively characterized user activities and their impact on network and battery [and] quantify many hitherto unknown aspects of

		106 United Kingdom)		smartphone usage" (p. 193).
Franceschi-Bicchierai (2015)	News Article			Describes the SE attack on CIA Director by teenagers.
Garba et al. (2015)	Review		Bring Your Own Device (BYOD) Information Security Mobile Computing Organizational Practices Privacy	"[A]ny attempt for organizations to adopt or implement BYOD without adequate attention to the security and privacy issues or challenges … may increase their risk of confidential information loss" (p. 52).
Geletkanycz and Hambrick (1997)	Descriptive	30 large publicly-traded firms in two industries: branded foods, computer	Performance Strategic conformity	"[G]reater understanding of interorganizationa l [sic] relations and the implications of external tie" (p. 673).
Granger (2001)	Descriptive			Provides real-world examples of SE.
Heartfield and Loukas (2015)	Taxonomy	Discusses research with 1900 malicious URLs, 308 users, and other	Deception Exploitation Execution Orchestration Vector	"It introduces a structured baseline for classifying semantic attacks by breaking them down into their components" (p. 0:31).
Keane et al. (1989)	Survey	362 male Vietnam-era	Combat Exposure	"[T]he three studies presented

		veterans across three studies	Scale	here confirms that the CES merits consideration for further use by clinicians and researchers" (p. 54).
Kennedy et al. (2001b)	Simulation using the De Jong Test Suit	P=20 or 100 N=20 or 100 (p. 306)	Emergent behavior (self-organization) Particles Swarm Theory	Interpretation and computer programs in relation to I. Minds are social. II. Particle swarms are a useful computational intelligence (soft computing) methodology (p. 395, 396).
Johnston et al. (2015)	Experiment	559 insiders of a Finland city government	Compliance Intention Formal Sanction Certainty Formal Sanction Severity Informal Sanction Certainty Informal Sanction Severity Intention to comply with recommended protective strategies	"This study develops and tests an enhanced fear appeal rhetorical framework that accounts for the distinction between threats to information assets and threats to human assets" (p. 130).

			Protection motivation theory Sanction Celerity Self-Efficacy Threat Severity Threat Susceptibility	
Junger et al. (2017)	Experiment	278 participants	Age Age Square Goals System Theory Priming Total Risk Warning	"This study found relatively high disclosure rates… Neither priming nor a warning influenced the degree of disclosure." (p. 85).
Lee et al. (2011)	Field Study	2 Firms	2 Price measures 3 consumer measures 3 consumer group measures for willingness to share personal information 4 Cost measures Personalization Scope Game theory Privacy calculus Profit	"[S]trategic choices of privacy protection can work as a competition-mitigating mechanism in personalization…. A firm's privacy protection strategy under competition should be based on the investment cost of protection and the size of the personalization scope" (pp. 440-441).

Luo et al. (2013)	Descriptive		Defenses Personality Traits Psychological Aspects Social Engineering Techniques	"in addition to advanced technologies counterattacking various security intrusions, human factors must be equally accounted for" (p. 7).
Maeterlinck (1930)	Exploratory		Ants Precursor to Swarm Theory Various other Swarming Species	One of the earliest swarm behavior references in the literature.
Mamonova and Koufaris (2016)	Experiment	Group 1: 222 technology users Group 2: 220 technology users	Government Intrusion Concerns Password Strength Privacy Concern Privacy Self-Efficacy	"[T]he exposure to government surveillance news led to the use of weaker passwords, suggesting that the exposure to government surveillance may trigger helplessness in relation to protecting privacy" (p. 64).
Martin (2015)	Exploratory		Aggregation Destructive Demand Downstream Uses Information Supply Chain Negative Externality os Surveillance	"[I]dentified the Big Data Industry as having both economic and ethical issues at the individual firm, supply chain and general industry level and has suggested associated solutions to

			Potential for Secondary Market Upstream Supplier Use of Consumer-Level Data	preserve sustainable industry practices" (p.85).
McCallister et al. (2010)	Descriptive		Defines key terms associated with privacy and personal information.	NIST 800-122 (Guide to Protecting the Confidentiality of Personally Identifiable Information (PII))
Meguerdichian et al. (2001)	Simulation and case studies	Two to eight Sensors	Exposure Exposure-Based Coverage Model	"[W]e presented an efficient and effective algorithm for minimal exposure paths for any given distribution and characteristics of sensor networks" (p. 148).
Minkus et al. (2015)	Descriptive	2,383 Adult Facebook Users via shallow data mine limited to public posts Survey of 357 Adult Facebook Users 1,089 Instagram Users	Birthday Face Name Location Matched to Voter's registration for demographics	"We can therefore conclude that although a substantial percentage of parents are compromising the privacy of their children in their public Facebook pages, significantly more are doing so among Facebook friends" (p. 782).

Mitnick and Simon (2002)	Descriptive			Brought social engineering into the mainstream. Social engineering attack cycle
Moon (2000)	Experiment via interview using a computer as interviewer	30 participants	Reciprocity Self-disclosure Theory of social response	The wording and sequence of questions can successfully solicit intimate details from users via computer. Explicit reward is not required to solicit personal information from a user successfully.
Mouton et al. (2016)	Descriptive		Theory of Group Conformity SE attack -Compliance Principles -Goal -Medium -Social Engineer -Target -Techniques SE Framework - Attack Formation -Debrief -Develop Relationship	Neither the literature or news media provide all the information concerning an attack. Usually little, if any, information is known about a potential attack. Little is known as to where the information is obtained for a SE attack. Little is known as to what information is available for a SE attack.

			-Exploit Relationship -Preparation Information Gathering	
Olmstead and Smith (2017)	Survey	1,014 adult-aged U.S. citizens	Demographics	64% of Americans have experienced a data breach. 12% use password management software.
Orgill et al. (2004)	Questionnaire	32 participants -26 gave their username -19 gave their password -7 gave login credential information above their own access -4 asked for a name badge or identification	Department Number Surveyed Password Username	"This study demonstrated that even in a company where security is a concern, these human traits [trust others, assist others, gain favor] can be ill-used if proper preventative measures are not taken … This study also shows the importance of assessing security effectiveness through means such as audits.… In order for an audit to be effective, the auditor has to be at least as thorough, through preliminary studying, planning, and execution as a

				potential social engineer would be" (p. 181). Some departments had more training and resisted the social engineer better.
Orlikowski and Baroudi (1991)	Review	155 Information systems articles	Epistemology Frequency Journal	"[R]esearchers should ensure that they adopt a perspective that is compatible with their own research interests and predispositions, while remaining open to the possibility of other assumptions and interests" (p. 24).
Peltier (2006)	Review			Magazine article describing SE to readers.
Perloff (2010)	Exploratory		Persuasion	Extensive discussion on persuasion, which is used in many SE attack vectors.
Raskar et al. (2006)	Descriptive	3 Cases	Coded blur Chops Flat blur	Demonstrated how manipulation of exposure increased clarity of the subject.
Rosenbaum (2015)	Survey *Dissertation	53 SMEs	Privacy Violation Scale	"[E]vidence strongly suggested that some practitioners were less willing to commit privacy violations than

				were other practitioners; this is based upon some practitioners identifications with various moral and computing Hallmark Features" (p. 115).
Schwartz and Solove (2011)	Exploratory		"Information can be about an (1) identified, (2) identifiable, or (3) non-identifiable person" (p. 1877).	"PII 2.0 protects information that relates either to an identified or identifiable person, and associates different legal interests with each category" (p. 1894).
Shapiro et al. (2006)	Exploratory		Attention Attitude Exposure Intention Mindfulness	"We have attempted to provide a first formulation of a model to describe how mindfulness might be fostering transformation and change" (pp. 384-385).
Smith et al. (2011)	Exploratory	Four decades of literature: 320 Privacy Articles 128 Books and Book Sections	Antecedents Outcomes Privacy Concerns	"[T]he overall [privacy] research stream has been suboptimized [sic] because of its disjointed nature" (p. 1008).
Solove (2006)	Exploratory		Information Collection	"I have attempted to provide a clearer and more

		Information Dissemination Information Processing Invasion	robust account of privacy—one that provides us with a framework for understanding privacy problems" (p. 558).
Tetri and Vuorinen (2013)	Descriptive	Actor-Network Theory	Describes issues in SE research and suggests the theories from the psychology literature should only be applied to the persuasion component of SE.
Wolff (2016)	Exploratory	Classification of perverse effects Duality of technology Technology-Interaction perverse effects Theory of unintended consequences User-Interaction perverse effects	"This classification scheme is intended as a step beyond simply warning defenders that they have to be careful when adding new security controls by giving them a framework for analyzing the different possible mechanisms by which those controls may interact with the system and its users to introduce new vulnerabilities and produce perverse effects" (p. 615).
Xu et al. (2011)	Exploratory	Covert vs. Overt	"[T]he findings of this research have provided

			Exchange Theory Interpersonal Differences Personalization Privacy Calculus Purchase Intention Willingness to Share Personal Information in Location-Aware Marketing	preliminary empirical evidence about how users strike a balance between value and risk" (p. 50).
Youssef et al. (2013)	Cross-Sectional Field Study	1,488 military personnel and veterans serving after September 2001	Beck Depression Inventory-Second Edition Beck Scale for Suicide Ideation Combat Exposure Scale Connor-Davidson Resilience Scale Davidson Trauma Scale Traumatic Life Events Questionnaire	"The study findings suggest that comprehensive assessment of both childhood trauma and resilience among military personnel and veterans can contribute to the understanding of their clinical status in terms of depression and suicidal ideation, and ultimately their clinical care" (p. 116).
Zhang et al. (2014)	Experiment	220 online U.S. resident adults	Attitude	"[T] he security cue heightens perceived threat

	Behavioral Intention Instant Gratification cue Security cue Threat Trust	but also encourages greater disclosure of one's account and network strength on social media" (P. 113).

Personal Information

The term OSPI is sparingly used in the literature, though it is described extensively throughout the privacy literature as any personal information belonging to an individual extended to include any being publicly available (Federal Trade Commission, 2000; Schwartz & Solove, 2011). Rogers et al. (1977) fully integrated personal information with the definition of self, "as a list of terms or features that have been derived from a lifetime of experience with personal data" (p. 677). Furthermore, the literature appears to infer that the tendency of people to share information may be more of an attempt to process one's respective life than an intentional self-disclosure (Rogers et al., 1977). Mitnick and Simon (2002) described open-source information as "SEC filings and annual reports, marketing brochures, patent applications, press clippings, industry magazines, Web site content, and also dumpster diving" (p. 310). Maynard et al. (2015) described the accessibility of PII due to content associated with a social media service and Application Program Interface (API), such as Twitter hashtags and posts. Oltmann (2010) described a continual degradation of the privacy of Facebook users sharing photos, data, and preferences. Sanders (2012) discussed the advent of credit reporting agencies using information collected from social networking sites. The Privacy Act of 1974 provides a

broad understanding of personal information, when defining a record to include personal, medical, criminal, education, employment histories, etc., (5 U.S.C. § 552a). The literature also discusses the existence of underground hacker markets where attack vectors, targets, and compromised PII are shared (Benjamin & Chen, 2012; Coleman & Golub, 2008; Jasper, 2017).

Following Schwartz and Solove (2011), OSPI is comprised of PUI (information which does not identify an individual), PII (information which can be used for identification), and PDI (information which explicitly identifies an individual). The primary source of OSPI is from people themselves (Acquisti et al., 2015), the organizations they work for (Federal Bureau of Investigation, 2015a), and social network sites (Acquisti et al., 2015; Federal Bureau of Investigation, 2012). Additional sources of OSPI such as data mining technologies can be used from command prompts on personal computers of any modern operating system (Russell, 2013), while credit reports and background checks can easily be requested even without consent (Sanders, 2012). Simple friend requests on social networks may reveal extreme amounts of PII and PDI (Boyd & Ellison, 2007; Maar, 2013; Mouton et al., 2016). The literature describes OSPI as personal information that is available openly to everyone who has access to the Internet (Fleisher, 2008).

The literature also discusses personalization, another exposure threat to privacy which may directly feed OSPI (Chellappa & Sin, 2005; Lee et al., 2011; Sutanto et al., 2013; Xu et al., 2011). Data brokers have formed entire supply chains (termed herein as privacy chains) of PDI, PII, and PUI pooled from a variety of sources and compiled into datasets, which are then repackaged and made available (Anthes, 2014; Kang et al., 2011).

Similarly, FIPS 199 (2004) provided precedence for information categories including privacy, medical, financial, etc. Additionally, research has indicated that people are sharing an increasing amount of PII on social networks and continue to do so despite being warned against it (Acquisti et al., 2015; Olmstead & Smith, 2017). Acquisti and Grossklags (2005) concluded "preliminary data show that privacy attitudes and behavior are complex but are also compatible with the explanation that time inconsistencies in discounting could lead to under-protection and overrelease [sic] of personal information" (p. 32). Krishnamurthy and Wills (2009) described the risk associated with exposure where specific identification of an American can be accomplished with only their date of birth, gender, and postal zip code. However, little is known in the literature about the role that OSPI play in SE attacks or even how much personal information is required for a successful attack (Krishnamurthy & Wills, 2009; Mouton et al., 2016; Tetri & Vuorinen, 2013).

Personal information is essentially the existence of an individual relegated to data points (Rogers et al., 1977). The literature described personal information as contextual (Culnan, 1993), having three levels of harm (McCallister et al., 2010), and three levels of exposure (Schwartz & Solove, 2011), which is the foundation of RQ1, RQ2, as well as RQ3. A summary appears in Table 2 of the literature referenced in this section.

Table 2

Summary of Personal Information Literature

Study	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
5 U.S.C. § 552a	Standard		Record	Defines various components of

				personal information, including medical, education, employment, criminal, and other histories.
Acquisti and Grossklags (2005)	Survey	119 Students 19–54 years old	General Privacy Concern Offline Identity Online Identity Personal Profile Professional Profile Sexual and Political Identity	"The evidence points to an alternation of awareness and unawareness from one scenario to the other" (p. 29). "Although respondents realize the risks associated with links between different pieces of personal data, they are not fully aware of how powerful those links are" (p. 30). "Even if individuals have access to complete information about their privacy risks and modes of protection, they might not be able to process vast amounts of data to formulate a rational privacy-sensitive decision" (p. 30).
Acquisti et al. (2015)	Literature review		Self-Disclosure Social Penetration Theory	"Norms and behaviors regarding private and public realms

				greatly differ across cultures, within cultures, while varying dramatically for the same individual, and for societies, over time" (p. 513).
Anthes (2014)	Review			"Asking consumers to 'opt out' of data collection at myriad companies they have never heard of is unrealistic, and the existing online "notice and consent" forms—in which users "agree" to the collection and use of personal data—are ineffective because they are mostly ignored by consumers" (P. 30).
Benjamin and Chen (2012)	Exploratory	28,537 hackers 723,555 forum posts	Average Message Length Control Theory Number of Replies Number of Threads Involved Reputation Tenure Sum of Attachments Total Messages	"Hackers that contributed to cognitive advance of their community or were considerably active had the highest reputations" (p. 6).

Boyd and Ellison (2007)	Descriptive	Historical overview Serves as an introduction of seven Articles for a special issue	Exposure Signaling Theory	A formal definition of "social network sites" (p. 211). Overview of Social Network Sites and underlying methodology such as "friending".
Chellappa and Sin (2005)	Empirical study	243 Consumers	Consumer Concern for Privacy Likelihood of Using Personalization Services Value of Online Personalization	"the consumers' value for personalization is almost two times (0.59 vs. −0.34) more influential than the consumers' concern for privacy in determining usage of personalization services" (p. 197).
Coleman and Golub (2008)	Descriptive		Liberalism, Anarchism, Hacker Ethics Political Theory	"hacker practice makes visible socially relevant questions to those interested in the legal politics of information access" (p. 271).
Federal Trade Commission (2000)	Descriptive		Access Choice Notice Privacy Privacy Seal Security Self-regulation	FIPS (Privacy Online: Fair Information Practices in the Electronic Marketplace) "Because self-regulatory initiatives to date fall far short of broad-based implementation of

			self-regulatory programs, the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will follow the standards adopted by industry leaders" (p. ii).
FIPS 199 (2004)	Descriptive	Information Type Potential Impact	FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems
Jasper (2017)	Review		Discusses Cyber Threat Intelligence Integration Center. "Therefore, the timely sharing of relevant and actionable cyber threat intelligence, in the context of cyber threat information and indicators, is imperative to reducing the impact of attacks" (p. 62).
Kang et al. (2011)	Descriptive	Personal Data Stream Personal Data Vault	"Instead of direct behavioral regulation or blind faith in the market, our strategy is to modify indirectly

			Privacy Rights Management	the information ecosystem by introducing a new species, the [Personal Data Guardian]" (p. 847).
Krishnamurthy and Wills (2009)	Longitudinal Study	127 test data set sites 81 Web sites across nine categories	Company Acquisitions Cookies First-Party Content JavaScript Root Domain Subdomain Third-Party Content	"… users are being tracked by multiple entities when accessing a first-party site… [and] existing privacy protection techniques have limitations in preventing privacy diffusion" (p. 15).
Lee et al. (2011)	Field Study	Two Firms	Two Price measures Three consumer measures Three consumer group measures for willingness to share personal information Four Cost measures Personalization Scope Game theory Privacy calculus Profit	"[S]trategic choices of privacy protection can work as a competition-mitigating mechanism in personalization…. A firm's privacy protection strategy under competition should be based on the investment cost of protection and the size of the personalization scope" (pp. 440-441).
Maar (2013)	Survey	49 professional users of social	Benefit Deception Risks Ease of Use	"The study appears to indicate that the three concerns of privacy, deception,

		networking sites	Habit Linkage Ownership Permeability Personal Norm Privacy Risks Response Efficacy Security Risks Self-Efficacy Trust	and security drive the three factors of information protection, boundary permeability, linkage, and ownership respectively" (p. 268). "This study has found that perceived benefits of online social network may motivate users to commit personally to protecting its integrity, but may induce users to relax their vigilance and develop poor online habits" (pp. 268-269).
Martin (2015)	Exploratory		Aggregation Downstream Uses Information Supply Chain Negative Externality Potential for Secondary Market Destructive DemandUpstream Supplier Use of Consumer-Level Data	"[I]dentified the Big Data Industry as having both economic and ethical issues at the individual firm, supply chain and general industry level and has suggested associated solutions to preserve sustainable industry practices" (p.85).
Maynard et al. (2015)	Descriptive	1.8 million tweets, 42		Describes open-source data mining

		political themes, 20 topics		(GATE) involving social networks.
Mitnick and Simon (2002)	Descriptive			Brought social engineering into the mainstream. Social engineering attack cycle
Mouton et al. (2016)	Descriptive		Theory of Group Conformity SE attack -Compliance Principles -Goal -Medium -Social Engineer -Target -Techniques SE Framework - Attack Formation -Debrief -Develop Relationship -Exploit Relationship -Preparation Information Gathering	Neither the literature or news media provide all the information concerning an attack. Usually little, if any, information is known about a potential attack. Little is known as to where the information is obtained for a SE attack. Little is known as to what information is available for a SE attack.
Olmstead and Smith (2017)	Survey	1,014 adult-aged US citizens	Demographics	64% of Americans have experienced a data breach. **12% use password management**

Oltmann (2010)	Exploratory			"If more users could be convinced to adjust their privacy settings, that could help preserve online privacy, which in turn might protect some of society's expectations for privacy in the broader offline world… [otherwise] our overall privacy will decrease" (p. 4).
Rogers et al. (1977)	Experiment	32 students - 16 Female -16 Male 40 adjectives	Self Self-reference	"In the realm of human information processing it is difficult to conceive of an encoding device that carries more potential for the rich embellishment of stimulus input than does self-reference" (p. 687).
Russell (2013)				A book providing tools and instructions for data mining popular social networking sites and online technologies.
Sanders (2012)	Descriptive Non-peer-reviewed, non-journal			Discusses the use of Social Media by credit reporting agencies

Schwartz and Solove (2011)	Exploratory		Identifiable Personal Information Identified Personal Information Unidentifiable Personal Information	"PII 2.0 protects information that relates either to an identified or identifiable person, and associates different legal interests with each category" (p. 1894).
Sutanto et al. (2013)	Field experiment	193 participants	Information Boundary Theory User Gratification Theory	Users assume marketers are using their information, amidst advertisements,
Tetri and Vuorinen (2013)	Descriptive		Actor-Network Theory	Describes issues in SE research and suggests the theories from the psychology literature should only be applied to the persuasion component of SE.
Xu et al. (2011)	Exploratory		Covert vs. Overt Exchange Theory Interpersonal Differences Personalization Privacy Calculus Willingness to share personal information in location-aware marketing Purchase Intention	"[T]he findings of this research have provided preliminary empirical evidence about how users strike a balance between value and risk" (p. 50).

Personally Distinguishable Information

According to the literature, that not all personal information holds the same significance (Heurix et al., 2015; Hong & Thong, 2013; McCallister et al., 2010; Mitnick & Simon, 2002; Schwartz & Solove, 2011). Schwartz and Solove (2011) declared, "All current legal models for this concept are flawed" (p. 1835), while discussing the lack of consensus within the U.S. to define privacy legally and precisely. Additionally, Schwartz and Solove (2011) believed that there is no merit to whether data are identifiable to a specific person when focusing on whether or not information is PII versus non-PII. McCallister et al. (2010) discussed the concept of impact levels due to exposure, while describing confidentiality breaches.

McCallister et al. (2010) referred to the information used to identify an individual as being distinguishable, providing a subset of PII to separate ultimate exposure leading to definite identification from a generic catchall of potential exposure. Safety guides also warn users not to post GPS, social security number, security clearance, or information that can be used to answer security questions on Websites, on social media, etc. (Federal Bureau of Investigation, 2012, 2015b). PDI is defined as "any information about an individual maintained by an agency … that can be used to distinguish or trace an individual's identity … and is linked or linkable to an individual" (McCallister et al., 2010, Section 2.1). The primary difference between PII and PDI is the specificity of the information being directly connected to an individual's identity (e.g. a photograph or social security number) rather than only having the potential of identification (e.g. gender or zip code) (McCallister et al., 2010).

McCallister et al. (2010) integrated risk nomenclature to personal information, stating that some PII can prove "hazardous to both individuals and organizations" (p. ES-1) and that "unauthorized access, use, or disclosure of PII can seriously harm both individuals, by contributing to identity theft, blackmail, or embarrassment, and the organization, by reducing public trust in the organization or creating legal liability" (p. 2-1). (Schwartz & Solove, 2011) argued "that the continuum of risk is different for these categories. The result is that the necessary legal protections should generally be different for identified and identifiable data" (p. 1818). The literature clearly makes the distinction that the exposure of specific personal information that makes an individual distinguishable is a higher risk and should be treated as such. In following the literature, the SMEs will be asked to categorize items as PDI and to provide a weight to the PDI category. A summary appears in Table 3 of the literature referenced in this section.

Table 3

Summary of Personally Distinguishable Information Literature

Study	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Federal Bureau of Investigation (2012)	Editorial			Provides the users of social media tips on how to mitigate the use of personal information in SE threats.
Federal Bureau of Investigation (2015b)	Editorial			Informs parents on how to discuss social media and its dangers with children.
Heurix et al. (2015)	Descriptive		Anonymity Behavior Cardinality	"[W]e have presented a taxonomy which covers common aspects of [privacy-enhancing technologies] across

			Content Directionality Foundation Holder Identity Pseudonymity	different application areas and demonstrated its applicability by applying it on several well-known approaches with different aims, including handling privacy issues with data-at-rest, data-in-motion, and cryptography-based approaches with diverse properties and purposes" (p. 14).
Hong and Thong (2013)	Empirical	4,000 Internet users	Awareness Control Information Management Interaction Management Internet Privacy Concerns Inter-Web-Personal Multidimensional Development Theory	Four theoretical IPC frameworks, six dimensions of measure, clarification of control in IPC, validation of a third-order factor structure, study of the effects of inconsistent wording in instruments
McCallister et al. (2010)	Descriptive			NIST 800-122
Mitnick and Simon (2002)	Descriptive			Brought social engineering into the mainstream. Social engineering attack cycle
Schwartz and Solove (2011)	Exploratory		Identifiable Personal Information	"PII 2.0 protects information that relates either to an identified or identifiable person, and associates different legal

	Identified Personal Information	interests with each category" (p. 1894).
	Unidentifiable Personal Information	

Personally Identifiable Information

Prosch (2008) described the use of accounting principles for protecting PII. The credit card industry self-regulates standards for the handling of PII for financial transactions (PCI Security Standards Council, 2016). Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347) provided the foundation for the Federal Information Processing Standards for handling PII and other data: verification of personal identity of employees and contractors (Ferraiolo et al., 2013), requirements of using cryptology for non-classified information (Dworkin et al., 2001), classification of all information and information systems (FIPS 199, 2004), minimum security for information and information systems (Ross et al., 2006), digital signatures (Barker, 2013), secure hash standard (Dang, 2015), and a standard for the use of SHA-3 (Dworkin, 2015).

Ohm (2010) described PII as "an ever-expanding category" (p. 1742). Green (2017) stated, "Humanity produces 2.5 quintillion bytes of data daily" (p. 289). Schwartz and Solove (2011) described current PII definitions within privacy law to be inconsistent and insufficient. PII "refers to information that can be used to identify or locate an individual" (Chellappa & Sin, 2005, p. 188). Regulators, lawmakers, and organizational

policymakers typically view PII as the centroid of privacy issues (Schwartz & Solove, 2011). Peer and Acquisti (2016) discussed the extreme difficulty, if not an impossibility, of reversing the release of PII. The literature indicates that people feel an inability to control their PII (Culnan, 1993; Green, 2017; Palen & Dourish, 2003; Peer & Acquisti, 2016). Simpson (2016) reported that a large number of data breaches occurred, therein containing over a billion PII via 4,600 data breaches. Privacy Rights Clearinghouse (2018) indicated over 1.9 billion records had been exposed in 7,300 data breaches as of November 1, 2017. These studies appear to infer that eight billion records were released in a single year. Though the literature provides details as to the type of breach and the number of affected records, little is known as to what information was released or what specific personal information has been exposed.

PII is the catch-all nomenclature for personal information in much of the literature, regulation, and U.S. law, giving little regard to levels exposure (Schwartz & Solove, 2011). McCallister et al. (2010) associated personal information to measures of risk and harm, thereby indicated that a one-size-fits-all understanding of PII may be ineffective. The elicited feedback from the SMEs for RQ1 and RQ2, should help quantify PII as well as categorize it to produce a benchmarking instrument for measuring exposure for RQ3. A summary appears in Table 4 of the personal information literature referenced in this section.

Table 4

Summary of Personally Identifiable Information Literature

Study	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution

Barker (2013)	Descriptive		Digital Signature Algorithm RSA Digital Signature Elliptic Curve Digital Signature Algorithm	Digital Signature Standard (DSS) (FIPS 186-4)
Culnan (1993)	Survey	126 undergraduate students	Attitudes Toward Direct Mail Marketing Attitudes Toward Secondary Information Use Concern for Privacy Demographics	"60 percent or more of the participants hold negative attitudes toward … practices [involving] one or more of the following: acquisition and use of third-party information, use of financial information, profiling, and/or making inferences that some participants viewed as unwarranted or inappropriate" (p. 358).
Dang (2015)	Descriptive		SHA-1 SHA-224 SHA-56 SHA-384 SHA-512 SHA-512/224 SHA-512/256	Secure Hash Standard (SHS) (FIPS PUB 180-4)
Dworkin (2015)	Descriptive			SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (FIPS PUB 202)

Ferraiolo et al. (2013)	Descriptive	Personal Identity Verification	FIPS PUB 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors
Green (2017)	Exploratory	Class Action Data Breach Standing	"Consumer data breach cases appear to satisfy both of these elements [injuries that are non-economic and non-physical], because the harm is broadly diffused throughout the economy and some of the injuries alleged are non-economic and non-physical" (p.316).
Ohm (2010)	Exploratory	Anonymization Deanonymize Reidentification	"Easy reidentification … undermines decades of assumptions about robust anonymization, assumptions that have charted the course for business relationships, individual choices, and government regulations…. This Article offers the difficult but necessary way forward: Regulators must use the factors

			provided to assess the risks of reidentification and carefully balance these risks against countervailing values" (p. 1776).
Palen and Dourish (2003)	Case studies	Disclosure Identity Privacy Publicity Temporality / Time	"In offering both a framework and a vocabulary for talking about privacy and technology, our goal is to foster discussion between technology users, designers and analysts, and to encourage a more nuanced understanding of the impacts of technology on practice" (p. 8).
PCI Security Standards Council (2016)	Descriptive	Account Data Cardholder Data - Cardholder Name - Service Code - Expiration Date Sensitive Authentication Data - Full Track Data - CAV2, CVC2, CVV2, CID	Payment Card Industry Data Security Standard (PCI DSS)

			- Pin / Pin Block	
Peer and Acquisti (2016)		716 adults from Amazon Mechanical Turk and a university pool	Perceived Intrusiveness Self-Disclosure Reversibility Irreversible	Participants disclose more when they are not warned. Perceived intrusiveness increased with the prior declaration of reversibility or irreversibility. Perceived intrusiveness rated differently before vs after answering.
Privacy Rights Clearinghouse (2018)	Descriptive		Breach year Eight types of breaches Seven types of organization breached	Tracks and categorizes data breaches
Prosch (2008)	Descriptive		Access Choice and consent Collection Disclosure to third-parties Management Monitoring and enforcement Notice Privacy Lifecycle Maturity Model Quality Security Use and retention	AICPA Generally Accepted Privacy Principles [adapted from accounting]
Ross et al. (2006)	Descriptive			FIPS Publication 200: Minimum Security Requirements for

			Federal Information and Information Systems
Schwartz and Solove (2011)	Exploratory	Identifiable Personal Information Identified Personal Information Unidentifiable Personal Information	"PII 2.0 protects information that relates either to an identified or identifiable person, and associates different legal interests with each category" (p. 1894).
Simpson (2016)	Exploratory	Common Law of Torts Data Breach Elements of Personally Identifiable Data Importing EU Data Protection into American Law Regulatory Law Statutory Rights	"By adopting an improved definition of personally identifiable data, creating a new definition of data controllers and processors, and reforming statutory liability for data breaches, Americans can be protected, and protect themselves, from the serious risks posed by consumer data breaches both now and in the future" (p. 709).

Personally Unidentifiable Information

PUI is defined as "information that, taken alone, cannot be used to identify or locate an individual" (Chellappa & Sin, 2005, p. 188; Federal Trade Commission, 2000, p. 46).

Schwartz and Solove (2011) warned that modern technologies make it increasingly difficult to keep PUI as deidentified information. Acquisti and Gross (2009) described an algorithm for predicting social security numbers as well as associated PUI. Additionally, four random pieces of deidentified data from credit card metadata were shown to reidentify 90% of people, with women being easier than men (de Montjoye et al., 2015). Kang et al. (2011) described the dangers of modern technologies that people use to surveil portions of their lives or the lives of others.

The majority of PUI is intended to provide demographic and nonidentifying information (Schwartz & Solove, 2011). Sweeney (1997) demonstrated the ease of reidentification using only Zip Code, birth date, gender, and race – with only birth date and full ZIP Code required to identify 97% of voters. Benitez and Malin (2010) estimated the difficulty of reidentification when anonymized, classified as public-use, Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule protected data when combined with voter registration lists. Ohm (2010) declared anonymization and the concept of PUI a failure due to the literature showing adeptness in re-identifying individuals even using PUI as a starting point.

Though PUI is typically considered anonymous or deidentified information (Schwartz & Solove, 2011), the literature describes several methodologies for the reidentification of an individual based on only a few pieces of demographic data (Sweeney, 1997). Rather than sidelining PUI as supposedly anonymous information, SMEs were asked to assign weights to reflect the level of exposure each has in and of itself. A summary appears in Table 5 of the literature referenced in this section.

Table 5

Summary of Personally Unidentifiable Information

Study	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Benitez and Malin (2010)	Mixed Methods -Survey of State's Elections Office -Quantitative Analysis	State populations segmented by combinations of County of Residence, Gender, Date of Birth, Race, and Birth Year	Estimated Proportion of a Population in a Group Expected number of Re-Identification General Attacker Monetary Cost of Re-Identification Voter Attacker	"This research provided a set of approaches for estimating the likelihood that de-identified information can be re-identified in the context of data sharing policies associated with the HIPAA Privacy Rule" (p. 177).
Chellappa and Sin (2005)	Empirical study	243 consumers	value of online personalization consumer concern for privacy likelihood of using personalization services	"the consumers' value for personalization is almost two times (0.59 vs. −0.34) more influential than the consumers' concern for privacy in determining usage of personalization services" (p. 197).
de Montjoye et al. (2015)	Field Study	Credit card records of 1.1 million people in 10,000 shops over three months.	Price Resolution Risk of reidentification Spatial Resolution Temporal Resolution Unicity	"Our results render the concept of PII, on which the applicability of U.S. and European Union (EU) privacy laws depend, inadequate for metadata data sets…. our findings highlight the need to

			reform our data protection mechanisms beyond PII and anonymity and toward a more quantitative assessment of the likelihood of reidentification" (p. 539).
Federal Trade Commission (2000)	Descriptive	Access Choice Notice Privacy Privacy Seal Security Self-regulation	FIPS (Privacy Online: Fair Information Practices in the Electronic Marketplace) "Because self-regulatory initiatives to date fall far short of broad-based implementation of self-regulatory programs, the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will follow the standards adopted by industry leaders" (p. ii).
Kang et al. (2011)	Exploratory	Personal Data Stream Personal Data Vault Privacy Rights Management	"Instead of direct behavioral regulation or blind faith in the market, our strategy is to modify indirectly the information ecosystem by introducing a new species, the

				[Personal Data Guardian]" (p. 847).
Ohm (2010)	Exploratory		Anonymization Deanonymize Reidentification	"Easy reidentification … undermines decades of assumptions about robust anonymization, assumptions that have charted the course for business relationships, individual choices, and government regulations…. This Article offers the difficult but necessary way forward: Regulators must use the factors provided to assess the risks of reidentification and carefully balance these risks against countervailing values" (p. 1776).
Schwartz and Solove (2011)	Exploratory		Identifiable Personal Information Identified Personal Information Unidentifiable Personal Information	"PII 2.0 protects information that relates either to an identified or identifiable person, and associates different legal interests with each category" (p. 1894).
Sweeney (1997)	Descriptive	53,033 Voter Records	μ-Argus System Datafly System Scrub System	"What is needed is a rational set of disclosure principles, based on comprehensive analysis of the

	fundamental issues, which are unlikely to evolve from piecemeal reactions to random incidents" (p. 108).

Social Engineering (SE)

SE "is a combination of techniques used to manipulate victims into divulging confidential information or performing actions that compromise security" (Luo et al., 2013, p. 2). It has been possible to group the SE literature into three main streams: attack vectors (Heartfield & Loukas, 2015; Hong, 2012; Jakobsson, 2016), defense (Conteh & Schmick, 2016; Mouton et al., 2016; Tetri & Vuorinen, 2013), and the human component (Atkins & Huang, 2013; Krombholz et al., 2013; Luo et al., 2013; Mitnick & Simon, 2002; Workman, 2007). Supporting documentation provides statistics and information as to the number of reported events and the average cost to the victims (Federal Bureau of Investigation, 2015a, 2016). Occasionally, the details of a specific attack are released via the media providing insight into the phenomena (Federal Bureau of Investigation, 2016; Franceschi-Bicchierai, 2015), but this is not the norm as organizations are unwilling to share specifics (Mouton et al., 2016).

The literature typically associates persuasion, deception and exploitation with SE (Harl, 1997; Workman, 2007). Mitnick and Simon (2002) used the elaboration likelihood model to outline SE attack construction, whereas Allen (2006) contrasted the SE attack with the software development cycle. Krombholz et al. (2013) introduced a SE taxonomy. Mouton et al. (2014) crafted a SE ontology and discussed the composition of a

satisfactory definition, though limiting their own contribution to requiring computer technology. Mouton et al. (2016) provided templates that facilitate SE mitigation and assessment.

Greening (1996) conducted an experiment by which SE was used to obtain valid passwords from many of their 175 student participants. Orgill et al. (2004) used an "auditor" to determine the level of effort necessary to retrieve username and password information through a SE attack. The auditor did not work at the company, though he gained access, dressed similar to their computer department, found a name badge, and then collected usernames and passwords via conversations while walking through the building (Orgill et al., 2004). Hasle et al. (2005) performed a phishing experiment to determine the level of resistance to SE for each of the 120 participants using automation via the Web and email.

Allen (2006) introduced a four-step SE model: information gathering, relationship development, exploitation, execution. Peltier (2006) divided SE into two categories: technology-based and human-based, as well as applied social psychology to SE in the area of persuasion. Peltier (2006) found that gender played a significant role in the SE success. Workman (2007) conducted an empirical study of 588 participants using a questionnaire and observation grounded in threat assessment theory as well as the elaboration likelihood model. Workman (2007) found that trust, friendliness and perceived authority were contributing factors for successful SE attacks. Workman (2008) used cognitive dissonance theory and reactance theory to find how specific personality types can fall prey to SE attacks. Bilge et al. (2009) described the use of automated systems for cloning a social network profile from a single social networking site or across

multiple services. Bilge et al. (2009) defeated 215 CAPTCHAs and extracted information from approximately 6000 Web pages and 40,000 profiles each day – culminating with the contact information of five million people as well as the complete profile of 1.2 million people. Bilge et al. (2009) opted to stop their crawlers due to far surpassing their expectations, though they appear to have been able to continue indefinitely.

Chitrey et al. (2012) described the typical motivations for SE attacks: access to proprietary information (30%), financial gain (23%), competitive advantage (21%), enjoyment (11%), revenge (10%), and other (5%). Hong (2012) provided an overview of the composition and execution of phishing, an SE attack vector. Almomani et al. (2013) provided a literature survey of how detection of phishing emails occurs. Atkins and Huang (2013) codified 100 phishing emails and 100 advanced-fee emails into persuasion categories as well as triggers. Atkins and Huang (2013) found the primary triggers and persuasion techniques used in SE were those that grabbed the attention of target or asked them to verify their account credentials.

Luo et al. (2013) described effective defenses against SE relying heavily on security policy as well as presented an argument that a correlation may exist between personality types and vulnerability to SE. Tetri and Vuorinen (2013) conducted a literature review of 40 journal articles, thereby suggested improvements in research quality and found that very few SE articles were empirical, while the majority were descriptive. Johnston et al. (2015) measured compliance with company policy via an enhanced fear appeal grounded on protection motivation theory and found that informal sanctions provide sufficient influence to raise awareness of security defensiveness. Neupane et al. (2015) conducted a three-dimensional study of phishing detection and warnings. Neupane et al. (2015) found

personality types are significant to the success of SE phishing attacks and that people do not spend enough time looking at emails, subsequently failing to detect phishing attacks.

Conteh and Schmick (2016) provided a literature review of phishing research and suggested that repetition in training may improve detection of fake emails and Web sites. Heartfield and Loukas (2015) discussed semantic SE attacks, intentional manipulation of graphical representations to deceive the recipient, and provided a taxonomy to break an attack down to its base components to allow for faster defense through policy, training, and technology systems. Jakobsson (2016) described the compositing and execution of BEC. Mouton et al. (2016) presented attack templates to provide a methodology to apply other frameworks to SE research.

Mitnick and Simon (2002) brought the human component of SE into a mainstream discussion between technical experts and decision makers with a collection of examples easily understood and communicated by both groups. The idea of the human component being the weakest link continues with researchers looking to internal characteristics and external influences contrasted against specific SE attack vectors (Fan et al., 2017). Heartfield and Loukas (2015) proposed the need for investigating methodologies to mitigate risk associated with user weakness as well as provided a mechanism to measure user susceptibility to SE, thereby extending the SE attack cycle put forth by Mitnick and Simon (2002). Additionally, the literature has found gender and psychological traits to have significance in successful SE attacks, which is of particular interest to RQ4 (Neupane et al., 2015; Peltier, 2006; Workman, 2008).

The SE literature is primarily explorative and descriptive with very few theoretical or empirical works (Tetri & Vuorinen, 2013). Much of the effort thus far, is a narrow after-

the-fact examination of a specific SE attack vector, which may or may not generalize into further research or application (Luo et al., 2013; Mouton et al., 2016; Tetri & Vuorinen, 2013). The literature describes how the simple act of looking at a phishing email for more than a few seconds is enough for the user to accept it as authentic (Neupane et al., 2015; Wenyin et al., 2005). Systems such as BLADE, CANTINA+, and JSAND can be used to filter the harmful effects of phishing emails and BEC (Heartfield & Loukas, 2015), but have little effect on the face-to-face persuasions that the literature indicates people have trouble detecting (Perloff, 2010; Workman, 2007, 2008).

The SE domain has a few noted issues: generalizability (Heartfield & Loukas, 2015; Mouton et al., 2016), applicability (Neupane et al., 2015; Tetri & Vuorinen, 2013; Wenyin et al., 2005), and polarization (Conteh & Schmick, 2016; Junger et al., 2017; Luo et al., 2013; Mitnick & Simon, 2002). Generalization is a major issue in the SE literature in that little is known on who is conducting the SE attack (Heartfield & Loukas, 2015), where exactly the information was obtained (Mouton et al., 2016), or how many times the vector and information were successfully used (Jasper, 2017). The entire attack cycle is specific to the context defined by the persuasion, vector, and susceptibility of the target (Heartfield & Loukas, 2015; Mitnick & Simon, 2002).

The applicability of SE research may have limited effect between contexts as Neupane et al. (2015) noted the significance of personality type has on the success of an attack. Additionally, Tetri and Vuorinen (2013) suggested that functional dimensions of an SE attack are more important than the vector by which it occurred. Polarization within the SE domain is observed when contrasting the literature that stated there is no protection from SE (Conteh & Schmick, 2016; Junger et al., 2017) with those providing

insight into the phenomena by providing a means to investigate and measure (Heartfield & Loukas, 2015; Luo et al., 2013; Mitnick & Simon, 2002; Mouton et al., 2016).

The literature coalesces on the following assumption: SE attacks are continually increasing in number (Federal Bureau of Investigation, 2015a; Heartfield & Loukas, 2015; Hong, 2012; Tetri & Vuorinen, 2013; Workman, 2008) and the benefit of research has been minimal (Jasper, 2017; Junger et al., 2017; Luo et al., 2013; Mouton et al., 2016). A summary appears in Table 6 of the social engineering literature referenced in this section.

Table 6

Summary of Social Engineering Literature

Study	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Allen (2006)	Descriptive		The Cycle: Information Gathering Developing Relationship Exploitation Execution	"[T]here will always be the possibility of the 'human factor' being influenced by a social, political and/or cultural event" (p. 9).
Almomani et al. (2013)	Survey		Authentication techniques Client-side tools and filters Network-level protection Server-side filters and classifiers User Education	"This survey improves the understanding of the phishing emails problem, the current solution space, and the future scope to filter phishing emails" (p. 2087).

Atkins and Huang (2013)		100 advanced-fee emails 100 phishing emails	Incentives Persuasion techniques Triggers	"[A]lert/warning/attention and account verification were the two primary triggers used to raise the attention of e-mail recipients…. This study also discovered that social engineers have constructed statements in positive and negative manners to persuade readers to fall victim to their scams" (p. 30).
Bilge et al. (2009)	Descriptive	Used iCloner to clone the profiles of five people. The system then contacted 705 distinct people. This process continued until over one million people had their profiles completely exposed.	Captcha defeat iCloner Scoring system to determine if multiple accounts on a social media network belong to the same person.	"In this paper, we investigate how easy it would be for a potential attacker to launch automated crawling and identity theft (i.e., cloning) attacks against five popular social networking sites. We present and experimentally evaluate two identity theft attacks" (p. 560). A very high percentage of those contacted from cloned accounts click on "friend" requests.
Chitrey et al. (2012)	Questionnaire	90 responders located in India	Internet Security Awareness Program and Training	Provides data that infers that culturally, people in India have an elevated weakness level to SE attacks. New employees, customers, and IT professionals are the

				most likely targets of SE.
Conteh and Schmick (2016)	Review			"[W]hile technology has a role to play in reducing the impact of social engineering attacks, the vulnerability resides with human behaviour [sic], human impulses and psychological predispositions that can be influenced through education" (p. 37).
Fan et al. (2017)	Exploratory		I-E based model of human weakness for social engineering investigation Psychological states	"We captured two essential levels – [fourteen] internal characteristics of human nature and [nine] external circumstance influences - that shape the human weakness for social engineering" (p. 10).
Federal Bureau of Investigation (2015a)	Report	7,000 companies	business email compromise	"According to IC3, since the beginning of 2015 there has been a 270 percent increase in identified BEC victims" (p. 2).
Federal Bureau of Investigation (2016)	Report		State-sponsored actors	State-sponsored cyber threats (Iran).
Franceschi-Bicchierai (2015)	News Article			Describes the attack on CIA Director by teenagers.
Greening (1996)	Simulation of a large-scale SE attack	338 students over 16 days.		Students continued to respond to the e-mail, even after the students were given a second email and formal

		175 responded to a phishing e-mail 138 of the responses were valid passwords		announcement of the phishing exercise. Very few [61] people attempted to report the attack, and the majority [49] of those complaints were only curious.
Harl (1997)	Editorial		Early work describing SE and the human as the weakest link.	"Contrary to popular belief, it is often easier to hack people than [S]endmail. But it takes far less effort to have employees who can prevent and detect attempts at social engineering than it is to secure any [U]nix system" (p. 5).
Hasle et al. (2005)	Experiment	120 users separated into four groups of 30 over three days. 59 people were active in that they completed a survey [31] or were presented with a login box [28].	Social Engineering Resistance Metric	"Our experiment shows that it is relatively cheap and easy to mount a large scale [sic] SE attack (or experiment) with a high success rate" (p. 141).
Heartfield and Loukas (2015)	Taxonomy	Discusses research with 1900 malicious URLs, 308	Deception vector Exploitation Execution	"It introduces a structured baseline for classifying semantic attacks by breaking

12 citations		users, and other	Orchestration	them down into their components" (p. 0:31).
Hong (2012)	Descriptive			"Phishing also causes new problems for organizations, as they blur traditional security perimeters. One's lawyers and accountants may be attacked to surreptitiously gain access to documents. Facebook and other social media provide more contextual details that can be used for spear-phishing attacks. An employee falling for a phish in one context may cause a headache for your organization because of reused passwords" (pp. 6-7).
Jakobsson (2016)	Case-studies in chapter format			"The best way to develop and deploy ways to identify and measure the problem and how it changes is to identify not only what the scammers do, but also why…. Understanding why the scammers do what they do, we must also understand their intended victims, what they do—and fail to do" (p. 126).

Jasper (2017)	Review			Discusses Cyber Threat Intelligence Integration Center. "Therefore, the timely sharing of relevant and actionable cyber threat intelligence, in the context of cyber threat information and indicators, is imperative to reducing the impact of attacks" (p. 62).
Johnston et al. (2015)	Sequential mixed-methods Qualitative via interviews Quantitative via experimental design	Potential: 2,475 insiders Complete responses from 559 insiders of multiple organization within a city government Four organizational leaders were interviewed.	Compliance intention Conventional fear appeal Perceived threat Severity Perceived threat susceptibility Perceived self-efficacy Perceived response efficacy Fear Appears Formal sanction certainty Formal sanction severity Information sanction certainty Informal sanction severity Protection motivation theory	"We argue that the reason for these disappointing results [in fear appeals research in information security] from the inadequacy of the conventional fear appeal rhetorical framework and the misspecification of [protection motivation theory] within the information security literature… This study develops and tests an enhanced fear appeal rhetorical framework that accounts for the distinction between threats to information assets and threats to human assets" (p. 130). The enhanced fear appeal framework

			Sanction celerity	
Junger et al. (2017)	Experiment	278 participants	Age Age Square Goals System Theory Priming Total Risk Warning	"This study found relatively high disclosure rates… Neither priming nor a warning influenced the degree of disclosure." (p. 85).
Krombholz et al. (2013)	Taxonomy		Channel (How) Operator (What) Social Engineering Taxonomy Type	"[W]e introduced a comprehensive taxonomy to classify social engineering attacks with respect to the attack channel, the operator, different types of social engineering and specific attack scenarios" (p. 34).
Luo et al. (2013)	Descriptive		Personality traits Psychological aspects Social engineering Techniques Defenses	"in addition to advanced technologies counterattacking various security intrusions, human factors must be equally accounted for" (p. 7).
Mitnick and Simon (2002)	Descriptive			Brought social engineering into the mainstream. Social engineering attack cycle
Mouton et al. (2016)	Descriptive		Theory of Group Conformity SE attack	Neither the literature or news media provide all the information concerning an attack.

			Goal Medium Social engineer Target Compliance principles Techniques SE framework Preparation Information gathering Attack formation Exploit relationship Develop relationship Debrief	Usually little, if any, information is known about a potential attack. Little is known as to where the information is obtained for a SE attack. Little is known as to what information is available for a SE attack. Social engineering attack detection model
Neupane et al. (2015)	Experiment	25 participants Malware test (20 randomized trials) -10 warning -10 non-warning -Phishing detection (37 randomized trials) -13 real -12 fake	Gaze durations Number of fixations	"[O]ur results showed that users do not spend enough time looking at key phishing indicators and often fail at detecting these attacks, although they may be highly engaged in the task and subconsciously processing real sites differently than fake sites" (p. 489).

		-12 difficult fake		
Orgill et al. (2004)	Questionnaire	32 participants -26 gave their username -19 gave their password -Seven gave login credential informatio n above their own access -Four asked for a name badge or identificati on	Department Number Surveyed Password Username	"This study demonstrated that even in a company where security is a concern, these human traits [trust others, assist others, gain favor] can be ill-used if proper preventative measures are not taken … This study also shows the importance of assessing security effectiveness through means such as audits.… In order for an audit to be effective, the auditor has to be at least as thorough, through preliminary studying, planning, and execution as a potential social engineer would be" (p. 181). Some departments had more training and resisted the social engineer better.
Peltier (2006)	Review			Magazine article describing SE to readers.
Perloff (2010)	Exploratory		Persuasion	Extensive discussion on persuasion, which is used in many SE attack vectors.
Tetri and Vuorinen (2013)	Descriptive		Actor-Network Theory	Describes issues in SE research and suggests the theories from the psychology literature should only be applied

				to the persuasion component of SE.
Wenyin et al. (2005)	Exploratory	Eight Phishing Web pages Six Attacked true Web pages 320 authentic home pages of banking institutions	Phishing Visual Similarity Between Two Web Pages -block level -layout -overall style Web page segmentation	"Preliminary results show that our approach can successfully detect the phishing webpages [sic] with few false alarms for online use" (p. 1061).
Workman (2007)	Field study - Questionnaire - Observation	588 participants from a single organization	Affective Commitment Continuance Commitment Normative Commitment Obedience Reactance Subjective Behaviors Threat Severity Trust Vulnerability	Elaboration likelihood model Threat assessment theory "[W]e found that people who are high in normative commitment feel obligated to reciprocate social engineering gestures and favors such as receiving free software or gift certificates by giving up company email addresses, employee identification numbers, financial and insurance data, and other confidential and sensitive information… people who are high in continuance commitment tend to provide information to escalating requests… High affective commitment was also

				found to contribute to successful social engineering" (pp. 327-328). Everyone is susceptible to SE to some degree.
Workman (2008)	Field Study	588 participants from a single U.S. organizatio n	Control for Age, Gender, and Education	"Our investigation has attempted to bridge the theory that explains how people are persuaded through peripheral routes with the social engineering outcomes using an empirical field study in which we investigated whether the factors that account for how people are persuaded in marketing campaigns to make purchases may apply as well to social engineering to give up confidential information" (p. 10).

Theory of Mind (TOM)

The theoretical foundation for this research draws on the Theory Of Mind (TOM). Herbsleb (2005) called for external theories to be used to bring greater understanding to computer science, specifically in software design research. While communicating complex concepts, software designers use anthropomorphic examples, which TOM research indicates is problematic for autistic people (Herbsleb, 2005). The context of the TOM is that an individual "imputes mental states to himself and others" (Premack & Woodruff, 1978, p. 515). Baron-Cohen et al. (1985) stated, "The ability to make inferences about what other people believe to be the case in a given situation allows one

to predict what they will do" (p. 39). Likewise, an individual does not have a TOM when he does not recognize the state of mind of another individual he is interacting with (Premack & Woodruff, 1978). For example, if two people are standing next to the water cooler and one tells a joke, the other person can only have TOM if they perceive the exchange as a joke (Baron-Cohen, 1997). TOM has been used to study chimpanzees (Premack & Woodruff, 1978), children (Baron-Cohen, 1997), autism (Leslie, 1987), and normal adults (Krombholz et al., 2013; Saxe et al., 2006). TOM also offers multiple ingresses into this research study: pretense, representation, pretending, and deception (Baron-Cohen, 1992; Leslie, 1987). Pretense is the intentional distortion of reality (Leslie, 1987), which is used in SE during phishing and other attacks (Mitnick & Simon, 2002). Representation is how an individual views the world (Leslie, 1987).

Workman (2007) described how an individual's representation of an actor might provide trust during a SE attack, even though facts do not fit the reality. Pretending occurs when someone acts as if one thing is real, when he knows that it isn't (Leslie, 1987), which can be observed in many SE attack vectors (Marczak & Paxson, 2017; Tetri & Vuorinen, 2013). Deception involves making someone believe an untruth (Baron-Cohen, 1992) and serves as the primary tool of SE and semantic attacks (Heartfield & Loukas, 2015; Mitnick & Simon, 2002).

Kennedy et al. (2001a) supposed that TOM might have inadvertently crept into academia when researchers superimpose their assumptions and abilities to their participants. In the literature, TOM is also used to describe an inability to understand the anthropomorphic descriptions used by software engineers to communicate complex abstract concepts during daily communication, such as a section of code "knowing,"

“seeing,” or “dying” (Herbsleb, 2005). Kennedy et al. (2001a) warned that academics should not mistakenly assume a TOM with ordinary people, as not everyone has been trained to seek out explanations for phenomena methodically nor do they embody the expertise of the researcher. Krombholz et al. (2013) noted that the TOM of IS is not shared or even valued by SE attackers, while being used as a weapon against the knowledge workers themselves (Krombholz et al., 2013).

TOM literature endeavors to observe the mind with the understanding that mental states can allow the explanation and prediction of the behavior of others (Premack & Woodruff, 1978). While TOM tends to observe the persuasion (conviction, belief) of a subject, much of SE literature describes the use of persuasion (Mitnick & Simon, 2002; Mouton et al., 2016; Tetri & Vuorinen, 2013) in the commission of attacks. Both SE and TOM literature describe how poorly people detect deception (Krombholz et al., 2015; Luo et al., 2013; Mitnick & Simon, 2002; Workman, 2008). For example, Saxe et al. (2006) empirically found that participants answering questions concerning a deceptive instrument demonstrated a slower response (mean 2.89 seconds) than false belief questions (mean 2.63 seconds).

The relevance of using TOM as a lens for SE research is supported by Luo et al. (2013), O'keefe (2002), and Peltier (2006). Luo et al. (2013) called for research to investigate how SE attacks can occur due to user participation with OSPI made readily available via social networking sites, thereby empowering deception. Peltier (2006) described the creation of a TOM so that all employees within an organization understand their significance in cyber defense. Keysar et al. (2003) argued that adults fail to associate the beliefs of someone and their actual behavior correctly. O'keefe (2002) suggested that

research move beyond linguistic persuasion and on to visual instruments, such as an instrument that measures exposure to SE, i.e., SEXI, as well as those seen in BEC, phishing, and other SE attacks. A summary appears in Table 7 of the literature referenced in this section.

Table 7

Summary of Theory of Mind Literature

Study	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Baron-Cohen et al. (1985)	Experiment	61 Children -20 Autistic -14 Down Syndrome -27 Clinically normal	Wimmer and Perner's puppet play paradigm	"The fact that every single child taking part in the experiment correctly answered the control questions allows us to conclude that they all knew (and implicitly believed) that the marble was put somewhere else after Sally had left" (p. 42). "We therefore conclude that the autistic children did not appreciate the difference between their own and the doll's knowledge" (p. 43). The ability to know and believe

				something is separate from having a TOM.
Heartfield and Loukas (2015)	Taxonomy	Discusses research with 1900 malicious URLs, 308 users, and other	Deception Exploitation Execution Orchestration Vector	"It introduces a structured baseline for classifying semantic attacks by breaking them down into their components" (p. 0:31).
Herbsleb (2005)	Exploratory		Behavioral Science Computer Science Interdisciplinary Multidisciplinary	"As a field we have benefited enormously from our borrowings from behavioral science…. We need to continue in this strong interdisciplinary path, and … nurture our own theoretical tradition" (p. 26).
Kennedy et al. (2001a)	Review		Gestalt psychology Suggest an assumed theory of mind amongst researchers.	Provides an overview of the study of the mind.
Keysar et al. (2003)	Two Experiments	38 College students 40 College students (20 male / 20 female)	False belief Hidden object Ignorance	"[T]he ability to take the conceptual perspective of the other is an indispensable element in the fully-developed adult theory of mind. Our findings show that adults do not reliably consult this crucial

			knowledge about what others know when they interpret what others mean" (p. 37).
Krombholz et al. (2013)	Taxonomy	Social engineering taxonomy Channel (How) Operator (What) Type	"[W]e introduced a comprehensive taxonomy to classify social engineering attacks with respect to the attack channel, the operator, different types of social engineering and specific attack scenarios" (p. 34).
Leslie (1987)	Exploratory	Decoupling model of pretense Metarepresentational theory Pretend Pretense Representation	"[T]he view advanced here offers for the first time a principled explanation for both the peculiarities of pretense and for the existence of these generalizations" (p. 424).
Luo et al. (2013)	Descriptive	Social engineering Psychological aspects Personality traits Techniques Defenses	"in addition to advanced technologies counterattacking various security intrusions, human factors must be equally accounted for" (p. 7).

Marczak and Paxson (2017)	Interviews	30 participants associated with the Middle East and Horn of Africa over two years	Government surveillance Perception of Risk	"Despite the availability of free online tools to check links and attachments, our subject population does not appear to widely use such resources" (p.162).
Mitnick and Simon (2002)	Descriptive			Brought social engineering into the mainstream. Social engineering attack cycle
Mouton et al. (2016)	Descriptive		Theory of Group Conformity SE attack -Compliance Principles -Goal -Medium -Social Engineer -Target -Techniques SE Framework - Attack Formation -Debrief -Develop Relationship -Exploit Relationship -Preparation Information Gathering	Neither the literature or news media provide all the information concerning an attack. Usually little, if any, information is known about a potential attack. Little is known as to where the information is obtained for a SE attack. Little is known as to what information is available for a SE attack.

O'keefe (2002)	Review		Attitudes Normative Considerations Self-Efficacy	"Systematic thought about processes of persuasion can be traced back to the ancient Greeks, but as these developments attest, the study of persuasion continues to be a locus of exciting theoretical, empirical, and methodological developments" (p. 40).
Peltier (2006)	Review			Magazine article describing SE to readers.
Premack and Woodruff (1978)	Experiment	Chimpanzee	Problem comprehension	"In assuming that other individuals want, think, believe, and the like, one infers states that are not directly observable and one uses these states anticipatorily, to predict the behavior of others as well as one's own. These inferences, which amount to a theory of mind, are, to our knowledge, universal in human adults" (p. 525).

Saxe et al. (2006)	Experiment	12 participants	fMRI brain scans Belief > Photo Stories (for TOM) Incompatible > Compatible response selection Overlap of TOM and Response	"Although they were given the same physical stimuli, and made the same correct responses, when subjects construed their task in terms of belief attribution, they responded faster, and selectively recruited an additional brain region than in the control task" (p. 294). "We found a striking lack of overlap in the brain regions implicated in executive control (specifically response selection and inhibition) and in ToM tasks" (p. 296). TOM (belief attribution) uses entirely different areas of the brain than response selection.
Tetri and Vuorinen (2013)	Descriptive		Actor-network theory	Describes issues in SE research and suggests the theories from the psychology literature should

				only be applied to the persuasion component of SE.
Workman (2007)	Field study -Questionnaire - Observation	588 participants from a single organization	Affective Commitment Continuance Commitment Normative Commitment Obedience Reactance Subjective Behaviors Threat Severity Trust Vulnerability	Elaboration likelihood model Threat assessment theory "[W]e found that people who are high in normative commitment feel obligated to reciprocate social engineering gestures and favors such as receiving free software or gift certificates by giving up company email addresses, employee identification numbers, financial and insurance data, and other confidential and sensitive information… people who are high in continuance commitment tend to provide information to escalating requests… High affective commitment was also found to

				contribute to successful social engineering" (pp. 327-328).
Workman (2008)	Field Study	588 participants from a single U.S. organization	Control for age, gender, and education	"Our investigation has attempted to bridge the theory that explains how people are persuaded through peripheral routes with the social engineering outcomes using an empirical field study in which we investigated whether the factors that account for how people are persuaded in marketing campaigns to make purchases may apply as well to social engineering to give up confidential information" (p. 10).

Summary of What is Known and Unknown

A review of various aspects of SE and personal information was conducted to provide a foundation for this study. Through this review of the literature, the constructs of exposure, personal information, and TOM were identified as they relate to social

engineering. The literature review describes what is known and unknown about the constructs in this research study. Research regarding SE extended across fields including IS, psychology, law, and business.

SE continues to plague organizations in increasingly alarming amounts (Acquisti et al., 2015; Bélanger & Crossler, 2011). Much of the research into the SE phenomena is primarily explorative and descriptive with limited theoretical or empirical works (Tetri & Vuorinen, 2013; Workman, 2007, 2008). Researchers described efforts thus far as narrow examination of limited details related to a specific SE attack vector, which may or may not generalize into further research or application (Luo et al., 2013; Mouton et al., 2016; Tetri & Vuorinen, 2013). SE literature has offered taxonomy (Heartfield & Loukas, 2015), templates (Mouton et al., 2016), examples of actual attacks (Dadkhah & Quliyeva, 2014; Federal Bureau of Investigation, 2015a, 2016; Krombholz et al., 2013) and occasional empirical research (Neupane et al., 2015; Workman, 2007, 2008).

SE and TOM literature describe how poorly people detect deception (Krombholz et al., 2015; Luo et al., 2013; Saxe et al., 2006; Workman, 2008). In response, the SE literature has called for a mechanism to provide some level of insight into the available information, which can be weaponized into a cyber attack (Heartfield & Loukas, 2015; Mouton et al., 2016; Peer & Acquisti, 2016; Tetri & Vuorinen, 2013). The privacy literature describes the availability of OSPI via social networks (Acquisti et al., 2015; Greenwood et al., 2016), credit bureaus (Sanders, 2012), personalization (Chellappa & Sin, 2005; Xu et al., 2011), and simple mining programs (Russell, 2013). Similarly, Schwartz and Solove (2011) postulated the enhanced definition of PII to differentiate PUI

and PDI would “provide different regimes of regulation for each … standard” (p. 1877) “by considering the applicability of FIPs [Fair Information Practices]” (p. 1879).

TOM is a theory from the psychology literature, which is used to observe the mind with the understanding that mental states can allow the explanation and prediction of the behavior of others (Leslie, 1987; Premack & Woodruff, 1978). Herbsleb (2005) described the unexpected properties of cognitive abilities within computer science where people can fumble through simple tasks while easily completing complicated ones. The literature also indicates that certain personality types (Workman, 2008) and genders are more susceptible to SE (Peltier, 2006). Neupane et al. (2015) found that the possibility of a successful phishing event significantly increased if the target was sleep deprived, distracted, or simply looked at the instrument too long.

The literature has called for an understanding of what information is available and how it can be weaponized into SE attack vectors (Heartfield & Loukas, 2015; Mouton et al., 2016). Disappointingly, the SE literature has not provided the return on the investment originally hoped for (Conteh & Schmick, 2016; Heartfield & Loukas, 2015). Little is known as to the availability of information used in SE or how said information is obtained and weaponized into attack vectors (Luo et al., 2013; Mouton et al., 2016). Though researchers discussed security policy at length (Acquisti et al., 2016; Bishop & Gates, 2008; Parrish & Nicolas-Rocca, 2012), more research is required to understand the effect of organizational security training on the type and amount of OSPI shared by users in their personal lives (Anderson & Agarwal, 2010; Boss et al., 2015; Tetri & Vuorinen, 2013). Additionally, little is known as to the specificity of available OSPI (Heartfield & Loukas, 2015; Mouton et al., 2016) and the level of exposure that information poses

(Oltmann, 2010). The effects of TOM on the exposure of personal information are also largely not understood (Herbsleb, 2005; Tetri & Vuorinen, 2013).

The constructs of exposure (Keane et al., 1989; Youssef et al., 2013), personal information (Schwartz & Solove, 2011), and TOM (Leslie, 1987) were identified as they relate to SE. Very limited research has explored these constructs within a single study. Therefore, additional research is warranted to examine exposure, personal information, and TOM to determine their contribution to SE.

This research assessed the SE exposure of 100 individuals. The advent of social media, personalization and other technologies has facilitated the exponential increase of available personal information (Acquisti et al., 2015; Mitnick & Simon, 2002). Social engineers have access to OSPI, and a growing concern in SE literature is that the information is being weaponized into SE attack vectors (Heartfield & Loukas, 2015; Mouton et al., 2016; Tetri & Vuorinen, 2013). Because of this phenomenon, users may be exposing themselves and inadvertently the organization that employs them. Therefore, assessing the exposure, personal information, and TOM of individuals may provide a better understanding of SE.

Chapter 3

Methodology

Introduction

The purpose of this chapter is to detail the research methods used in this study. This research study was classified as developmental research. Richey and Klein (2005) stated, "It is not uncommon for a developmental research project to also utilize multiple research methodologies and designs, with different designs again being used for different phases of the project" (p. 31). This research study comprised a literature review, expert panel feedback via the Delphi method, and quantitative data collection.

Ellis and Levy (2009) stated, "developmental research attempts to answer the question: How can researchers build a 'thing' to address the problem? It is especially applicable when there is not an adequate solution to even test for efficacy in addressing the problem" (p. 328). Salkind (2012) stated that a benefit of developmental research is that it can:

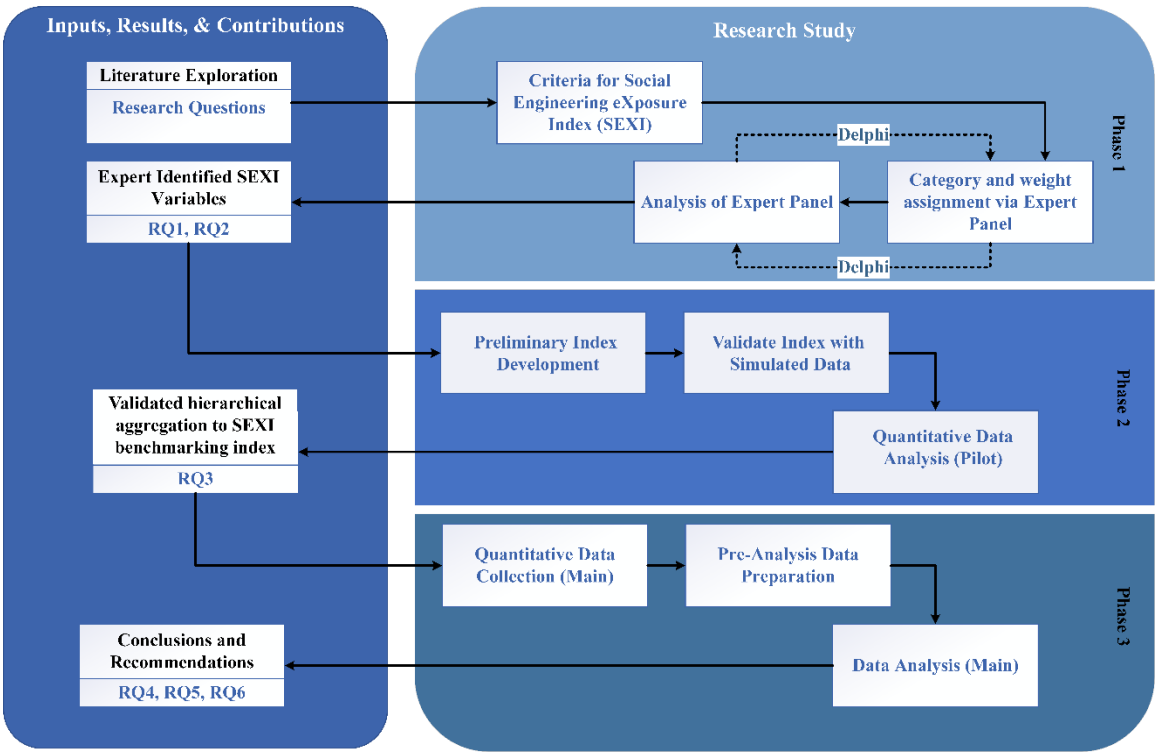
> Describe a particular phenomenon in a way that communicates the overall picture of whatever is being studied. Although these methods do not allow the luxury of implying any cause-and-effect relationship between variables, their use provides the tools needed to answer questions that are otherwise unanswerable. (p. 210)

Richey and Klein (2005) stated, "Developmental research seeks to create knowledge grounded in data systematically derived from practice… In addition, it is a way to establish new procedures, techniques, and tools based upon a methodical analysis of specific cases" (p. 24).

According to Ellis and Levy (2009), developmental research involves three components: 1) criteria establishment and validation, 2) formal development via accepted process, and 3) determination of criteria satisfaction. Richey and Klein (2005) maintained that developmental research is comprised of a literature review, a Delphi method, and instrument / tool validation. This research study follows the precedence of the body of knowledge with a literature review, Delphi method, and instrument validation to satisfy the Ellis and Levy (2009) three components of developmental research. Figure 4 illustrates the design of this research study.

Figure 4

The SEXI three phase development research design



Prior research has utilized a literature review to better understand the information privacy literature (Pavlou, 2011), privacy in the digital age (Bélanger & Crossler, 2011),

and the privacy literature through an interdisciplinary lens (Smith et al., 2011). In this research, a literature review was performed to ascertain the candidate components of personal information as well as to determine a gap requiring further study. Richey and Klein (2005) stated, “In developmental research the conceptual framework for the study may be found in literature from actual practice environments (for example, an evaluation report) as well as from traditional research literature directed toward theory construction” (p. 29). A gap was discovered, in that little is known as to the SE attack composition, available personal information, or potential attack vectors (Heartfield & Loukas, 2015; Luo et al., 2013; Mouton et al., 2016; Tetri & Vuorinen, 2013).

For this research study, a literature review provided candidate components of personal information for consideration in the SEXI benchmarking instrument, named herein as Personal Information Candidate Components (PICCs). Table 8 illustrates the contextuality and ambiguity of personal information described previously in the literature (Culnan, 1993; Solove, 2006). Table 8 also presents the PICCs categorized as PUI, PII, PDI, or generalized in accordance with the respective source and provides the respective label that will be used for analysis. The information presented in Table 8 is based on source definition and usage. For example, Schwartz and Solove (2011) placed an item in multiple categories due to context, while McCallister et al. (2010) designated some items as capable of identifying a unique individual and others as not contributing to identification – while categorizing all as PII.

Table 8

PICCs by Source with Page Numbers

Label	Item	PUI	PII	PDI	Generalized
PC001	Acceleration via personal tracking				Kang (814)
PC002	Account numbers		McCallister (ES-1)	McCallister (2-2)	PCI DSS (7)
PC003	Activities (daily life)		McCallister (ES-2)		
PC004	Age	Schwartz (1824)	McCallister (A-3)		
PC005	Agency seal / Organizational logo				FIPS 201 (29)
PC006	Alias		McCallister (ES-1)		
PC007	Area code		McCallister (ES-2)		
PC008	Audit log of user actions		McCallister (2-1)		
PC009	Biometric records (retina, iris, voice signature, facial geometry, facial recognition)		McCallister (ES-1)	McCallister (2-1)	FIPS 201 (44) Martin (68)
PC010	Bluetooth connections to other devices				Kang (816)
PC011	Calorie counting with images of food				Kang (815)
PC012	Cardholder name				PCI DSS (7)
PC013	Cell phone number		McCallister (2-2)		
PC014	Cell tower location				Kang (816)
PC015	Credit card account number		McCallister (ES-1)	Schwartz (1848) McCallister (2-2)	PCI DSS (7)

PC016	Credit card CAV2 / CVC2 / CVV2 / CID				PCI DSS (7)
PC017	Card expiration date				FIPS 201 (27) PCI DSS (7)
PC018	Credit card pin				PCI DSS (7)
PC019	Credit card service code				PCI DSS (7)
PC020	Credit score	McCallister (2-1)			
PC021	Criminal history		McCallister (B-1)		
PC022	Date of birth	Schwartz (1842)	McCallister (ES-2)	McCallister (2-1)	Acquisti (511)
PC023	Demographics	Sweeney (104)			HIPAA (89)
PC024	Driver's license [number]		McCallister (ES-1)	FIPS 201 (9) McCallister (2-2)	
PC025	Education information		McCallister (2-1) Schwartz (1822)		
PC026	Electricity usage				Kang (840) Martin (68)
PC027	Electronic facial image / Selfie		McCallister (ES-1)	McCallister (2-2)	FIPS 201 (39)
PC028	E-mail address		McCallister (ES-1) Schwartz (1857)		
PC029	Employee identification			McCallister (A-1)	
PC030	Employment history		McCallister (B-1)		
PC031	Employment information		McCallister (ES-2)		
PC032	Family income	Schwartz (1851)			
PC033	Favorite movies	Schwartz (1851)			
PC034	Favorite restaurants	Schwartz (1851)			
PC035	Favorite television shows	Schwartz (1851)			
PC036	Financial records / information, balances		McCallister (ES-2)	Schwartz (1882)	
PC037	Fingerprints		McCallister (ES-1)		FIPS 201 (6)

PC038	Fingerprints of two fingers				FIPS 201 (6)
PC039	Full name		McCallister (ES-1) Schwartz (1864)	McCallister (2-1) Schwartz (1848)	Schwartz (1830)
PC040	Full set of fingerprints				FIPS 201 (6)
PC041	Gender	Schwartz (1842)	McCallister (4-5)		Acquisti (513)
PC042	Genetic information	Schwartz (1845)			Kang (840)
PC043	Geographical indicators (location, i.e., city name, latitude, longitude, etc.)		McCallister (ES-2)		
PC044	Global Positioning Systems (GPS)				Kang (840) Martin (68)
PC045	Handwriting		McCallister (ES-1)		
PC046	High school name				Acquisti (511)
PC047	Holographic images (on identification)				FIPS 201 (23)
PC048	Host-specific persistent static identifier (system / host name, etc.)		McCallister (2-2)		
PC049	IP address (network location of a network device; dynamic / fixed)	Schwartz (1838)	McCallister (2-2) Schwartz (1839)		PCI DSS (12) Schwartz (1818)
PC050	Laser etches (on identification)				FIPS 201 (23)
PC051	License plate				Martin (68)
PC052	MAC address (hardware ID of network device)		McCallister (2-2)		
PC053	Maiden name		McCallister (ES-1)	McCallister (2-2)	
PC054	Marital status	Schwartz (1851)			
PC055	Medical history		McCallister (2-2)		
PC056	Medical information	Schwartz (1845)	McCallister (ES-2)		

PC057	Medical test results		McCallister (2-2)		
PC058	Mental health	Schwartz (1824)			HIPAA (89)
PC059	Mother's maiden name		McCallister (ES-1)	McCallister (2-1)	
PC060	Nationality		McCallister (A-3)		
PC061	Newsletter subscription		McCallister (ES-3)		
PC062	Organization affiliation / membership	Schwartz (1851)			FIPS 201 (27)
PC063	Owned property (Mortgage, vehicle Registration, title)	Schwartz (1851)		Schwartz (1882)	
PC064	Parent's middle name		McCallister (3-3)		
PC065	Partner(s) Name		McCallister (3-3)		Acquisti (510)
PC066	Passport number		McCallister (ES-1)	FIPS 201 (9) McCallister (2-1)	
PC067	Password		McCallister (B-4)		PCI DSS (76)
PC068	Patient identification Number			McCallister (2-2)	
PC069	Payment for healthcare				HIPAA (89)
PC070	Persistent Identifier (customer number held in cookie, processor serial number, alphanumeric identifier)		Schwartz (1832)	Schwartz (1855)	
PC071	Personal heart-rate meter				Kang (814)
PC072	Photographic image		McCallister (2-2)		Acquisti (512)
PC073	Physical health				HIPAA (89)
PC074	Place of birth		McCallister (ES-2)	McCallister (2-1)	
PC075	Place of sensing moment				Kang (814)
PC076	Political views		McCallister (3-3)		Acquisti (510)

PC077	Professional title		McCallister (3-5)		
PC078	Provision of healthcare				HIPAA (89)
PC079	Race		McCallister (ES-2)		
PC080	Rank				FIPS 201 (28)
PC081	Recent purchases	Kang (825) Schwartz (1851)		Kang (825) Martin (71)	
PC082	Religion		McCallister (ES-2)		
PC083	Salary information		McCallister (2-2)		
PC084	Search engine query (miscellaneous to vanity)	Schwartz (1847)	Schwartz (1848)	Schwartz (1848)	Acquisti (510)
PC085	Sexual fantasy / behavior		McCallister (3-3)		Acquisti (513) Moon (336)
PC086	Sexual orientation		McCallister (3-3)		Acquisti (510)
PC087	Signature (digital)				FIPS 201 (40)
PC088	Signature (handwritten)				FIPS 201 (28)
PC089	Social media profile				Acquisti (509)
PC090	Social Security Number		McCallister (ES-1) Schwartz (1864)	FIPS 201 (9) McCallister (2-1) Schwartz (1824)	
PC091	Status updates		McCallister (2-1)		Kang (815)
PC092	Street address		McCallister (ES-1)		Schwartz (1830)
PC093	Tax records		McCallister (3-3)		
PC094	Taxpayer identification number		McCallister (ES-1)	McCallister (2-2)	
PC095	Telephone number		McCallister (2-2)		
PC096	Location / Time of sensing moment (self-surveillance via smartphone, fitness device)				Kang (814)
PC097	Timestamp of Web page visit		McCallister (3-3)		
PC098	Uniform Resource Locator (URL) of last Web page		McCallister (3-6)		

PC099	Unique health identifier			HIPAA (191)
PC100	User identification		McCallister (4-8)	
PC101	Web browser history	Schwartz (1858)		
PC102	Weight		McCallister (ES-2)	
PC103	Work phone		McCallister (2-2)	
PC104	X-Rays		McCallister (2-2)	
PC105	ZIP Code	Schwartz (1842)	McCallister (ES-3)	

1

The Delphi method has been used to bring clarification, definition, and an enhanced understanding of complex problems, such as the one posed in this research study. The Delphi method has been used to refine a measure of resistance behavior (Rivard & Lapointe, 2012) and to identify information and communication technologies research issues (Lee, 2016). Dalkey and Helmer (1963) provided the following characteristics of the Delphi method, "Its object is to obtain the most reliable consensus of opinion of a group of experts. It attempts to achieve this by a series of intensive questionnaires interspersed with controlled opinion feedback" (p. 458). Delphi research typically consists of anonymity, iteration, controlled feedback, and an aggregated response (von der Gracht, 2012). This research followed the literature by soliciting cybersecurity experts to participate in a Delphi method involving multiple rounds of surveys, thereby providing feedback. Specifically, this research assessed the feedback of the SMEs for the purpose of designing the SEXI benchmarking instrument (Ramim & Lichvar, 2014).

For this research, the stop criteria for the Delphi study triggered if over 75% of SME responses on PICC identification as one of the DNA, PUI, PII, or PDI across all items in a single round (von der Gracht, 2012). A second stop condition triggered if there is 15% or less change in the categorization of all the PICCs between two consecutive rounds, thereby reaching stability (Dajani et al., 1979; von der Gracht, 2012). Consensus for this Delphi study was defined as 75% for the PICC items presented to the SMEs with a 1 – 10 scale, as shown in Appendix C, and 80% for items presented to SMEs by exposure category, as shown in Appendix D (Diamond et al., 2014; von der Gracht, 2012). Following Fitch et al. (2001), "the two-round process is designed to sort" the PICCs into three categories of exposure (p. 5). Schwartz and Solove (2011) declared, "Despite the

importance of the concept of PII to privacy law and regulation, there remains a lack of consensus in the United States about how to define it. All current legal models for this concept are flawed" (p. 1835). Therefore, this research developed an instrument to measure exposure due to OSPI. Any PICC placed within the same personal information category: PDI, PII, or PUI by at least 75% of SMEs were included in the SEXI benchmarking instrument. Items not reaching consensus were accessed on an individual basis.

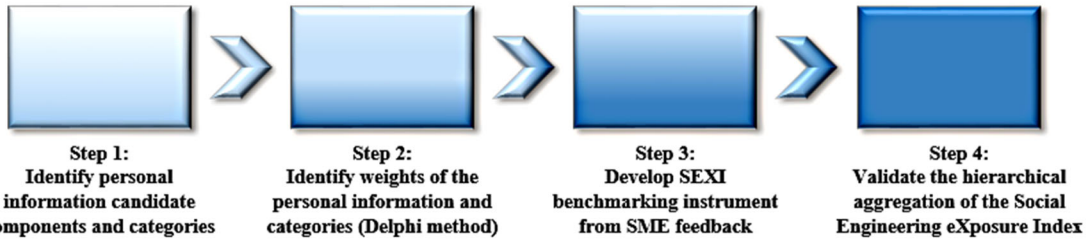
The main RQ that this study addressed was: What are the expert-approved required components comprising an index of exposure to social engineering attacks due to OSPI? Richey and Klein (2005) stated:

> research questions, rather than hypotheses, commonly serve as the organizing framework for developmental studies. This tactic is appropriate if there is not a firm base in the literature that one can use as a basis for formulating a hypothesis…, especially if the problem focuses on emerging technologies (p. 27).

This research study comprises six RQs, with RQ1, RQ2, and RQ3 seeking the development of the SEXI benchmarking instrument, while RQ4, RQ5, as well as RQ6 focus on validation. Figure 5 illustrates the primary steps of the Delphi method in this research.

Figure 5

The Delphi method process culminating in instrument validation



Four steps were required to conduct the Delphi portion of this research. The first step involved a review of the literature to ascertain PICCs that were presented to SMEs for them to assess the level of exposure for each component. PICCs with the median SME score of ≤ 1 are designated as not being personal information, those in the 1 – 3 range are categorized as PUI, those in the 4 – 8 range as PII, and those in the 9 – 10 range as PDI. Table 9 presents the classifications of each exposure category.

Table 9

Classification of Exposure Categories for SME Round 1 Feedback

Category	Exposure Level	Low Threshold	High Threshold
DNA	Does Not Apply	0	≤ 1
PUI	Unidentifiable	> 1	≤ 3
PII	Identifiable	≥ 4	≤ 8
PDI	Identified	≥ 9	≤10

The second step was to facilitate iterations of the Delphi method using Internet surveys presenting the PICCs to SMEs for assessment and feedback. Survey Monkey hosted the surveys and functioned as the data collection platform, while providing the expert panel anonymity. Appendix C presents the first-round survey instrument to be administered to the panel of experts collecting information concerning the work environment, demographic information, and SEXI assessments from the SMEs.

The second survey, presented in Appendix D, provided the results of the first survey to the SMEs seeking their agreement. This cycle continued until a stop criterion was triggered, thereby ending the Delphi process and Phase 1 (see Figure 4). Step 3 and Phase 2 began with the construction of the SEXI benchmarking instrument, based on feedback from the SMEs. The contributions of the SMEs were assessed and reported to address RQ1, RQ2, and RQ3.

The second phase operationalized a SEXI using OSPI. To answer RQ4, this study attempted to measure the exposure of 50 Fortune 500 executives and 50 Hollywood personas to SE due to OSPI. Data collection used the SME prescribed SEXI instrument to track the existence of each personal information indicator found, while not collecting any personal information. Appendix E illustrates the data collection instrument that was used to measure the exposure of the executives and personas. Once all data collection was completed, the second phase concluded. The final phase involved the analysis and reporting of the data to answer RQ4, RQ5, and RQ6.

The Delphi method allows this study to perform quantitative assessments of the SEXI instrument (Creswell, 2012). However, little discernable literature existed at the time of this research addressing exposure to SE due to OSPI. This study first sought to understand the phenomena. This study was descriptive in that it endeavors to collect data that describes characteristics of personal exposure using candidate components of personal information, placed into three categories defined herein as PUI, PII, or PDI.

Research Methods

This study used a developmental research approach comprising three phases. Van den Akker et al. (2012) stated, developmental research involves the development of a

prototypical product and “generating methodological directions for the design and evaluation of such products” (p. 4). According to Ellis and Levy (2009), developmental research is “applicable when there is not an adequate solution to even test for efficacy in addressing the problem and presupposes that researchers don’t even know how to go about building a solution that can be tested” (p. 328). Ellis and Levy (2009) concluded that “developmental research attempts to answer the question: How can researchers build a ‘thing’ to address the problem?” (p. 328). Ellis and Levy (2009) described developmental research as consisting of three components, with the first, “establishing and validating criteria the product must meet” (p. 328). Reviewing and establishing the criteria of SEXI from the literature on this topic met this component. Second, “follow a formalized, accepted process for developing the product” (Ellis & Levy, 2009, p. 326). This second component was satisfied by creating a set of criteria from literature to be used to develop the SEXI benchmarking instrument. The third component is “subjecting the product to a formalized, accepted process to determine if it satisfies the criteria” (Ellis & Levy, 2009, p. 326). The third component was satisfied by the expert panel evaluating SEXI by way of assessing PICCs obtained from literature review and identifying the significance of each criterion as PDI, PII, or PUI. The relative importance of each criterion within each measure, along with a relative importance of the measures, were aggregated to develop the SEXI instrument.

The expert panel was elicited from the official information security groups and organizations via official social media venues. Cybersecurity experts who took part in the study were presented with OSPI properties (i.e., last name, social security number, etc.) and their suggested categories, obtained from the literature review from Acquisti et al.

(2015), Ferraiolo et al. (2013), “HIPAA” (1996), Kang et al. (2011), Martin (2015), McCallister et al. (2010), Moon (2000), Schwartz and Solove (2011), as well as Sweeney (1997) (see Table 8). The first survey began the information privacy iterations by presenting 105 PICCs from the literature to the SMEs. The expert panel was asked to assign exposure ratings to each personal information indicator as well as exposure categories. The second survey asked the SMEs to categorize the SME-suggested personal information indicators as well as evaluate those items designated during the first survey as not belonging to personal information. At the conclusion of phase one, phase two began with the development of the SEXI instrument based on SME feedback (Ellis & Levy, 2009).

The first phase (see Figure 4) addressed RQ1 and RQ2, with the development and evaluation of the SEXI benchmarking instrument to be used to assess 50 executives of Fortune 500 companies and 50 Hollywood personas (a group under constant exposure) via an expert panel using the Delphi expert methodology. Clayton (1997) maintained that group size for Delphi panels should be between 15 – 30 for experts if they share a common discipline and 5 – 10 if they do not necessarily form a statistical population. The expert panel was elicited from academia and practitioners holding industry certification.

This study used two surveys. The first survey (see Appendix C) facilitated an understanding of the composition of the panel of experts and presented the initial PICCs as well as collected work environment, background, demographic information, while eliciting feedback on the PICCs from the SMEs. The second survey (see Appendix D) presented the results of the first survey to the SMEs, eliciting their agreement with the assessments of the panel expert during the first round.

These surveys ensured the requirements for this study are met. The first requirement was that each member of the panel of experts shares a TOM. This requirement was met by evaluating the cybersecurity experience and work environment of the SMEs (see Appendix C). The second requirement was an extensive background. This requirement was met by ensuring respondents have experience in information privacy. The third requirement of this study was that the participants fit within the context of U.S. privacy considerations. This requirement was met by ensuring each SME has at least one industry-accepted certification. Responses for any panel member not meeting these requirements were excluded.

In phase two of this research, RQ3 addressed the development of the instrument based on the categorization and weight of PICCs feedback of the SME as well as data collection on a random selection of 50 Fortune 500 executives and 50 Hollywood personas. The SEXI benchmarking instrument was used to collect data from OSPI sources on 100 individuals denoting the existence, not specifics, of personal information in publicly accessible venues (see Appendix E). Table 10 presents the collection of anonymized data indicating if the specified information was found and an indicator of where it was found (i.e., FB = Facebook, LN = Linkedin, GS = Google Search).

Table 10

Data Collection Methodology of Personal Information Participant

Source	Identifier	DOB	Home Address	Postal Code	Picture	Gender
GS	F001-C3	0	1	1	0	0
FB	F001-C3	1	0	0	1	1
LN	F007-C1	1	1	0	1	1
GS	F002-C4	1	1	1	0	1

Phase three of this research study included both the pre-analysis data screening and the data analysis from the data collected using the SEXI benchmarking instrument (see Figure 4). The results of the data analysis were used to assess 100 individuals and develop comparison reports addressing RQ4, RQ5, and RQ6. The comparison report included graphical representation where appropriate, i.e., from the SEXI aggregation, etc. RQ6 may be of interest as it compares the SEXI of Hollywood persons with the SEXI of executives of Fortune 500 companies with privacy, risk management, and cybersecurity implementations.

Instrument and Measures

Instruments

This research study followed the developmental methodology in pursuit of a SEXI. This research elicited responses from an expert panel to assess the validity of criteria content, identify measures, and establish weight allocations based on three sub-measures, each ranging from 0.0 to 1.0: the Measurement of Personally Distinguishable Iinformation (PDIM), the Measurement of Personally Identifiable Information (PIIM), and the Measurement of Personally Unidentifiable Information (PUIM) (McCallister et al., 2010; Schwartz & Solove, 2011).

Two instruments used in this study are supported by literature via a review that found an excess of 105 PICCs in articles by Acquisti et al. (2015), Ferraiolo et al. (2013), “HIPAA” (1996), Kang et al. (2011), Martin (2015), McCallister et al. (2010), Moon (2000), Schwartz and Solove (2011), as well as Sweeney (1997) (see Table 8). To reduce the number of items presented to the SMEs, identical measures, i.e., demographics from any source (Sweeney, 1997) and demographics created by or for a healthcare professional

("HIPAA", 1996), were consolidated as demographics. The set of PICCs offered to the SMEs totaled 105, which is presented in Table 8.

The first instrument collected the assessments of 105 PICCs from a panel of experts via a Delphi method eliciting their opinion on the level of exposure of an individual due to a particular PICC, in and of itself. The respective assessments of each SME identified each PICC as PDI, PII, PUI, DNA, or UNF. In addition, the SMEs were asked to suggest items that are currently not represented in the list of 105 PICCs. The aggregate assessments of the SMEs provided the initial weights and categories of each PICC. Following Fitch et al. (2001), the SMEs were presented each PICC on a scale of 1 to 10, where "1" means minimum exposure of an individual due to the item and "10" means maximum exposure of the individual as the item identifies them. A middle rating of "5" denotes a potential of identification in the PICC. The 1-10 scales were treated as ordinal scales, and as such, the median of the responses from the SMEs were used rather than the mean (von der Gracht, 2012). This is primarily due to the inability to define the distance between points (Linstone & Turoff, 1975). The SMEs rated the PICCs at least twice via a Delphi method. Subsequent rounds were added as necessary to reach a consensus on each PICC. Linstone and Turoff (1975) discussed similar usage of the Delphi method "to identify and estimate linear weights for those aspects of experience, which they judged to be important in determining the quality of life or sense of well-being of an individual" (p. 383). This study differs from the Delphi study described by Linstone and Turoff (1975) as in that study, the initial 200-300 components were based on the feedback of SMEs, while this research presents 105 PICCs to SMEs from the literature review and elicits additional PICCs from the panel of experts. Following the Delphi study described by Linstone and

Turoff (1975), this research sought to cluster a large list of components into those having a similar trait (i.e., exposure level). The findings from the Delphi study described by Linstone and Turoff (1975) "indicated that group relative importance ratings produce reasonable ratio scales, and that the reliability of such judgments across randomly selected groups is high" (p. 383).

The second instrument presented the aggregate groupings of the first instrument to the SMEs. The median values were used to assign categories to the PICCs, as shown in Table 9. The items in the second instrument were presented via a nominal scale grouped by SME-identified categories (e.g., DNA, PDI, PII, PUI), thereby providing a mechanism for each expert to consider each PICC amongst items in the same category. The SME suggested items from the first instrument were placed with the PICCs in the category suggested (e.g., DNA, PDI, PII, PUI) and presented to the SMEs. Appendix D provides the second instrument.

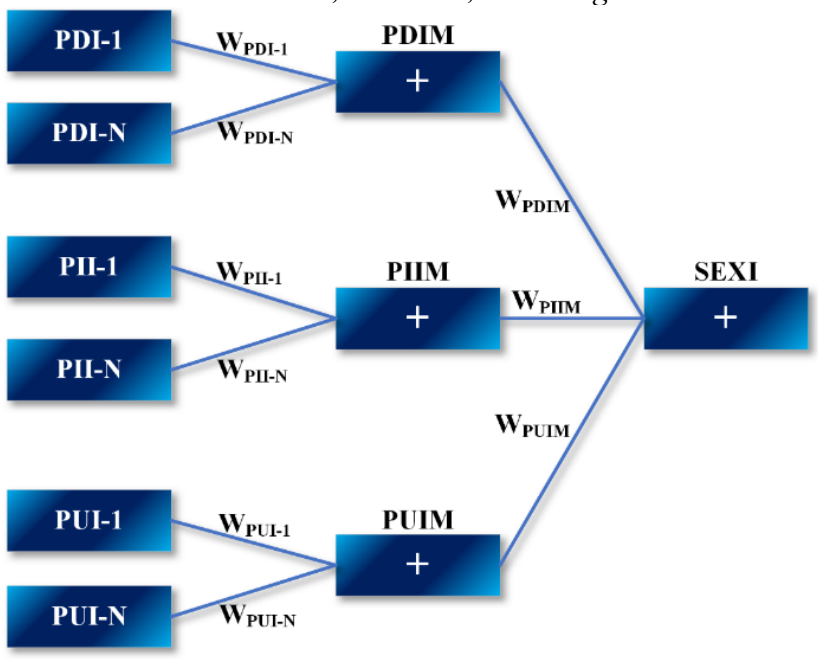
Measures

The intent of this research was to develop a single index value (SEXI) that is representative of the exposure to SE due to OSPI, as measured by PUI, PII, PDI. Three primary measurements were used to identify each, in and of itself, PICC: PDI – *definitively* identify someone, PII – the *potential* of identifying a specific individual, and PUI – having no chance to identify an individual on its own. Two additional non-instrument measurements were used: the first to designate items the SMEs identify for removal from the lists collected via literature review as not applying to personal information (DNA), as well as a second to designate items as not being familiar to the respective expert panel member (UNF). A 1-10 scale was used to assess the exposure of

each PICC, where "1" indicated minimum exposure and "10" represented maximum exposure. A middle rating of "5" indicated the item had the potential to identify an individual. PICCs with the median SME score of "0" were designated as not being personal information, those in the 1 – 3 range were categorized as PUI, those in the 4 – 8 range as PII, and those in the 9 – 10 range as PDI (see Table 9). The SME-approved value for each PICC served to indicate its component weight. The measurement of each category (i.e. PDIM, PIIM, PUIM) was the total of the sum of its components multiplied by the SME-identified category weight. Figure 6 illustrates the hierarchical structure from the three measures.

Figure 6

The SEXI hierarchical structure: index, measures, and categories



The SME responses were used to assess 50 executives of Fortune 500 companies and 50 Hollywood personas by measuring the criteria established by the expert panel. Following Eom and Paek (2009), SEXI is calculated with an additive linear model. The

subsequent equations indicate the computations to be used in the constructs as well as the summation.

Table 11 presents the PICCs designated as Personally Distinguishable Information Components (PDIC). Equation 1 presents the PDIM where *i* = the number of PICCs categorized as PDI, and PDIM is calculated by multiplying the SME-indicated weight by the existence of a PDIC.

$$PDIM = \sum_{i=1}^{n} \mathrm{PDI_i} = \sum_{i=1}^{n} \mathrm{w_i PDIC_i} \quad (1)$$

$$PDIM = \sum_{i=1}^{12} \mathrm{w_i PDIC_i}$$

$$= \left(\frac{1}{32.528}\right)[(2.806 \cdot \mathrm{PDIC_1}) + (2.639 \cdot \mathrm{PDIC_2}) + (2.639 \cdot \mathrm{PDIC_3})$$

$$+ (2.639 \cdot \mathrm{PDIC_4}) + (2.722 \cdot \mathrm{PDIC_5}) + (2.944 \cdot \mathrm{PDIC_6})$$

$$+ (2.694 \cdot \mathrm{PDIC_7}) + (2.694 \cdot \mathrm{PDIC_8}) + (2.611 \cdot \mathrm{PDIC_9})$$

$$+ (2.639 \cdot \mathrm{PDIC_{10}}) + (2.806 \cdot \mathrm{PDIC_{11}}) + (2.694 \cdot \mathrm{PDIC_{12}})]$$

$$0 \leq PDIM \leq 1$$

Table 11

Expert Panel Designated Personally Distinguishable Information Components

Identifier	Designation	Description
PIC009	PDI001	Biometric records
PIC015	PDI002	Credit card account number
PIC021	PDI003	Criminal history
PIC024	PDI004	Driver's license [number]
PIC027	PDI005	Electronic facial image / selfie
PIC040	PDI006	Full set of fingerprints
PIC042	PDI007	Genetic information

PIC066	PDI008	Passport number
PIC072	PDI009	Photographic image
PIC087	PDI010	Signature Digital
PIC090	PDI011	Social Security Number
PIC093	PDI012	Tax records

Table 12 presents the PICCs designated as Personally Identifiable Information Components (PIIC). Equation 2 presents the PIIM where *i* = the number of PICCs categorized as PII and PIIM is calculated by multiplying the SME-indicated weight by the existence of a PIIC.

$$PIIM = \sum_{i=1}^{n} \mathrm{PII_i} = \sum_{i=1}^{n} \mathrm{w_i PIIC_i} \tag{2}$$

$$PIIM = \sum_{i=1}^{57} \mathrm{w_i PIIC_i}$$

$$= \left(\frac{1}{124.45}\right)[(2.278 \cdot \mathrm{PIIC_1}) + (1.917 \cdot \mathrm{PIIC_2}) + (1.917 \cdot \mathrm{PIIC_3}) + \cdots$$

$$+ (2.028 \cdot \mathrm{PIIC_{55}}) + (1.972 \cdot \mathrm{PIIC_{56}}) + (1.806 \cdot \mathrm{PIIC_{57}})]$$

$$0 \leq PIIM \leq 1$$

Table 12

Expert Panel Designated Personally Identifiable Information Components

Identifier	Designation	Description
PIC002	PII001	Account numbers
PIC003	PII002	Activities
PIC006	PII003	Alias
PIC008	PII004	Audit log of user actions
PIC010	PII005	Bluetooth connections to other devices
PIC012	PII006	Cardholder name

PIC013	PII007	Cell phone number
PIC014	PII008	Cell tower location
PIC016	PII009	Credit card CAV2 / CVC2 / CVV2 / CID
PIC022	PII010	Date of birth
PIC023	PII011	Demographics
PIC025	PII012	Education information
PIC028	PII013	E-mail address
PIC029	PII014	Employee identification
PIC030	PII015	Employment history
PIC031	PII016	Employment information
PIC036	PII017	Financial records / information, balances
PIC037	PII018	Fingerprints
PIC038	PII019	Fingerprints of two fingers
PIC039	PII020	Full name
PIC043	PII021	Geographical indicators
PIC044	PII022	Global Positioning Systems (GPS)
PIC045	PII023	Handwriting
PIC047	PII024	Holographic images
PIC048	PII025	Host-specific persistent static identifier
PIC049	PII026	IP address
PIC051	PII027	License plate
PIC052	PII028	MAC address
PIC053	PII029	Maiden name
PIC055	PII030	Medical history
PIC056	PII031	Medical information
PIC057	PII032	Medical test results
PIC058	PII033	Mental health
PIC059	PII034	Mother's maiden name
PIC062	PII035	Organization affiliation / membership
PIC063	PII036	Owned property
PIC065	PII037	Partner(s) name
PIC067	PII038	Password
PIC068	PII039	Patient identification number
PIC069	PII040	Payment for health care
PIC070	PII041	Persistent Identifier
PIC074	PII042	Place of birth
PIC077	PII043	Professional title
PIC081	PII044	Recent purchases

PIC084	PII045	Search engine query
PIC088	PII046	Signature Handwritten
PIC089	PII047	Social media profile
PIC092	PII048	Street address
PIC094	PII049	Taxpayer identification number
PIC095	PII050	Telephone number
PIC096	PII051	Location / Time of sensing moment
PIC099	PII052	Unique health identifier
PIC100	PII053	User identification
PIC101	PII054	Web browser history
PIC103	PII055	Work phone
PIC104	PII056	X-Rays
PIC105	PII057	ZIP Code

Table 13 presents the PICCs designated as Personally Unidentifiable Information Components (PUIC). Equation 3 presents the PUIM where *i* = the number of PICCs categorized as PUI and PUIM is calculated by multiplying the SME-indicated weight by the existence of a PICC.

$$PUIM = \sum_{i=1}^{n} \mathrm{PUI_i} = \sum_{i=1}^{n} \mathrm{w_i PUIC_i} \tag{3}$$

$$PUIM = \sum_{i=1}^{36} \mathrm{w_i PUIC_i}$$

$$= \left(\frac{1}{58.33}\right)[(1.778 \cdot \mathrm{PUIC_1}) + (1.722 \cdot \mathrm{PUIC_2}) + (1.694 \cdot \mathrm{PUIC_3}) + \cdots$$

$$+ (1.750 \cdot \mathrm{PUIC_{34}}) + (1.722 \cdot \mathrm{PUIC_{35}}) + (1.583 \cdot \mathrm{PUIC_{36}})]$$

$$0 \leq PUIM \leq 1$$

Table 13

Expert Panel Designated Personally Unidentifiable Information Components

Identifier	Designation	Description
PIC001	PUI001	Acceleration via personal tracking
PIC004	PUI002	Age
PIC005	PUI003	Agency seal / Organizational logo
PIC007	PUI004	Area code
PIC011	PUI005	Calorie counting with images of food
PIC017	PUI006	Card expiration date
PIC018	PUI007	Credit card pin
PIC019	PUI008	Credit card service code
PIC020	PUI009	Credit score
PIC026	PUI010	Electricity usage
PIC032	PUI011	Family income
PIC033	PUI012	Favorite movies
PIC034	PUI013	Favorite restaurants
PIC035	PUI014	Favorite television shows
PIC041	PUI015	Gender
PIC046	PUI016	High school name
PIC050	PUI017	Laser etches
PIC054	PUI018	Marital status
PIC060	PUI019	Nationality
PIC061	PUI020	Newsletter subscription
PIC064	PUI021	Parent's middle name
PIC071	PUI022	Personal heart-rate meter
PIC073	PUI023	Physical health
PIC075	PUI024	Place of sensing moment
PIC076	PUI025	Political views
PIC078	PUI026	Provision of health care
PIC079	PUI027	Race
PIC080	PUI028	Rank
PIC082	PUI029	Religion
PIC083	PUI030	Salary information
PIC085	PUI031	Sexual fantasy / behavior
PIC086	PUI032	Sexual orientation
PIC091	PUI033	Status updates
PIC097	PUI034	Timestamp of Web page visit
PIC098	PUI035	Uniform Resource Locator (URL) of last Web page
PIC102	PUI036	Weight

Equation 4 presents a single index value (SEXI) that is representative of the exposure to SE due to OSPI as measured by the sum of PDIM, PIIM, and PUIM each multiplied by their respective SME-indicated category weight.

$$\text{SEXI} = (\text{W}_{\text{PDI}}PDIM) + (\text{W}_{\text{PII}}PIIM) + (\text{W}_{\text{PUI}}PUIM) \quad (4)$$

$$\text{SEXI} = (50.21 \cdot PDIM) + (34.47 \cdot PIIM) + (15.32 \cdot PUIM)$$

$$0 \leq SEXI \leq 100$$

Validity and Reliability

An expert panel evaluated the candidate components of SEXI, following a Delphi technique, derived from prior pertinent literature that described personal information where an individual is unidentifiable, identifiable, and identified (McCallister et al., 2010; Schwartz & Solove, 2011). The PICCs were presented to the SMEs in a 10-point Likert scale, ranging from 1 (PUI) to 10 (PDI). Items identified as not applying to personal information (DNA) were reported and removed from the SEXI benchmarking instrument. Feedback from an expert panel using the Delphi expert methodology provided a weighted value to each item (Ramim & Lichvar, 2014). The instrument used to evaluate SEXI for each executive utilized nominal scores indicating if exposure was found with a true or false status (Bhattacherjee, 2012; Cohen, 1960). Finally, the TOM of the SMEs were assessed using nominal and Likert scales to evaluate the privacy practices implemented by SMEs to ensure each meets the requirements of this study (Anderson & Agarwal, 2010; Chellappa & Sin, 2005).

The recruitment of SMEs was not limited to a single type of industry or government to avoid expert panel bias associated with the topic of privacy. Privacy has existed in the literature for centuries (Pavlou, 2011) and preconceptions may have been formed by organizational policy (Mouton et al., 2016), legal mandates dictating behaviors and activities of organizations (Culnan & Williams, 2009; FIPS 199, 2004; McCallister et al., 2010; Ross et al., 2006), as well as industry expectations (Barker, 2013; PCI Security Standards Council, 2016; Ryan & Loeffler, 2010). Tversky and Kahneman (1975) as well as Lewis (2017) discussed additional bias that may affect expert panels: significance assumed by familiarity, relative significance, imagined significance, and significance associated with frequency. To combat these potential expert panel bias, the list of construct items was combined and alphabetized before their consideration.

Validity and reliability were addressed in this research by eliciting the feedback from an expert panel to verify and establish weights used for each item in the first instrument (Ramim & Lichvar, 2014). Mortality is due to participant attrition, subsequently changing the group composition before the study is completed (Salkind, 2012) and is a threat when Delphi expert methodology is used, so a minimum of 15 respondents is necessary for each survey (Clayton, 1997). Testing bias was not a threat as no pre-test was administered (Salkind, 2012; Sekaran & Bougie, 2013). To establish instrument validity for this study the content and constructs were evaluated (Sekaran & Bougie, 2013) and feedback from the panel of experts was solicited for ensuring SEXI is accurately measuring the exposure to SE (Sekaran & Bougie, 2013; Straub et al., 2004; Straub, 1989). External validity was addressed in that this study is not using a contrived setting, thereby being increasingly generalizable (Bhattacherjee, 2012; Sekaran & Bougie, 2013).

Institutional Review Board (IRB) approval was obtained prior to any data collection or Delphi iteration. Appendix A presents the IRB approval letter. The SEXI benchmarking instrument had the potential to acquire PII for each participant via OSPI. This research did not collect any such information. The purpose of this study was not to collect personal information, but to evaluate the SEXI for each participant. Any personal information obtained through this study was destroyed.

Sample

This research sought the consensus of 35 SMEs, which satisfies the requirement of the literature of 15 – 30 (Clayton, 1997). The resulting instrument was used to assess the SEXI of 50 top executives of organizations from multiple industries and 50 Hollywood personas using convenience sampling from information gathered via OSPI. Creswell (2012) stated, "in convenience sampling the researcher selects participants because they are willing and available to be studied" (p. 167). Sekaran and Bougie (2013) suggested for sample sizes to be between 30 and 500 for most research and noted that the sample size should be at least 10 times the number of variables under investigation.

Pre-analysis Data Screening

Mertler and Reinhart (2013) stated pre-analysis screening is mandatory and should be conducted before statistical analysis. The survey questions used an online research medium (see Appendices C & D), while the SEXI benchmarking instrument used found/not found nomenclature (see Appendix E). The results were examined multiple times for accuracy via Statistical Package for the Social Sciences (SPSS®) (Mertler & Reinhart, 2013). The proper actions were taken for outliers, missing data, and other anomalies (Mertler & Reinhart, 2013).

Data Analysis

Data analysis was conducted on each data set. Four types of data analysis were performed: Factorial Analysis of Variance (ANOVA), frequencies and percentages, chi-square tests of independence, as well as *t*-test between groups (Mertler & Reinhart, 2013). Data aggregation was addressed by providing each participant with a unique identifier that was used to validate the individual's entry. Following Linstone and Turoff (1975), the following sections served to document and report on each Delphi round. Equation 5 presents the function used to covert the Round 1 personal information exposure responses to the corresponding personal information category assigned by the SMEs in Round 2 as defined in Table 9.

$$([\text{10-point scale value}] * 0.2) + 1 \; = \text{Exposure Category } [\text{PDI, PII, or PUI}] \qquad (5)$$

Summary

This chapter provided an overview of the methodology used during this developmental research. This design science study used an approach involving quantitative methods to develop and validate a SEXI using OSPI to assist in identifying and classifying SE vulnerabilities. Internet access was required as it served to interact with SMEs, conduct surveys, develop the benchmarking instrument, access OSPI, and to host the secure Website to aggregate as well as assess 50 executives of Fortune 500 companies and 50 Hollywood personas.

Surveys were facilitated by the use of Survey Monkey. The SEXI benchmarking instrument used in this research was developed in Microsoft Excel. Data analysis was performed by using Microsoft Excel version 2008 and transferred to IBM SPSS version 26 for analysis.

Chapter 4

Results

Overview

This chapter presents the results of the developmental study and includes an analysis of the data collection processes as well as the statistical methodology. First, the expert panel composition, feedback, consensus, and PICC assignment to the three categories of personal information (PDI, PII, & PUI) will be presented. This is followed by a discussion on the SEXI data collection, pre-analysis, and analysis. The chapter concludes with a summary of the results of the use of the SEXI benchmarking instrument, the process used for data analysis, and the presentation of the specific findings for each RQ.

Expert Panel

Appendix C presents the first-round survey instrument administered to the panel of experts collecting information concerning the work environment, demographic information, and SEXI assessments from the SMEs. Round 1 commenced August 2018 and concluded in February 2019. Potential Delphi participants were notified of the extensive size and time requirements to complete the survey and instructed not to begin the survey unless they could finish it. Appendix D presents the second-round survey administered to the SMEs. Round 2 commenced in February 2019 and concluded in April 2019. Potential Delphi participants were notified that the second survey, though smaller than the first survey, required several minutes to complete.

Data Collection and Analysis

For the Delphi rounds of this study, individuals were approached from personal contacts, LinkedIn, Reddit closed privacy groups, and closed information security-related Facebook groups requiring administrative approval for access. The process is documented in Chapter 3. Round 1 had 19 responses having a completion rate of 100%. Round 2 had 17 responses having a completion rate of 90%. First, the backgrounds and biographical composition of SMEs are presented. Second, the work environment privacy context is described. Finally, the SME elicited weights for the various components are presented.

Pre-Analysis Data Screening

Responses from the SMEs were collected using online forms via Survey Monkey. All feedback was exported to Microsoft Excel, tabulated, and reviewed. Responses were reviewed to ensure each response was recorded, complete, and intelligible. No invalid responses were found. Many of the questions provided an open-ended response, thereby removing response-set bias for those respective questions.

IBM SPSS version 26 was used to perform a check for multivariate outliers via Mahalanobis Distance and Box Plots. No multivariate outliers having significance were found. All responses were retained and accepted for analysis. Respondents were coded using three-digit identifiers, with the first representing the survey round and the remaining digits the response number.

Expert Panel Demographics and Composition

The Delphi panel was recruited from a variety of information security professionals via Facebook closed information security and privacy groups, LinkedIn, Reddit closed privacy groups, and contacts. Due to the contextuality of personal information

classification in the literature, a dissimilar group of SMEs was desired. The 11 demographic questions were administered to the SMEs. Table 14 presents a summary of the Delphi Panel demographics with 37% of the participants between 45 and 49 years of age, 47% having a doctorate, 32% being female, and 37% functioning primarily as practitioners. Additionally, approximately half of the SMEs had a military / law enforcement background.

Table 14

Descriptive Statistics of the SMEs (N=19)

Group		Frequency	Percentage
Age			
	25-29	1	5.3%
	30-34	1	5.3%
	40-44	4	21.1%
	45-49	7	36.8%
	50-54	1	5.3%
	55-59	2	10.5%
	60-64	2	10.5%
	65+	1	5.3%
Education			
	Some college, no degree earned	2	10.5%
	Bachelors	2	10.5%
	Masters	6	31.6%
	Doctorate	9	47.4%
Gender			
	Female	6	31.6%
	Male	13	68.4%
Law Enforcement Experience		2	10.5%
Military Background		9	47.4%
Professional Focus			
	Academia	3	15.8%
	Mostly academic, occasional practitioner efforts	3	15.8%
	Evenly between academic and practitioner efforts	3	15.8%
	Practitioner	7	36.8%
	Mostly practitioner, occasional academic efforts	3	15.8%

Table 15 presents a summary of the certifications held by the SMEs, which number approximately three dozen, including several not included in the survey. The Delphi Panel comprised experts having certifications from a variety of specializations, including healthcare, information security, information systems, and the Department of Defense. The CISSP certification was held by 42% of the SMEs along with 26% having the CEH certification.

Table 15

Summary of Certifications Held by Delphi Panel Participants (N=19)

Certification	Number of SMEs Having
[CAP] Certified Authorization Professional	2
[CCENT] Cisco Certified Entry Networking Technician	2
[CCEP] Certified Compliance & Ethics Professional	1
[CCEP-I] Certified Compliance & Ethics Professional-International	1
[CCFE] Certified Computer Forensics Examiner	2
[CCFP] Certified Cyber Forensics Professional	1
[CCNA] Cisco Certified Network Administrator	1
[CEH] Certified Ethical Hacker	5
[CHC] Certified in Healthcare Compliance	1
[CHPC] Certified in Healthcare Privacy Compliance	1
[CISA] Certified Information Systems Auditor	2
[CISM] Certified Information Security Manager	2
[CISSP] Certified Information Systems Security Professional	8
[CRISC] Certified in Risk and Information Systems Control	1
[CSX] Cybersecurity Nexus Certificate	1
DOD Cyber Workforce	1
[GSEC] GIAC Security Essentials Certification, [GCFE] GIAC Certified Forensics Examiner, [GCFA] GIAC Certified Forensic Analyst, [GCIA] GIAC Certified Intrusion Analyst, [GCIH] GIAC Certified Incident Handler, [GASF] GIAC Advanced Smartphone Forensics, [GCCC] GIAC Critical Controls Certification, [GCPM] GIAC Certified Project Manager Certification, [PMP] Project Management Professional	1

[ISSAP] Information System Security Architecture Professional	1
[ISSEP] Information Systems Security Engineering Professional	
[ISSMP] Information Systems Security Management Professional	
[ITIL] IT Infrastructure Library	1
[MTA] Microsoft Technology Associate	1
[Sec+] Security+	2
[SSCP] Systems Security Certified Practitioner	1
No Certifications	3

Table 16 presents a summary of the SMEs' occupational positions and industries. The 19 SMEs selected 16 current occupations and 42 positions across 12 industries. The largest concentration of SMEs was spread across IS/IT Professors and Consultants working in the Government and Information Technology industries. Additional occupations not provided on the survey were provided by the SMEs.

Table 16

Summary of SMEs Occupation(s) (N=19)

Group		Frequency
Occupation		
	Chief Information Officer (CIO)	2
	Chief Information Security Officer (CISO)	2
	Chief Knowledge Officer (CKO)	1
	Chief Privacy Officer (CPO)	1
	Chief Security Officer (CSO)	1
	Compliance and audit	1
	Consultant	8
	Cybersecurity Manager	1
	Cyber Security Engineering	1
	Department of Defense – USAF	1
	Founding Owner	1
	IS/IT Professor	9
	Law Enforcement	1
	Mobile Device Management Backend	1
	Security Manager	1
	Security Specialist	4
Industry		
	Banking & Finance	2
	Consulting	4
	Education	5
	Energy	1

Federal Government – DoD	1
Healthcare	5
Government	11
Information Technology	8
Law Enforcement	1
Manufacturing	1
Not-For-Profit/Non-Profit	1
Retail	2

Table 17 provides a summary of the self-identified experience of the Delphi panel as Cybersecurity professionals. The SMEs were also asked to indicate the years of experience working specifically with information privacy. Over 63% of the SMEs indicated at least 10 years of Cybersecurity experience, while 53% had at least ten 10 years of working with information privacy.

Table 17

Summary of SMEs Cybersecurity and Information Privacy Experience (N=19)

Group	Frequency	Percentage
Years as a Cybersecurity professional		
1-3 years	2	10.5%
4-5 years	2	10.5%
7-9 years	3	15.8%
10-12 years	1	5.3%
13-15 years	5	26.3%
19-21 years	1	5.3%
22+ years	5	26.3%
Years working with information privacy		
1-3 years	2	10.5%
4-5 years	2	10.5%
7-9 years	5	26.3%
10-12 years	1	5.3%
13-15 years	2	10.5%
16-18 years	1	5.3%
19-21 years	1	5.3%
22+ years	5	26.3%

Social Engineering and Personal Information in the Work Environment

The SMEs were asked several questions to ascertain their perception and experience for SE attempts within their work environment, as well as gather their opinion on the implementation of security policy as it relates to privacy and personal information. The majority of the SMEs (79%) had at least seven years of cybersecurity experience working with information privacy.

The objective of the questions was to provide a mechanism to assess the TOM of the panel of experts with regards to the implementation and execution of organizational privacy policy and SE attempts. Table 18 provides a summary of the information security culture of the SMEs' work environments, while Table 19 provides a summary of the work environment consequences of violating privacy policy.

Table 18

Summary SMEs Work Environment: Information Security Culture (N=19)

Question	Mean	Median	Mode
BG01 [Policy] I work for an organization that has a well-defined privacy policy.	5.74	7.00	7
BG02 [TrainingPrivacy] I work for an organization that has mandatory training for privacy.	5.74	7.00	7
BG03 [Consequences] I work for an organization that has consequences for violating the privacy policy.	5.79	6.00	7
BG04 [TrainingSE] I work for an organization that has mandatory social engineering training.	5.37	6.00	7
BG05 [SecurityAudits] I work for an organization that has security audits.	5.79	6.00	7
BG06 [Pretending] I work for an organization that has experienced an attempt to gain access to unauthorized assets through someone pretending to be another individual.	5.79	6.00	7
BG07 [Persuasion] I work for an organization that has experienced an attempt to gain access to unauthorized assets at my organization through persuasion.	5.37	6.00	6

BG08 [AuthorityBypassPolicy] I work for an organization where someone has the authority to bypass policy on a case-by-case basis.	5.00	6.00	6
BG09 [UnauthorizedBypassPolicy] I work for an organization where an employee bypassed policy without authorization.	4.53	5.00	4
BG10 [Repercussion] I work for an organization where an employee bypassed policy without repercussion.	4.00	4.00	4
BG11 [PrivacyVsEfficiency] I work for an organization where employees feel like they must choose between privacy policy and efficiency.	3.84	4.00	2
BG12 [PrivacyCulture] I work for an organization where employees are shown ways to bypass policy by other employees.	2.74	2.00	1

Table 19

Summary SMEs Work Environment: Consequences

Responses	**Frequency**	**Percentage**
BG13 [Consequence] I work for an organization where violating the privacy policy typically results in:		
No Consequence	2	10.5%
Informal Verbal Warning	1	5.3%
Formal Verbal Reprimand	3	15.8%
Written Reprimand	5	26.3%
Temporary Suspension of Duties	2	10.5%
Reassignment	1	5.3%
Termination / Legal Issues	5	26.3%

Delphi Round 1

In Round 1, the panel of experts was elicited for their opinion on the level of exposure of an individual due to a particular PICC, in and of itself. Table 9 established the thresholds for each category using a 10-point Likert scale. Table 20 presents the conversion and transformation of Round 1 responses to the three personal information categories based on the thresholds set forth in Table 9.

Table 20

Conversion of Round 1 Responses to Round 2 Exposure Categories

10-point scale	Conversion	Category	Category Transformed
0	1	DNA	0
1	1.2	PUI	1
2	1.4	PUI	1
3	1.6	PUI	1
4	1.8	PII	2
5	2	PII	2
6	2.2	PII	2
7	2.4	PII	2
8	2.6	PII	2
9	2.8	PDI	3
10	3	PDI	3

Table 21 presents the consensus analysis of the first round of SME feedback, where four items met the minimum 75% requirement (indicated in bold italics). While very few items reached the minimum requirement, this developmental research presents all consensus levels in Table 21 to provide as much information as possible to facilitate future research. A total of 64 items had a minimum of 51% consensus as to which category each PICC belonged. No items were recommended for removal by the SMEs, and subsequently presented to the expert panel during the subsequent round.

Table 21

Round 1 Consensus

Identifier	Description	DNA	PUI	PUI	PDI
PIC001	Acceleration via personal tracking	0.21	0.21	0.32	0.26
PIC002	Account numbers	0.00	0.00	0.53	0.47
PIC003	Activities	0.00	0.11	0.68	0.21
PIC004	Age	0.05	0.26	0.53	0.16
PIC005	Agency seal / Organizational logo	0.00	0.21	0.58	0.21
PIC006	Alias	0.11	0.16	0.32	0.42
PIC007	Area code	0.00	0.37	0.53	0.11

PIC008	Audit log of user actions	0.11	0.05	0.32	0.53
PIC009	Biometric records	0.00	0.05	0.11	***0.84***
PIC010	Bluetooth connections to other devices	0.00	0.05	0.63	0.32
PIC011	Calorie counting with images of food	0.11	0.42	0.42	0.05
PIC012	Cardholder name	0.05	0.00	0.37	0.58
PIC013	Cell phone number	0.00	0.11	0.32	0.58
PIC014	Cell tower location	0.00	0.21	0.37	0.42
PIC015	Credit card account number	0.05	0.05	0.16	0.74
PIC016	Credit card CAV2 / CVC2 / CVV2 / CID	0.00	0.16	0.21	0.63
PIC017	Card expiration date	0.00	0.32	0.37	0.32
PIC018	Credit card pin	0.00	0.32	0.47	0.21
PIC019	Credit card service code	0.05	0.32	0.42	0.21
PIC020	Credit score	0.00	0.32	0.53	0.16
PIC021	Criminal history	0.00	0.05	0.37	0.58
PIC022	Date of birth	0.00	0.16	0.32	0.53
PIC023	Demographics	0.00	0.16	0.37	0.47
PIC024	Driver's license [number]	0.00	0.05	0.26	0.68
PIC025	Education information	0.05	0.05	0.74	0.16
PIC026	Electricity usage	0.05	0.58	0.32	0.05
PIC027	Electronic facial image / selfie	0.00	0.00	0.42	0.58
PIC028	E-mail address	0.00	0.00	0.58	0.42
PIC029	Employee identification	0.00	0.11	0.32	0.58
PIC030	Employment history	0.11	0.05	0.37	0.47
PIC031	Employment information	0.05	0.05	0.37	0.53
PIC032	Family income	0.00	0.26	0.63	0.11
PIC033	Favorite movies	0.00	0.53	0.42	0.05
PIC034	Favorite restaurants	0.00	0.42	0.47	0.11
PIC035	Favorite television shows	0.00	0.53	0.37	0.11
PIC036	Financial records / information, balances	0.00	0.21	0.16	0.63
PIC037	Fingerprints	0.11	0.00	0.68	0.21
PIC038	Fingerprints of two fingers	0.05	0.00	0.63	0.32
PIC039	Full name	0.05	0.21	0.63	0.11
PIC040	Full set of fingerprints	0.00	0.00	0.00	***1.00***
PIC041	Gender	0.00	0.63	0.26	0.11
PIC042	Genetic information	0.00	0.00	0.32	0.68
PIC043	Geographical indicators	0.00	0.05	***0.84***	0.11
PIC044	Global Positioning Systems (GPS)	0.05	0.05	0.68	0.21
PIC045	Handwriting	0.00	0.00	0.58	0.42
PIC046	High school name	0.00	0.26	0.63	0.11
PIC047	Holographic images	0.05	0.00	0.63	0.32
PIC048	Host-specific persistent static identifier	0.21	0.05	0.53	0.21

PIC049	IP address	0.00	0.16	0.47	0.37
PIC050	Laser etches	0.32	0.11	0.32	0.26
PIC051	License plate	0.00	0.11	0.58	0.32
PIC052	MAC address	0.00	0.21	0.42	0.37
PIC053	Maiden name	0.00	0.00	0.53	0.47
PIC054	Marital status	0.11	0.26	0.47	0.16
PIC055	Medical history	0.00	0.21	0.21	0.58
PIC056	Medical information	0.05	0.16	0.21	0.58
PIC057	Medical test results	0.00	0.26	0.21	0.53
PIC058	Mental health	0.00	0.26	0.21	0.53
PIC059	Mother's maiden name	0.00	0.16	0.42	0.42
PIC060	Nationality	0.00	0.37	0.21	0.42
PIC061	Newsletter subscription	0.05	0.42	0.47	0.05
PIC062	Organization affiliation / membership	0.05	0.16	0.63	0.16
PIC063	Owned property	0.00	0.05	0.47	0.47
PIC064	Parent's middle name	0.00	0.32	0.58	0.11
PIC065	Partner(s) name	0.05	0.21	0.47	0.26
PIC066	Passport number	0.00	0.16	0.16	0.68
PIC067	Password	0.00	0.21	0.37	0.42
PIC068	Patient identification number	0.00	0.16	0.21	0.63
PIC069	Payment for health care	0.05	0.16	0.47	0.32
PIC070	Persistent Identifier	0.05	0.11	0.26	0.58
PIC071	Personal heart-rate meter	0.05	0.32	0.37	0.26
PIC072	Photographic image	0.05	0.00	0.32	0.63
PIC073	Physical health	0.05	0.32	0.32	0.32
PIC074	Place of birth	0.00	0.21	0.37	0.42
PIC075	Place of sensing moment	0.47	0.16	0.16	0.21
PIC076	Political views	0.00	0.32	0.53	0.16
PIC077	Professional title	0.00	0.26	0.53	0.21
PIC078	Provision of health care	0.05	0.37	0.37	0.21
PIC079	Race	0.11	0.32	0.32	0.26
PIC080	Rank	0.11	0.26	0.42	0.21
PIC081	Recent purchases	0.00	0.16	0.74	0.11
PIC082	Religion	0.00	0.37	0.42	0.21
PIC083	Salary information	0.05	0.26	0.42	0.26
PIC084	Search engine query	0.00	0.21	0.53	0.26
PIC085	Sexual fantasy / behavior	0.00	0.32	0.53	0.16
PIC086	Sexual orientation	0.00	0.37	0.42	0.21
PIC087	Signature Digital	0.05	0.11	0.16	0.68
PIC088	Signature Handwritten	0.00	0.05	0.37	0.58
PIC089	Social media profile	0.00	0.05	0.42	0.53

PIC090	Social Security Number	0.00	0.05	0.05	***0.89***
PIC091	Status updates	0.11	0.16	0.47	0.26
PIC092	Street address	0.00	0.05	0.47	0.47
PIC093	Tax records	0.00	0.11	0.21	0.68
PIC094	Taxpayer identification number	0.00	0.16	0.26	0.58
PIC095	Telephone number	0.00	0.00	0.68	0.32
PIC096	Location / Time of sensing moment	0.00	0.05	0.47	0.47
PIC097	Timestamp of Web page visit	0.00	0.32	0.47	0.21
PIC098	Uniform Resource Locator (URL) of last Web page	0.00	0.32	0.42	0.26
PIC099	Unique health identifier	0.05	0.21	0.32	0.42
PIC100	User identification	0.11	0.16	0.32	0.42
PIC101	Web browser history	0.00	0.11	0.63	0.26
PIC102	Weight	0.00	0.32	0.63	0.05
PIC103	Work phone	0.00	0.21	0.47	0.32
PIC104	X-Rays	0.00	0.26	0.37	0.37
PIC105	ZIP Code	0.00	0.37	0.37	0.26

Table 22 presents the consensus summary for the first Delphi round (N=19).

Table 22

Round 1 Consensus Overview Showing Number of SME Designated Items

Range		Number of Items	Cumulative Number of Items	Cumulative Percentage
>= .75		4	4	3.81%
>= .7	< .75	3	7	6.67%
>= .6	< .7	23	30	28.57%
>= .51	< .6	34	64	60.95%
< .51		41	105	100%

Delphi Round 2

Table 23 presents the consensus analysis of the second round of SME feedback, where seven items met the minimum 80% requirement (indicated in bold italics). A total of 73 PICCs were categorically placed by the SMEs with a minimum of 51% consensus. Table 24 presents the consensus summary for the second Delphi round.

Table 23

Items Reaching 80% Consensus in Round 2

Identifier	Description	DNA	PUI	PUI	PDI
PIC001	Acceleration via personal tracking	0.06	0.12	0.65	0.18
PIC002	Account numbers	0.00	0.12	0.71	0.18
PIC003	Activities	0.00	0.41	0.47	0.12
PIC004	Age	0.00	0.53	0.29	0.18
PIC005	Agency seal / Organizational logo	0.00	0.71	0.24	0.06
PIC006	Alias	0.06	0.35	0.35	0.24
PIC007	Area code	0.00	0.65	0.24	0.12
PIC008	Audit log of user actions	0.06	0.06	0.53	0.35
PIC009	Biometric records	0.00	0.06	0.06	***0.88***
PIC010	Bluetooth connections to other devices	0.00	0.35	0.47	0.18
PIC011	Calorie counting with images of food	0.12	0.65	0.24	0.00
PIC012	Cardholder name	0.00	0.06	0.35	0.59
PIC013	Cell phone number	0.00	0.06	0.24	0.71
PIC014	Cell tower location	0.00	0.24	0.65	0.12
PIC015	Credit card account number	0.00	0.06	0.18	0.76
PIC016	Credit card CAV2 / CVC2 / CVV2 / CID	0.06	0.18	0.24	0.53
PIC017	Card expiration date	0.00	0.71	0.18	0.12
PIC018	Credit card pin	0.06	0.29	0.59	0.06
PIC019	Credit card service code	0.06	0.35	0.47	0.12
PIC020	Credit score	0.00	0.71	0.18	0.12
PIC021	Criminal history	0.00	0.00	0.24	0.76
PIC022	Date of birth	0.06	0.12	0.59	0.24
PIC023	Demographics	0.00	0.35	0.35	0.29
PIC024	Driver's license [number]	0.06	0.00	0.18	0.76
PIC025	Education information	0.00	0.12	0.71	0.18
PIC026	Electricity usage	0.18	0.53	0.29	0.00
PIC027	Electronic facial image / selfie	0.00	0.00	0.12	***0.88***
PIC028	E-mail address	0.00	0.12	0.53	0.35
PIC029	Employee identification	0.06	0.06	0.12	0.76
PIC030	Employment history	0.00	0.06	0.47	0.47
PIC031	Employment information	0.00	0.18	0.24	0.59
PIC032	Family income	0.06	0.47	0.41	0.06
PIC033	Favorite movies	0.18	0.47	0.24	0.12
PIC034	Favorite restaurants	0.06	0.59	0.24	0.12
PIC035	Favorite television shows	0.06	0.59	0.29	0.06
PIC036	Financial records / information, balances	0.06	0.00	0.29	0.65
PIC037	Fingerprints	0.06	0.00	0.18	0.76
PIC038	Fingerprints of two fingers	0.06	0.00	0.18	0.76
PIC039	Full name	0.00	0.06	0.53	0.41

PIC040	Full set of fingerprints	0.00	0.00	0.12	***0.88***
PIC041	Gender	0.00	0.59	0.29	0.12
PIC042	Genetic information	0.00	0.00	0.29	0.71
PIC043	Geographical indicators	0.00	0.35	0.35	0.29
PIC044	Global Positioning Systems (GPS)	0.06	0.12	0.71	0.12
PIC045	Handwriting	0.00	0.18	0.59	0.24
PIC046	High school name	0.00	0.47	0.41	0.12
PIC047	Holographic images	0.00	0.29	0.47	0.24
PIC048	Host-specific persistent static identifier	0.00	0.24	0.65	0.12
PIC049	IP address	0.00	0.24	0.65	0.12
PIC050	Laser etches	0.12	0.24	0.47	0.18
PIC051	License plate	0.00	0.12	0.47	0.41
PIC052	MAC address	0.00	0.29	0.47	0.24
PIC053	Maiden name	0.00	0.18	0.71	0.12
PIC054	Marital status	0.06	0.59	0.35	0.00
PIC055	Medical history	0.00	0.00	0.47	0.53
PIC056	Medical information	0.00	0.00	0.35	0.65
PIC057	Medical test results	0.06	0.06	0.29	0.59
PIC058	Mental health	0.00	0.24	0.47	0.29
PIC059	Mother's maiden name	0.00	0.18	0.71	0.12
PIC060	Nationality	0.00	0.59	0.35	0.06
PIC061	Newsletter subscription	0.06	0.53	0.29	0.12
PIC062	Organization affiliation / membership	0.00	0.24	0.71	0.06
PIC063	Owned property	0.00	0.06	0.41	0.53
PIC064	Parent's middle name	0.00	0.59	0.35	0.06
PIC065	Partner(s) name	0.06	0.12	0.59	0.24
PIC066	Passport number	0.00	0.00	0.12	***0.88***
PIC067	Password	0.00	0.41	0.47	0.12
PIC068	Patient identification number	0.00	0.00	0.35	0.65
PIC069	Payment for health care	0.06	0.29	0.41	0.24
PIC070	Persistent Identifier	0.06	0.00	0.29	0.65
PIC071	Personal heart-rate meter	0.06	0.59	0.29	0.06
PIC072	Photographic image	0.00	0.06	0.18	0.76
PIC073	Physical health	0.12	0.41	0.29	0.18
PIC074	Place of birth	0.00	0.35	0.41	0.24
PIC075	Place of sensing moment	0.18	0.41	0.29	0.12
PIC076	Political views	0.12	0.47	0.35	0.06
PIC077	Professional title	0.00	0.29	0.59	0.12
PIC078	Provision of health care	0.06	0.29	0.53	0.12
PIC079	Race	0.00	0.53	0.41	0.06
PIC080	Rank	0.06	0.41	0.29	0.24

PIC081	Recent purchases	0.00	0.24	0.65	0.12
PIC082	Religion	0.12	0.47	0.35	0.06
PIC083	Salary information	0.12	0.35	0.41	0.12
PIC084	Search engine query	0.06	0.41	0.47	0.06
PIC085	Sexual fantasy / behavior	0.06	0.47	0.29	0.18
PIC086	Sexual orientation	0.06	0.59	0.29	0.06
PIC087	Signature Digital	0.00	0.06	0.06	***0.88***
PIC088	Signature Handwritten	0.00	0.12	0.29	0.59
PIC089	Social media profile	0.06	0.06	0.12	0.76
PIC090	Social Security Number	0.00	0.06	0.12	***0.82***
PIC091	Status updates	0.12	0.24	0.53	0.12
PIC092	Street address	0.06	0.06	0.65	0.24
PIC093	Tax records	0.00	0.06	0.06	***0.88***
PIC094	Taxpayer identification number	0.00	0.06	0.18	0.76
PIC095	Telephone number	0.06	0.12	0.59	0.24
PIC096	Location / Time of sensing moment	0.00	0.18	0.65	0.18
PIC097	Timestamp of Web page visit	0.00	0.53	0.35	0.12
PIC098	Uniform Resource Locator (URL) of last Web page	0.12	0.41	0.35	0.12
PIC099	Unique health identifier	0.00	0.12	0.41	0.47
PIC100	User identification	0.06	0.18	0.35	0.41
PIC101	Web browser history	0.00	0.35	0.47	0.18
PIC102	Weight	0.06	0.53	0.35	0.06
PIC103	Work phone	0.00	0.24	0.59	0.18
PIC104	X-Rays	0.00	0.35	0.47	0.18
PIC105	ZIP Code	0.06	0.41	0.29	0.24

Table 24

Round 2 Consensus Overview Showing Number of SME Designated Items

Range	Number of Items	Cumulative Number of Items	Cumulative Percentage
>= .80	7	7	6.67%
>= .70 < .80	20	27	25.71%
>= .60 < .70	13	40	38.10%
>= .51 < .60	33	73	69.52%
< .51	32	105	100%

Consensus Analysis Between Rounds

Table 25 presents the median analysis of the two rounds of the SMEs' feedback with the media for each PICC for the respective round provided, as well as if consensus was reached between the two rounds. The median analysis provided a consensus for 78 items (74%).

Table 25

Subject Matter Experts Consensus Median Analysis

Identifier	Description	Round 1	Round 2	Consensus
PC001	Acceleration via personal tracking	2	2	Yes
PC002	Account numbers	2	2	Yes
PC003	Activities	2	2	Yes
PC004	Age	2	1	No
PC005	Agency seal / Organizational logo	2	1	No
PC006	Alias	2	2	Yes
PC007	Area code	2	1	No
PC008	Audit log of user actions	3	2	No
PC009	Biometric records	3	3	Yes
PC010	Bluetooth connections to other devices	2	2	Yes
PC011	Calorie counting with images of food	1	1	Yes
PC012	Cardholder name	3	3	Yes
PC013	Cell phone number	3	3	Yes
PC014	Cell tower location	2	2	Yes
PC015	Credit card account number	3	3	Yes
PC016	Credit card CAV2/CVC2/ CVV2/CID	3	3	Yes
PC017	Card expiration date	2	1	No
PC018	Credit card pin	2	2	Yes
PC019	Credit card service code	2	2	Yes
PC020	Credit score	2	1	No
PC021	Criminal history	3	3	Yes
PC022	Date of birth	3	2	No
PC023	Demographics	2	2	Yes
PC024	Driver's license [number]	3	3	Yes
PC025	Education information	2	2	Yes
PC026	Electricity usage	1	1	Yes
PC027	Electronic facial image / selfie	3	3	Yes

PC028	E-mail address	2	2	Yes
PC029	Employee identification	3	3	Yes
PC030	Employment history	2	2	Yes
PC031	Employment information	3	3	Yes
PC032	Family income	2	1	No
PC033	Favorite movies	1	1	Yes
PC034	Favorite restaurants	2	1	No
PC035	Favorite television shows	1	1	Yes
PC036	Financial records / information, balances	3	3	Yes
PC037	Fingerprints	2	3	No
PC038	Fingerprints of two fingers	2	3	No
PC039	Full name	2	2	Yes
PC040	Full set of fingerprints	3	3	Yes
PC041	Gender	1	1	Yes
PC042	Genetic information	3	3	Yes
PC043	Geographical indicators	2	2	Yes
PC044	Global Positioning Systems (GPS)	2	2	Yes
PC045	Handwriting	2	2	Yes
PC046	High school name	2	2	Yes
PC047	Holographic images	2	2	Yes
PC048	Host-specific persistent static identifier	2	2	Yes
PC049	IP address	2	2	Yes
PC050	Laser etches	2	2	Yes
PC051	License plate	2	2	Yes
PC052	MAC address	2	2	Yes
PC053	Maiden name	2	2	Yes
PC054	Marital status	2	1	No
PC055	Medical history	3	3	Yes
PC056	Medical information	3	3	Yes
PC057	Medical test results	3	3	Yes
PC058	Mental health	3	2	No
PC059	Mother's maiden name	2	2	Yes
PC060	Nationality	2	1	No
PC061	Newsletter subscription	2	1	No
PC062	Organization affiliation / membership	2	2	Yes
PC063	Owned property	2	3	No
PC064	Parent's middle name	2	1	No
PC065	Partner(s) name	2	2	Yes
PC066	Passport number	3	3	Yes
PC067	Password	2	2	Yes

PC068	Patient identification number	3	3	Yes
PC069	Payment for health care	2	2	Yes
PC070	Persistent Identifier	3	3	Yes
PC071	Personal heart-rate meter	2	1	No
PC072	Photographic image	3	3	Yes
PC073	Physical health	2	1	No
PC074	Place of birth	2	2	Yes
PC075	Place of sensing moment	1	1	Yes
PC076	Political views	2	1	No
PC077	Professional title	2	2	Yes
PC078	Provision of health care	2	2	Yes
PC079	Race	2	1	No
PC080	Rank	2	2	Yes
PC081	Recent purchases	2	2	Yes
PC082	Religion	2	1	No
PC083	Salary information	2	2	Yes
PC084	Search engine query	2	2	Yes
PC085	Sexual fantasy / behavior	2	1	No
PC086	Sexual orientation	2	1	No
PC087	Signature Digital	3	3	Yes
PC088	Signature Handwritten	3	3	Yes
PC089	Social media profile	3	3	Yes
PC090	Social Security Number	3	3	Yes
PC091	Status updates	2	2	Yes
PC092	Street address	2	2	Yes
PC093	Tax records	3	3	Yes
PC094	Taxpayer identification number	3	3	Yes
PC095	Telephone number	2	2	Yes
PC096	Location / Time of sensing moment	2	2	Yes
PC097	Timestamp of Web page visit	2	1	No
PC098	Uniform Resource Locator (URL) of last Web page	2	1	No
PC099	Unique health identifier	2	2	Yes
PC100	User identification	2	2	Yes
PC101	Web browser history	2	2	Yes
PC102	Weight	2	1	No
PC103	Work phone	2	2	Yes
PC104	X-Rays	2	2	Yes
PC105	ZIP Code	2	2	Yes

The level of SME agreement was reported using the standard deviation and the mean of central tendency (Boone & Boone, 2012). Stability was measured by comparing the results of two different rounds to evaluate consistency in the median of responses for each PICC (Dajani et al., 1979; von der Gracht, 2012). The significant mean differences in the exposure categories (e.g., PDI, PII, & PUI) were evaluated by performing one-way ANOVA addressing RQ3 (Boone & Boone, 2012; Norman, 2010). RQ5 was addressed by performing an ANOVA for each demographic group. RQ6 was addressed by performing a *t*-test on the two groups: 50 executives of Fortune 500 organizations and 50 Hollywood personas (Norman, 2010).

Expert Panel SEXI Feedback

As previously noted, 19 SMEs participated in the first round of the survey and completed all the questions in the survey, thus provided a complete response. Appendix C presents the first-round survey provided to the SMEs. The SMEs were tasked with assigning a level of exposure to each of the 105 PICCs on a scale of one to ten. The SMEs were also provided DNA ("does not apply") and UNF ("unfamiliar") options of reach of the PICCs. The second-round survey, presented in Appendix D, had 17 SMEs participate and subsequently complete the survey by assigning the PICCs to DNA ("does not apply"), PDI, PII, or PUI categories.

RQ1 Analysis: SME Designated SEXI Components

The SMEs were asked to approve personal information components for an index of SE exposure. During two rounds of expert panel feedback, the SMEs were asked to assign level of exposure and subsequently categories to PICCs. Table 26 presents the

SME designated SEXI items arranged alphabetically within categorical groups with 11.4% designated at PDI, 54.3% as PII, and 34.3% as PUI.

Table 26

SME Designated SEXI Components

Personally Distinguishable Items			
PDI001	Biometric records	PDI007	Genetic information
PDI002	Credit card account number	PDI008	Passport number
PDI003	Criminal history	PDI009	Photographic image
PDI004	Driver's license [number]	PDI010	Signature Digital
PDI005	Electronic facial image / selfie	PDI011	Social Security Number
PDI006	Full set of fingerprints	PDI012	Tax records

Personally Identifiable Items					
PII001	Account numbers	PII029	Maiden name	PII057	ZIP Code
PII002	Activities	PII030	Medical history		
PII003	Alias	PII031	Medical information		
PII004	Audit log of user actions	PII032	Medical test results		
PII005	Bluetooth connections to other devices	PII033	Mental health		
PII006	Cardholder name	PII034	Mother's maiden name		
PII007	Cell phone number	PII035	Organization affiliation / membership		
PII008	Cell tower location	PII036	Owned property		
PII009	Credit card CAV2 / CVC2 / CVV2 / CID	PII037	Partner(s) name		
PII010	Date of birth	PII038	Password		
PII011	Demographics	PII039	Patient identification number		
PII012	Education information	PII040	Payment for health care		
PII013	E-mail address	PII041	Persistent Identifier		
PII014	Employee identification	PII042	Place of birth		
PII015	Employment history	PII043	Professional title		
PII016	Employment information	PII044	Recent purchases		
PII017	Financial records / information, balances	PII045	Search engine query		
PII018	Fingerprints	PII046	Signature Handwritten		
PII019	Fingerprints of two fingers	PII047	Social media profile		

PII020	Full name	PII048	Street address
PII021	Geographical indicators	PII049	Taxpayer identification number
PII022	Global Positioning Systems (GPS)	PII050	Telephone number
PII023	Handwriting	PII051	Location / Time of sensing moment
PII024	Holographic images	PII052	Unique health identifier
PII025	Host-specific persistent static identifier	PII053	User identification
PII026	IP address	PII054	Web browser history
PII027	License plate	PII055	Work phone
PII028	MAC address	PII056	X-Rays

Personally Unidentifiable Items

PUI001	Acceleration via personal tracking	PUI019	Nationality
PUI002	Age	PUI020	Newsletter subscription
PUI003	Agency seal / Organizational logo	PUI021	Parent's middle name
PUI004	Area code	PUI022	Personal heart-rate meter
PUI005	Calorie counting with images of food	PUI023	Physical health
PUI006	Card expiration date	PUI024	Place of sensing moment
PUI007	Credit card pin	PUI025	Political views
PUI008	Credit card service code	PUI026	Provision of health care
PUI009	Credit score	PUI027	Race
PUI010	Electricity usage	PUI028	Rank
PUI011	Family income	PUI029	Religion
PUI012	Favorite movies	PUI030	Salary information
PUI013	Favorite restaurants	PUI031	Sexual fantasy / behavior
PUI014	Favorite television shows	PUI032	Sexual orientation
PUI015	Gender	PUI033	Status updates
PUI016	High school name	PUI034	Timestamp of Web page visit
PUI017	Laser etches	PUI035	Uniform Resource Locator (URL) of last Web page
PUI018	Marital status	PUI036	Weight

RQ2 Analysis: SME Designated SEXI Categories

The SMEs were asked to approve categories for the identified set of personal information components. Three potential categories were presented to the SMEs derived from the body of literature. The SMEs indicated approval for the categories by providing categorical weights. Table 27 presents the SME approved SEXI categories as well as the respective level of personal information exposure risk.

Table 27

Risk Association of SME Designated SEXI Categories

	PDI	**PII**	**PUI**
Name	Personally Distinguishable Items	Personally Identifiable Items	Personally Unidentifiable Items
Exposure Level	High	Moderate	Low

RQ3 Analysis: Weights for Criteria and Measures

The SMEs were asked to attribute a level of exposure in the first round and assign an exposure category in the second round. Table 20 presented the methodology used to transform the exposure level to a category as defined in Equation 5. The mean of the values of both rounds was used to assign weights to each of the 105 PICCs. Table 28 presents the 12 PICCs designated as PDICs and their respective weights ranging from 2.61 to 2.94.

Table 28

Expert Panel Designated Personally Distinguishable Information Weights

Designation	Description	Weight
PDI001	Biometric records	2.8055556
PDI002	Credit card account number	2.6388889
PDI003	Criminal history	2.6388889

PDI004	Driver's license [number]	2.6388889
PDI005	Electronic facial image / selfie	2.7222222
PDI006	Full set of fingerprints	2.9444444
PDI007	Genetic information	2.6944444
PDI008	Passport number	2.6944444
PDI009	Photographic image	2.6111111
PDI010	Signature Digital	2.6388889
PDI011	Social Security Number	2.8055556
PDI012	Tax records	2.6944444

Table 29 presents the 57 PICCs designated as PIICs and their respective weights ranging from 1.81 to 2.56. Table 30 presents the 36 PICCs designated as PUICs and their respective weights ranging from 1.22 to 1.78.

Table 29

Expert Panel Designated Personally Identifiable Information Weights

Designation	Description	Weight
PII001	Account numbers	2.2777778
PII002	Activities	1.9166667
PII003	Alias	1.9166667
PII004	Audit log of user actions	2.2222222
PII005	Bluetooth connections to other devices	2.0555556
PII006	Cardholder name	2.5000000
PII007	Cell phone number	2.5555556
PII008	Cell tower location	2.0555556
PII009	Credit card CAV2 / CVC2 / CVV2 / CID	2.3611111
PII010	Date of birth	2.1944444
PII011	Demographics	2.1388889
PII012	Education information	2.0277778
PII013	E-mail address	2.3333333
PII014	Employee identification	2.5277778
PII015	Employment history	2.3055556
PII016	Employment information	2.3888889
PII017	Financial records / information, balances	2.4722222
PII018	Fingerprints	2.3055556

PII019	Fingerprints of two fingers	2.4166667
PII020	Full name	2.0555556
PII021	Geographical indicators	2.0000000
PII022	Global Positioning Systems (GPS)	1.9722222
PII023	Handwriting	2.2500000
PII024	Holographic images	2.0833333
PII025	Host-specific persistent static identifier	1.8055556
PII026	IP address	2.0555556
PII027	License plate	2.2500000
PII028	MAC address	2.0555556
PII029	Maiden name	2.2222222
PII030	Medical history	2.4444444
PII031	Medical information	2.4722222
PII032	Medical test results	2.3333333
PII033	Mental health	2.1666667
PII034	Mother's maiden name	2.1111111
PII035	Organization affiliation / membership	1.8611111
PII036	Owned property	2.4444444
PII037	Partner(s) name	1.9722222
PII038	Password	1.9722222
PII039	Patient identification number	2.5555556
PII040	Payment for health care	1.9444444
PII041	Persistent Identifier	2.4444444
PII042	Place of birth	2.0555556
PII043	Professional title	1.8888889
PII044	Recent purchases	1.9166667
PII045	Search engine query	1.8055556
PII046	Signature Handwritten	2.5000000
PII047	Social media profile	2.5277778
PII048	Street address	2.2500000
PII049	Taxpayer identification number	2.5555556
PII050	Telephone number	2.1666667
PII051	Location / Time of sensing moment	2.2222222
PII052	Unique health identifier	2.2222222
PII053	User identification	2.0833333
PII054	Web browser history	2.0000000
PII055	Work phone	2.0277778

PII056	X-Rays	1.9722222
PII057	ZIP Code	1.8055556

Table 30

Expert Panel Designated Personally Unidentifiable Information Weights

Designation	Description	Weight
PUI001	Acceleration via personal tracking	1.7777778
PUI002	Age	1.7222222
PUI003	Agency seal / Organizational logo	1.6944444
PUI004	Area code	1.6111111
PUI005	Calorie counting with images of food	1.2777778
PUI006	Card expiration date	1.7222222
PUI007	Credit card pin	1.7777778
PUI008	Credit card service code	1.7222222
PUI009	Credit score	1.6388889
PUI010	Electricity usage	1.2500000
PUI011	Family income	1.6666667
PUI012	Favorite movies	1.4166667
PUI013	Favorite restaurants	1.5555556
PUI014	Favorite television shows	1.4722222
PUI015	Gender	1.5000000
PUI016	High school name	1.7500000
PUI017	Laser etches	1.6111111
PUI018	Marital status	1.5000000
PUI019	Nationality	1.7777778
PUI020	Newsletter subscription	1.5000000
PUI021	Parent's middle name	1.6388889
PUI022	Personal heart-rate meter	1.6111111
PUI023	Physical health	1.7222222
PUI024	Place of sensing moment	1.2222222
PUI025	Political views	1.6111111
PUI026	Provision of health care	1.7222222
PUI027	Race	1.6388889
PUI028	Rank	1.7222222
PUI029	Religion	1.6111111
PUI030	Salary information	1.7222222
PUI031	Sexual fantasy / behavior	1.7222222
PUI032	Sexual orientation	1.6111111

PUI033	Status updates	1.7777778
PUI034	Timestamp of Web page visit	1.7500000
PUI035	URL of last Web page	1.7222222
PUI036	Weight	1.5833333

In addition to the assignment of the PICCs to the exposure categories, the SMEs were asked to allocate the relative weight for each of the three measures (PDIM, PIIM, & PUIM) within the SEXI. The SMEs allocated 100 points across the measures. The mean of the SME responses was used to establish the SEXI category weights. Table 31 presents the expert panel category weight distribution for the SEXI. The sum of the categorical weights equaled 100% with each respective weight providing a basis to associate risk assessments. Table 32 presents the normalization coefficients for each Expert Panel designated category of PICCs, wherein each component indicates the existence (1) of the respective PDIC, PIIC, and PUIC or not (0).

Table 31

Expert Panel SEXI Category Weight Distribution

Category	Number of Items	Measurement	Weight
PDI	12	PDIM	50.21%
PII	57	PIIM	34.47%
PUI	36	PUIM	15.32%

Table 32

Normalization Coefficients Derived From Expert Panel Feedback

Category	Number of items	Normalization Coefficient	Minimum	Maximum
PDI	12	1/32.527777777	0	32.527777777

PII	57	1/124.444444448	0	124.444444448
PUI	36	1/58.333333332	0	58.333333332

SEXI of 100 Individuals

In the second phase of this study, a preliminary instrument was developed to assess data collection and quantitative data analysis. Development started in April 2018 and concluded in April 2019. Google+ and Twitter were used as the data sources due to their straightforward APIs and data accessibility. On April 2, 2019, Google+ shut down their services for consumers. By the end of April 2019, the base data structure was defined and used as the foundation to build a working instrument.

For the third phase of the study six widely used sources were evaluated for accuracy and found unreliable or simply fake. Development of the instrument progressed through December 2019 targeting OSPI found at PublicData.com, FullContact.com, and Twitter. When necessary, the real name of the Hollywood Persona was used. Appendix E presents the SEXI data collection form.

All values were initialized to null (not found). At the end of processing, if any PICC was no longer null, it was switched to true (found). Table 33 presents the OSPI sources used in the data collection for the SEXI.

Table 33

OSPI Data Sources Used For SEXI Data Collection

Category	Corporate Executives	Hollywood Personas
Contact /Demographics / Geographic	AdvancedBackgroundCheck.com Intellius.com PublicData.com VoterRecords.com	AdvancedBackgroundCheck.com CelebrityInside.com Intellius.com NNDB.com

		PublicData.com VoterRecords.com
Employment	Bloomberg.com LinkedIn.com	IMDB.com LinkedIn.com
Financials	Sec.gov Salary.com Wallmine.com	CelebrityNetWorth.com CelebsMoney.com NetWorthBro.com NetWorthPost.org SportsLeeda.com TheNetWorthPortal.com
Images	Images.Google.com Twitter.com	Images.Google.com Twitter.com
Searches	Google.com	Google.com
Signatures /Autographs /Handwriting	Images.Google.com Sec.gov	Images.Google.com

RQ4 Analysis: 100 Individuals Assessed and Classified Using OSPI

Analysis was performed on 50 executives of Fortune 500 companies and 50 Hollywood personas. It was observed that executives in the population might have been in the same position at the same company for decades, while others changed multiple times within a decade, while others occupied multiple positions simultaneously in non-competitive organizations. Hollywood personas could be involved in multiple, a single, or no projects within a calendar year. Table 34 presents descriptive statistics of the population with the demographic medians indicated in italics, specifically: Age=55, Gender= 52% Male, Income=$2,550,000, Marital Status=Not Married, and Estimated Worth=$20,000,000. To meet the two-item requirement of ANOVA, age 29 was added to

age group 3 and CCPAO was merged with CCO. Table 35 presents the descriptive statistics of the SEXI of the population (N=100, M=29.23, SD= 4.51).

1 **Table 34**

2 *Descriptive Statistics of the Population (N=100)*

Item	Percentage (%)
Age	
29-34	2
35-39	4
40-44	8
45-49	16
50-54	*17*
55-59	25
60-64	9
65+	19
Gender	
Male	*65*
Female	35
Income (1000s)	
0-281	36
282-1,659	9
1,660-3,099	*9*
3,100-4,999	9
5,000-9,599	9
9,600-1,3999	9
14,000-23,499	9
23,500+	10
Marital Status	
No	*52*
Yes	48
Estimated Worth (1000s)	
0-499	17
500-5,199	10
5,200-7,999	8
8,000-13,999	10
14,000-23,399	*9*
23,400-49,999	9
50,000-89,999	9
90,000-179,999	9
180,000-399,999	9
400,000+	10

Industry	
Aerospace and Defense	5
Automotive Retailing, Services	6
Energy	6
Engineering & Construction	2
Financial Data Services	3
Food and Drug Stores	2
Food Services	3
Health Care: Insurance and Managed Care	3
Homebuilders	3
Railroads	3
Securities	3
Semiconductors and Other Electronic Components	3
Specialty Retailers: Other	3
Transportation	2
Wholesalers: Electronics and Office Equipment	3
Big Screen	23
Small Screen	25
Writer	2
Organizational Position	
CAO	2
CCPAO / CCO	2
CEO	18
CFO	11
CHRO	5
CIO	6
CMO	2
COO	4
Actor	23
Producer	25
Writer	2
Philanthropic	
No	41
Yes	59
Military Police Experience	
No	96
Yes	4

Table 35

SEXI Descriptive Statistics of the Population (N=100)

	N	Min	Max	Mean	SD	Skewness		Kurtosis	
						Statistic	Std. Error	Statistic	Std. Error
SEXI	100	19.6683	43.8211	29.2312	4.51	0.069	0.241	0.493	0.478
Valid N (listwise)	100								

For a PICC item to be designated as found, the item needed to be specifically located, stated, or directly derived from other data. Examples of derived data include Age (PUI002) from the Date of birth (PII010), GPS (PII022) coordinates from a full address, and employment history from movie credits. An electronic facial image / selfie (PDI005) only met the criteria if the face of the individual served as the primary subject, whereas a Photographic image (PDI009) could be anything associated with the individual. Autographs were viewed as handwriting samples, rather than Signature Handwritten. Signature Digital required an SSL authority, hash, and encryption keys. Hollywood persona's legal names were used for Full name (PII020). Table 36 presents a summary of found / not found SEXI items.

Table 36

Summary of SEXI Data Collection for Executives and Hollywood Personas

Item	Description	Execs		HPers		All	
		Found	Not Found	Found	Not Found	Found	Not Found
PDI001	Biometric records	0%	100%	0%	100%	0%	100%
PDI002	Credit card account number	0%	100%	0%	100%	0%	100%

PDI003	Criminal history	0%	100%	14%	86%	7%	93%
PDI004	Driver's license [number]	66%	34%	48%	52%	57%	43%
PDI005	Electronic facial image / selfie	100%	0%	100%	0%	100%	0%
PDI006	Full set of fingerprints	0%	100%	0%	100%	0%	100%
PDI007	Genetic information	0%	100%	0%	100%	0%	100%
PDI008	Passport number	0%	100%	0%	100%	0%	100%
PDI009	Photographic image	100%	0%	100%	0%	100%	0%
PDI010	Signature Digital	0%	100%	0%	100%	0%	100%
PDI011	Social Security Number	0%	100%	2%	98%	1%	99%
PDI012	Tax records	0%	100%	0%	100%	0%	100%
PII001	Account numbers	0%	100%	0%	100%	0%	100%
PII002	Activities	88%	12%	98%	2%	93%	7%
PII003	Alias	28%	72%	94%	6%	61%	39%
PII004	Audit log of user actions	0%	100%	0%	100%	0%	100%
PII005	Bluetooth connections to other devices	0%	100%	0%	100%	0%	100%
PII006	Cardholder name	0%	100%	0%	100%	0%	100%
PII007	Cell phone number	66%	34%	48%	52%	57%	43%
PII008	Cell tower location	0%	100%	2%	98%	1%	99%
PII009	Credit card CAV2 / CVC2 / CVV2 / CID	0%	100%	0%	100%	0%	100%
PII010	Date of birth	82%	18%	100%	0%	91%	9%
PII011	Demographics	100%	0%	100%	0%	100%	0%
PII012	Education information	94%	6%	100%	0%	97%	3%
PII013	E-mail address	64%	36%	86%	14%	75%	25%
PII014	Employee identification	0%	100%	0%	100%	0%	100%
PII015	Employment history	92%	8%	100%	0%	96%	4%
PII016	Employment information	98%	2%	100%	0%	99%	1%
PII017	Financial records / information, balances	44%	56%	6%	94%	25%	75%
PII018	Fingerprints	0%	100%	0%	100%	0%	100%
PII019	Fingerprints of two fingers	0%	100%	0%	100%	0%	100%
PII020	Full name	100%	0%	100%	0%	100%	0%
PII021	Geographical indicators	100%	0%	100%	0%	100%	0%
PII022	Global Positioning Systems (GPS)	98%	2%	96%	4%	97%	3%
PII023	Handwriting	6%	94%	26%	74%	16%	84%
PII024	Holographic images	0%	100%	0%	100%	0%	100%

PII025	Host-specific persistent static identifier	40%	60%	94%	6%	67%	33%
PII026	IP address	2%	98%	0%	100%	1%	99%
PII027	License plate	0%	100%	2%	98%	1%	99%
PII028	MAC address	0%	100%	2%	98%	1%	99%
PII029	Maiden name	0%	100%	34%	66%	17%	83%
PII030	Medical history	0%	100%	4%	96%	2%	98%
PII031	Medical information	26%	74%	44%	56%	35%	65%
PII032	Medical test results	0%	100%	0%	100%	0%	100%
PII033	Mental health	0%	100%	4%	96%	2%	98%
PII034	Mother's maiden name	2%	98%	70%	30%	36%	64%
PII035	Organization affiliation / membership	100%	0%	100%	0%	100%	0%
PII036	Owned property	22%	78%	66%	34%	44%	56%
PII037	Partner(s) name	42%	58%	94%	6%	68%	32%
PII038	Password	0%	100%	0%	100%	0%	100%
PII039	Patient identification number	0%	100%	0%	100%	0%	100%
PII040	Payment for health care	0%	100%	0%	100%	0%	100%
PII041	Persistent Identifier	84%	16%	96%	4%	90%	10%
PII042	Place of birth	2%	98%	100%	0%	51%	49%
PII043	Professional title	100%	0%	100%	0%	100%	0%
PII044	Recent purchases	66%	34%	44%	56%	55%	45%
PII045	Search engine query	0%	100%	0%	100%	0%	100%
PII046	Signature Handwritten	6%	94%	90%	10%	48%	52%
PII047	Social media profile	64%	36%	94%	6%	79%	21%
PII048	Street address	100%	0%	94%	6%	97%	3%
PII049	Taxpayer identification number	0%	100%	0%	100%	0%	100%
PII050	Telephone number	86%	14%	94%	6%	90%	10%
PII051	Location / Time of sensing moment	0%	100%	0%	100%	0%	100%
PII052	Unique health identifier	0%	100%	0%	100%	0%	100%
PII053	User identification	28%	72%	94%	6%	61%	39%
PII054	Web browser history	0%	100%	0%	100%	0%	100%
PII055	Work phone	0%	100%	0%	100%	0%	100%
PII056	X-Rays	0%	100%	0%	100%	0%	100%
PII057	ZIP Code	100%	0%	96%	4%	98%	2%
PUI001	Acceleration via personal tracking	0%	100%	2%	98%	1%	99%
PUI002	Age	100%	0%	100%	0%	100%	0%
PUI003	Agency seal / Organizational logo	98%	2%	80%	20%	89%	11%
PUI004	Area code	94%	6%	82%	18%	88%	12%

PUI005	Calorie counting with images of food	0%	100%	0%	100%	0%	100%
PUI006	Card expiration date	0%	100%	0%	100%	0%	100%
PUI007	Credit card pin	0%	100%	0%	100%	0%	100%
PUI008	Credit card service code	0%	100%	0%	100%	0%	100%
PUI009	Credit score	0%	100%	0%	100%	0%	100%
PUI010	Electricity usage	0%	100%	0%	100%	0%	100%
PUI011	Family income	62%	38%	88%	12%	75%	25%
PUI012	Favorite movies	0%	100%	8%	92%	4%	96%
PUI013	Favorite restaurants	0%	100%	2%	98%	1%	99%
PUI014	Favorite television shows	0%	100%	2%	98%	1%	99%
PUI015	Gender	100%	0%	100%	0%	100%	0%
PUI016	High school name	14%	86%	80%	20%	47%	53%
PUI017	Laser etches	0%	100%	0%	100%	0%	100%
PUI018	Marital status	50%	50%	94%	6%	72%	28%
PUI019	Nationality	98%	2%	100%	0%	99%	1%
PUI020	Newsletter subscription	0%	100%	0%	100%	0%	100%
PUI021	Parent's middle name	2%	98%	44%	56%	23%	77%
PUI022	Personal heart-rate meter	0%	100%	0%	100%	0%	100%
PUI023	Physical health	0%	100%	40%	60%	20%	80%
PUI024	Place of sensing moment	0%	100%	0%	100%	0%	100%
PUI025	Political views	68%	32%	68%	32%	68%	32%
PUI026	Provision of health care	0%	100%	0%	100%	0%	100%
PUI027	Race	92%	8%	98%	2%	95%	5%
PUI028	Rank	0%	100%	0%	100%	0%	100%
PUI029	Religion	0%	100%	68%	32%	34%	66%
PUI030	Salary information	72%	28%	72%	28%	72%	28%
PUI031	Sexual fantasy / behavior	8%	92%	18%	82%	13%	87%

PUI032	Sexual orientation	8%	92%	94%	6%	51%	49%
PUI033	Status updates	80%	20%	50%	50%	65%	35%
PUI034	Timestamp of Web page visit	0%	100%	0%	100%	0%	100%
PUI035	Uniform Resource Locator (URL) of last Web page	0%	100%	0%	100%	0%	100%
PUI036	Weight	0%	100%	88%	12%	44%	56%

RQ5 Analysis: SEXI Demographic Analysis of the Population

The one-way ANOVA was conducted to investigate SEXI differences due to age. Table 37 presents the SEXI descriptive statistics for the population (N=100). Results revealed minor difference (p=0.013) between the 55-59 and 65+ age groups. Figure 7 presents the minimum, maximum, and mean SEXI values for each age group. Overall, age had very little contribution for the SEXI for our population (N=100).

Table 37

SEXI Descriptive Statistics for Age

	N	M	SD	SE	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
29-34	2	30.0850	5.5601	3.9316	-19.8708	80.0409	26.1534	34.0166
35-39	4	28.5884	5.8446	2.9223	19.2883	37.8884	20.1901	33.3891
40-44	8	30.0644	2.7330	0.9663	27.7795	32.3492	27.1946	34.1486
45-49	16	30.2013	5.7756	1.4439	27.1237	33.2789	20.6677	39.1979
50-54	17	28.9975	3.8142	0.9251	27.0365	30.9586	20.1254	34.0798
55-59	25	27.4822	4.0229	0.8046	25.8217	29.1428	19.6683	37.8443
60-64	9	28.0821	4.5402	1.5134	24.5923	31.5720	21.0818	34.1325
65+	19	31.1641	4.4572	1.0226	29.0157	33.3124	22.6923	43.8211

Total	100	29.2313	4.5100	0.4510	28.3364	30.1262	19.6683	43.8211

Table 38, presents the SEXI ANOVA age results, shows no significance [$F(7, 92) = 1.32$, $p = 0.249$]. Table 39 presents the SEXI multiple comparisons for age, where most age groups show no significance between the various age groups. The Tukey HSD post hoc test was conducted to determine which age categories were significantly different.

Table 38

SEXI ANOVA for Age

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	183.986	7	26.284	1.322	0.249
Within Groups	1829.716	92	19.888		
Total	2013.702	99			

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

Table 39

SEXI Multiple Comparisons for Age

	(I) Age	(J) Age	Mean Difference (I-J)	SE	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Tukey HSD	29-34	35-39	1.4967	3.86	1.000	-10.4830	13.4763
		40-44	0.0207	3.53	1.000	-10.9152	10.9566
		45-49	-0.1163	3.34	1.000	-10.4909	10.2584
		50-54	1.0875	3.33	1.000	-9.2532	11.4282
		55-59	2.6028	3.28	0.990	-7.5623	12.7679
		60-64	2.0029	3.49	1.000	-8.8108	12.8166
		65+	-1.0790	3.32	1.000	-11.3623	9.2043
	35-39	29-34	-1.4967	3.86	1.000	-13.4763	10.4830
		40-44	-1.4760	2.73	1.000	-9.9469	6.9949
		45-49	-1.6129	2.49	1.000	-9.3458	6.1199
		50-54	-0.4092	2.48	1.000	-8.0964	7.2780
		55-59	1.1061	2.4	1.000	-6.3431	8.5554

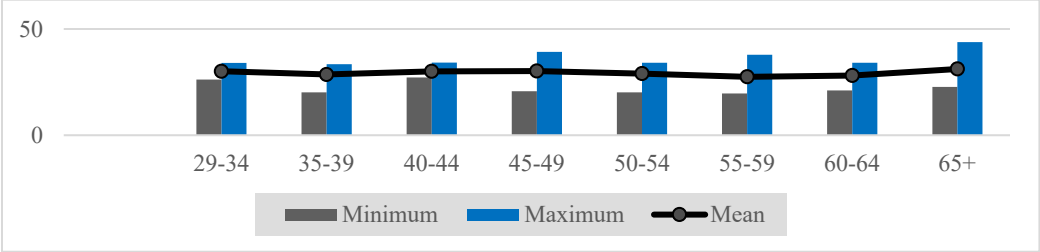
	60-64	0.5062	2.68	1.000	-7.8063	8.8188
	65+	-2.5757	2.45	0.970	-10.1855	5.0341
40-44	29-34	-0.0207	3.53	1.000	-10.9566	10.9152
	35-39	1.4760	2.73	1.000	-6.9949	9.9469
	45-49	-0.1369	1.93	1.000	-6.1268	5.8529
	50-54	1.0668	1.91	1.000	-4.8640	6.9976
	55-59	2.5821	1.81	0.840	-3.0368	8.2011
	60-64	1.9822	2.17	0.980	-4.7394	8.7038
	65+	-1.0997	1.88	1.000	-6.9298	4.7304
45-49	29-34	0.1163	3.34	1.000	-10.2584	10.4909
	35-39	1.6129	2.49	1.000	-6.1199	9.3458
	40-44	0.1369	1.93	1.000	-5.8529	6.1268
	50-54	1.2037	1.55	0.990	-3.6145	6.0220
	55-59	2.7190	1.43	0.550	-1.7097	7.1477
	60-64	2.1191	1.86	0.950	-3.6446	7.8829
	65+	-0.9628	1.51	1.000	-5.6564	3.7309
50-54	29-34	-1.0875	3.33	1.000	-11.4282	9.2532
	35-39	0.4092	2.48	1.000	-7.2780	8.0964
	40-44	-1.0668	1.91	1.000	-6.9976	4.8640
	45-49	-1.2037	1.55	0.990	-6.0220	3.6145
	55-59	1.5153	1.4	0.960	-2.8333	5.8638
	60-64	0.9154	1.84	1.000	-4.7870	6.6178
	65+	-2.1665	1.49	0.830	-6.7846	2.4516
55-59	29-34	-2.6028	3.28	0.990	-12.7679	7.5623
	35-39	-1.1061	2.4	1.000	-8.5554	6.3431
	40-44	-2.5821	1.81	0.840	-8.2011	3.0368
	45-49	-2.7190	1.43	0.550	-7.1477	1.7097
	50-54	-1.5153	1.4	0.960	-5.8638	2.8333
	60-64	-0.5999	1.73	1.000	-5.9772	4.7774
	65+	-3.6818	1.36	0.130	-7.8919	0.5283
60-64	29-34	-2.0029	3.49	1.000	-12.8166	8.8108
	35-39	-0.5062	2.68	1.000	-8.8188	7.8063
	40-44	-1.9822	2.17	0.980	-8.7038	4.7394
	45-49	-2.1191	1.86	0.950	-7.8829	3.6446
	50-54	-0.9154	1.84	1.000	-6.6178	4.7870
	55-59	0.5999	1.73	1.000	-4.7774	5.9772
	65+	-3.0819	1.8	0.680	-8.6794	2.5156
65+	29-34	1.0790	3.32	1.000	-9.2043	11.3623
	35-39	2.5757	2.45	0.970	-5.0341	10.1855
	40-44	1.0997	1.88	1.000	-4.7304	6.9298

		45-49	0.9628	1.51	1.000	-3.7309	5.6564
		50-54	2.1665	1.49	0.830	-2.4516	6.7846
		55-59	3.6818	1.36	0.130	-0.5283	7.8919
		60-64	3.0819	1.8	0.680	-2.5156	8.6794
Games-Howell	29-34	35-39	1.4967	4.9	1.000	-39.2904	42.2837
		40-44	0.0207	4.05	1.000	-97.7796	97.8210
		45-49	-0.1163	4.19	1.000	-76.1756	75.9431
		50-54	1.0875	4.04	1.000	-98.5571	100.7321
		55-59	2.6028	4.01	0.990	-102.5025	107.7081
		60-64	2.0029	4.21	1.000	-71.3510	75.3567
		65+	-1.0790	4.06	1.000	-96.1807	94.0226
	35-39	29-34	-1.4967	4.9	1.000	-42.2837	39.2904
		40-44	-1.4760	3.08	1.000	-18.2742	15.3222
		45-49	-1.6129	3.26	1.000	-17.3906	14.1648
		50-54	-0.4092	3.07	1.000	-17.2744	16.4560
		55-59	1.1061	3.03	1.000	-16.0360	18.2482
		60-64	0.5062	3.29	1.000	-15.2473	16.2597
		65+	-2.5757	3.1	0.980	-19.2113	14.0599
	40-44	29-34	-0.0207	4.05	1.000	-97.8210	97.7796
		35-39	1.4760	3.08	1.000	-15.3222	18.2742
		45-49	-0.1369	1.74	1.000	-5.9377	5.6639
		50-54	1.0668	1.34	0.990	-3.4735	5.6071
		55-59	2.5821	1.26	0.480	-1.7186	6.8828
		60-64	1.9822	1.8	0.950	-4.4030	8.3674
		65+	-1.0997	1.41	0.990	-5.8153	3.6159
	45-49	29-34	0.1163	4.19	1.000	-75.9431	76.1756
		35-39	1.6129	3.26	1.000	-14.1648	17.3906
		40-44	0.1369	1.74	1.000	-5.6639	5.9377
		50-54	1.2037	1.71	1.000	-4.4410	6.8485
		55-59	2.7190	1.65	0.720	-2.7494	8.1874
		60-64	2.1191	2.09	0.970	-4.9232	9.1615
		65+	-0.9628	1.77	1.000	-6.7494	4.8239
	50-54	29-34	-1.0875	4.04	1.000	-100.7321	98.5571
		35-39	0.4092	3.07	1.000	-16.4560	17.2744
		40-44	-1.0668	1.34	0.990	-5.6071	3.4735
		45-49	-1.2037	1.71	1.000	-6.8485	4.4410
		55-59	1.5153	1.23	0.920	-2.4286	5.4592
		60-64	0.9154	1.77	1.000	-5.3361	7.1668
		65+	-2.1665	1.38	0.760	-6.6162	2.2832

	55-59	29-34	-2.6028	4.01	0.990	-107.7081	102.5025
		35-39	-1.1061	3.03	1.000	-18.2482	16.0360
		40-44	-2.5821	1.26	0.480	-6.8828	1.7186
		45-49	-2.7190	1.65	0.720	-8.1874	2.7494
		50-54	-1.5153	1.23	0.920	-5.4592	2.4286
		60-64	-0.5999	1.71	1.000	-6.7333	5.5335
		65+	-3.6818	1.3	0.120	-7.8612	0.4976
	60-64	29-34	-2.0029	4.21	1.000	-75.3567	71.3510
		35-39	-0.5062	3.29	1.000	-16.2597	15.2473
		40-44	-1.9822	1.8	0.950	-8.3674	4.4030
		45-49	-2.1191	2.09	0.970	-9.1615	4.9232
		50-54	-0.9154	1.77	1.000	-7.1668	5.3361
		55-59	0.5999	1.71	1.000	-5.5335	6.7333
		65+	-3.0819	1.83	0.700	-9.4308	3.2669
	65+	29-34	1.0790	4.06	1.000	-94.0226	96.1807
		35-39	2.5757	3.1	0.980	-14.0599	19.2113
		40-44	1.0997	1.41	0.990	-3.6159	5.8153
		45-49	0.9628	1.77	1.000	-4.8239	6.7494
		50-54	2.1665	1.38	0.760	-2.2832	6.6162
		55-59	3.6818	1.3	0.120	-0.4976	7.8612
		60-64	3.0819	1.83	0.700	-3.2669	9.4308

Figure 7

SEXI for population for age



The one-way ANOVA was conducted to investigate SEXI differences due to gender. It was observed that more personal information appeared readily available for Hollywood Persona females (e.g. body measurements, sexual history, etc.) that may lead to an assumption of a significant difference due to gender, which was not the case.

Surprisingly, the existence of a maiden name found for several females was not enough to significantly increase the SEXI for the group. Table 40 presents the SEXI descriptive statistics for the population (65 males & 35 females) (N=100).

Table 40

SEXI Descriptive Statistics for Gender

	N	M	SD	SE	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
Male	65	29.5772	4.73226	0.58696	28.40461	30.7498	19.6683	43.82105
Female	35	28.58888	4.05203	0.68492	27.19696	29.98081	20.19013	36.99099
Total	100	29.23129	4.51004	0.451	28.3364	30.12618	19.6683	43.82105

Table 41, presents the SEXI ANOVA gender results, shows no significance in difference between males and females [$F(1, 98) = 1.09$, $p = 0.298$]. No post hoc tests were conducted due to two ordinal categories of genders.

Table 41

SEXI ANOVA for Gender

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	22.222	1	22.222	1.094	0.298
Within Groups	1991.48	98	20.321		
Total	2013.702	99			

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

The one-way ANOVA was conducted to investigate SEXI differences due to income. Table 42 presents the SEXI descriptive statistics for the income of the population (N=100). Table 43, presents the SEXI ANOVA results, shows significance for income of the population [$F(7, 92) = 2.15$, $p < 0.05$].

Table 42

SEXI Descriptive Statistics for Income (1000s)

	N	M	SD	SE	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
0-281	36	29.779	4.620	0.770	28.216	31.343	21.056	43.821
282-1659	9	31.395	3.647	1.216	28.592	34.198	25.525	36.991
1660-3099	9	27.389	5.454	1.818	23.197	31.581	20.125	37.844
3100-4999	9	25.385	3.075	1.025	23.021	27.749	20.190	29.715
5000-9599	9	28.698	3.472	1.157	26.029	31.367	20.668	32.522
9600-13999	9	27.883	3.596	1.199	25.118	30.647	19.668	32.625
14000-23499	9	30.295	6.191	2.064	25.536	35.053	20.082	39.198
23500+	10	31.168	2.512	0.794	29.372	32.965	26.268	34.149
Total	100	29.231	4.510	0.451	28.336	30.126	19.668	43.821

Table 43

SEXI ANOVA for Income (1000s)

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	283.257	7	40.465	2.151	***0.046****
Within Groups	1730.445	92	18.809		
Total	2013.702	99			

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

Table 44 presents the SEXI multiple comparisons for income. Tukey HSD and Games-Howell post hoc tests were conducted to determine which income categories were significantly different. The Games-Howell indicated a significant difference between the 3100-4999 income group with the 0-281 (p<0.05), 282-1659 (p<0.05), and 23500+ (p<0.01) income groups for the population.

Table 44

1 *SEXI Multiple Comparisons for Income*

	(I) Income	(J) Income	Mean Difference (I-J)	SE	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Tukey HSD	0-281	282-1659	-1.61562	1.61629	0.973	-6.62904	3.39781
		1660-3099	2.39037	1.61629	0.817	-2.62306	7.40379
		3100-4999	4.39423	1.61629	0.130	-0.61920	9.40765
		5000-9599	1.08122	1.61629	0.998	-3.93220	6.09465
		9600-13999	1.89658	1.61629	0.937	-3.11685	6.91000
		14000-23499	-0.51531	1.61629	1.000	-5.52874	4.49811
		23500+	-1.38907	1.55029	0.986	-6.19777	3.41964
	282-1659	0-281	1.61562	1.61629	0.973	-3.39781	6.62904
		1660-3099	4.00598	2.04446	0.515	-2.33555	10.34752
		3100-4999	6.00984	2.04446	0.076	-0.33169	12.35138
		5000-9599	2.69684	2.04446	0.889	-3.64469	9.03838
		9600-13999	3.51219	2.04446	0.676	-2.82934	9.85373
		14000-23499	1.10030	2.04446	0.999	-5.24123	7.44184
		23500+	0.22655	1.99269	1.000	-5.95441	6.40752
	1660-3099	0-281	-2.39037	1.61629	0.817	-7.40379	2.62306
		282-1659	-4.00598	2.04446	0.515	-10.34752	2.33555
		3100-4999	2.00386	2.04446	0.976	-4.33768	8.34539
		5000-9599	-1.30914	2.04446	0.998	-7.65068	5.03239
		9600-13999	-0.49379	2.04446	1.000	-6.83533	5.84774
		14000-23499	-2.90568	2.04446	0.845	-9.24722	3.43585
		23500+	-3.77943	1.99269	0.557	-9.96040	2.40153
	3100-4999	0-281	-4.39423	1.61629	0.130	-9.40765	0.61920
		282-1659	-6.00984	2.04446	0.076	-12.35138	0.33169
		1660-3099	-2.00386	2.04446	0.976	-8.34539	4.33768

	5000-9599	-3.31300	2.04446	0.737	-9.65454	3.02853
	9600-13999	-2.49765	2.04446	0.923	-8.83919	3.84388
	14000-23499	-4.90954	2.04446	0.253	-11.25108	1.43199
	23500+	-5.78329	1.99269	0.084	-11.96426	0.39767
5000-9599	0-281	-1.08122	1.61629	0.998	-6.09465	3.93220
	282-1659	-2.69684	2.04446	0.889	-9.03838	3.64469
	1660-3099	1.30914	2.04446	0.998	-5.03239	7.65068
	3100-4999	3.31300	2.04446	0.737	-3.02853	9.65454
	9600-13999	0.81535	2.04446	1.000	-5.52618	7.15689
	14000-23499	-1.59654	2.04446	0.994	-7.93807	4.74500
	23500+	-2.47029	1.99269	0.918	-8.65125	3.71067
9600-13999	0-281	-1.89658	1.61629	0.937	-6.91000	3.11685
	282-1659	-3.51219	2.04446	0.676	-9.85373	2.82934
	1660-3099	0.49379	2.04446	1.000	-5.84774	6.83533
	3100-4999	2.49765	2.04446	0.923	-3.84388	8.83919
	5000-9599	-0.81535	2.04446	1.000	-7.15689	5.52618
	14000-23499	-2.41189	2.04446	0.936	-8.75342	3.92965
	23500+	-3.28564	1.99269	0.719	-9.46660	2.89532
14000-23499	0-281	0.51531	1.61629	1.000	-4.49811	5.52874
	282-1659	-1.10030	2.04446	0.999	-7.44184	5.24123
	1660-3099	2.90568	2.04446	0.845	-3.43585	9.24722
	3100-4999	4.90954	2.04446	0.253	-1.43199	11.25108
	5000-9599	1.59654	2.04446	0.994	-4.74500	7.93807
	9600-13999	2.41189	2.04446	0.936	-3.92965	8.75342
	23500+	-0.87375	1.99269	1.000	-7.05472	5.30721
23500+	0-281	1.38907	1.55029	0.986	-3.41964	6.19777
	282-1659	-0.22655	1.99269	1.000	-6.40752	5.95441
	1660-3099	3.77943	1.99269	0.557	-2.40153	9.96040
	3100-4999	5.78329	1.99269	0.084	-0.39767	11.96426
	5000-9599	2.47029	1.99269	0.918	-3.71067	8.65125

		9600-13999	3.28564	1.99269	0.719	-2.89532	9.46660
		14000-23499	0.87375	1.99269	1.000	-5.30721	7.05472
Games-Howell	0-281	282-1659	-1.61562	1.43901	0.942	-6.63499	3.40375
		1660-3099	2.39037	1.97431	0.913	-4.86606	9.64680
		3100-4999	4.39423	1.28217	***0.048****	0.02736	8.76109
		5000-9599	1.08122	1.39002	0.992	-3.73366	5.89611
		9600-13999	1.89658	1.42483	0.874	-3.06359	6.85674
		14000-23499	-0.51531	2.20253	1.000	-8.71878	7.68815
		23500+	-1.38907	1.10624	0.907	-5.01067	2.23254
	282-1659	0-281	1.61562	1.43901	0.942	-3.40375	6.63499
		1660-3099	4.00598	2.18693	0.611	-3.71414	11.72611
		3100-4999	6.00984	1.59019	***0.028****	0.48345	11.53623
		5000-9599	2.69684	1.67836	0.740	-3.11576	8.50945
		9600-13999	3.51219	1.70730	0.478	-2.39891	9.42329
		14000-23499	1.10030	2.39497	1.000	-7.45516	9.65577
		23500+	0.22655	1.45207	1.000	-4.89638	5.34948
	1660-3099	0-281	-2.39037	1.97431	0.913	-9.64680	4.86606
		282-1659	-4.00598	2.18693	0.611	-11.72611	3.71414
		3100-4999	2.00386	2.08707	0.973	-5.48437	9.49209
		5000-9599	-1.30914	2.15501	0.998	-8.95034	6.33205
		9600-13999	-0.49379	2.17763	1.000	-8.19050	7.20291
		14000-23499	-2.90568	2.75010	0.957	-12.44710	6.63574
		23500+	-3.77943	1.98385	0.574	-11.07836	3.51950
	3100-4999	0-281	-4.39423	1.28217	***0.048****	-8.76109	-0.02736
		282-1659	-6.00984	1.59019	***0.028****	-11.53623	-0.48345
		1660-3099	-2.00386	2.08707	0.973	-9.49209	5.48437
		5000-9599	-3.31300	1.54600	0.431	-8.67584	2.04984
		9600-13999	-2.49765	1.57737	0.753	-7.97630	2.98100

	14000-23499	-4.90954	2.30415	0.449	-13.28449	3.46541
	23500+	-5.78329	1.29681	***0.008*** **	-10.29172	-1.27486
5000-9599	0-281	-1.08122	1.39002	0.992	-5.89611	3.73366
	282-1659	-2.69684	1.67836	0.740	-8.50945	3.11576
	1660-3099	1.30914	2.15501	0.998	-6.33205	8.95034
	3100-4999	3.31300	1.54600	0.431	-2.04984	8.67584
	9600-13999	0.81535	1.66622	1.000	-4.95432	6.58502
	14000-23499	-1.59654	2.36586	0.996	-10.08981	6.89673
	23500+	-2.47029	1.40354	0.653	-7.39899	2.45841
9600-13999	0-281	-1.89658	1.42483	0.874	-6.85674	3.06359
	282-1659	-3.51219	1.70730	0.478	-9.42329	2.39891
	1660-3099	0.49379	2.17763	1.000	-7.20291	8.19050
	3100-4999	2.49765	1.57737	0.753	-2.98100	7.97630
	5000-9599	-0.81535	1.66622	1.000	-6.58502	4.95432
	14000-23499	-2.41189	2.38648	0.964	-10.94882	6.12505
	23500+	-3.28564	1.43803	0.363	-8.35221	1.78092
14000-23499	0-281	0.51531	2.20253	1.000	-7.68815	8.71878
	282-1659	-1.10030	2.39497	1.000	-9.65577	7.45516
	1660-3099	2.90568	2.75010	0.957	-6.63574	12.44710
	3100-4999	4.90954	2.30415	0.449	-3.46541	13.28449
	5000-9599	1.59654	2.36586	0.996	-6.89673	10.08981
	9600-13999	2.41189	2.38648	0.964	-6.12505	10.94882
	23500+	-0.87375	2.21109	1.000	-9.10804	7.36054
23500+	0-281	1.38907	1.10624	0.907	-2.23254	5.01067
	282-1659	-0.22655	1.45207	1.000	-5.34948	4.89638
	1660-3099	3.77943	1.98385	0.574	-3.51950	11.07836
	3100-4999	5.78329	1.29681	***0.008*** **	1.27486	10.29172
	5000-9599	2.47029	1.40354	0.653	-2.45841	7.39899
	9600-13999	3.28564	1.43803	0.363	-1.78092	8.35221
	14000-23499	0.87375	2.21109	1.000	-7.36054	9.10804

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

The one-way ANOVA was conducted to investigate SEXI differences due to marital status. No post hoc tests were conducted due to only two ordinal categories of marital status. Table 45 presents the SEXI descriptive statistics for the population (N=100). Table 46, presents the SEXI ANOVA results, shows borderline significance for marital status [$F(1, 98) = 3.05$, p =0.084].

Table 45

SEXI Descriptive Statistics for Marital Status

	N	M	SD	SE	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
No	52	28.482	4.395	0.609	27.258	29.706	20.082	39.198
Yes	48	30.043	4.538	0.655	28.725	31.361	19.668	43.821
Total	100	29.231	4.510	0.451	28.336	30.126	19.668	43.821

For those with a marital status, it was observed that a spouse might also be named, discussed, or photographed during public events, social media postings, private ceremonies, etc., thereby contributing to the SEXI of each party. In many instances, the availability of marital status provided direct access to additional PICCs, such as maiden name, address, and affiliations.

Table 46

SEXI ANOVA for Marital Status

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	60.809	1	60.809	3.051	0.084
Within Groups	1952.893	98	19.927		
Total	2013.702	99			

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

The one-way ANOVA was conducted to investigate SEXI differences due to estimated worth. Table 47 presents the SEXI descriptive statistics for the population estimated worth (N=100). Table 48, presents the SEXI ANOVA results, shows significance for estimated worth [$F(9, 90) = 3.02$, $p < 0.01$]. Figure 8 presents the estimated worth SEXI for the population. It was observed that the largest group of estimated income was found in the sub $500,000 estimated worth group.

Table 47

SEXI Descriptive Statistics for Estimated Worth (Millions)

	N	M	SD	SE	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
0-.499	17	26.084	3.341	0.810	24.366	27.802	19.668	30.38
.5 - 5.19	10	27.744	5.081	1.607	24.109	31.378	21.082	37.844
5.2 - 7.9	8	27.541	5.149	1.821	23.236	31.846	20.125	34.017
8 - 13.9	10	28.574	3.104	0.982	26.354	30.795	22.692	33.606
14 - 23.39	9	30.966	6.324	2.108	26.105	35.827	20.668	43.821
23.4 - 49.9	9	30.051	3.398	1.133	27.439	32.663	26.142	34.358
50 - 89.9	9	30.924	3.951	1.317	27.887	33.961	23.365	36.913
90 - 179.9	9	28.581	4.263	1.421	25.304	31.857	20.082	32.625
180 - 399.9	9	33.303	3.970	1.323	30.252	36.354	27.195	39.198
400+	10	31.176	2.459	0.778	29.417	32.935	26.268	34.149
Total	100	29.231	4.51	0.451	28.336	30.126	19.668	43.821

Table 48

SEXI ANOVA for Estimated Worth (1000s)

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	467.442	9	51.938	3.023	***0.003*****
Within Groups	1546.26	90	17.181		
Total	2013.702	99			

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

Figure 8

SEXI for the population for estimated worth (1000s)

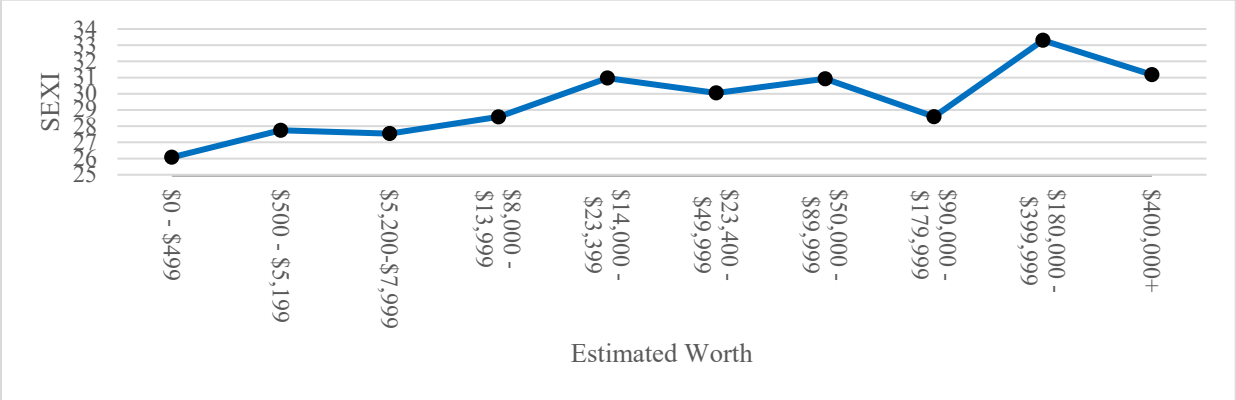


Table 49 presents the SEXI multiple comparisons for estimated worth. Tukey HSD and Games-Howell post hoc tests were conducted to determine which estimated worth categories were significantly different. There was a significant difference between the 0-499 and the 180000-399999 ($p<0.01$) estimated worth groups. The 400000+ group showed a borderline difference ($p=0.077$) with the 0-4999 group.

Table 49

SEXI Multiple Comparisons for Estimated Worth

	(I) EstWorth (millions)	(J) EstWorth (millions)	Mean Difference (I-J)	SE	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Tukey HSD	0-.499	.5 - 5.19	-1.66	1.652	0.991	-7.019	3.7

	5.2 - 7.9	-1.457	1.777	0.998	-7.223	4.309
	8 - 13.9	-2.49	1.652	0.886	-7.85	2.869
	14 - 23.39	-4.882	1.709	0.134	-10.426	0.662
	23.4 - 49.9	-3.967	1.709	0.386	-9.511	1.577
	50 - 89.9	-4.84	1.709	0.141	-10.384	0.704
	90 - 179.9	-2.497	1.709	0.904	-8.04	3.047
	180 - 399.9	-7.219	1.709	***0.002****	-12.762	-1.675
	400+	-5.092	1.652	0.077	-10.452	0.267
.5 - 5.19	0-.499	1.66	1.652	0.991	-3.7	7.019
	5.2 - 7.9	0.203	1.966	1.000	-6.176	6.581
	8 - 13.9	-0.831	1.854	1.000	-6.845	5.183
	14 - 23.39	-3.222	1.904	0.797	-9.401	2.957
	23.4 - 49.9	-2.308	1.904	0.969	-8.487	3.871
	50 - 89.9	-3.18	1.904	0.809	-9.359	2.999
	90 - 179.9	-0.837	1.904	1.000	-7.016	5.342
	180 - 399.9	-5.559	1.904	0.116	-11.738	0.62
	400+	-3.433	1.854	0.701	-9.447	2.581
5.2 - 7.9	0-.499	1.457	1.777	0.998	-4.309	7.223
	.5 - 5.19	-0.203	1.966	1.000	-6.581	6.176
	8 - 13.9	-1.033	1.966	1.000	-7.412	5.346
	14 - 23.39	-3.425	2.014	0.792	-9.96	3.11
	23.4 - 49.9	-2.51	2.014	0.962	-9.045	4.024
	50 - 89.9	-3.383	2.014	0.804	-9.917	3.152
	90 - 179.9	-1.04	2.014	1.000	-7.574	5.495
	180 - 399.9	-5.762	2.014	0.133	-12.296	0.773
	400+	-3.635	1.966	0.702	-10.014	2.744
8 - 13.9	0-.499	2.49	1.652	0.886	-2.869	7.85
	.5 - 5.19	0.831	1.854	1.000	-5.183	6.845
	5.2 - 7.9	1.033	1.966	1.000	-5.346	7.412
	14 - 23.39	-2.392	1.904	0.961	-8.571	3.787
	23.4 - 49.9	-1.477	1.904	0.999	-7.656	4.702
	50 - 89.9	-2.35	1.904	0.965	-8.529	3.829
	90 - 179.9	-0.007	1.904	1.000	-6.186	6.172
	180 - 399.9	-4.729	1.904	0.292	-10.907	1.45
	400+	-2.602	1.854	0.923	-8.616	3.412

14 - 23.39	0-.499	4.882	1.709	0.134	-0.662	10.426
	.5 - 5.19	3.222	1.904	0.797	-2.957	9.401
	5.2 - 7.9	3.425	2.014	0.792	-3.11	9.96
	8 - 13.9	2.392	1.904	0.961	-3.787	8.571
	23.4 - 49.9	0.915	1.954	1.000	-5.425	7.254
	50 - 89.9	0.042	1.954	1.000	-6.297	6.381
	90 - 179.9	2.385	1.954	0.967	-3.954	8.725
	180 - 399.9	-2.337	1.954	0.971	-8.676	4.003
	400+	-0.21	1.904	1.000	-6.389	5.969
23.4 - 49.9	0-.499	3.967	1.709	0.386	-1.577	9.511
	.5 - 5.19	2.308	1.904	0.969	-3.871	8.487
	5.2 - 7.9	2.51	2.014	0.962	-4.024	9.045
	8 - 13.9	1.477	1.904	0.999	-4.702	7.656
	14 - 23.39	-0.915	1.954	1.000	-7.254	5.425
	50 - 89.9	-0.873	1.954	1.000	-7.212	5.467
	90 - 179.9	1.47	1.954	0.999	-4.869	7.81
	180 - 399.9	-3.252	1.954	0.812	-9.591	3.088
	400+	-1.125	1.904	1.000	-7.304	5.054
50 - 89.9	0-.499	4.84	1.709	0.141	-0.704	10.384
	.5 - 5.19	3.18	1.904	0.809	-2.999	9.359
	5.2 - 7.9	3.383	2.014	0.804	-3.152	9.917
	8 - 13.9	2.35	1.904	0.965	-3.829	8.529
	14 - 23.39	-0.042	1.954	1.000	-6.381	6.297
	23.4 - 49.9	0.873	1.954	1.000	-5.467	7.212
	90 - 179.9	2.343	1.954	0.971	-3.996	8.683
	180 - 399.9	-2.379	1.954	0.968	-8.718	3.961
	400+	-0.252	1.904	1.000	-6.431	5.927
90 - 179.9	0-.499	2.497	1.709	0.904	-3.047	8.04
	.5 - 5.19	0.837	1.904	1.000	-5.342	7.016
	5.2 - 7.9	1.04	2.014	1.000	-5.495	7.574
	8 - 13.9	0.007	1.904	1.000	-6.172	6.186
	14 - 23.39	-2.385	1.954	0.967	-8.725	3.954
	23.4 - 49.9	-1.47	1.954	0.999	-7.81	4.869
	50 - 89.9	-2.343	1.954	0.971	-8.683	3.996
	180 - 399.9	-4.722	1.954	0.329	-11.061	1.618

		400+	-2.595	1.904	0.935	-8.774	3.583
	180 - 399.9	0-.499	7.219	1.709	***0.002****	1.675	12.762
		.5 - 5.19	5.559	1.904	0.116	-0.62	11.738
		5.2 - 7.9	5.762	2.014	0.133	-0.773	12.296
		8 - 13.9	4.729	1.904	0.292	-1.45	10.907
		14 - 23.39	2.337	1.954	0.971	-4.003	8.676
		23.4 - 49.9	3.252	1.954	0.812	-3.088	9.591
		50 - 89.9	2.379	1.954	0.968	-3.961	8.718
		90 - 179.9	4.722	1.954	0.329	-1.618	11.061
		400+	2.126	1.904	0.982	-4.052	8.305
	400+	0-.499	5.092	1.652	0.077	-0.267	10.452
		.5 - 5.19	3.433	1.854	0.701	-2.581	9.447
		5.2 - 7.9	3.635	1.966	0.702	-2.744	10.014
		8 - 13.9	2.602	1.854	0.923	-3.412	8.616
		14 - 23.39	0.21	1.904	1.000	-5.969	6.389
		23.4 - 49.9	1.125	1.904	1.000	-5.054	7.304
		50 - 89.9	0.252	1.904	1.000	-5.927	6.431
		90 - 179.9	2.595	1.904	0.935	-3.583	8.774
		180 - 399.9	-2.126	1.904	0.982	-8.305	4.052
Games-Howell	0-.499	.5 - 5.19	-1.66	1.799	0.993	-8.37	5.051
		5.2 - 7.9	-1.457	1.993	0.998	-9.367	6.453
		8 - 13.9	-2.49	1.273	0.635	-6.993	2.012
		14 - 23.39	-4.882	2.258	0.528	-13.741	3.977
		23.4 - 49.9	-3.967	1.393	0.199	-9.031	1.097
		50 - 89.9	-4.84	1.546	0.133	-10.573	0.893
		90 - 179.9	-2.497	1.636	0.860	-8.621	3.627
		180 - 399.9	-7.219	1.552	***0.009****	-12.974	-1.464
		400+	-5.092	1.123	***0.005****	-9.003	-1.182
	.5 - 5.19	0-.499	1.66	1.799	0.993	-5.051	8.37
		5.2 - 7.9	0.203	2.428	1.000	-8.718	9.123
		8 - 13.9	-0.831	1.883	1.000	-7.758	6.096
		14 - 23.39	-3.222	2.65	0.958	-12.928	6.483
		23.4 - 49.9	-2.308	1.966	0.966	-9.48	4.864
		50 - 89.9	-3.18	2.078	0.862	-10.703	4.342
		90 - 179.9	-0.837	2.145	1.000	-8.588	6.913

	180 - 399.9	-5.559	2.081	0.260	-13.094	1.976
	400+	-3.433	1.785	0.657	-10.145	3.28
5.2 - 7.9	0-.499	1.457	1.993	0.998	-6.453	9.367
	.5 - 5.19	-0.203	2.428	1.000	-9.123	8.718
	8 - 13.9	-1.033	2.068	1.000	-9.066	6.999
	14 - 23.39	-3.425	2.785	0.955	-13.672	6.822
	23.4 - 49.9	-2.51	2.144	0.964	-10.701	5.681
	50 - 89.9	-3.383	2.247	0.868	-11.822	5.056
	90 - 179.9	-1.04	2.309	1.000	-9.65	7.571
	180 - 399.9	-5.762	2.251	0.321	-14.21	2.686
	400+	-3.635	1.98	0.705	-11.557	4.286
8 - 13.9	0-.499	2.49	1.273	0.635	-2.012	6.993
	.5 - 5.19	0.831	1.883	1.000	-6.096	7.758
	5.2 - 7.9	1.033	2.068	1.000	-6.999	9.066
	14 - 23.39	-2.392	2.325	0.983	-11.353	6.57
	23.4 - 49.9	-1.477	1.499	0.989	-6.919	3.965
	50 - 89.9	-2.35	1.643	0.899	-8.376	3.677
	90 - 179.9	-0.007	1.727	1.000	-6.385	6.372
	180 - 399.9	-4.729	1.647	0.196	-10.775	1.318
	400+	-2.602	1.252	0.563	-7.121	1.917
14 - 23.39	0-.499	4.882	2.258	0.528	-3.977	13.741
	.5 - 5.19	3.222	2.65	0.958	-6.483	12.928
	5.2 - 7.9	3.425	2.785	0.955	-6.822	13.672
	8 - 13.9	2.392	2.325	0.983	-6.57	11.353
	23.4 - 49.9	0.915	2.393	1.000	-8.177	10.007
	50 - 89.9	0.042	2.486	1.000	-9.255	9.339
	90 - 179.9	2.385	2.542	0.992	-7.055	11.826
	180 - 399.9	-2.337	2.489	0.992	-11.642	6.968
	400+	-0.21	2.247	1.000	-9.074	8.653
23.4 - 49.9	0-.499	3.967	1.393	0.199	-1.097	9.031
	.5 - 5.19	2.308	1.966	0.966	-4.864	9.48
	5.2 - 7.9	2.51	2.144	0.964	-5.681	10.701
	8 - 13.9	1.477	1.499	0.989	-3.965	6.919
	14 - 23.39	-0.915	2.393	1.000	-10.007	8.177
	50 - 89.9	-0.873	1.737	1.000	-7.218	5.473

	90 - 179.9	1.47	1.817	0.997	-5.192	8.133
	180 - 399.9	-3.252	1.742	0.689	-9.615	3.112
	400+	-1.125	1.374	0.997	-6.203	3.953
50 - 89.9	0-.499	4.84	1.546	0.133	-0.893	10.573
	.5 - 5.19	3.18	2.078	0.862	-4.342	10.703
	5.2 - 7.9	3.383	2.247	0.868	-5.056	11.822
	8 - 13.9	2.35	1.643	0.899	-3.677	8.376
	14 - 23.39	-0.042	2.486	1.000	-9.339	9.255
	23.4 - 49.9	0.873	1.737	1.000	-5.473	7.218
	90 - 179.9	2.343	1.937	0.960	-4.718	9.404
	180 - 399.9	-2.379	1.867	0.946	-9.177	4.42
	400+	-0.252	1.53	1.000	-5.994	5.49
90 - 179.9	0-.499	2.497	1.636	0.860	-3.627	8.621
	.5 - 5.19	0.837	2.145	1.000	-6.913	8.588
	5.2 - 7.9	1.04	2.309	1.000	-7.571	9.65
	8 - 13.9	0.007	1.727	1.000	-6.372	6.385
	14 - 23.39	-2.385	2.542	0.992	-11.826	7.055
	23.4 - 49.9	-1.47	1.817	0.997	-8.133	5.192
	50 - 89.9	-2.343	1.937	0.960	-9.404	4.718
	180 - 399.9	-4.722	1.942	0.369	-11.797	2.353
	400+	-2.595	1.62	0.826	-8.727	3.536
180 - 399.9	0-.499	7.219	1.552	***0.009***	1.464	12.974
	.5 - 5.19	5.559	2.081	0.260	-1.976	13.094
	5.2 - 7.9	5.762	2.251	0.321	-2.686	14.21
	8 - 13.9	4.729	1.647	0.196	-1.318	10.775
	14 - 23.39	2.337	2.489	0.992	-6.968	11.642
	23.4 - 49.9	3.252	1.742	0.689	-3.112	9.615
	50 - 89.9	2.379	1.867	0.946	-4.42	9.177
	90 - 179.9	4.722	1.942	0.369	-2.353	11.797
	400+	2.126	1.535	0.912	-3.638	7.891
400+	0-.499	5.092	1.123	***0.005***	1.182	9.003
	.5 - 5.19	3.433	1.785	0.657	-3.28	10.145
	5.2 - 7.9	3.635	1.98	0.705	-4.286	11.557
	8 - 13.9	2.602	1.252	0.563	-1.917	7.121
	14 - 23.39	0.21	2.247	1.000	-8.653	9.074

23.4 - 49.9	1.125	1.374	0.997	-3.953	6.203
50 - 89.9	0.252	1.53	1.000	-5.49	5.994
90 - 179.9	2.595	1.62	0.826	-3.536	8.727
180 - 399.9	-2.126	1.535	0.912	-7.891	3.638

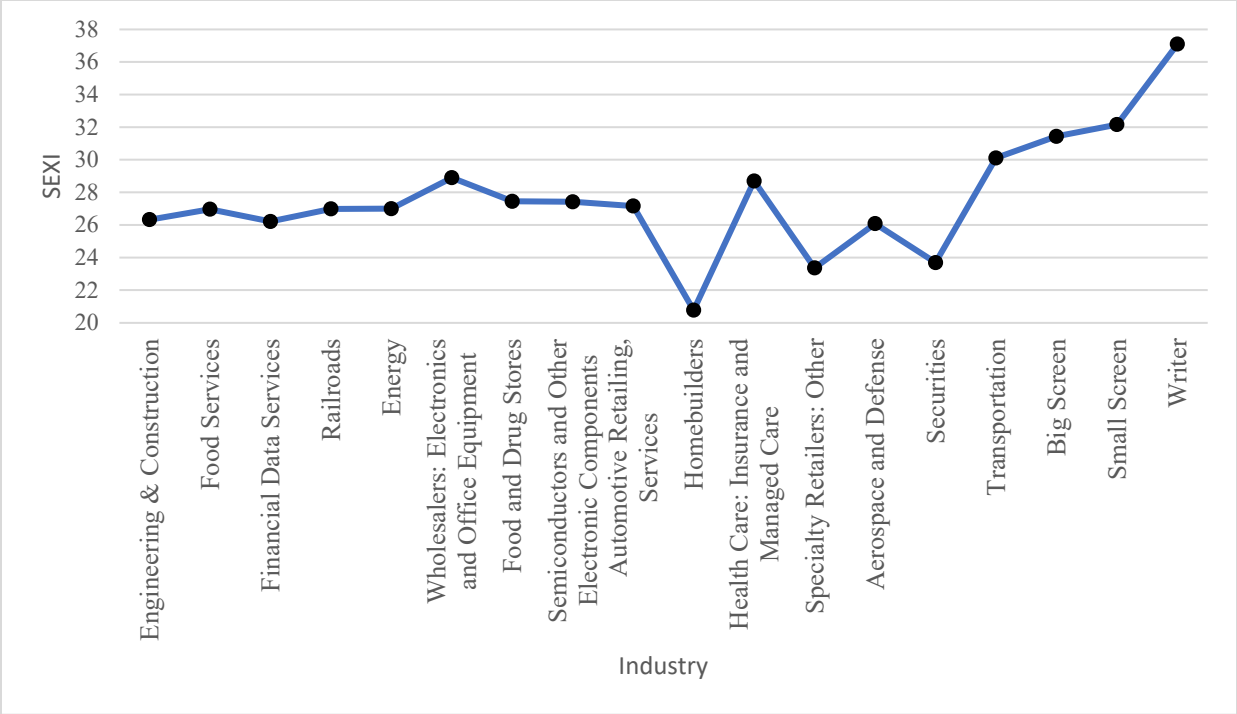
The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

The one-way ANOVA was conducted to investigate SEXI differences due to industry. Figure 9 presents the average SEXI for each industry represented for the population. Table 50 presents the SEXI descriptive statistics for the population (N=100). Table 51, presents the SEXI ANOVA results, shows significance for industry [$F(17, 82) = 5.34$, $p < 0.001$].

Table 52 presents the SEXI multiple comparisons for industry. Tukey HSD post hoc tests were conducted to determine which industries were significantly different. There was a significant difference between writers and Energy (p<0.05), Homebuilders (p<0.001), Specialty Retailers: Other (p<0.01), Aerospace and Defense (p<0.05), as well as Securities (p<0.01). There was also a significant difference between Small Screen Hollywood personas and Homebuilders (p<0.001), Specialty Retailers: Other (p<0.01), Aerospace and Defense (p<0.05), as well as Securities (p<0.05).

Figure 9

SEXI for industries represented by the population



Writers showed a borderline significance with Automotive Retailing, Services (p=0.055). Big Screen Hollywood Personas also indicated a significant difference with Homebuilders (p<0.05), Specialty Retailers: Other (p<0.001), as well as Securities (p<0.05). It was observed that Writers appear to have the highest SEXI values, which may be attributed to their affiliation to multiple industries, such as writing screen plays (Small Screen), scripts (Big Screen), short stories, and novels, thereby providing multiple channels of exposure as each industry group may stereotypically focus on specific public information. Interestingly, there was no significant difference between Writers, Big Screen Hollywood Personas, or Small Screen Hollywood Personas. There were also no significant differences found within the industries of the executives.

Table 50

SEXI Descriptive Statistics for Industry

	N	M	SD	SE	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
Engineering & Construction	2	26.324	8.766	6.198	-52.433	105.080	20.125	32.522
Food Services	3	26.963	1.569	0.906	23.067	30.860	25.243	28.314
Financial Data Services	3	26.214	5.132	2.963	13.465	38.963	20.668	30.795
Railroads	3	26.981	3.090	1.784	19.305	34.656	23.541	29.522
Energy	6	26.999	2.933	1.197	23.921	30.077	23.365	30.278
Wholesalers: Electronics and Office Equipment	3	28.897	1.128	0.652	26.094	31.700	27.610	29.716
Food and Drug Stores	2	27.449	1.230	0.869	16.402	38.496	26.579	28.318
Semiconductors and Other Electronic Components	3	27.417	1.644	0.949	23.333	31.502	25.525	28.494
Automotive Retailing, Services	6	27.157	3.488	1.424	23.496	30.818	21.175	30.110
Homebuilders	3	20.776	0.508	0.293	19.515	22.037	20.190	21.082
Health Care: Insurance and Managed Care	3	28.696	1.464	0.845	25.060	32.332	27.737	30.380
Specialty Retailers: Other	3	23.362	3.732	2.155	14.091	32.633	19.668	27.132
Aerospace and Defense	5	26.078	3.937	1.761	21.190	30.967	20.082	30.681
Securities	3	23.688	2.139	1.235	18.375	29.000	22.228	26.142
Transportation	2	30.109	1.500	1.061	16.629	43.590	29.048	31.170
Big Screen	23	31.436	3.548	0.740	29.901	32.970	24.347	39.198
Small Screen	25	32.154	2.994	0.599	30.918	33.390	26.509	37.844
Writer	2	37.097	9.509	6.724	-48.337	122.532	30.373	43.821
Total	100	29.231	4.510	0.451	28.336	30.126	19.668	43.821

Table 51

SEXI ANOVA for Industry

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1058.318	17	62.254	5.343	***.000******
Within Groups	955.383	82	11.651		
Total	2013.702	99			

The mean difference is significant at $*p < 0.05$, $**p < 0.01$, $***p < 0.001$.

Table 52

SEXI Multiple Comparisons for Industry

(I) Industry	(J) Industry	Mean Difference (I-J)	SE	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Tukey HSD						
Engineering & Construction	Food Services	-0.639	3.116	1.000	-11.865	10.586
	Financial Data Services	0.11	3.116	1.000	-11.116	11.335
	Railroads	-0.657	3.116	1.000	-11.882	10.568
	Energy	-0.675	2.787	1.000	-10.715	9.365
	Wholesalers: Electronics and Office Equipment	-2.573	3.116	1.000	-13.798	8.652
	Food and Drug Stores	-1.125	3.413	1.000	-13.422	11.171
	Semiconductors and Other Electronic Components	-1.094	3.116	1.000	-12.319	10.131
	Automotive Retailing, Services	-0.833	2.787	1.000	-10.873	9.207
	Homebuilders	5.548	3.116	0.942	-5.677	16.773
	Health Care: Insurance and Managed Care	-2.372	3.116	1.000	-13.597	8.853
	Specialty Retailers: Other	2.962	3.116	1.000	-8.263	14.187
	Aerospace and Defense	0.245	2.856	1.000	-10.043	10.533
	Securities	2.636	3.116	1.000	-8.589	13.861
	Transportation	-3.786	3.413	1.000	-16.082	8.511
	Big Screen	-5.112	2.516	0.845	-14.177	3.953
	Small Screen	-5.83	2.508	0.664	-14.866	3.206
	Writer	-10.774	3.413	0.159	-23.07	1.523
Food Services	Engineering & Construction	0.639	3.116	1.000	-10.586	11.865
	Financial Data Services	0.749	2.787	1.000	-9.291	10.789
	Railroads	-0.017	2.787	1.000	-10.057	10.023
	Energy	-0.036	2.414	1.000	-8.73	8.659
	Wholesalers: Electronics and Office Equipment	-1.934	2.787	1.000	-11.974	8.106
	Food and Drug Stores	-0.486	3.116	1.000	-11.711	10.739
	Semiconductors and Other Electronic Components	-0.454	2.787	1.000	-10.494	9.586
	Automotive Retailing, Services	-0.194	2.414	1.000	-8.889	8.501
	Homebuilders	6.187	2.787	0.735	-3.853	16.227
	Health Care: Insurance and Managed Care	-1.733	2.787	1.000	-11.773	8.308
	Specialty Retailers: Other	3.601	2.787	0.998	-6.439	13.641

	Aerospace and Defense	0.885	2.493	1.000	-8.095	9.865
	Securities	3.275	2.787	0.999	-6.765	13.315
	Transportation	-3.146	3.116	1.000	-14.371	8.079
	Big Screen	-4.472	2.095	0.788	-12.021	3.076
	Small Screen	-5.191	2.086	0.545	-12.704	2.322
	Writer	-10.134	3.116	0.126	-21.359	1.091
Financial Data Services	Engineering & Construction	-0.11	3.116	1.000	-11.335	11.116
	Food Services	-0.749	2.787	1.000	-10.789	9.291
	Railroads	-0.766	2.787	1.000	-10.806	9.274
	Energy	-0.784	2.414	1.000	-9.479	7.91
	Wholesalers: Electronics and Office Equipment	-2.683	2.787	1.000	-12.723	7.357
	Food and Drug Stores	-1.235	3.116	1.000	-12.46	9.99
	Semiconductors and Other Electronic Components	-1.203	2.787	1.000	-11.243	8.837
	Automotive Retailing, Services	-0.943	2.414	1.000	-9.638	7.752
	Homebuilders	5.438	2.787	0.883	-4.602	15.478
	Health Care: Insurance and Managed Care	-2.481	2.787	1.000	-12.522	7.559
	Specialty Retailers: Other	2.852	2.787	1.000	-7.188	12.892
	Aerospace and Defense	0.136	2.493	1.000	-8.844	9.116
	Securities	2.526	2.787	1.000	-7.514	12.567
	Transportation	-3.895	3.116	0.998	-15.12	7.33
	Big Screen	-5.221	2.095	0.543	-12.77	2.327
	Small Screen	-5.94	2.086	0.305	-13.453	1.573
	Writer	-10.883	3.116	0.068	-22.108	0.342
Railroads	Engineering & Construction	0.657	3.116	1.000	-10.568	11.882
	Food Services	0.017	2.787	1.000	-10.023	10.057
	Financial Data Services	0.766	2.787	1.000	-9.274	10.806
	Energy	-0.018	2.414	1.000	-8.713	8.677
	Wholesalers: Electronics and Office Equipment	-1.916	2.787	1.000	-11.956	8.124
	Food and Drug Stores	-0.468	3.116	1.000	-11.693	10.757
	Semiconductors and Other Electronic Components	-0.437	2.787	1.000	-10.477	9.603
	Automotive Retailing, Services	-0.176	2.414	1.000	-8.871	8.519
	Homebuilders	6.205	2.787	0.731	-3.836	16.245
	Health Care: Insurance and Managed Care	-1.715	2.787	1.000	-11.755	8.325
	Specialty Retailers: Other	3.619	2.787	0.998	-6.421	13.659
	Aerospace and Defense	0.902	2.493	1.000	-8.078	9.882
	Securities	3.293	2.787	0.999	-6.747	13.333
	Transportation	-3.129	3.116	1.000	-14.354	8.096
	Big Screen	-4.455	2.095	0.793	-12.003	3.093
	Small Screen	-5.173	2.086	0.551	-12.687	2.34

Energy	Writer	-10.117	3.116	0.128	-21.342	1.108
	Engineering & Construction	0.675	2.787	1.000	-9.365	10.715
	Food Services	0.036	2.414	1.000	-8.659	8.73
	Financial Data Services	0.784	2.414	1.000	-7.91	9.479
	Railroads	0.018	2.414	1.000	-8.677	8.713
	Wholesalers: Electronics and Office Equipment	-1.898	2.414	1.000	-10.593	6.797
	Food and Drug Stores	-0.45	2.787	1.000	-10.49	9.59
	Semiconductors and Other Electronic Components	-0.419	2.414	1.000	-9.114	8.276
	Automotive Retailing, Services	-0.158	1.971	1.000	-7.258	6.941
	Homebuilders	6.223	2.414	0.481	-2.472	14.918
	Health Care: Insurance and Managed Care	-1.697	2.414	1.000	-10.392	6.998
	Specialty Retailers: Other	3.637	2.414	0.988	-5.058	12.332
	Aerospace and Defense	0.92	2.067	1.000	-6.526	8.366
	Securities	3.311	2.414	0.996	-5.384	12.006
	Transportation	-3.111	2.787	1.000	-13.151	6.929
	Big Screen	-4.437	1.565	0.312	-10.074	1.2
	Small Screen	-5.155	1.552	0.106	-10.745	0.435
	Writer	-10.099	2.787	***0.047****	-20.139	-0.059
Wholesalers: Electronics and Office Equipment	Engineering & Construction	2.573	3.116	1.000	-8.652	13.798
	Food Services	1.934	2.787	1.000	-8.106	11.974
	Financial Data Services	2.683	2.787	1.000	-7.357	12.723
	Railroads	1.916	2.787	1.000	-8.124	11.956
	Energy	1.898	2.414	1.000	-6.797	10.593
	Food and Drug Stores	1.448	3.116	1.000	-9.777	12.673
	Semiconductors and Other Electronic Components	1.479	2.787	1.000	-8.561	11.52
	Automotive Retailing, Services	1.74	2.414	1.000	-6.955	10.435
	Homebuilders	8.121	2.787	0.268	-1.919	18.161
	Health Care: Insurance and Managed Care	0.201	2.787	1.000	-9.839	10.241
	Specialty Retailers: Other	5.535	2.787	0.867	-4.505	15.575
	Aerospace and Defense	2.819	2.493	1.000	-6.162	11.799
	Securities	5.209	2.787	0.915	-4.831	15.249
	Transportation	-1.212	3.116	1.000	-12.438	10.013
	Big Screen	-2.539	2.095	0.999	-10.087	5.01
	Small Screen	-3.257	2.086	0.982	-10.77	4.256
	Writer	-8.2	3.116	0.443	-19.425	3.025
Food and Drug Stores	Engineering & Construction	1.125	3.413	1.000	-11.171	13.422
	Food Services	0.486	3.116	1.000	-10.739	11.711
	Financial Data Services	1.235	3.116	1.000	-9.99	12.46

	Railroads	0.468	3.116	1.000	-10.757	11.693
	Energy	0.45	2.787	1.000	-9.59	10.49
	Wholesalers: Electronics and Office Equipment	-1.448	3.116	1.000	-12.673	9.777
	Semiconductors and Other Electronic Components	0.031	3.116	1.000	-11.194	11.257
	Automotive Retailing, Services	0.292	2.787	1.000	-9.748	10.332
	Homebuilders	6.673	3.116	0.784	-4.552	17.898
	Health Care: Insurance and Managed Care	-1.247	3.116	1.000	-12.472	9.978
	Specialty Retailers: Other	4.087	3.116	0.997	-7.138	15.312
	Aerospace and Defense	1.371	2.856	1.000	-8.917	11.659
	Securities	3.761	3.116	0.999	-7.464	14.986
	Transportation	-2.66	3.413	1.000	-14.957	9.636
	Big Screen	-3.987	2.516	0.980	-13.052	5.078
	Small Screen	-4.705	2.508	0.912	-13.741	4.331
	Writer	-9.648	3.413	0.317	-21.945	2.648
Semiconductors and Other Electronic Components	Engineering & Construction	1.094	3.116	1.000	-10.131	12.319
	Food Services	0.454	2.787	1.000	-9.586	10.494
	Financial Data Services	1.203	2.787	1.000	-8.837	11.243
	Railroads	0.437	2.787	1.000	-9.603	10.477
	Energy	0.419	2.414	1.000	-8.276	9.114
	Wholesalers: Electronics and Office Equipment	-1.479	2.787	1.000	-11.52	8.561
	Food and Drug Stores	-0.031	3.116	1.000	-11.257	11.194
	Automotive Retailing, Services	0.261	2.414	1.000	-8.434	8.956
	Homebuilders	6.642	2.787	0.622	-3.399	16.682
	Health Care: Insurance and Managed Care	-1.278	2.787	1.000	-11.318	8.762
	Specialty Retailers: Other	4.056	2.787	0.991	-5.984	14.096
	Aerospace and Defense	1.339	2.493	1.000	-7.641	10.319
	Securities	3.73	2.787	0.997	-6.31	13.77
	Transportation	-2.692	3.116	1.000	-13.917	8.533
	Big Screen	-4.018	2.095	0.897	-11.566	3.53
	Small Screen	-4.737	2.086	0.701	-12.25	2.777
	Writer	-9.68	3.116	0.178	-20.905	1.545
Automotive Retailing, Services	Engineering & Construction	0.833	2.787	1.000	-9.207	10.873
	Food Services	0.194	2.414	1.000	-8.501	8.889
	Financial Data Services	0.943	2.414	1.000	-7.752	9.638
	Railroads	0.176	2.414	1.000	-8.519	8.871
	Energy	0.158	1.971	1.000	-6.941	7.258
	Wholesalers: Electronics and Office Equipment	-1.74	2.414	1.000	-10.435	6.955
	Food and Drug Stores	-0.292	2.787	1.000	-10.332	9.748

	Semiconductors and Other Electronic Components	-0.261	2.414	1.000	-8.956	8.434
	Homebuilders	6.381	2.414	0.435	-2.314	15.076
	Health Care: Insurance and Managed Care	-1.539	2.414	1.000	-10.234	7.156
	Specialty Retailers: Other	3.795	2.414	0.981	-4.9	12.49
	Aerospace and Defense	1.078	2.067	1.000	-6.367	8.524
	Securities	3.469	2.414	0.993	-5.226	12.164
	Transportation	-2.953	2.787	1.000	-12.993	7.088
	Big Screen	-4.279	1.565	0.375	-9.916	1.358
	Small Screen	-4.997	1.552	0.137	-10.587	0.593
	Writer	-9.94	2.787	0.055	-19.98	0.1
Homebuilders	Engineering & Construction	-5.548	3.116	0.942	-16.773	5.677
	Food Services	-6.187	2.787	0.735	-16.227	3.853
	Financial Data Services	-5.438	2.787	0.883	-15.478	4.602
	Railroads	-6.205	2.787	0.731	-16.245	3.836
	Energy	-6.223	2.414	0.481	-14.918	2.472
	Wholesalers: Electronics and Office Equipment	-8.121	2.787	0.268	-18.161	1.919
	Food and Drug Stores	-6.673	3.116	0.784	-17.898	4.552
	Semiconductors and Other Electronic Components	-6.642	2.787	0.622	-16.682	3.399
	Automotive Retailing, Services	-6.381	2.414	0.435	-15.076	2.314
	Health Care: Insurance and Managed Care	-7.92	2.787	0.309	-17.96	2.12
	Specialty Retailers: Other	-2.586	2.787	1.000	-12.626	7.454
	Aerospace and Defense	-5.302	2.493	0.793	-14.282	3.678
	Securities	-2.912	2.787	1.000	-12.952	7.128
	Transportation	-9.333	3.116	0.227	-20.559	1.892
	Big Screen	-10.66	2.095	***0.000******	-18.208	-3.111
	Small Screen	-11.378	2.086	***0.000******	-18.891	-3.865
	Writer	-16.321	3.116	***0.000******	-27.546	-5.096
Health Care: Insurance and Managed Care	Engineering & Construction	2.372	3.116	1.000	-8.853	13.597
	Food Services	1.733	2.787	1.000	-8.308	11.773
	Financial Data Services	2.481	2.787	1.000	-7.559	12.522
	Railroads	1.715	2.787	1.000	-8.325	11.755
	Energy	1.697	2.414	1.000	-6.998	10.392
	Wholesalers: Electronics and Office Equipment	-0.201	2.787	1.000	-10.241	9.839
	Food and Drug Stores	1.247	3.116	1.000	-9.978	12.472
	Semiconductors and Other Electronic Components	1.278	2.787	1.000	-8.762	11.318
	Automotive Retailing, Services	1.539	2.414	1.000	-7.156	10.234
	Homebuilders	7.92	2.787	0.309	-2.12	17.96

	Specialty Retailers: Other	5.334	2.787	0.898	-4.706	15.374
	Aerospace and Defense	2.617	2.493	1.000	-6.363	11.597
	Securities	5.008	2.787	0.938	-5.032	15.048
	Transportation	-1.414	3.116	1.000	-12.639	9.811
	Big Screen	-2.74	2.095	0.997	-10.288	4.808
	Small Screen	-3.458	2.086	0.969	-10.972	4.055
	Writer	-8.402	3.116	0.400	-19.627	2.824
Specialty Retailers: Other	Engineering & Construction	-2.962	3.116	1.000	-14.187	8.263
	Food Services	-3.601	2.787	0.998	-13.641	6.439
	Financial Data Services	-2.852	2.787	1.000	-12.892	7.188
	Railroads	-3.619	2.787	0.998	-13.659	6.421
	Energy	-3.637	2.414	0.988	-12.332	5.058
	Wholesalers: Electronics and Office Equipment	-5.535	2.787	0.867	-15.575	4.505
	Food and Drug Stores	-4.087	3.116	0.997	-15.312	7.138
	Semiconductors and Other Electronic Components	-4.056	2.787	0.991	-14.096	5.984
	Automotive Retailing, Services	-3.795	2.414	0.981	-12.49	4.9
	Homebuilders	2.586	2.787	1.000	-7.454	12.626
	Health Care: Insurance and Managed Care	-5.334	2.787	0.898	-15.374	4.706
	Aerospace and Defense	-2.717	2.493	1.000	-11.697	6.264
	Securities	-0.326	2.787	1.000	-10.366	9.714
	Transportation	-6.748	3.116	0.769	-17.973	4.478
	Big Screen	-8.074	2.095	***0.024****	-15.622	-0.526
	Small Screen	-8.792	2.086	***0.007****	-16.305	-1.279
	Writer	-13.735	3.116	***0.004****	-24.961	-2.51
Aerospace and Defense	Engineering & Construction	-0.245	2.856	1.000	-10.533	10.043
	Food Services	-0.885	2.493	1.000	-9.865	8.095
	Financial Data Services	-0.136	2.493	1.000	-9.116	8.844
	Railroads	-0.902	2.493	1.000	-9.882	8.078
	Energy	-0.92	2.067	1.000	-8.366	6.526
	Wholesalers: Electronics and Office Equipment	-2.819	2.493	1.000	-11.799	6.162
	Food and Drug Stores	-1.371	2.856	1.000	-11.659	8.917
	Semiconductors and Other Electronic Components	-1.339	2.493	1.000	-10.319	7.641
	Automotive Retailing, Services	-1.078	2.067	1.000	-8.524	6.367
	Homebuilders	5.302	2.493	0.793	-3.678	14.282
	Health Care: Insurance and Managed Care	-2.617	2.493	1.000	-11.597	6.363

	Specialty Retailers: Other	2.717	2.493	1.000	-6.264	11.697
	Securities	2.391	2.493	1.000	-6.589	11.371
	Transportation	-4.031	2.856	0.994	-14.319	6.257
	Big Screen	-5.357	1.684	0.150	-11.425	0.71
	Small Screen	-6.076	1.672	***0.046****	-12.1	-0.052
	Writer	-11.019	2.856	***0.023****	-21.307	-0.731
Securities	Engineering & Construction	-2.636	3.116	1.000	-13.861	8.589
	Food Services	-3.275	2.787	0.999	-13.315	6.765
	Financial Data Services	-2.526	2.787	1.000	-12.567	7.514
	Railroads	-3.293	2.787	0.999	-13.333	6.747
	Energy	-3.311	2.414	0.996	-12.006	5.384
	Wholesalers: Electronics and Office Equipment	-5.209	2.787	0.915	-15.249	4.831
	Food and Drug Stores	-3.761	3.116	0.999	-14.986	7.464
	Semiconductors and Other Electronic Components	-3.73	2.787	0.997	-13.77	6.31
	Automotive Retailing, Services	-3.469	2.414	0.993	-12.164	5.226
	Homebuilders	2.912	2.787	1.000	-7.128	12.952
	Health Care: Insurance and Managed Care	-5.008	2.787	0.938	-15.048	5.032
	Specialty Retailers: Other	0.326	2.787	1.000	-9.714	10.366
	Aerospace and Defense	-2.391	2.493	1.000	-11.371	6.589
	Transportation	-6.422	3.116	0.830	-17.647	4.803
	Big Screen	-7.748	2.095	***0.038****	-15.296	-0.2
	Small Screen	-8.466	2.086	***0.012****	-15.98	-0.953
	Writer	-13.41	3.116	***0.005****	-24.635	-2.184
Transportation	Engineering & Construction	3.786	3.413	1.000	-8.511	16.082
	Food Services	3.146	3.116	1.000	-8.079	14.371
	Financial Data Services	3.895	3.116	0.998	-7.33	15.12
	Railroads	3.129	3.116	1.000	-8.096	14.354
	Energy	3.111	2.787	1.000	-6.929	13.151
	Wholesalers: Electronics and Office Equipment	1.212	3.116	1.000	-10.013	12.438
	Food and Drug Stores	2.66	3.413	1.000	-9.636	14.957
	Semiconductors and Other Electronic Components	2.692	3.116	1.000	-8.533	13.917
	Automotive Retailing, Services	2.953	2.787	1.000	-7.088	12.993
	Homebuilders	9.333	3.116	0.227	-1.892	20.559
	Health Care: Insurance and Managed Care	1.414	3.116	1.000	-9.811	12.639
	Specialty Retailers: Other	6.748	3.116	0.769	-4.478	17.973
	Aerospace and Defense	4.031	2.856	0.994	-6.257	14.319
	Securities	6.422	3.116	0.830	-4.803	17.647

	Big Screen	-1.326	2.516	1.000	-10.391	7.739
	Small Screen	-2.045	2.508	1.000	-11.081	6.991
	Writer	-6.988	3.413	0.837	-19.284	5.309
Big Screen	Engineering & Construction	5.112	2.516	0.845	-3.953	14.177
	Food Services	4.472	2.095	0.788	-3.076	12.021
	Financial Data Services	5.221	2.095	0.543	-2.327	12.77
	Railroads	4.455	2.095	0.793	-3.093	12.003
	Energy	4.437	1.565	0.312	-1.2	10.074
	Wholesalers: Electronics and Office Equipment	2.539	2.095	0.999	-5.01	10.087
	Food and Drug Stores	3.987	2.516	0.980	-5.078	13.052
	Semiconductors and Other Electronic Components	4.018	2.095	0.897	-3.53	11.566
	Automotive Retailing, Services	4.279	1.565	0.375	-1.358	9.916
	Homebuilders	10.66	2.095	***0.000****	3.111	18.208
	Health Care: Insurance and Managed Care	2.74	2.095	0.997	-4.808	10.288
	Specialty Retailers: Other	8.074	2.095	***0.024****	0.526	15.622
	Aerospace and Defense	5.357	1.684	0.150	-0.71	11.425
	Securities	7.748	2.095	***0.038****	0.2	15.296
	Transportation	1.326	2.516	1.000	-7.739	10.391
	Small Screen	-0.718	0.986	1.000	-4.271	2.834
	Writer	-5.662	2.516	0.715	-14.727	3.403
Small Screen	Engineering & Construction	5.83	2.508	0.664	-3.206	14.866
	Food Services	5.191	2.086	0.545	-2.322	12.704
	Financial Data Services	5.94	2.086	0.305	-1.573	13.453
	Railroads	5.173	2.086	0.551	-2.34	12.687
	Energy	5.155	1.552	0.106	-0.435	10.745
	Wholesalers: Electronics and Office Equipment	3.257	2.086	0.982	-4.256	10.77
	Food and Drug Stores	4.705	2.508	0.912	-4.331	13.741
	Semiconductors and Other Electronic Components	4.737	2.086	0.701	-2.777	12.25
	Automotive Retailing, Services	4.997	1.552	0.137	-0.593	10.587
	Homebuilders	11.378	2.086	***0.000****	3.865	18.891
	Health Care: Insurance and Managed Care	3.458	2.086	0.969	-4.055	10.972
	Specialty Retailers: Other	8.792	2.086	***0.007****	1.279	16.305
	Aerospace and Defense	6.076	1.672	***0.046****	0.052	12.1
	Securities	8.466	2.086	***0.012****	0.953	15.98
	Transportation	2.045	2.508	1.000	-6.991	11.081
	Big Screen	0.718	0.986	1.000	-2.834	4.271
	Writer	-4.943	2.508	0.874	-13.979	4.093

Writer	Engineering & Construction	10.774	3.413	0.159	-1.523	23.07
	Food Services	10.134	3.116	0.126	-1.091	21.359
	Financial Data Services	10.883	3.116	0.068	-0.342	22.108
	Railroads	10.117	3.116	0.128	-1.108	21.342
	Energy	10.099	2.787	***0.047****	0.059	20.139
	Wholesalers: Electronics and Office Equipment	8.2	3.116	0.443	-3.025	19.425
	Food and Drug Stores	9.648	3.413	0.317	-2.648	21.945
	Semiconductors and Other Electronic Components	9.68	3.116	0.178	-1.545	20.905
	Automotive Retailing, Services	9.94	2.787	0.055	-0.1	19.98
	Homebuilders	16.321	3.116	***0.000****	5.096	27.546
	Health Care: Insurance and Managed Care	8.402	3.116	0.400	-2.824	19.627
	Specialty Retailers: Other	13.735	3.116	***0.004****	2.51	24.961
	Aerospace and Defense	11.019	2.856	***0.023****	0.731	21.307
	Securities	13.41	3.116	***0.005****	2.184	24.635
	Transportation	6.988	3.413	0.837	-5.309	19.284
	Big Screen	5.662	2.516	0.715	-3.403	14.727
	Small Screen	4.943	2.508	0.874	-4.093	13.979
Games-Howell						
Engineering & Construction	Food Services	-0.639	6.264	1.000	-231.539	230.26
	Financial Data Services	0.11	6.87	1.000	-123.854	124.073
	Railroads	-0.657	6.45	1.000	-182.682	181.368
	Energy	-0.675	6.313	1.000	-216.316	214.966
	Wholesalers: Electronics and Office Equipment	-2.573	6.232	1.000	-244.28	239.133
	Food and Drug Stores	-1.125	6.259	1.000	-233.828	231.578
	Semiconductors and Other Electronic Components	-1.094	6.271	1.000	-229.897	227.71
	Automotive Retailing, Services	-0.833	6.36	1.000	-203.45	201.784
	Homebuilders	5.548	6.205	0.989	-246.191	257.287
	Health Care: Insurance and Managed Care	-2.372	6.256	1.000	-236.076	231.333
	Specialty Retailers: Other	2.962	6.562	1.000	-158.282	164.206
	Aerospace and Defense	0.245	6.444	1.000	-182.467	182.958
	Securities	2.636	6.32	1.000	-211.158	216.43
	Transportation	-3.786	6.288	0.999	-227.187	219.616
	Big Screen	-5.112	6.242	0.994	-243.311	233.087
	Small Screen	-5.83	6.227	0.985	-249.404	237.743
	Writer	-10.774	9.145	0.975	-117.447	95.9
Food Service	Engineering & Construction	0.639	6.264	1.000	-230.26	231.539

	Financial Data Services	0.749	3.098	1.000	-28.945	30.443
	Railroads	-0.017	2.001	1.000	-15.689	15.654
	Energy	-0.036	1.501	1.000	-7.564	7.493
	Wholesalers: Electronics and Office Equipment	-1.934	1.116	0.880	-9.489	5.622
	Food and Drug Stores	-0.486	1.255	1.000	-11.003	10.031
	Semiconductors and Other Electronic Components	-0.454	1.312	1.000	-8.839	7.931
	Automotive Retailing, Services	-0.194	1.688	1.000	-8.571	8.184
	Homebuilders	6.187	0.952	0.114	-2.769	15.143
	Health Care: Insurance and Managed Care	-1.733	1.239	0.963	-9.661	6.196
	Specialty Retailers: Other	3.601	2.337	0.920	-16.306	23.509
	Aerospace and Defense	0.885	1.98	1.000	-9.798	11.567
	Securities	3.275	1.531	0.739	-7.029	13.58
	Transportation	-3.146	1.395	0.702	-16.566	10.274
	Big Screen	-4.472	1.169	0.199	-10.915	1.97
	Small Screen	-5.191	1.086	0.126	-12.055	1.673
	Writer	-10.134	6.785	0.898	-264.155	243.887
Financial Data Services	Engineering & Construction	-0.11	6.87	1.000	-124.073	123.854
	Food Services	-0.749	3.098	1.000	-30.443	28.945
	Railroads	-0.766	3.459	1.000	-25.87	24.337
	Energy	-0.784	3.196	1.000	-28.07	26.501
	Wholesalers: Electronics and Office Equipment	-2.683	3.034	0.997	-34.244	28.878
	Food and Drug Stores	-1.235	3.088	1.000	-31.423	28.953
	Semiconductors and Other Electronic Components	-1.203	3.111	1.000	-30.577	28.171
	Automotive Retailing, Services	-0.943	3.288	1.000	-26.69	24.805
	Homebuilders	5.438	2.978	0.833	-28.224	39.1
	Health Care: Insurance and Managed Care	-2.481	3.081	0.999	-32.624	27.661
	Specialty Retailers: Other	2.852	3.664	1.000	-21.873	27.577
	Aerospace and Defense	0.136	3.447	1.000	-24.036	24.308
	Securities	2.526	3.21	0.999	-24.914	29.967
	Transportation	-3.895	3.147	0.973	-32.916	25.125
	Big Screen	-5.221	3.054	0.869	-36.028	25.586
	Small Screen	-5.94	3.023	0.793	-37.814	25.934
	Writer	-10.883	7.348	0.909	-155.509	133.743
Railroads	Engineering & Construction	0.657	6.45	1.000	-181.368	182.682
	Food Services	0.017	2.001	1.000	-15.654	15.689
	Financial Data Services	0.766	3.459	1.000	-24.337	25.87
	Energy	-0.018	2.149	1.000	-13.958	13.921

	Wholesalers: Electronics and Office Equipment	-1.916	1.899	0.993	-19.033	15.2
	Food and Drug Stores	-0.468	1.985	1.000	-17.01	16.073
	Semiconductors and Other Electronic Components	-0.437	2.021	1.000	-15.932	15.058
	Automotive Retailing, Services	-0.176	2.283	1.000	-13.658	13.305
	Homebuilders	6.205	1.808	0.420	-13.457	25.867
	Health Care: Insurance and Managed Care	-1.715	1.974	0.998	-17.67	14.239
	Specialty Retailers: Other	3.619	2.797	0.977	-14.606	21.843
	Aerospace and Defense	0.902	2.507	1.000	-12.973	14.777
	Securities	3.293	2.17	0.936	-11.601	18.186
	Transportation	-3.129	2.076	0.931	-19.544	13.286
	Big Screen	-4.455	1.931	0.682	-20.618	11.708
	Small Screen	-5.173	1.882	0.553	-22.465	12.118
	Writer	-10.117	6.956	0.909	-216.389	196.155
Energy	Engineering & Construction	0.675	6.313	1.000	-214.966	216.316
	Food Services	0.036	1.501	1.000	-7.493	7.564
	Financial Data Services	0.784	3.196	1.000	-26.501	28.07
	Railroads	0.018	2.149	1.000	-13.921	13.958
	Wholesalers: Electronics and Office Equipment	-1.898	1.363	0.977	-8.702	4.905
	Food and Drug Stores	-0.45	1.48	1.000	-8.95	8.049
	Semiconductors and Other Electronic Components	-0.419	1.528	1.000	-8.131	7.293
	Automotive Retailing, Services	-0.158	1.861	1.000	-8.557	8.241
	Homebuilders	6.223	1.233	0.067	-0.45	12.895
	Health Care: Insurance and Managed Care	-1.697	1.466	0.995	-8.998	5.604
	Specialty Retailers: Other	3.637	2.465	0.943	-14.184	21.457
	Aerospace and Defense	0.92	2.129	1.000	-9.502	11.342
	Securities	3.311	1.72	0.831	-6.002	12.624
	Transportation	-3.111	1.6	0.813	-13.472	7.25
	Big Screen	-4.437	1.407	0.291	-10.871	1.998
	Small Screen	-5.155	1.339	0.145	-11.596	1.286
	Writer	-10.099	6.83	0.902	-249.571	229.374
Wholesalers: Electronics and Office Equipment	Engineering & Construction	2.573	6.232	1.000	-239.133	244.28
	Food Services	1.934	1.116	0.880	-5.622	9.489
	Financial Data Services	2.683	3.034	0.997	-28.878	34.244
	Railroads	1.916	1.899	0.993	-15.2	19.033
	Energy	1.898	1.363	0.977	-4.905	8.702
	Food and Drug Stores	1.448	1.086	0.954	-10.378	13.274
	Semiconductors and Other Electronic Components	1.479	1.151	0.976	-6.448	9.407

	Automotive Retailing, Services	1.74	1.566	0.996	-6.199	9.679
	Homebuilders	8.121	0.714	***0.022****	2.212	14.03
	Health Care: Insurance and Managed Care	0.201	1.067	1.000	-6.873	7.276
	Specialty Retailers: Other	5.535	2.251	0.640	-16.11	27.18
	Aerospace and Defense	2.819	1.877	0.952	-7.858	13.495
	Securities	5.209	1.396	0.306	-5.536	15.954
	Transportation	-1.212	1.245	0.991	-18.092	15.667
	Big Screen	-2.539	0.986	0.534	-7.062	1.985
	Small Screen	-3.257	0.885	0.199	-7.785	1.271
	Writer	-8.2	6.755	0.950	-272.389	255.989
Food and Drug Stores	Engineering & Construction	1.125	6.259	1.000	-231.578	233.828
	Food Services	0.486	1.255	1.000	-10.031	11.003
	Financial Data Services	1.235	3.088	1.000	-28.953	31.423
	Railroads	0.468	1.985	1.000	-16.073	17.01
	Energy	0.45	1.48	1.000	-8.049	8.95
	Wholesalers: Electronics and Office Equipment	-1.448	1.086	0.954	-13.274	10.378
	Semiconductors and Other Electronic Components	0.031	1.287	1.000	-10.513	10.576
	Automotive Retailing, Services	0.292	1.669	1.000	-8.745	9.329
	Homebuilders	6.673	0.917	0.224	-16.446	29.792
	Health Care: Insurance and Managed Care	-1.247	1.212	0.993	-11.822	9.328
	Specialty Retailers: Other	4.087	2.324	0.860	-16.519	24.693
	Aerospace and Defense	1.371	1.964	1.000	-9.78	12.521
	Securities	3.761	1.51	0.618	-7.964	15.486
	Transportation	-2.66	1.372	0.799	-19.297	13.976
	Big Screen	-3.987	1.142	0.357	-13.088	5.114
	Small Screen	-4.705	1.056	0.272	-15.91	6.5
	Writer	-9.648	6.78	0.912	-265.359	246.062
Semiconductors and Other Electronic Components	Engineering & Construction	1.094	6.271	1.000	-227.71	229.897
	Food Services	0.454	1.312	1.000	-7.931	8.839
	Financial Data Services	1.203	3.111	1.000	-28.171	30.577
	Railroads	0.437	2.021	1.000	-15.058	15.932
	Energy	0.419	1.528	1.000	-7.293	8.131
	Wholesalers: Electronics and Office Equipment	-1.479	1.151	0.976	-9.407	6.448
	Food and Drug Stores	-0.031	1.287	1.000	-10.576	10.513
	Automotive Retailing, Services	0.261	1.711	1.000	-8.242	8.763
	Homebuilders	6.642	0.993	0.110	-2.849	16.132
	Health Care: Insurance and Managed Care	-1.278	1.271	0.997	-9.454	6.898

	Specialty Retailers: Other	4.056	2.355	0.873	-15.597	23.709
	Aerospace and Defense	1.339	2	1.000	-9.383	12.061
	Securities	3.73	1.557	0.643	-6.604	14.063
	Transportation	-2.692	1.424	0.818	-15.868	10.484
	Big Screen	-4.018	1.203	0.311	-10.851	2.815
	Small Screen	-4.737	1.122	0.192	-12.056	2.583
	Writer	-9.68	6.791	0.912	-261.714	242.354
Automotive Retailing, Services	Engineering & Construction	0.833	6.36	1.000	-201.784	203.45
	Food Services	0.194	1.688	1.000	-8.184	8.571
	Financial Data Services	0.943	3.288	1.000	-24.805	26.69
	Railroads	0.176	2.283	1.000	-13.305	13.658
	Energy	0.158	1.861	1.000	-8.241	8.557
	Wholesalers: Electronics and Office Equipment	-1.74	1.566	0.996	-9.679	6.199
	Food and Drug Stores	-0.292	1.669	1.000	-9.329	8.745
	Semiconductors and Other Electronic Components	-0.261	1.711	1.000	-8.763	8.242
	Homebuilders	6.381	1.454	0.121	-1.588	14.349
	Health Care: Insurance and Managed Care	-1.539	1.656	0.999	-9.768	6.69
	Specialty Retailers: Other	3.795	2.583	0.949	-13.11	20.7
	Aerospace and Defense	1.078	2.265	1.000	-9.637	11.794
	Securities	3.469	1.885	0.867	-6.21	13.149
	Transportation	-2.953	1.776	0.912	-13.277	7.372
	Big Screen	-4.279	1.605	0.498	-11.934	3.377
	Small Screen	-4.997	1.545	0.298	-12.711	2.717
	Writer	-9.94	6.873	0.909	-236.773	216.892
Homebuilders	Engineering & Construction	-5.548	6.205	0.989	-257.287	246.191
	Food Services	-6.187	0.952	0.114	-15.143	2.769
	Financial Data Services	-5.438	2.978	0.833	-39.1	28.224
	Railroads	-6.205	1.808	0.420	-25.867	13.457
	Energy	-6.223	1.233	0.067	-12.895	0.45
	Wholesalers: Electronics and Office Equipment	-8.121	0.714	***0.022****	-14.03	-2.212
	Food and Drug Stores	-6.673	0.917	0.224	-29.792	16.446
	Semiconductors and Other Electronic Components	-6.642	0.993	0.110	-16.132	2.849
	Automotive Retailing, Services	-6.381	1.454	0.121	-14.349	1.588
	Health Care: Insurance and Managed Care	-7.92	0.894	0.054	-16.136	0.297
	Specialty Retailers: Other	-2.586	2.175	0.975	-26.685	21.513
	Aerospace and Defense	-5.302	1.785	0.435	-16.356	5.752
	Securities	-2.912	1.269	0.692	-15.908	10.085

	Transportation	-9.333	1.101	0.202	-41.208	22.541
	Big Screen	-10.66	0.796	***0.000******	-13.762	-7.557
	Small Screen	-11.378	0.667	***0.000******	-13.995	-8.761
	Writer	-16.321	6.73	0.700	-289.837	257.195
Health Care: Insurance and Managed Care	Engineering & Construction	2.372	6.256	1.000	-231.333	236.076
	Food Services	1.733	1.239	0.963	-6.196	9.661
	Financial Data Services	2.481	3.081	0.999	-27.661	32.624
	Railroads	1.715	1.974	0.998	-14.239	17.67
	Energy	1.697	1.466	0.995	-5.604	8.998
	Wholesalers: Electronics and Office Equipment	-0.201	1.067	1.000	-7.276	6.873
	Food and Drug Stores	1.247	1.212	0.993	-9.328	11.822
	Semiconductors and Other Electronic Components	1.278	1.271	0.997	-6.898	9.454
	Automotive Retailing, Services	1.539	1.656	0.999	-6.69	9.768
	Homebuilders	7.92	0.894	0.054	-0.297	16.136
	Specialty Retailers: Other	5.334	2.315	0.684	-14.953	25.621
	Aerospace and Defense	2.617	1.953	0.979	-8.031	13.265
	Securities	5.008	1.496	0.358	-5.305	15.321
	Transportation	-1.414	1.356	0.990	-15.31	12.483
	Big Screen	-2.74	1.123	0.612	-8.667	3.187
	Small Screen	-3.458	1.036	0.328	-9.712	2.795
	Writer	-8.402	6.777	0.947	-265.074	248.271
Specialty Retailers: Other	Engineering & Construction	-2.962	6.562	1.000	-164.206	158.282
	Food Services	-3.601	2.337	0.920	-23.509	16.306
	Financial Data Services	-2.852	3.664	1.000	-27.577	21.873
	Railroads	-3.619	2.797	0.977	-21.843	14.606
	Energy	-3.637	2.465	0.943	-21.457	14.184
	Wholesalers: Electronics and Office Equipment	-5.535	2.251	0.640	-27.18	16.11
	Food and Drug Stores	-4.087	2.324	0.860	-24.693	16.519
	Semiconductors and Other Electronic Components	-4.056	2.355	0.873	-23.709	15.597
	Automotive Retailing, Services	-3.795	2.583	0.949	-20.7	13.11
	Homebuilders	2.586	2.175	0.975	-21.513	26.685
	Health Care: Insurance and Managed Care	-5.334	2.315	0.684	-25.621	14.953
	Aerospace and Defense	-2.717	2.783	0.998	-19.268	13.835
	Securities	-0.326	2.483	1.000	-18.745	18.093
	Transportation	-6.748	2.402	0.526	-26.704	13.209
	Big Screen	-8.074	2.278	0.372	-28.826	12.679
	Small Screen	-8.792	2.236	0.322	-30.704	13.12
	Writer	-13.735	7.061	0.797	-198.672	171.202

Aerospace and Defense	Engineering & Construction	-0.245	6.444	1.000	-182.958	182.467
	Food Services	-0.885	1.98	1.000	-11.567	9.798
	Financial Data Services	-0.136	3.447	1.000	-24.308	24.036
	Railroads	-0.902	2.507	1.000	-14.777	12.973
	Energy	-0.92	2.129	1.000	-11.342	9.502
	Wholesalers: Electronics and Office Equipment	-2.819	1.877	0.952	-13.495	7.858
	Food and Drug Stores	-1.371	1.964	1.000	-12.521	9.78
	Semiconductors and Other Electronic Components	-1.339	2	1.000	-12.061	9.383
	Automotive Retailing, Services	-1.078	2.265	1.000	-11.794	9.637
	Homebuilders	5.302	1.785	0.435	-5.752	16.356
	Health Care: Insurance and Managed Care	-2.617	1.953	0.979	-13.265	8.031
	Specialty Retailers: Other	2.717	2.783	0.998	-13.835	19.268
	Securities	2.391	2.151	0.996	-8.901	13.683
	Transportation	-4.031	2.056	0.813	-15.855	7.793
	Big Screen	-5.357	1.91	0.466	-15.744	5.03
	Small Screen	-6.076	1.86	0.330	-16.668	4.516
	Writer	-11.019	6.951	0.880	-218.097	196.059
Securities	Engineering & Construction	-2.636	6.32	1.000	-216.43	211.158
	Food Services	-3.275	1.531	0.739	-13.58	7.029
	Financial Data Services	-2.526	3.21	0.999	-29.967	24.914
	Railroads	-3.293	2.17	0.936	-18.186	11.601
	Energy	-3.311	1.72	0.831	-12.624	6.002
	Wholesalers: Electronics and Office Equipment	-5.209	1.396	0.306	-15.954	5.536
	Food and Drug Stores	-3.761	1.51	0.618	-15.486	7.964
	Semiconductors and Other Electronic Components	-3.73	1.557	0.643	-14.063	6.604
	Automotive Retailing, Services	-3.469	1.885	0.867	-13.149	6.21
	Homebuilders	2.912	1.269	0.692	-10.085	15.908
	Health Care: Insurance and Managed Care	-5.008	1.496	0.358	-15.321	5.305
	Specialty Retailers: Other	0.326	2.483	1.000	-18.093	18.745
	Aerospace and Defense	-2.391	2.151	0.996	-13.683	8.901
	Transportation	-6.422	1.628	0.280	-19.441	6.598
	Big Screen	-7.748	1.439	0.101	-17.465	1.969
	Small Screen	-8.466	1.372	0.091	-19.017	2.085
	Writer	-13.41	6.836	0.794	-251.066	224.246
Transportation	Engineering & Construction	3.786	6.288	0.999	-219.616	227.187
	Food Services	3.146	1.395	0.702	-10.274	16.566

	Financial Data Services	3.895	3.147	0.973	-25.125	32.916
	Railroads	3.129	2.076	0.931	-13.286	19.544
	Energy	3.111	1.6	0.813	-7.25	13.472
	Wholesalers: Electronics and Office Equipment	1.212	1.245	0.991	-15.667	18.092
	Food and Drug Stores	2.66	1.372	0.799	-13.976	19.297
	Semiconductors and Other Electronic Components	2.692	1.424	0.818	-10.484	15.868
	Automotive Retailing, Services	2.953	1.776	0.912	-7.372	13.277
	Homebuilders	9.333	1.101	0.202	-22.541	41.208
	Health Care: Insurance and Managed Care	1.414	1.356	0.990	-12.483	15.31
	Specialty Retailers: Other	6.748	2.402	0.526	-13.209	26.704
	Aerospace and Defense	4.031	2.056	0.813	-7.793	15.855
	Securities	6.422	1.628	0.280	-6.598	19.441
	Big Screen	-1.326	1.293	0.991	-14.834	12.182
	Small Screen	-2.045	1.218	0.869	-19.089	15
	Writer	-6.988	6.807	0.977	-253.843	239.867
Big Screen	Engineering & Construction	5.112	6.242	0.994	-233.087	243.311
	Food Services	4.472	1.169	0.199	-1.97	10.915
	Financial Data Services	5.221	3.054	0.869	-25.586	36.028
	Railroads	4.455	1.931	0.682	-11.708	20.618
	Energy	4.437	1.407	0.291	-1.998	10.871
	Wholesalers: Electronics and Office Equipment	2.539	0.986	0.534	-1.985	7.062
	Food and Drug Stores	3.987	1.142	0.357	-5.114	13.088
	Semiconductors and Other Electronic Components	4.018	1.203	0.311	-2.815	10.851
	Automotive Retailing, Services	4.279	1.605	0.498	-3.377	11.934
	Homebuilders	10.66	0.796	***0.000*****	7.557	13.762
	Health Care: Insurance and Managed Care	2.74	1.123	0.612	-3.187	8.667
	Specialty Retailers: Other	8.074	2.278	0.372	-12.679	28.826
	Aerospace and Defense	5.357	1.91	0.466	-5.03	15.744
	Securities	7.748	1.439	0.101	-1.969	17.465
	Transportation	1.326	1.293	0.991	-12.182	14.834
	Small Screen	-0.718	0.952	1.000	-4.245	2.809
	Writer	-5.662	6.764	0.993	-266.573	255.249
Small Screen	Engineering & Construction	5.83	6.227	0.985	-237.743	249.404
	Food Services	5.191	1.086	0.126	-1.673	12.055
	Financial Data Services	5.94	3.023	0.793	-25.934	37.814
	Railroads	5.173	1.882	0.553	-12.118	22.465
	Energy	5.155	1.339	0.145	-1.286	11.596

	Wholesalers: Electronics and Office Equipment	3.257	0.885	0.199	-1.271	7.785
	Food and Drug Stores	4.705	1.056	0.272	-6.5	15.91
	Semiconductors and Other Electronic Components	4.737	1.122	0.192	-2.583	12.056
	Automotive Retailing, Services	4.997	1.545	0.298	-2.717	12.711
	Homebuilders	11.378	0.667	***0.000******	8.761	13.995
	Health Care: Insurance and Managed Care	3.458	1.036	0.328	-2.795	9.712
	Specialty Retailers: Other	8.792	2.236	0.322	-13.12	30.704
	Aerospace and Defense	6.076	1.86	0.330	-4.516	16.668
	Securities	8.466	1.372	0.091	-2.085	19.017
	Transportation	2.045	1.218	0.869	-15	19.089
	Big Screen	0.718	0.952	1.000	-2.809	4.245
	Writer	-4.943	6.75	0.997	-270.879	260.993
Writer	Engineering & Construction	10.774	9.145	0.975	-95.9	117.447
	Food Services	10.134	6.785	0.898	-243.887	264.155
	Financial Data Services	10.883	7.348	0.909	-133.743	155.509
	Railroads	10.117	6.956	0.909	-196.155	216.389
	Energy	10.099	6.83	0.902	-229.374	249.571
	Wholesalers: Electronics and Office Equipment	8.2	6.755	0.950	-255.989	272.389
	Food and Drug Stores	9.648	6.78	0.912	-246.062	265.359
	Semiconductors and Other Electronic Components	9.68	6.791	0.912	-242.354	261.714
	Automotive Retailing, Services	9.94	6.873	0.909	-216.892	236.773
	Homebuilders	16.321	6.73	0.700	-257.195	289.837
	Health Care: Insurance and Managed Care	8.402	6.777	0.947	-248.271	265.074
	Specialty Retailers: Other	13.735	7.061	0.797	-171.202	198.672
	Aerospace and Defense	11.019	6.951	0.880	-196.059	218.097
	Securities	13.41	6.836	0.794	-224.246	251.066
	Transportation	6.988	6.807	0.977	-239.867	253.843
	Big Screen	5.662	6.764	0.993	-255.249	266.573
	Small Screen	4.943	6.75	0.997	-260.993	270.879

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

The one-way ANOVA was conducted to investigate SEXI differences due to organizational position. Table 53 presents the SEXI descriptive statistics for the population (N=100). Table 54, presents the SEXI ANOVA results, shows significance for organizational position [$F(10, 89) = 7.19$, $p < 0.001$].

Table 53

SEXI Descriptive Statistics for Organizational Position

	N	M	SD	SE	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
CMO	2	23.826	5.233	3.700	-23.190	70.842	20.125	27.526
CFO	11	25.858	3.406	1.027	23.570	28.146	20.190	30.278
CCPAO / CCO	2	25.309	2.862	2.024	-0.402	51.021	23.286	27.333
CAO	2	24.576	1.463	1.034	11.432	37.719	23.541	25.610
COO	4	25.186	4.469	2.235	18.074	32.297	20.668	30.110
CEO	18	27.192	4.016	0.947	25.195	29.190	19.668	32.522
CIO	6	28.155	0.984	0.402	27.122	29.187	27.132	29.716
CHRO	5	26.216	3.125	1.398	22.335	30.096	21.056	28.670
Actor	23	31.436	3.548	0.740	29.901	32.970	24.347	39.198
Producer	25	32.154	2.994	0.599	30.918	33.390	26.509	37.844
Writer	2	37.097	9.509	6.724	-48.337	122.532	30.373	43.821
Total	100	29.231	4.510	0.451	28.336	30.126	19.668	43.821

Table 54

SEXI ANOVA For Organizational Position

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	899.513	10	89.951	7.185	**0.000*****
Within Groups	1114.189	89	12.519		
Total	2013.702	99			

The mean difference is significant at $^{*}p$ <0.05, $^{**}p$ <0.01, $^{***}p$ <0.001.

There was a significant difference between Writer and CMO (p<0.5), CFO (p<0.01), CCPAO/CCO (p<0.05), CAO (p<0.05), COO (p<0.01), CEO (p<0.05), CHRO (p<0.05), as well as borderline significant difference with CIO (p=0.09). There was a significant difference between Producer and CFO (p<0.001), COO (p<0.05), CEO (p<0.01), CHRO (p<0.05), as well as borderline significant difference with CMO (p=0.07). There was a significant difference between Actor and CFO (p<0.01), CEO (p<0.05), as well as COO

(borderline at p=0.06). Table 55 presents the SEXI multiple comparisons for organizational position. Tukey HSD post hoc tests were conducted to determine which organizational position categories were significantly different. Figure 10 presents the average SEXI for each organizational position represented for the population.

Table 55

SEXI Multiple Comparisons for Organizational Position

	(I) OrgPos	(J) OrgPos	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Tukey HSD	CMO	CFO	-2.032	2.720	1.000	-11.018	6.954
		CCPAO / CCO	-1.484	3.538	1.000	-13.174	10.207
		CAO	-0.750	3.538	1.000	-12.440	10.940
		COO	-1.360	3.064	1.000	-11.484	8.764
		CEO	-3.367	2.637	0.970	-12.080	5.347
		CIO	-4.329	2.889	0.917	-13.874	5.216
		CHRO	-2.390	2.960	0.999	-12.171	7.391
		Actor	-7.610	2.608	0.134	-16.228	1.008
		Producer	-8.328	2.600	0.066	-16.919	0.262
		Writer	-13.272	3.538	***0.013****	-24.962	-1.581
	CFO	CMO	2.032	2.720	1.000	-6.954	11.018
		CCPAO / CCO	0.549	2.720	1.000	-8.438	9.535
		CAO	1.282	2.720	1.000	-7.704	10.268
		COO	0.672	2.066	1.000	-6.154	7.498
		CEO	-1.335	1.354	0.996	-5.809	3.139
		CIO	-2.297	1.796	0.970	-8.230	3.636
		CHRO	-0.358	1.908	1.000	-6.663	5.947
		Actor	-5.578	1.297	***0.002****	-9.863	-1.292
		Producer	-6.296	1.280	***0.000*****	-10.526	-2.067
		Writer	-11.239	2.720	***0.004****	-20.226	-2.253
	CCPAO / CCO	CMO	1.484	3.538	1.000	-10.207	13.174
		CFO	-0.549	2.720	1.000	-9.535	8.438
		CAO	0.734	3.538	1.000	-10.956	12.424
		COO	0.123	3.064	1.000	-10.000	10.247

		CEO	-1.883	2.637	1.000	-10.596	6.830
		CIO	-2.845	2.889	0.996	-12.390	6.700
		CHRO	-0.906	2.960	1.000	-10.687	8.874
		Actor	-6.126	2.608	0.411	-14.744	2.492
		Producer	-6.845	2.600	0.248	-15.435	1.746
		Writer	-11.788	3.538	***0.046****	-23.478	-0.098
	CAO	CMO	0.750	3.538	1.000	-10.940	12.440
		CFO	-1.282	2.720	1.000	-10.268	7.704
		CCPAO / CCO	-0.734	3.538	1.000	-12.424	10.956
		COO	-0.610	3.064	1.000	-10.734	9.514
		CEO	-2.617	2.637	0.996	-11.330	6.096
		CIO	-3.579	2.889	0.976	-13.124	5.966
		CHRO	-1.640	2.960	1.000	-11.421	8.141
		Actor	-6.860	2.608	0.250	-15.478	1.758
		Producer	-7.578	2.600	0.135	-16.169	1.012
		Writer	-12.522	3.538	***0.025****	-24.212	-0.832
	COO	CMO	1.360	3.064	1.000	-8.764	11.484
		CFO	-0.672	2.066	1.000	-7.498	6.154
		CCPAO / CCO	-0.123	3.064	1.000	-10.247	10.000
		CAO	0.610	3.064	1.000	-9.514	10.734
		CEO	-2.007	1.956	0.994	-8.469	4.455
		CIO	-2.969	2.284	0.967	-10.515	4.577
		CHRO	-1.030	2.374	1.000	-8.872	6.812
		Actor	-6.250	1.917	0.056	-12.583	0.083
		Producer	-6.968	1.905	***0.018****	-13.264	-0.673
		Writer	-11.911	3.064	***0.009****	-22.035	-1.788
	CEO	CMO	3.367	2.637	0.970	-5.347	12.080
		CFO	1.335	1.354	0.996	-3.139	5.809
		CCPAO / CCO	1.883	2.637	1.000	-6.830	10.596
		CAO	2.617	2.637	0.996	-6.096	11.330
		COO	2.007	1.956	0.994	-4.455	8.469
		CIO	-0.962	1.668	1.000	-6.473	4.549
		CHRO	0.977	1.789	1.000	-4.933	6.886
		Actor	-4.243	1.113	***0.011****	-7.922	-0.564
		Producer	-4.962	1.094	***0.001****	-8.575	-1.348
		Writer	-9.905	2.637	***0.013****	-18.618	-1.192
	CIO	CMO	4.329	2.889	0.917	-5.216	13.874
		CFO	2.297	1.796	0.970	-3.636	8.230
		CCPAO / CCO	2.845	2.889	0.996	-6.700	12.390
		CAO	3.579	2.889	0.976	-5.966	13.124

		COO	2.969	2.284	0.967	-4.577	10.515
		CEO	0.962	1.668	1.000	-4.549	6.473
		CHRO	1.939	2.143	0.998	-5.140	9.018
		Actor	-3.281	1.622	0.634	-8.640	2.078
		Producer	-3.999	1.608	0.327	-9.314	1.315
		Writer	-8.943	2.889	0.087	-18.488	0.602
	CHRO	CMO	2.390	2.960	0.999	-7.391	12.171
		CFO	0.358	1.908	1.000	-5.947	6.663
		CCPAO / CCO	0.906	2.960	1.000	-8.874	10.687
		CAO	1.640	2.960	1.000	-8.141	11.421
		COO	1.030	2.374	1.000	-6.812	8.872
		CEO	-0.977	1.789	1.000	-6.886	4.933
		CIO	-1.939	2.143	0.998	-9.018	5.140
		Actor	-5.220	1.746	0.113	-10.988	0.548
		Producer	-5.938	1.733	***0.035****	-11.665	-0.211
		Writer	-10.882	2.960	***0.017****	-20.662	-1.101
	Actor	CMO	7.610	2.608	0.134	-1.008	16.228
		CFO	5.578	1.297	***0.002****	1.292	9.863
		CCPAO / CCO	6.126	2.608	0.411	-2.492	14.744
		CAO	6.860	2.608	0.250	-1.758	15.478
		COO	6.250	1.917	0.056	-0.083	12.583
		CEO	4.243	1.113	***0.011****	0.564	7.922
		CIO	3.281	1.622	0.634	-2.078	8.640
		CHRO	5.220	1.746	0.113	-0.548	10.988
		Producer	-0.718	1.022	1.000	-4.096	2.659
		Writer	-5.662	2.608	0.531	-14.280	2.956
	Producer	CMO	8.328	2.600	0.066	-0.262	16.919
		CFO	6.296	1.280	***0.000*****	2.067	10.526
		CCPAO / CCO	6.845	2.600	0.248	-1.746	15.435
		CAO	7.578	2.600	0.135	-1.012	16.169
		COO	6.968	1.905	***0.018****	0.673	13.264
		CEO	4.962	1.094	***0.001****	1.348	8.575
		CIO	3.999	1.608	0.327	-1.315	9.314
		CHRO	5.938	1.733	***0.035****	0.211	11.665
		Actor	0.718	1.022	1.000	-2.659	4.096
		Writer	-4.943	2.600	0.715	-13.534	3.647
	Writer	CMO	13.272	3.538	***0.013****	1.581	24.962
		CFO	11.239	2.720	***0.004****	2.253	20.226
		CCPAO / CCO	11.788	3.538	***0.046****	0.098	23.478
		CAO	12.522	3.538	***0.025****	0.832	24.212

		COO	11.911	3.064	***0.009***	1.788	22.035
		CEO	9.905	2.637	***0.013***	1.192	18.618
		CIO	8.943	2.889	0.087	-0.602	18.488
		CHRO	10.882	2.960	***0.017***	1.101	20.662
		Actor	5.662	2.608	0.531	-2.956	14.280
		Producer	4.943	2.600	0.715	-3.647	13.534
Games-Howell	CMO	CFO	-2.032	3.840	0.999	-98.316	94.252
		CCPAO / CCO	-1.484	4.217	1.000	-62.671	59.704
		CAO	-0.750	3.842	1.000	-97.811	96.311
		COO	-1.360	4.323	1.000	-52.294	49.574
		CEO	-3.367	3.819	0.974	-103.801	97.068
		CIO	-4.329	3.722	0.921	-129.694	121.037
		CHRO	-2.390	3.955	0.997	-80.683	75.903
		Actor	-7.610	3.773	0.712	-118.621	103.402
		Producer	-8.328	3.748	0.668	-125.958	109.301
		Writer	-13.272	7.675	0.776	-123.959	97.416
	CFO	CMO	2.032	3.840	0.999	-94.252	98.316
		CCPAO / CCO	0.549	2.269	1.000	-31.648	32.745
		CAO	1.282	1.458	0.991	-7.543	10.107
		COO	0.672	2.459	1.000	-12.675	14.019
		CEO	-1.335	1.397	0.996	-6.284	3.615
		CIO	-2.297	1.103	0.606	-6.549	1.955
		CHRO	-0.358	1.734	1.000	-7.661	6.945
		Actor	-5.578	1.266	***0.009***	-10.135	-1.020
		Producer	-6.296	1.189	***0.002***	-10.673	-1.920
		Writer	-11.239	6.802	0.802	-227.676	205.197
	CCPAO / CCO	CMO	1.484	4.217	1.000	-59.704	62.671
		CFO	-0.549	2.269	1.000	-32.745	31.648
		CAO	0.734	2.273	1.000	-34.426	35.894
		COO	0.123	3.015	1.000	-19.219	19.466
		CEO	-1.883	2.234	0.983	-36.754	32.988
		CIO	-2.845	2.063	0.871	-63.729	58.039
		CHRO	-0.906	2.459	1.000	-25.011	23.198
		Actor	-6.126	2.155	0.523	-49.757	37.504
		Producer	-6.845	2.110	0.474	-57.514	43.824
		Writer	-11.788	7.022	0.793	-181.251	157.675
	CAO	CMO	0.750	3.842	1.000	-96.311	97.811
		CFO	-1.282	1.458	0.991	-10.107	7.543
		CCPAO / CCO	-0.734	2.273	1.000	-35.894	34.426
		COO	-0.610	2.462	1.000	-14.818	13.597

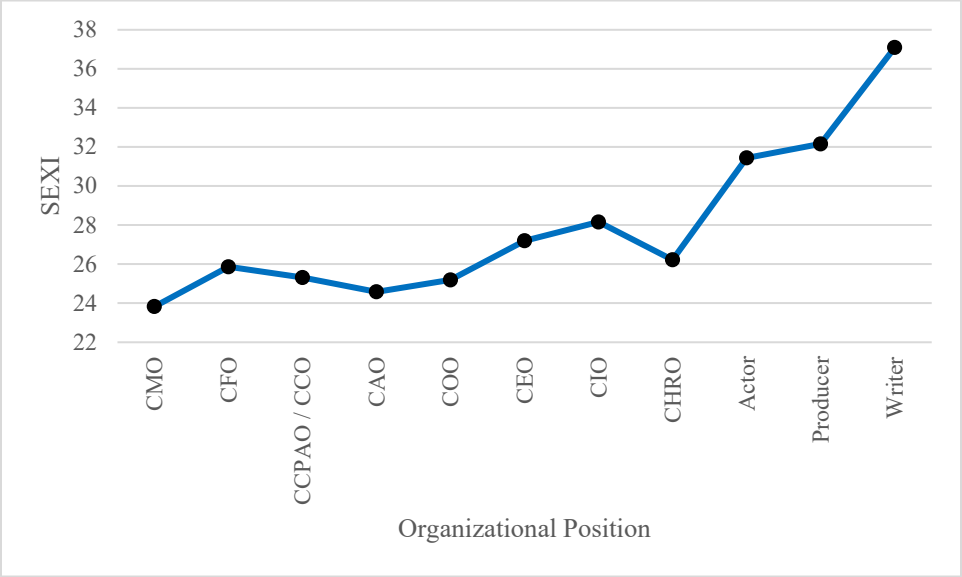
		CEO	-2.617	1.402	0.723	-11.713	6.480
		CIO	-3.579	1.110	0.457	-24.932	17.774
		CHRO	-1.640	1.739	0.988	-11.063	7.783
		Actor	-6.860	1.272	0.142	-18.154	4.434
		Producer	-7.578	1.195	0.145	-21.760	6.603
		Writer	-12.522	6.803	0.755	-228.906	203.863
	COO	CMO	1.360	4.323	1.000	-49.574	52.294
		CFO	-0.672	2.459	1.000	-14.019	12.675
		CCPAO / CCO	-0.123	3.015	1.000	-19.466	19.219
		CAO	0.610	2.462	1.000	-13.597	14.818
		CEO	-2.007	2.427	0.995	-15.502	11.488
		CIO	-2.969	2.270	0.918	-17.852	11.915
		CHRO	-1.030	2.636	1.000	-14.148	12.089
		Actor	-6.250	2.354	0.428	-20.271	7.771
		Producer	-6.968	2.313	0.340	-21.365	7.429
		Writer	-11.911	7.085	0.792	-168.930	145.107
	CEO	CMO	3.367	3.819	0.974	-97.068	103.801
		CFO	1.335	1.397	0.996	-3.615	6.284
		CCPAO / CCO	1.883	2.234	0.983	-32.988	36.754
		CAO	2.617	1.402	0.723	-6.480	11.713
		COO	2.007	2.427	0.995	-11.488	15.502
		CIO	-0.962	1.028	0.996	-4.650	2.726
		CHRO	0.977	1.688	1.000	-6.222	8.175
		Actor	-4.243	1.201	***0.040****	-8.381	-0.106
		Producer	-4.962	1.120	***0.005****	-8.857	-1.066
		Writer	-9.905	6.790	0.850	-229.674	209.865
	CIO	CMO	4.329	3.722	0.921	-121.037	129.694
		CFO	2.297	1.103	0.606	-1.955	6.549
		CCPAO / CCO	2.845	2.063	0.871	-58.039	63.729
		CAO	3.579	1.110	0.457	-17.774	24.932
		COO	2.969	2.270	0.918	-11.915	17.852
		CEO	0.962	1.028	0.996	-2.726	4.650
		CHRO	1.939	1.454	0.923	-5.677	9.555
		Actor	-3.281	0.842	***0.020****	-6.236	-0.326
		Producer	-3.999	0.721	***0.000*****	-6.540	-1.459
		Writer	-8.943	6.736	0.882	-245.495	227.610
	CHRO	CMO	2.390	3.955	0.997	-75.903	80.683
		CFO	0.358	1.734	1.000	-6.945	7.661
		CCPAO / CCO	0.906	2.459	1.000	-23.198	25.011
		CAO	1.640	1.739	0.988	-7.783	11.063

		COO	1.030	2.636	1.000	-12.089	14.148
		CEO	-0.977	1.688	1.000	-8.175	6.222
		CIO	-1.939	1.454	0.923	-9.555	5.677
		Actor	-5.220	1.581	0.190	-12.458	2.018
		Producer	-5.938	1.521	0.117	-13.296	1.420
		Writer	-10.882	6.868	0.818	-210.125	188.361
	Actor	CMO	7.610	3.773	0.712	-103.402	118.621
		CFO	5.578	1.266	***0.009****	1.020	10.135
		CCPAO / CCO	6.126	2.155	0.523	-37.504	49.757
		CAO	6.860	1.272	0.142	-4.434	18.154
		COO	6.250	2.354	0.428	-7.771	20.271
		CEO	4.243	1.201	***0.040****	0.106	8.381
		CIO	3.281	0.842	***0.020****	0.326	6.236
		CHRO	5.220	1.581	0.190	-2.018	12.458
		Producer	-0.718	0.952	0.999	-3.951	2.514
		Writer	-5.662	6.764	0.978	-233.126	221.802
	Producer	CMO	8.328	3.748	0.668	-109.301	125.958
		CFO	6.296	1.189	***0.002****	1.920	10.673
		CCPAO / CCO	6.845	2.110	0.474	-43.824	57.514
		CAO	7.578	1.195	0.145	-6.603	21.760
		COO	6.968	2.313	0.340	-7.429	21.365
		CEO	4.962	1.120	***0.005****	1.066	8.857
		CIO	3.999	0.721	***0.000*****	1.459	6.540
		CHRO	5.938	1.521	0.117	-1.420	13.296
		Actor	0.718	0.952	0.999	-2.514	3.951
		Writer	-4.943	6.750	0.988	-236.769	226.882
	Writer	CMO	13.272	7.675	0.776	-97.416	123.959
		CFO	11.239	6.802	0.802	-205.197	227.676
		CCPAO / CCO	11.788	7.022	0.793	-157.675	181.251
		CAO	12.522	6.803	0.755	-203.863	228.906
		COO	11.911	7.085	0.792	-145.107	168.930
		CEO	9.905	6.790	0.850	-209.865	229.674
		CIO	8.943	6.736	0.882	-227.610	245.495
		CHRO	10.882	6.868	0.818	-188.361	210.125
		Actor	5.662	6.764	0.978	-221.802	233.126
		Producer	4.943	6.750	0.988	-226.882	236.769

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

Figure 10

SEXI for organizational position for the population



The one-way ANOVA was conducted to investigate SEXI differences due to philanthropic contributions. Table 56 presents the SEXI descriptive statistics for the population (N=100). Table 57, presents the SEXI ANOVA results, shows significance for philanthropic contributions [$F(1, 98) = 12.36$, $p < 0.01$]. For the population, it was observed philanthropic contributions were often associated with press releases, events, and notices posted on the organization web site. These notifications typically include images, names, ages, geographical information, marital status via spouse mention, organization affiliation, position, industry, etc.

Table 56

SEXI Descriptive Statistics for Philanthropic Contributions

	N	M	SD	SE	95% Confidence Interval for Mean	Min	Max

					Lower Bound	Upper Bound		
No	41	27.430	4.916	0.768	25.878	28.982	19.668	43.821
Yes	59	30.483	3.764	0.490	29.502	31.464	20.082	39.198
Total	100	29.231	4.510	0.451	28.336	30.126	19.668	43.821

Table 57

SEXI ANOVA for Philanthropic Contributions

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	225.474	1	225.474	12.357	**0.001****
Within Groups	1788.228	98	18.247		
Total	2013.702	99			

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

The one-way ANOVA was conducted to investigate SEXI differences due to military / police experience. Table 58 presents the SEXI descriptive statistics for the population (N=100).

Table 58

SEXI Descriptive Statistics for Military / Police Experience

	N	M	SD	SE	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
No	96	29.26867	4.51537	0.46085	28.35377	30.18357	19.66830	43.82105
Yes	4	28.33419	4.94763	2.47381	20.46141	36.20697	24.34743	35.54129
Total	100	29.23129	4.51004	0.45100	28.33640	30.12618	19.66830	43.82105

Table 59, presents the SEXI ANOVA results, shows no significance for military / police experience [$F(1, 98) = 12.36$, p =0.69]. There were only 4 people across the

population having prior military or police experience. In contrast, nine members of the expert panel held military or police experience.

Table 59

SEXI ANOVA For Military Police Experience

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	3.353	1	3.353	0.163	0.687
Within Groups	2010.348	98	20.514		
Total	2013.702	99			

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

RQ6 Analysis: SEXI Analysis of Executives and Hollywood Personas

For RQ6, analysis was performed to investigate differences between the two groups: Executives of Fortune 500 companies and Hollywood Personas. Table 60 presents the *t*-test normal distribution data for the Execs and Hpers and indicates the distributions were sufficiently normal for the purposes of conducting a *t*-test (i.e., skewness < |2.0| and kurtosis < |9.0|) (Schmider et al., 2010).

Table 60

T-Test *Normal Distribution Data*

	N	M	SD	SE	Skewness	Kurtosis
Execs	50	26.44136	3.47880	0.49198	-.543	-.820
Hpers	50	32.02122	3.62061	0.51203	.573	1.256
Total	100	29.23129	4.51004	0.45100	.069	.493

The independent samples *t*-test was associated with a statistically significant effect, t (98) = 7.858, p<0.001. Cohen's delta (d) = 1.69 indicating a very large effect size (Cohen, 1992; Sawilowsky, 2009). The confidence interval was 4.17 to 7.99. With the *df*

(98) and the α level (0.05), the critical *t-value* is equal to |1.984|. The calculated *t-value* was equal to |7.858|. Table 61 presents the descriptive statistics associated with SEXI. Table 62 presents the SEXI ANOVA results for Execs and Hpers. There was a statistically significant difference between groups as determined by one-way ANOVA [$F(1, 98) = 61.75$, $p < 0.001$].

Table 61

Descriptive Statistics Associated with SEXI

	N	M	SD	SE	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
Execs	50	26.44136	3.47879	0.49198	25.45270	27.43002	19.66830	32.52197
Hpers	50	32.02122	3.62061	0.51203	30.99226	33.05019	24.34743	43.82105
Total	100	29.23129	4.51004	0.45100	28.33640	30.12618	19.66830	43.82105

Table 62

SEXI ANOVA For Executives and Hollywood Personas

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	778.371	1	778.371	61.749	**.000*** **
Within Groups	1235.33	98	12.605		
Total	2013.702	99			

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001.

Data analysis for Phase 3 showed the most significant SEXI demographics were associated with Industry and Organizational Position ($p<0.001$). The next significant SEXI demographics were associated with Estimated Income and Philanthropic Contributions (p <0.01). Income was also significant ($p<0.05$), while Marital Status was

borderline significant (p=0.08) for SEXI demographics. Age, Gender, and Military / Police Experience were not significant for SEXI demographics. Table 63 presents a summary of the SEXI Results by Demographics across all members of the population.

Table 63

SEXI Results by Demographics (N=100)

Item	df	Mean Square Between Groups	F	Sig.
Age	7	26.284	1.322	0.249
Gender	1	22.222	1.094	0.298
Income	***7***	***40.465***	***2.151***	***0.046****
Marital Status	1	60.809	3.051	0.084ǂ
Estimated Worth	***9***	***51.938***	***3.023***	***0.003****
Industry	***17***	***62.254***	***5.343***	***0.000*****
Organization Position	***10***	***89.951***	***7.185***	***0.000*****
Philanthropic Contributions	***1***	***225.474***	***12.357***	***0.001****
Military Police Experience	1	3.353	0.163	0.687

The mean difference is significant at *p <0.05, **p <0.01, ***p <0.001, ǂ borderline p <0.09.

The Execs group (N=50) was associated with a SEXI M = 26.44 (SD = 3.48). By comparison, the Hpers (N = 50) was associated with a numerically larger SEXI M = 32.02 (SD = 3.62). A statistically significant difference was shown between the Execs and Hpers groups (p < 0.001). Hpers Writers were associated with the highest SEXI overall M=37.10 (SD = 4.51), while the Execs CIOs were associated with the highest SEXI for the group M = 28.6 (SD = 0.98).

Summary

The process for the SEXI development began with the collection of 105 PICCs from a variety of literature sources. In Round 1, the PICCs were presented to SMEs asked to indicate where in the range of 1 (minimal exposure) to 10 (maximum exposure) each

item, can in and of itself, identify a given individual using a 10-point Likert Scale. In Round 2, the PICCs were presented to SMEs asked to categorize each as not being personal information, PUI, PII, or PDI.

Pre-analysis was performed using Mahalanobis Distance and Box Plots via IBM SPSS to detect outliers, and no items showed a significant value requiring removal. Round 1 responses were converted to Round 2 categories. Analysis was performed on each respective round as well as across both rounds. Consensus was found across 78 of the 105 items. All SME responses were reported and summarized.

This chapter contained the results and data analysis performed by this developmental research study. This study used a three-phased approach, with each phase addressing at least one research question. In the first phase a literature review was performed to ascertain potential personal information components, which were presented to a Delphi panel addressing RQ1 and RQ2. An instrument was developed in Phase 2, to address RQ3, using the PDI, PII, PII components, weights, and categories from the SME feedback. The third phases consisted of data collection and analysis to address RQ4, RQ5, and RQ6. Table 63 presents a summary of the SEXI Results by Demographics across all members of the population.

Data collection and analysis of the SMEs' feedback addressed the first three research questions of this study. For RQ1, SMEs' feedback was assessed to determine the set of personal information components for an index of SE exposure. For RQ2, SMEs feedback was assessed to determine the approved categories for the identified set of personal information components. For RQ3, SMEs feedback was assessed to identify weights of

1 the personal information components and categories that enable a validated hierarchical
2 aggregation to the SEXI benchmarking index.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

Prior research has shown the information being used to execute SE attacks typically originates at the target or those closely associated with them (Heartfield & Loukas, 2015; Junger et al., 2017; Luo et al., 2013). Studies have also shown a significant increase of personal information exposed on social networking sites and an overall willingness to provide personal content by Americans (Acquisti et al., 2015; Boyd & Ellison, 2007; Hong & Thong, 2013). Olmstead and Smith (2017) stated that 64% of Americans had been exposed via a data breach. The availability of OSPI allows potential hackers to glean necessary information to successfully social engineer an exposed target via a myriad of attack vectors (Heartfield & Loukas, 2015; Luo et al., 2013). Due to the proliferation of SE attacks due to publicly available OSPI (Heartfield & Loukas, 2015; Maynard et al., 2015; Mitnick & Simon, 2002), the need exists to assess the exposure of personal information. This study built upon prior research that called for a tool to serve as a predictor and determinant for potential SE attacks (Heartfield & Loukas, 2015; Mohaisen et al., 2017) seeking the specificity of available information (Tetri & Vuorinen, 2013). Additionally, Schwartz and Solove (2011) suggested the delineation of personal information that will *definitively* identify someone, while McCallister et al. (2010) as well as Schwartz and Solove (2011) suggested a third demarcation of personal information that has *no chance* to identify an individual on its own. Herein, these additional PII categories were declared as PDI and PUI, respectively.

The main goal of this developmental research study was to develop and validate SEXI using OSPI to assist in identifying and classifying SE vulnerabilities. This study achieved the six goals via a three-phased approached with each phase addressing at least one research question. In the first phase, a literature review was performed to ascertain 105 potential personal information components, which were presented to a Delphi panel and addressed the first two goals of this study. The first specific goal of this research study was to gather the SME-approved components for an index of SE exposure by eliciting quantitative feedback on personal information. The second specific goal of this research study was to assign categories to personal information components based on exposure.

In the second phase, an instrument was developed, and the third goal of this study was addressed. The third specific goal of this research study was to develop and validate, using SMEs, the components and hierarchical weights for SEXI via a Delphi method. The SEXI instrument was created using the feedback from the SMEs.

The third phase consisted of data collection and analysis, therein addressing the remaining goals. The fourth specific goal of this research study was to apply the SEXI instrument to measure the OSPI exposure of 50 executives of Fortune 500 organizations and 50 Hollywood celebrities. The fifth specific goal of this research study was to assess and statistically test for significant mean differences of the SEXI of 100 individuals based on demographical indicators of age, gender, income, marital status, estimated worth, industry, organizational position, philanthropic contributions, and prior military/police experience. The sixth specific goal of this research study was to compare the SEXI results

from the set of US executives to those of Hollywood personas in an effort to uncover which group is more vulnerable to SE attack from an OSPI exposure perspective.

Discussion

First, this developmental research study ascertained SMEs perception and experience for SE attempts within their work environment, as well as gather their opinion on the implementation of security policy as it relates to privacy and personal information. Second, this developmental research study resulted in a defining a comprehensive list of 105 validated PICCs. Third, this study resulted in establishing validated weights and measures for the PICCs. Fourth, this study resulted in establishing three categories of personal information: PDI, PII, and PUI. Fifth, this study resulted in establishing categorical weights for personal information based on the level of exposure the respective category represents. Sixth, this study resulted in establishing the SEXI benchmarking index for measuring the personal information exposure due to OSPI. Sixth, this study measured the SEXI of 50 Fortune 500 Executives and 50 Hollywood Personas. Last, this study compared the SEXI of the group of Hollywood Executives to that of the Hollywood Personas.

The data analysis was performed using one-way ANOVA in Phase 3 revealed that age, gender, and military/police experience are not significant in the SEXI assessment. Moreover, the data analysis of Phase 3 revealed that income, estimated worth, industry, organizational position, as well as philanthropic contributions are significant, and suggest differences in SEXI assessment scores. Marital Status is significant at $p < 0.09$. Therefore, a result of this study shows that income, worth, employment, philanthropic contributions, and marital status found in OSPI can significantly increase the SEXI of an

individual. Moreover, another result of this study shows that Hollywood Personas have a significantly higher SEXI than Fortune 500 Executives.

Overall, every Fortune 500 Executive and Hollywood Persona assessed had a SEXI value greater than zero due to OSPI consisting of Electronic facial image / selfie, Photographic image, Demographics, Full Name, Geographical indicators, Organization affiliation / membership, Professional title, Age, and Gender. Additionally, 90% or more also had their Activities, Date of Birth, Education Information, Employment History, Employment Information, Global Positioning Systems, Persistent Identifier, Street Address, Telephone Number, Zip Code, Nationality, and Race available via OSPI.

Phase 1 of this study had limitations due to the large data collection instruments that required a high level of commitment from the SMEs. While potential SMEs were informed of the time requirements before they began their feedback, several took over 30 minutes to complete the forms. Phase 2 of this study had limitations due to the viability of data sources to test an instrument with, before data collection was performed. During the development of the preliminary instrument, Google+ was shut down for most users and the Cambridge Analytica scandal caused Facebook to drastically alter their personal information API. In addition, other data sources miserably failed authentication of their data. Initially, the instrument was to have between three and five sources. The final instrument ended up using approximately two dozen data sources. A possible inconsequential limitation of this study is that many data sources are required for data collection. For this study, data sources were selected that had the potential of providing data for the respective group.

Implications

This research study contributes to the privacy body of knowledge by providing weights, measures, and categories of exposure to the PICCs presented in the literature. This study contributes to the SE literature by providing an index to assess exposure of personal information to SE attacks and as an example of using OSPI to gather information to target specific groups. The information security body of knowledge can also benefit by this research study with the correlation of the low, moderate, and high risk nomenclature to the exposure categories of personal information. This research study contributes to the cybersecurity body of knowledge by providing organizations with validated materials for providing personal information exposure assessments. Specifically, the literature has shown that regarding personal information and privacy, the research tends to be contextual and ambiguous as to the significance of personal information components. Accordingly, the body of knowledge on personal information did not appear to view the topic without context, nor did it measure or categorize the exposure of individual PICCs. Therefore, this study provides valuable information by quantifying and categorizing personal information exposure without contextual constraints. SEXI will help organizations identify the potential risk and exposure associated with the personal information they are collecting, securing, and storing. Moreover, if the weights and measures of this study are implemented by organizations, this should increase overall personal information data security by providing a quantifiable measure of the data collected, accessed, and stored, while potentially offering the means to understand which personal information components provide the greatest exposure and risk.

Recommendations and Future Research

This study was a developmental research study and outlined an approach for designing, developing, validating, and employing a benchmarking instrument assessment tool for measuring the exposure of personal information due to OSPI using a Delphi method. Mitnick and Simon (2002), McCallister et al. (2010), Schwartz and Solove (2011), Pavlou (2011), Junger et al. (2017) discussed the issue of privacy being contextual and thereby idiosyncratic. The approach demonstrated by this research assessed personal information outside contextual restraints and is transferable to multiple fields of study where an instrument is developed or used. This research study provides several opportunities for future research studies to be conducted.

SEXI Benchmarking Instrument

First, the SEXI benchmarking instrument can be used on a larger sample, other groups, organizational members, and even random individuals having no known group affiliation as well as conduct more robust data analysis to determine the exposure of personal information (Bélanger & Crossler, 2011). Second, the SEXI benchmarking index is large. Future studies can research streamlining the SEXI benchmarking index, by reducing the number of PICCs, creating subcategories (i.e. biometrics, demographics, cyber presence, physical footprint), increase validity, etc. (DeLone & McLean, 2003). As this study developed a benchmarking index, more refinement should be expected and explored. Several PICCs were not found for any of the Hollywood personas or executives. This may leave an opportunity to consider the removal of some items and the adjustment of the normalization coefficients. SEXI could also be expanded to include new PICCs not included in the index. Third, ascertaining the minimum SEXI measure

that indicates an individual has been identified as defined by PDI, PII, and PUI (Schwartz & Solove, 2011). Fourth, future research can attempt to associate the SEXI benchmarking index to monetary value.

Data Collection and Storage

Fifth, future studies could use the SEXI benchmarking index to assess the potential exposure of collected personal information data for organizations, government agencies, online forms, social media profiles, etc. (Mouton et al., 2016). Sixth, future research can use SEXI as a pretest and posttest while investigating the potential change of SEXI once a population interacts (e.g., requests removal/addition) with OSPI (Wolff, 2016; Xu et al., 2011). Seventh, future studies can review, assess, and quantify the level of exposure for PICCs contained in breach data, stored data, and requested data using the SEXI benchmarking index (Lee et al., 2011; Mouton et al., 2016). Eighth, OSPI sources may contain erroneous or false data, as multiple sources evaluated during this study proved to contain fake or erroneous data. The SEXI benchmarking index could be used to evaluate data sources against authenticated data (Fleisher, 2008). Ninth, perceived personal information exposure versus what is measured by SEXI could be studied (Junger et al., 2017; Zhang et al., 2014).

Social Engineering and Data Breaches

Tenth, integration of the Privacy Web and Privacy Chain concepts into SEXI by ascertaining the original source and proliferation of respective PICCs for any given individual (Heartfield & Loukas, 2015; Tetri & Vuorinen, 2013). Eleventh, the SEXI benchmarking instrument can be used as assess, aggregate, and analyze SE events as well

as data breaches to improve the SE literature that has limited quantifiable attack vector data (Heartfield & Loukas, 2015; Mouton et al., 2016).

Information Security Culture

Twelfth, the SME feedback indicated surprising Information Security Culture data that future studies may build upon and expand, with 32% stating that their organization had minimal consequences to procedure violation as well as the majority of working environments were described as having a culture that circumvents policy (Culnan & Williams, 2009; Johnston et al., 2015; Luo et al., 2013).

Summary

The research problem addressed by this study is the proliferation of SE attacks due to publicly available OSPI. Social engineers are able to pretend and persuade even experts into behaving favorably for the attacker, even when they suspect something is wrong and are mandated as well as trained to take appropriate defensive action (Allen, 2006; Heartfield & Loukas, 2015).

The availability of OSPI has grown substantially over recent years and looks to have exponential growth as more people gain access to the Web and service providers continually introduce innovative mechanisms for self-disclosure (Acquisti et al., 2015). Prior research has shown the information being used to execute SE attacks typically originates at the target or those closely associated with them (Heartfield & Loukas, 2015; Junger et al., 2017; Luo et al., 2013). Studies have also shown a significant increase of personal information exposed on social networking sites and the overall willingness to provide personal content by Americans (Acquisti et al., 2015; Boyd & Ellison, 2007; Hong & Thong, 2013). The Privacy Rights Clearinghouse (2018) logged approximately

10 billion breached data records between 2005 and 2018. Additionally, Olmstead and Smith (2017) found that 64% of Americans had been exposed via a data breach.

According to Jasper (2017), often data from breaches are shared on the hacker underground marketplace within 72 hours, facilitating further successful attacks using the information. Public release of protected information serves as the foundation for SE attackers to mount attacks through unknown vectors using a massive amount of accurate data to orchestrate a cacophony of SE attacks (Mouton et al., 2016; Tetri & Vuorinen, 2013).

The main goal of this research was to develop and validate a SEXI via the Delphi method using OSPI to assist in identifying and classifying SE vulnerabilities. This work built upon the work of multiple disciplines within the body of knowledge. The initial SEXI benchmarking index was based on Swarm Theory concepts (i.e. swarm, foragers, food sources) discussed at length by Kennedy et al. (2001b). From the PDI literature, this study was building upon the idea of multiple categories of PII presented by Schwartz and Solove (2011). From PII literature, this study is building upon McCallister et al. (2010) who associated personal information to measures of risk and harm, and indicated that a one-size-fits-all understanding of PII may be ineffective. From the PUI literature, this study is building upon Ohm (2010) who declared anonymization and the concept of PUI a failure due to the literature showing adeptness in re-identifying individuals even using PUI as a starting point. From the SE literature, this study built upon Mouton et al. (2016) who described the difficulty of SE literature wherein neither the literature or news media provide all the information concerning an attack as well as very little is known about a potential attack, where the information is obtained for a SE attack, and what information

is available for a SE attack. Using TOM for the persuasion component of SE from the psychological literature addresses the issues in SE research raised by Tetri and Vuorinen (2013).

To achieve the main goal of this developmental research study, six specific goals were set to address six specific RQs using a three-phased approach, with Writers and CIOs showing the highest SEXI for their respective groups.

In Phase 1, this study used the Delphi method comprised of 19 cybersecurity experts in round one and 17 in round two who were tasked with the purpose of answering the first two RQs:

RQ1: What are the specific SME-panel approved set of personal information components for an index of SE exposure?

RQ2: What are the specific SME-panel approved categories for the identified set of personal information components?

First, this study conducted a thorough review of literature to establish a list of applicable PICCs and category delineations. Second, using anonymous online surveys, the Delphi method was implemented to present 105 PICCs to the expert panel to assign exposure ratings from minimum to maximum for each item in and of itself. The SMEs were also asked to assign a weight to personal information categories. During the second round, the panel of experts were asked to quantitatively assign each PICC to one of three personal information categories from the first round: PDI, PII, and PUI.

In Phase 2, the feedback from Phase 1 was used to answer the third research question and to create the SEXI benchmarking index:

RQ3: What are the specific SME-panel identified weights of the personal information components and categories that enable a validated hierarchical aggregation to the Social Engineering eXposure Index (SEXI) benchmarking index?

Second, the feedback from the two-round expert panel was analyzed and codified into a SEXI benchmarking index that was initially tested via Twitter and Google+. The final SEXI benchmarking index used almost two dozen sources.

In Phase 3, this research study used the SEXI benchmarking index to answer the remaining questions:

RQ4: How are 100 individuals assessed and classified by SEXI using OSPI?

RQ5: Are there any statistically significant mean differences of SEXI based on demographical indicators of age, gender, income, marital status, estimated worth, industry, organizational position, philanthropic contributions, and prior military/police experience?

RQ6: Do SEXI results from the set of US executives and Hollywood personas indicate one group being more vulnerable to SE attack from their OSPI exposure perspective?

The SEXI benchmarking index was used to assess 50 Fortune 500 Executives and 50 Hollywood Personas, by using OSPI to attempt to find each of the 105 PICCs for each member of the population (N=100) using “found/not found” indicators. Additionally, aggregated demographic data was assessed for the purpose of answering RQ5.

The results and data analysis from Phase 3 answered the remaining questions. The data analysis performed for RQ4 showed that SEXI was appropriate as OSPI was

available for each member of the population with over half of the 105 SEXI items were found for at least half of the population. The data analysis performed for RQ5 showed significant SEXI demographics are associated with Industry, Organizational Position, Estimated Income, Philanthropic Contributions, Income, and Marital Status (borderline). The RQ5 analysis suggests that six of the nine demographics produce differences in SEXI. The analysis performed for RQ6 showed that Hollywood Personas had a significantly higher SEXI than the Fortune 500 Executives suggesting increased exposure due to OSPI. Each of the Hollywood Personas organization positions held higher SEXI measures than all of those held by the Fortune 500 executives.

This research study contributed to the body of knowledge as well as the fields of privacy, SE, information security, cybersecurity, and personal information. This study resulted in quantitatively defining three categories of personal information: PDI, PII, and PUI. This study resulted in establishing validated weights and measures for the PICCs obtained via literature review. This study resulted in establishing and validating the SEXI benchmarking index. Therefore, the work presented herein may be used by individuals to understand their exposure to SE due to OSPI. The work presented in this developmental research study can be leveraged by organizations to better understand what information is available and the type of SE attack that may result from it. Additionally, risk assessments using the SEXI benchmarking index could be used to establish and enforce privacy, personal information, and cybersecurity policies.

In conclusion, other researchers can use the SEXI benchmarking index to measure diverse populations of interest. The SEXI benchmarking index can be used to assess exposure of personal information of organizational members, key organizational

positions, clients, competitors, vendors, etc. Risk assessments can be performed using the SEXI benchmarking index. Additionally, the SEXI benchmarking index can be extended to include any data source using JSON, XML, CSV, API or other data formats thereby increasing its accuracy as well as effectiveness. As it matures, SEXI can provide a mechanism to understand, source, and combat the availability of OSPI and reduce the potential of various attack vectors due to OSPI.

Appendix A

Institutional Review Board Approval Letter

NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **William Wilkerson**

From: **Ling Wang, Ph.D.,**
Center Representative, Institutional Review Board

Date: **December 8, 2017**

Re: **IRB #: 2017-700; Title, "Development of a Social Engineering eXposure Index (SEXI) using Open Source Personal Information"**

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 Category 2)**. 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 Ling Wang, 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: Yair Levy, 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

Email to Expert Panel: Request for Participation

Dear cybersecurity expert,

We need your help in providing expert feedback on a framework for an upcoming doctoral research study. I am a PhD Candidate in Information Systems with a concentration in Information Security at the College of Computing and Engineering, Nova Southeastern University, working under the supervision of Dr. Yair Levy in the Levy CyLab (https://infosec.nova.edu/cylab/). My research is seeking to develop an index to measure if there is (or to what extent the magnitude exists) exposure to social engineering via publicly available personal information. To develop the index, I need assistance from professionals that have extensive experience dealing with personal information privacy activities, not limited to information security, information privacy, social engineering, law, medical, application development, etc.

You will be asked to complete two surveys. The first survey, should take approximately 20 minutes, will help me to understand your work environment, experience, and will be used to develop the Social Engineering eXposure Index (SEXI) benchmark instrument to assess the level of exposure to social engineering due to publicly available personal information. The second survey, should take approximately 10 minutes, will ask for your feedback on the expert panel aggregate responses from the first-round survey. Your expertise is being solicited to review the proposed measurement criteria for the documented privacy components and provide your expert opinion regarding their relative significance by assigning weights and categories to develop a novel privacy-related exposure measure.

The information provided will be used only for this research study and in aggregated form. Your personal information will not be collected. Your anonymity is assured, and no negative effect will accompany your truthful responses. If you are willing to participate, please click on the link below for access to the first-round survey, to be completed by TBD using password: PASSWORD.

https://www.surveymonkey.com/r/SEXI-PhDStudy

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study. Should you wish to receive the findings of the study, please send me an email, and I will be happy to provide you with information about the academic research publication(s) resulting from this study.

Regards,
W. Shawn Wilkerson, Ph.D. Candidate

E-mail: ww364@nova.edu
Information Systems with a concentration in Information Security
College of Computing and Engineering
Nova Southeastern University

Yair Levy, Ph.D.
E-mail: levyy@nova.edu
Professor of Information Systems and Cybersecurity
College of Computing and Engineering
Nova Southeastern University
Levy CyLab: https://infosec.nova.edu/cylab/

Appendix C

Round I Expert Panel Survey

Dear cybersecurity expert,

Thank you for taking time to participate in this expert panel survey on the exposure to social engineering due to publicly available personal information. In this phase, you will be asked to provide some background information and general demographics. The requested information helps me understand the composition of the expert panel. **It is imperative that your answers are as truthful and honest as possible.** The information provided will be used only for this research study and in aggregated form. **No personal information will be collected. Your anonymity is assured, and no negative effect will accompany your truthful responses.**

This expert panel survey is part of a Ph.D. doctoral dissertation research study that seeks to develop the Social Engineering eXposure Index (SEXI) benchmark instrument to measure exposure to social engineering due to publicly available information. Before this study can move towards the classification of personal information items, I must better understand the composition of experts taking part in the study.

Part 1 – Work Environment. Answer the following questions with the most appropriate answer.

BG01 [Policy] I work for an organization that has a well-defined privacy policy.

○	○	○	○	○	○	○
1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG02 [TrainingPrivacy] I work for an organization that has mandatory training for privacy.

○	○	○	○	○	○	○
1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG03 [Consequences] I work for an organization that has consequences for violating the privacy policy.

○	○	○	○	○	○	○
1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG04 [TrainingSE] I work for an organization that has mandatory social engineering training.

○	○	○	○	○	○	○
1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG05 [SecurityAudits] I work for an organization that has security audits.

○	○	○	○	○	○	○
1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG06 [Pretending] I work for an organization that has experienced an attempt to gain access to unauthorized assets through someone pretending to be another individual.

○	○	○	○	○	○	○
1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG07 [Persuasion] I work for an organization that has experienced an attempt to gain access to unauthorized assets at my organization through persuasion.

○	○	○	○	○	○	○
1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG08 [AuthorityBypassPolicy] I work for an organization where someone has the authority to bypass policy on a case-by-case basis.

○	○	○	○	○	○	○

1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG09 [UnauthorizedBypassPolicy] I work for an organization where an employee bypassed policy without authorization.

○	○	○	○	○	○	○
1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG10 [Repercussion] I work for an organization where an employee bypassed policy without repercussion.

○	○	○	○	○	○	○
1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG11 [PrivacyVsEfficiency] I work for an organization where employees feel like they must choose between privacy policy and efficiency.

○	○	○	○	○	○	○
1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG12 [PrivacyCulture] I work for an organization where employees are shown ways to bypass policy by other employees.

○	○	○	○	○	○	○
1 – Strongly Disagree	2 – Disagree	3 – Somewhat Disagree	4 – Neither Agree or Disagree	5 – Somewhat Agree	6 – Agree	7 – Strongly Agree

BG13 [Consequence] I work for an organization where violating the privacy policy typically results in:

○	○	○	○	○	○	○

1 – No Consequence	2 – Informal Verbal Warning	3 – Formal Verbal Reprimand	4 – Written Reprimand	5 – Temporary Suspension of Duties	6 – Reassignment	7 – Termination / Legal Issues

Part 2 – Demographics

D01 [Gender] Gender:

1) Male
2) Female

D02 [Age] Age:

1) 19 – 24
2) 25 – 29
3) 30 – 34
4) 35 – 39
5) 40 – 44
6) 45 – 49
7) 50 – 54
8) 55 – 59
9) 60 – 64
10) 65+

D03 [Focus] How would you characterize your work focus?

1) Academia.
2) Mostly academic endeavors with occasional practitioner efforts.
3) Evenly between academic and practitioner efforts.
4) Practitioner.
5) Mostly practitioner endeavors with occasional academic efforts.
6) I am not affiliated with Information Security / Information Privacy.

DO4 [Educ] Please select the highest degree attained

1) Some college credit, no degree earned.
2) Trade/technical/vocational training

3) Associate
4) Bachelors
5) Masters
6) Doctorate

D05 [Certs] Which specialized industry certifications do you currently hold?

- □ [CAP] Certified Authorization Professional
- □ [CCENT] Cisco Certified Entry Networking Technician
- □ [CCEP] Certified Compliance & Ethics Professional
- □ [CCEP-I] Certified Compliance & Ethics Professional-International
- □ [CCFP] Certified Cyber Forensics Professional
- □ [CCSP] Certified Cloud Security Professional
- □ [CEH] Certified Ethical Hacker
- □ [CGEIT] Certified in the Governance of Enterprise IT
- □ [CHC] Certified in Healthcare Compliance
- □ [CHPC] Certified in Healthcare Privacy Compliance
- □ [CHRC] Certified in Healthcare Research Compliance
- □ [CIPM] Certified Information Privacy Manager
- □ [CIPP] Certified Information Privacy Professional
- □ [CIPT] Certified Information Privacy Technologist
- □ [CISA] Certified Information Systems Auditor
- □ [CISM] Certified Information Security Manager
- □ [CISSP] Certified Information Systems Security Professional
- □ [CRISC] Certified in Risk and Information Systems Control
- □ [CSSLP] Certified Secure Software Lifecycle Professional
- □ [CSX] Cybersecurity Nexus Certificate
- □ [CSX-P] Cybersecurity Nexus Certification
- □ [HCISPP] HealthCare Information Security and Privacy Practitioner
- □ [SSCP] Systems Security Certified Practitioner
- □ [OtherCert] Other: _____

D06 [CurrOcc] Current Occupation:

1) Chief Information Officer (CIO)
2) Chief Privacy Officer (CPO)
3) Chief Security Officer (CSO)
4) Chief Information Security Officer (CISO)
5) Consultant
6) IS/IT Professor
7) Law Enforcement
8) Law Professor
9) Privacy Lawyer
10) Privacy Specialist
11) Security Specialist
12) Other _____

D07 [CySecProYrs] Years as a Cybersecurity professional:

1) 1 – 3 Years
2) 4 – 6 Years
3) 7 – 9 Years
4) 10 – 12 Years
5) 13 – 15 Years
6) 16 – 18 Years
7) 19 – 21 Years
8) 22+ Years

D08 [Exp] Years working with information privacy:

1) 1 – 3 Years
2) 4 – 6 Years
3) 7 – 9 Years
4) 10 – 12 Years
5) 13 – 15 Years
6) 16 – 18 Years
7) 19 – 21 Years
8) 22+ Years

D09 [CurOccInd] Current Industry:

1) Banking & Finance
2) Consulting
3) Education
4) Energy
5) Healthcare
6) Government
7) Information Technology
8) Law Enforcement
9) Manufacturing
10) Retail
11) Telecommunication

12) Other

D10 [Mil] Have you ever served in the military?

- o Yes
- o No

D11 [Leo] Have you ever served in law enforcement?

- o Yes
- o No

Part 3 – Items contributing to identification via personal information

Personally identifiable information (PII) is typically thought of as including any personal information. In this section, you will be provided personal information candidate components that have been suggested or described by experts in leading journal articles, federal legislation, and in industry standards.

Read each item and select the best answer indicating where in the range of 1 (minimal exposure) to 10 (maximum exposure) the item, **can in and of itself**, identify a given individual. Select DNA for any item that you feel is not personal information. Select UNF for any item that you are unfamiliar with.

Definitions:

Does not Apply (DNA) – any information that is not personal information.
Unfamiliar (UNF) – any information that you are not familiar with.

	1 Minimum Exposure	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10 Maximum Exposure**	**DNA**	**UNF**
PC001 Acceleration via personal tracking	○	○	○	○	○	○	○	○	○	○	○	○
PC002 Account numbers	○	○	○	○	○	○	○	○	○	○	○	○
PC003 Activities (daily life)	○	○	○	○	○	○	○	○	○	○	○	○
PC004 Age	○	○	○	○	○	○	○	○	○	○	○	○

PC005 Agency seal / Organizational logo	○	○	○	○	○	○	○	○	○	○	○	○
PC006 Alias	○	○	○	○	○	○	○	○	○	○	○	○
PC007 Area code	○	○	○	○	○	○	○	○	○	○	○	○
PC008 Audit log of user actions	○	○	○	○	○	○	○	○	○	○	○	○
PC009 Biometric records (retina, iris, voice signature, facial geometry, facial recognition)	○	○	○	○	○	○	○	○	○	○	○	○
PC010 Bluetooth connections to other devices	○	○	○	○	○	○	○	○	○	○	○	○
PC011 Calorie counting with images of food	○	○	○	○	○	○	○	○	○	○	○	○
PC012 Cardholder name	○	○	○	○	○	○	○	○	○	○	○	○

1

	1 Minimum Exposure	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10 Maximum Exposure**	**DNA**	**UNF**
PC013 Cell phone number	○	○	○	○	○	○	○	○	○	○	○	○
PC014 Cell tower location	○	○	○	○	○	○	○	○	○	○	○	○
PC015 Credit card account number	○	○	○	○	○	○	○	○	○	○	○	○
PC016 Credit card CAV2 / CVC2 / CVV2 / CID	○	○	○	○	○	○	○	○	○	○	○	○
PC017 Card expiration date	○	○	○	○	○	○	○	○	○	○	○	○
PC018 Credit card pin	○	○	○	○	○	○	○	○	○	○	○	○
PC019 Credit card service code	○	○	○	○	○	○	○	○	○	○	○	○

PC020 Credit score	○	○	○	○	○	○	○	○	○	○	○	○
PC021 Criminal history	○	○	○	○	○	○	○	○	○	○	○	○
PC022 Date of birth	○	○	○	○	○	○	○	○	○	○	○	○
PC023 Demographics	○	○	○	○	○	○	○	○	○	○	○	○
PC024 Driver's license [number]	○	○	○	○	○	○	○	○	○	○	○	○

1

	1 Minimum Exposure	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10 Maximum Exposure**	**DNA**	**UNF**
PC025 Education information	○	○	○	○	○	○	○	○	○	○	○	○
PC026 Electricity usage	○	○	○	○	○	○	○	○	○	○	○	○
PC027 Electronic facial image / selfie	○	○	○	○	○	○	○	○	○	○	○	○
PC028 E-mail address	○	○	○	○	○	○	○	○	○	○	○	○
PC029 Employee identification	○	○	○	○	○	○	○	○	○	○	○	○
PC030 Employment history	○	○	○	○	○	○	○	○	○	○	○	○
PC031 Employment information	○	○	○	○	○	○	○	○	○	○	○	○
PC032 Family income	○	○	○	○	○	○	○	○	○	○	○	○
PC033 Favorite movies	○	○	○	○	○	○	○	○	○	○	○	○
PC034 Favorite restaurants	○	○	○	○	○	○	○	○	○	○	○	○
PC035 Favorite television shows	○	○	○	○	○	○	○	○	○	○	○	○
PC036 Financial records / information, balances	○	○	○	○	○	○	○	○	○	○	○	○

2

	1 Minimum Exposure	2	3	4	5	6	7	8	9	10 Maximum Exposure	DNA	UNF
PC037 Fingerprints	○	○	○	○	○	○	○	○	○	○	○	○
PC038 Fingerprints of two fingers	○	○	○	○	○	○	○	○	○	○	○	○
PC039 Full name	○	○	○	○	○	○	○	○	○	○	○	○
PC040 Full set of fingerprints	○	○	○	○	○	○	○	○	○	○	○	○
PC041 Gender	○	○	○	○	○	○	○	○	○	○	○	○
PC042 Genetic information	○	○	○	○	○	○	○	○	○	○	○	○
PC043 Geographical indicators (location, i.e. city name, latitude, longitude, etc.)	○	○	○	○	○	○	○	○	○	○	○	○
PC044 Global Positioning Systems (GPS)	○	○	○	○	○	○	○	○	○	○	○	○
PC045 Handwriting	○	○	○	○	○	○	○	○	○	○	○	○
PC046 High school name	○	○	○	○	○	○	○	○	○	○	○	○
PC047 Holographic images (on identification)	○	○	○	○	○	○	○	○	○	○	○	○
PC048 Host-specific persistent static identifier (system / hostname, etc.)	○	○	○	○	○	○	○	○	○	○	○	○

1

	1 Minimum Exposure	2	3	4	5	6	7	8	9	10 Maximum Exposure	DNA	UNF
PC049 IP address (network location of network device; dynamic / fixed)	○	○	○	○	○	○	○	○	○	○	○	○
PC050 Laser etches (on identification)	○	○	○	○	○	○	○	○	○	○	○	○
PC051 License plate	○	○	○	○	○	○	○	○	○	○	○	○

PC052 MAC address (hardware ID of network device)	○	○	○	○	○	○	○	○	○	○	○	○
PC053 Maiden name	○	○	○	○	○	○	○	○	○	○	○	○
PC054 Marital status	○	○	○	○	○	○	○	○	○	○	○	○
PC055 Medical history	○	○	○	○	○	○	○	○	○	○	○	○
PC056 Medical information	○	○	○	○	○	○	○	○	○	○	○	○
PC057 Medical test results	○	○	○	○	○	○	○	○	○	○	○	○
PC058 Mental health	○	○	○	○	○	○	○	○	○	○	○	○
PC059 Mother's maiden name	○	○	○	○	○	○	○	○	○	○	○	○
PC060 Nationality	○	○	○	○	○	○	○	○	○	○	○	○

1

	1 Minimum Exposure	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10 Maximum Exposure**	**DNA**	**UNF**
PC061 Newsletter subscription	○	○	○	○	○	○	○	○	○	○	○	○
PC062 Organization affiliation / membership	○	○	○	○	○	○	○	○	○	○	○	○
PC063 Owned property (mortgage, vehicle registration, title)	○	○	○	○	○	○	○	○	○	○	○	○
PC064 Parent's middle name	○	○	○	○	○	○	○	○	○	○	○	○
PC065 Partner(s) name	○	○	○	○	○	○	○	○	○	○	○	○
PC066 Passport number	○	○	○	○	○	○	○	○	○	○	○	○
PC067 Password	○	○	○	○	○	○	○	○	○	○	○	○
PC068 Patient identification number	○	○	○	○	○	○	○	○	○	○	○	○
PC069 Payment for health care	○	○	○	○	○	○	○	○	○	○	○	○
PC070 Persistent Identifier (customer number held in	○	○	○	○	○	○	○	○	○	○	○	○

cookie, processor serial number, alphanumeric identifier)	

1

	1 Minimum Exposure	2	3	4	5	6	7	8	9	10 Maximum Exposure	DNA	UNF
PC071 Personal heart-rate meter	○	○	○	○	○	○	○	○	○	○	○	○
PC072 Photographic image	○	○	○	○	○	○	○	○	○	○	○	○
PC073 Physical health	○	○	○	○	○	○	○	○	○	○	○	○
PC074 Place of birth	○	○	○	○	○	○	○	○	○	○	○	○
PC075 Place of sensing moment	○	○	○	○	○	○	○	○	○	○	○	○
PC076 Political views	○	○	○	○	○	○	○	○	○	○	○	○
PC077 Professional title	○	○	○	○	○	○	○	○	○	○	○	○
PC078 Provision of health care	○	○	○	○	○	○	○	○	○	○	○	○
PC079 Race	○	○	○	○	○	○	○	○	○	○	○	○
PC080 Rank	○	○	○	○	○	○	○	○	○	○	○	○
PC081 Recent purchases	○	○	○	○	○	○	○	○	○	○	○	○
PC082 Religion	○	○	○	○	○	○	○	○	○	○	○	○

2

	1 Minimum Exposure	2	3	4	5	6	7	8	9	10 Maximum Exposure	DNA	UNF
PC083 Salary information	○	○	○	○	○	○	○	○	○	○	○	○
PC084 Search engine query (miscellaneous to vanity)	○	○	○	○	○	○	○	○	○	○	○	○

PC085 Sexual fantasy / behavior	○	○	○	○	○	○	○	○	○	○	○	○
PC086 Sexual orientation	○	○	○	○	○	○	○	○	○	○	○	○
PC087 Signature (digital)	○	○	○	○	○	○	○	○	○	○	○	○
PC088 Signature (handwritten)	○	○	○	○	○	○	○	○	○	○	○	○
PC089 Social media profile	○	○	○	○	○	○	○	○	○	○	○	○
PC090 Social Security Number	○	○	○	○	○	○	○	○	○	○	○	○
PC091 Status updates	○	○	○	○	○	○	○	○	○	○	○	○
PC092 Street address	○	○	○	○	○	○	○	○	○	○	○	○
PC093 Tax records	○	○	○	○	○	○	○	○	○	○	○	○
PC094 Taxpayer identification number	○	○	○	○	○	○	○	○	○	○	○	○
PC095 Telephone number	○	○	○	○	○	○	○	○	○	○	○	○
PC096 Location / Time of sensing moment (self-surveillance via smartphone, fitness device)	○	○	○	○	○	○	○	○	○	○	○	○

1

	1 Minimum Exposure	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10 Maximum Exposure**	**DNA**	**UNF**
PC097 Timestamp of Web page visit	○	○	○	○	○	○	○	○	○	○	○	○
PC098 Uniform Resource Locator (URL) of last Web page	○	○	○	○	○	○	○	○	○	○	○	○
PC099 Unique health identifier	○	○	○	○	○	○	○	○	○	○	○	○

PC100	User identification	○	○	○	○	○	○	○	○	○	○	○
PC101	Web browser history	○	○	○	○	○	○	○	○	○	○	○
PC102	Weight	○	○	○	○	○	○	○	○	○	○	○
PC103	Work phone	○	○	○	○	○	○	○	○	○	○	○
PC104	X-Rays	○	○	○	○	○	○	○	○	○	○	○
PC105	ZIP Code	○	○	○	○	○	○	○	○	○	○	○

Part 4 – Provide any suggestions for Personally Unidentifiable Information (PUI) not in the personal information candidate components above. If you have no additional items, please enter NA.

Part 5 – Provide any suggestions for Personally Identifiable Information (PII) not in the personal information candidate components above. If you have no additional items, please enter NA

Part 6 – Provide any suggestions for Personally Distinguishable Information (PDI) not in the personal information candidate components above. If you have no additional items, please enter NA.

Part 7 – Category Weight Assignment

The three proposed measures will be assessed based on the clusters of criteria identified by the expert panel. What should the importance of each category be relative to the other categories?

Please allocate from 1 -100 points in each of the Social Engineering eXposure Index (SEXI) categories (all 100 points should be used):

Personally unidentifiable information (PUI) – any information that *cannot identify* an individual by itself.	W_{PUI} [ ]
Personally identifiable information (PII) – any information that can *potentially identify* an individual by itself and not be PDI or PUI.	W_{PII} [ ]
Personally distinguishable information (PDI) – any information that can *definitely identify* an individual by itself.	W_{PDI} [ ]

Appendix D

Round II Expert Panel Survey

Dear cybersecurity expert,

Thank you for taking time to participate in this expert panel survey on the exposure to social engineering due to publicly available personal information. In this phase, you will be asked to provide feedback on the placement of the personal information components by a panel of experts. The information provided will be used only for this research study and in aggregated form. **No personal information will be collected. Your anonymity is assured, and no negative effect will accompany your truthful responses.**

This expert panel survey is part of a Ph.D. doctoral dissertation research study that seeks to develop the Social Engineering eXposure Index (SEXI) benchmark instrument to measure exposure to social engineering due to publicly available information.

Categories:

Personally unidentifiable information (PUI) – any information that *cannot identify* an individual by itself.

Personally identifiable information (PII) – any information that can *potentially identify* an individual by itself and not be PDI or PUI.

Personally distinguishable information (PDI) – any information that can *definitely identify* an individual by itself.

Does not Apply (DNA) – any information that is not personal information.

Please read over the following lists and indicate the group the personal information item belongs in

1 – Items the expert panel designated as personal information *that cannot identify an individual by itself.* Using the category definitions above, please read over the following lists and indicate the group the item belongs.

	Does not Apply (DNA)	Cannot Identify (PUI)	Potentially Identify (PII)	Definitely Identify (PDI)
PC011 Calorie counting with images of food	○	○	○	○

PC026 Electricity usage	○	○	○	○
PC033 Favorite movies	○	○	○	○
PC034 Favorite restaurants	○	○	○	○
PC035 Favorite television shows	○	○	○	○
PC041 Gender	○	○	○	○
PC054 Marital status	○	○	○	○
PC061 Newsletter subscription	○	○	○	○
PC086 Sexual orientation	○	○	○	○
PC105 ZIP Code	○	○	○	○

2 – Items the expert panel designated as personal information that *can definitely identify an individual by itself.* Using the category definitions above, please read over the following lists and indicate the group the item belongs.

	Does not Apply (DNA)	Cannot Identify (PUI)	Potentially Identify (PII)	Definitely Identify (PDI)
PC008 Audit log of user actions	○	○	○	○
PC009 Biometric records (retina, iris, voice signature, facial geometry, facial recognition)	○	○	○	○
PC012 Cardholder name	○	○	○	○
PC013 Cell phone number	○	○	○	○
PC015 Credit card account number	○	○	○	○
PC016 Credit card CAV2 / CVC2 / CVV2 / CID	○	○	○	○
PC021 Criminal history	○	○	○	○

PC022 Date of birth	○	○	○	○
PC024 Driver's license [number]	○	○	○	○
PC027 Electronic facial image / selfie	○	○	○	○
PC029 Employee identification	○	○	○	○
PC030 Employment history	○	○	○	○
PC031 Employment information	○	○	○	○
PC036 Financial records / information, balances	○	○	○	○
PC040 Full set of fingerprints	○	○	○	○
PC042 Genetic information	○	○	○	○
PC055 Medical history	○	○	○	○
PC056 Medical information	○	○	○	○
PC057 Medical test results	○	○	○	○
PC058 Mental health	○	○	○	○
PC066 Passport number	○	○	○	○
PC068 Patient identification number	○	○	○	○
PC070 Persistent Identifier (customer number held in cookie, processor serial number, alphanumeric identifier)	○	○	○	○
PC072 Photographic image	○	○	○	○
PC087 Signature (digital)	○	○	○	○

PC088 Signature (handwritten)	○	○	○	○
PC089 Social media profile	○	○	○	○
PC090 Social Security Number	○	○	○	○
PC093 Tax records	○	○	○	○
PC094 Taxpayer identification number	○	○	○	○

3 – Items the expert panel designated as personal information *having the potential to identify an individual by itself that are not definite identifiers (PDI) or non-identifiers (PUI)*. Using the category definitions above, please read over the following lists and indicate the group the item belongs.

	Does not Apply (DNA)	Cannot Identify (PUI)	Potentially Identify (PII)	Definitely Identify (PDI)
PC001 Acceleration via personal tracking	○	○	○	○
PC002 Account numbers	○	○	○	○
PC003 Activities (daily life)	○	○	○	○
PC004 Age	○	○	○	○
PC005 Agency seal / Organizational logo	○	○	○	○
PC006 Alias	○	○	○	○
PC007 Area code	○	○	○	○
PC010 Bluetooth connections to other devices	○	○	○	○
PC014 Cell tower location	○	○	○	○
PC017 Card expiration date	○	○	○	○
PC018 Credit card pin	○	○	○	○
PC019 Credit card service code	○	○	○	○
PC020 Credit score	○	○	○	○

PC023 Demographics	○	○	○	○
PC025 Education information	○	○	○	○
PC028 E-mail address	○	○	○	○
PC032 Family income	○	○	○	○
PC037 Fingerprints	○	○	○	○
PC038 Fingerprints of two fingers	○	○	○	○
PC039 Full name	○	○	○	○
PC043 Geographical indicators (location, i.e. city name, latitude, longitude, etc.)	○	○	○	○
PC044 Global Positioning Systems (GPS)	○	○	○	○
PC045 Handwriting	○	○	○	○
PC046 High school name	○	○	○	○
PC047 Holographic images (on identification)	○	○	○	○
PC048 Host-specific persistent static identifier (system / hostname, etc.)	○	○	○	○
PC049 IP address (network location of network device; dynamic / fixed)	○	○	○	○
PC050 Laser etches (on identification)	○	○	○	○
PC051 License plate	○	○	○	○
PC052 MAC address (hardware ID of network device)	○	○	○	○
PC053 Maiden name	○	○	○	○
PC059 Mother's maiden name	○	○	○	○
PC060 Nationality	○	○	○	○

PC062 Organization affiliation / membership	○	○	○	○
PC063 Owned property (mortgage, vehicle registration, title)	○	○	○	○
PC064 Parent's middle name	○	○	○	○

4 – Items the expert panel designated as personal information *having the potential to identify an individual by itself that are not definite identifiers (PDI) or non-identifiers (PUI)*. Using the category definitions above, please read over the following lists and indicate the group the item belongs.

	Does not Apply (DNA)	Cannot Identify (PUI)	Potentially Identify (PII)	Definitely Identify (PDI)
PC065 Partner(s) name	○	○	○	○
PC067 Password	○	○	○	○
PC069 Payment for health care	○	○	○	○
PC071 Personal heart-rate meter	○	○	○	○
PC073 Physical health	○	○	○	○
PC074 Place of birth	○	○	○	○
PC075 Place of sensing moment	○	○	○	○
PC076 Political views	○	○	○	○
PC077 Professional title	○	○	○	○
PC078 Provision of health care	○	○	○	○
PC079 Race	○	○	○	○
PC080 Rank	○	○	○	○
PC081 Recent purchases	○	○	○	○
PC082 Religion	○	○	○	○
PC083 Salary information	○	○	○	○
PC084 Search engine query	○	○	○	○

(miscellaneous to vanity)				
PC085 Sexual fantasy / behavior	○	○	○	○
PC091 Status updates	○	○	○	○
PC092 Street address	○	○	○	○
PC095 Telephone number	○	○	○	○
PC096 Location / Time of sensing moment (self-surveillance via smartphone, fitness device)	○	○	○	○
PC097 Timestamp of Web page visit	○	○	○	○
PC098 Uniform Resource Locator (URL) of last Web page	○	○	○	○
PC099 Unique health identifier	○	○	○	○
PC100 User identification	○	○	○	○
PC101 Web browser history	○	○	○	○
PC102 Weight	○	○	○	○
PC103 Work phone	○	○	○	○
PC104 X-Rays	○	○	○	○

Part 2 – Expert suggested items from Round 1

Read each item and select the best answer indicating where in the range of 1 (minimal exposure) to 10 (maximum exposure) the item, can in and of itself, identify a given individual. Select DNA for any item that you feel is not personal information. Select UNF for any item that you are unfamiliar with.

Definitions:

Does not Apply (DNA) – any information that is not personal information.

Unfamiliar (UNF) – any information that you are not familiar with.

5 – Please indicate where in the range of 1 (minimal exposure) to 10 (maximum exposure) each item, can in and of itself, identify a given individual.

	Does not Apply (DNA)	Cannot Identify (PUI)	Potentially Identify (PII)	Definitely Identify (PDI)
PC200 Fitness tracker	○	○	○	○
PC201 Google applications	○	○	○	○
PC202 Voting program / ballot	○	○	○	○
PC203 Vehicle make & model	○	○	○	○
PC204 RSA pin/passcode	○	○	○	○
PC205 Clothing style	○	○	○	○
PC206 Voting district	○	○	○	○
PC207 Transportation method	○	○	○	○
PC220 Gravatar avatar	○	○	○	○
PC221 Reservation confirmation number	○	○	○	○
PC222 SSH Public key	○	○	○	○
PC223 E-mail message ID	○	○	○	○
PC230 GPG public key	○	○	○	○
PC231 Student identification number	○	○	○	○
PC232 Personal SSL / PKI type certificate	○	○	○	○
PC233 Rewards plan member	○	○	○	○

Appendix E

SEXI Data Collection Form

M081-03 (Nondescript identifier)

Label	Item	SRC1	SRC2	SRC3
PC001	Acceleration via personal tracking	□	□	□
PC002	Account numbers	□	□	□
PC003	Activities (daily life)	□	□	□
PC004	Age	□	□	□
PC005	Agency seal / Organizational logo	□	□	□
PC006	Alias	□	□	□
PC007	Area code	□	□	□
PC008	Audit log of user actions	□	□	□
PC009	Biometric records (retina, iris, voice signature, Facial geometry, facial recognition)	□	□	□
PC010	Bluetooth connections to devices	□	□	□
PC011	Calorie counting w/ images of food	□	□	□
PC012	Cardholder name	□	□	□
PC013	Cell phone number	□	□	□
PC014	Cell tower location	□	□	□
PC015	Credit card account number	□	□	□
PC016	Credit card CAV2 / CVC2 / CVV2 / CID	□	□	□
PC017	Card expiration date	□	□	□
PC018	Credit card pin	□	□	□
PC019	Credit card service code	□	□	□
PC020	Credit score	□	□	□
PC021	Criminal history	□	□	□
PC022	Date of birth	□	□	□
PC023	Demographics	□	□	□
PC024	Driver's license [number]	□	□	□
PC025	Education information	□	□	□
PC026	Electricity usage	□	□	□
PC027	Electronic facial image / Selfie	□	□	□
PC028	E-mail address	□	□	□
PC029	Employee identification	□	□	□
PC030	Employment history	□	□	□
PC031	Employment information	□	□	□

PC032	Family income	□	□	□
PC033	Favorite movies	□	□	□
PC034	Favorite restaurants	□	□	□
PC035	Favorite television shows	□	□	□
PC036	Financial records / information, balances	□	□	□
PC037	Fingerprints	□	□	□
PC038	Fingerprints of two fingers	□	□	□
PC039	Full name	□	□	□
PC040	Full set of fingerprints	□	□	□
PC041	Gender	□	□	□
PC042	Genetic information	□	□	□
PC043	Geographical indicators (location, i.e. city name, latitude, longitude, etc.)	□	□	□
PC044	GPS	□	□	□
PC045	Handwriting	□	□	□
PC046	High school name	□	□	□
PC047	Holographic images (on ID)	□	□	□
PC048	Host-specific persistent static identifier (system / hostname, etc.)	□	□	□
PC049	IP address	□	□	□
PC050	Laser etches (on ID)	□	□	□
PC051	License plate	□	□	□
PC052	MAC address	□	□	□
PC053	Maiden name	□	□	□
PC054	Marital status	□	□	□
PC055	Medical history	□	□	□
PC056	Medical information	□	□	□
PC057	Medical test results	□	□	□
PC058	Mental health	□	□	□
PC059	Mother's maiden name	□	□	□
PC060	Nationality	□	□	□
PC061	Newsletter subscription	□	□	□
PC062	Organization affiliation / membership	□	□	□
PC063	Owned property	□	□	□
PC064	Parent's middle name	□	□	□
PC065	Partner(s) Name	□	□	□
PC066	Passport number	□	□	□
PC067	Password	□	□	□
PC068	Patient identification Number	□	□	□
PC069	Payment for health care	□	□	□
PC070	Persistent Identifier (customer number held in cookie, processor serial number, alphanumeric	□	□	□

	identifier)			
PC071	Personal heart-rate meter	□	□	□
PC072	Photographic image	□	□	□
PC073	Physical health	□	□	□
PC074	Place of birth	□	□	□
PC075	Place of sensing moment	□	□	□
PC076	Political views	□	□	□
PC077	Professional title	□	□	□
PC078	Provision of health care	□	□	□
PC079	Race	□	□	□
PC080	Rank	□	□	□
PC081	Recent purchases	□	□	□
PC082	Religion	□	□	□
PC083	Salary information	□	□	□
PC084	Search engine query (miscellaneous to vanity)	□	□	□
PC085	Sexual fantasy / behavior	□	□	□
PC086	Sexual orientation	□	□	□
PC087	Signature (digital)	□	□	□
PC088	Signature (handwritten)	□	□	□
PC089	Social media profile	□	□	□
PC090	Social Security Number	□	□	□
PC091	Status updates	□	□	□
PC092	Street address	□	□	□
PC093	Tax records	□	□	□
PC094	Taxpayer identification number	□	□	□
PC095	Telephone number	□	□	□
PC096	Location / Time of sensing moment (self-surveillance via smartphone, fitness device)	□	□	□
PC097	Timestamp of Web page visit	□	□	□
PC098	Uniform Resource Locator (URL) of last Web page	□	□	□
PC099	Unique health identifier	□	□	□
PC100	User identification	□	□	□
PC101	Web browser history	□	□	□
PC102	Weight	□	□	□
PC103	Work phone	□	□	□
PC104	X-Rays	□	□	□
PC105	ZIP Code	□	□	□

1

References

5 U.S.C. § 552a.

18 U.S.C. § 2725.

42 U.S.C. § 200.82.

44 U.S.C. § 3552.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., & Gross, R. (2009). Predicting Social Security numbers from public data. *Proceedings of the National Academy of Sciences*, *106*(27), 10975-10980. https://doi.org/10.1073/pnas.0904891106

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3*(1), 26-33. https://doi.org/10.1109/MSP.2005.22

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442-492. https://doi.org/10.1257/jel.54.2.442

Allen, M. (2006). Social engineering: A means to violate a computer system. *SANS Institute, InfoSec Reading Room*.

Almomani, A., Gupta, B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. *Communications Surveys & Tutorials, IEEE*, *15*(4), 2070-2090. https://doi.org/10.1109/surv.2013.030713.00020

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions [Article]. *MIS Quarterly*, *34*(3), 613-A615. https://doi.org/10.2307/25750694

Anthes, G. (2014). Data brokers are watching you. *Communications of the ACM*, *58*(1), 28-30. https://doi.org/10.1145/2686740

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences*, *1*(03), 23. https://doi.org/10.4236/jss.2013.13004

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain [Article]. *Journal of Risk Research*, *12*(1), 1-11. https://doi.org/10.1080/13669870802488883

Bandura, A. (2001). Social cognitive theory of mass communication. *Media Psychology*, *3*(3), 265-299. https://doi.org/10.1207/s1532785xmep0303_03

Barker, E. B. (2013). *Digital signature standard (DSS)*. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/nist.fips.186-4

Baron-Cohen, S. (1992). Out of sight or out of mind? Another look at deception in autism. *Journal of Child psychology and Psychiatry*, *33*(7), 1141-1155. https://doi.org/10.1111/j.1469-7610.1992.tb00934.x

Baron-Cohen, S. (1997). *Mindblindness: An essay on autism and theory of mind*. MIT press.

Baron-Cohen, S., Leslie, A. M., & Frith, U. (1985). Does the autistic child have a "theory of mind"? *Cognition*, *21*(1), 37-46. https://doi.org/10.1016/0010-0277(85)90022-8

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems [Article]. *MIS Quarterly*, *35*(4), 1017-A1036. https://doi.org/10.2307/41409971

Benitez, K., & Malin, B. (2010). Evaluating re-identification risks with respect to the HIPAA privacy rule. *Journal of the American Medical Informatics Association*, *17*(2), 169-177. https://doi.org/10.1136/jamia.2009.000026

Benjamin, V., & Chen, H. (2012). Securing cyberspace: Identifying key actors in hacker communities. *2012 IEEE International Conference on Intelligence and Security Informatics*, 24-29. https://doi.org/10.1109/isi.2012.6283296

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices.* http://scholarcommons.usf.edu/oa_textbooks/3

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). All your contacts are belong to us: Automated identity theft attacks on social networks. *Proceedings of the 18th international conference on World wide web*, 551-560. https://doi.org/10.1145/1526709.1526784

Bishop, M., & Gates, C. (2008). *Defining the insider threat* [Conference Paper]. Proceedings of the 4th annual workshop on Cyber security and informaiton intelligence research developing strategies to meet the cyber security and information intelligence challenges ahead - CSIIRW '08, https://doi.org/10.1145/1413140.1413158

Boone, H. N., & Boone, D. A. (2012). Analyzing likert data. *Journal of extension*, *50*(2), 1-5.

Boss, S. R., Galletta, D. F., Benjamin Lowry, P., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors [Article]. *MIS Quarterly*, *39*(4), 837-864. https://doi.org/10.25300/misq/2015/39.4.5

Boyd, D. M. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Braun, T. D., Siegel, H. J., Beck, N., Bölöni, L. L., Maheswaran, M., Reuther, A. I., Robertson, J. P., Theys, M. D., Yao, B., Hensgen, D., & Freund, R. F. (2001). A comparison of eleven static heuristics for mapping a class of independent tasks onto heterogeneous distributed computing systems. *Journal of Parallel and Distributed Computing*, *61*(6), 810-837. https://doi.org/10.1006/jpdc.2000.1714

Chang, D., Krupka, E. L., Adar, E., & Acquisti, A. (2016). Engineering information disclosure: Norm shaping designs. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 587-597. https://doi.org/10.1145/2858036.2858346

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, *6*(2-3), 181-202. https://doi.org/10.1007/s10799-005-5879-y

Chitrey, A., Singh, D., & Singh, V. (2012). A comprehensive study of social engineering based attacks in india to develop a conceptual model. *International Journal of Information and Network Security*, *1*(2), 45. https://doi.org/10.11591/ijins.v1i2.426

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719-731. https://doi.org/10.1016/j.cose.2011.08.004

Clayton, M. J. (1997). Delphi: a technique to harness expert opinion for critical decision‐making tasks in education. *Educational Psychology*, *17*(4), 373-386. https://doi.org/10.1080/0144341970170401

Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, *20*(1), 37-46. https://doi.org/10.1177/001316446002000104

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *v112*(n1). https://doi.org/10.1037/0033-2909.112.1.155

Coleman, E. G., & Golub, A. (2008). Hacker practice moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*(3), 255-277. https://doi.org/10.1177/1463499608093814

Coleman, J. S. (2000). Social capital in the creation of human capital. *Knowledge and Social Capital*, 17-41. https://doi.org/10.1016/b978-0-7506-7222-1.50005-2

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23). https://doi.org/10.19101/IJACR.2016.623006

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (4th ed.). Pearson Education.

Culnan, M. J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, *17*(3), 341-363. https://doi.org/10.2307/249775

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323-342. https://doi.org/10.1111/1540-4560.00067

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches [Article]. *MIS Quarterly*, *33*(4), 673-687. https://doi.org/10.2307/20650322

Dadkhah, M., & Quliyeva, A. (2014). Social engineering in academic world. *Journal of Contemporary Applied Mathematics*, *4*(2), 3-5.

Dajani, J. S., Sincoff, M. Z., & Talley, W. K. (1979). Stability and agreement criteria for the termination of Delphi studies. *Technological Forecasting and Social Change*, *13*(1), 83-90. https://doi.org/10.1016/0040-1625(79)90007-6

Dalkey, N., & Helmer, O. (1963). An experimental application of the delphi method to the use of experts. *Management Science*, *9*(3), 458-467. https://doi.org/10.1287/mnsc.9.3.458

Dang, Q. H. (2015). *Secure hash standard*. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/nist.fips.180-4

de Montjoye, Y.-A., Radaelli, L., Singh, V. K., & Pentland, A. S. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, *347*(6221), 536-539. https://doi.org/10.1126/science.1256297

Defense Intelligence Agency. (2011). *Terms & definitions of interest for DOD counterintelligence professionals*. https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management Information Systems*, *19*(4), 9-30. http://www.jstor.org/stable/40398604

Diamond, I. R., Grant, R. C., Feldman, B. M., Pencharz, P. B., Ling, S. C., Moore, A. M., & Wales, P. W. (2014). Defining consensus: A systematic review recommends methodologic criteria for reporting of Delphi studies. *Journal of Clinical Epidemiology*, *67*(4), 401-409. https://doi.org/10.1016/j.jclinepi.2013.12.002

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80. https://doi.org/10.1287/isre.l060.0080

Dworkin, M. J. (2015). *SHA-3 standard: Permutation-based hash and extendable-output functions*. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/nist.fips.202

Dworkin, M. J., Barker, E. B., Nechvatal, J. R., Foti, J., Bassham, L. E., Roback, E., & Jr., J. F. D. (2001). *Advanced encryption standard (AES)*. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/nist.fips.197

Ellis, T. J., & Levy, Y. (2006). A systems approach to conduct an effective literature review in support of information systems research [Article]. *Informing Science: the International Journal of an Emerging Transdiscipline*, *9*, 181+. https://doi.org/10.1.1.98.2369

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, *6*, 323-337. https://doi.org/10.28945/1062

Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. N. (2014). TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems*, *32*(2). https://doi.org/10.1145/2619091

Eom, C. S., & Paek, J. H. (2009). Risk Index Model for Minimizing Environmental Disputes in Construction. *Journal of Construction Engineering and Management*, *135*(1), 34-41. https://doi.org/10.1061/(ASCE)0733-9364(2009)135:1(34)

Falaki, H., Mahajan, R., Kandula, S., Lymberopoulos, D., Govindan, R., & Estrin, D. (2010). Diversity in smartphone usage. *Proceedings of the 8th international*

conference on Mobile systems, applications, and services, 179-194. https://doi.org/10.1145/1814433.1814453

Fan, W., Lwakatare, K., & Rong, R. (2017). Social engineering: IE based model of human weakness for attack and defense investigations. *International Journal of Computer Network and Information Security*, *9*(1), 1-11. https://doi.org/10.5815/ijcnis.2017.01.01

Federal Bureau of Investigation. (2012). *Internet social networking risks*. https://www.fbi.gov/file-repository/internet-social-networking-risks-1.pdf/view

Federal Bureau of Investigation. (2015a). *Business e-mail compromise*. https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise

Federal Bureau of Investigation. (2015b). *Social media safety*. https://www.fbi.gov/audio-repository/news-podcasts-thisweek-social-media-safety.mp3/view

Federal Bureau of Investigation. (2016). *Iranians charged with hacking U.S. financial sector*. https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector/iranians-charged-with-hacking-us-financial-sector

Federal Trade Commission. (2000). Privacy online: Fair information practices in the electronic marketplace: A federal trade commission report to Congress. *Washington DC: FTC*.

Feijóo, C., Gómez-Barroso, J. L., & Voigt, P. (2014). Exploring the economic value of personal information from firms' financial statements. *International Journal of Information Management*, *34*(2), 248-256. https://doi.org/10.1016/j.ijinfomgt.2013.12.005

Ferraiolo, H., Cooper, D. A., Francomacaro, S., Mehta, K. L., & Sokol, A. W. (2013). *Personal identity verification (PIV) of federal employees and contractors*. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/nist.fips.201-2

FIPS 199. (2004). *Standards for security categorization of federal information and information systems*. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/nist.fips.199

Fitch, K., Bernstein, S. J., Aguilar, M. D., Burnand, B., & LaCalle, J. R. (2001). *The RAND/UCLA appropriateness method user's manual*. RAND CORP SANTA MONICA CA.

Fleisher, C. S. (2008). Using open source data in developing competitive and marketing intelligence. *European Journal of Marketing*, *42*(7/8), 852-866. https://doi.org/10.1108/03090560810877196

Franceschi-Bicchierai, L. (2015). *Teen hackers: A '5-year-old' could have hacked into CIA Director's emails*. Retrieved February 12, 2021 from https://motherboard.vice.com/read/teen-hackers-a-5-year-old-could-have-hacked-into-cia-directors-emails

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy & Security*, *11*(1), 38-54. https://doi.org/10.1080/15536548.2015.1010985

Geletkanycz, M. A., & Hambrick, D. C. (1997). The external ties of top executives: Implications for strategic choice and performance. *Administrative science quarterly*, *42*(4), 654-681. https://doi.org/10.2307/2393653

Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. *Security Focus, December*, *18*.

Green, N. (2017). Standing in the future: The case for a substantial risk theory of "injury in fact" in consumer data breach class actions. *Boston College Law Review*, *58*(1), 287-351. http://lawdigitalcommons.bc.edu/bclr/vol58/iss1/8/

Greening, T. (1996). Ask and ye shall receive: A study in "social engineering". *ACM SIGSAC*, *14*(2), 8-14. https://doi.org/10.1145/228292.228295

Greenwood, S., Perrin, A., & Duggan, M. (2016, November 11, 2016). *Social media update 2016*. Pew Research Center,. assets.pewresearch.org/wp-content/uploads/sites/14/2016/11/10132827/PI_2016.11.11_Social-Media-Update_FINAL.pdf

Harl, G. (1997). People hacking: The psychology of social engineering.

Hart, C. (1998). *Doing a literature review: Releasing the social science research imagination*. Sage Publications, Inc.

Hasle, H., Kristiansen, Y., Kintel, K., & Snekkenes, E. (2005). Measuring resistance to social engineering. *International Conference on Information Security Practice and Experience*, 132-143. https://doi.org/10.1007/978-3-540-31979-5_12

Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, *48*(3), 1-39. https://doi.org/10.1145/2835375

Herbsleb, J. D. (2005, 15-21 May 2005). Beyond computer science. Proceedings. 27th International Conference on Software Engineering, 2005. ICSE 2005., https://doi.org/10.1109/ICSE.2005.1553534

Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security*, *53*, 1-17. https://doi.org/10.1016/j.cose.2015.05.002

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81. https://doi.org/10.1145/2063176.2063197

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies [Article]. *MIS Quarterly*, *37*(1), 275-298. https://doi.org/10.25300/misq/2013/37.1.12

Jakobsson, M. (2016). Case study: Business email compromise. In M. Jakobsson (Ed.), *Understanding Social Engineering Based Scams* (pp. 115-122). Springer New York. https://doi.org/10.1007/978-1-4939-6457-4_11

Jasper, S. E. (2017). U.S. cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence*, *30*(1), 53-65. https://doi.org/10.1080/08850607.2016.1230701

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric [Article]. *MIS Quarterly*, *39*(1), 113-A117. https://doi.org/10.25300/misq/2015/39.1.06

Junger, M., Montoya, L., & Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, *66*, 75-87. https://doi.org/10.1016/j.chb.2016.09.012

Kang, J., Shilton, K., Estrin, D., & Burke, J. (2011). Self-surveillance privacy. *Iowa Law Review*, *97*, 809-848. https://doi.org/10.2139/ssrn.1729332

Karaduman, İ. (2013). The effect of social media on personal branding efforts of top level executives. *Procedia - Social and Behavioral Sciences*, *99*, 465-473. https://doi.org/10.1016/j.sbspro.2013.10.515

Keane, T. M., Fairbank, J. A., Caddell, J. M., Zimering, R. T., Taylor, K. L., & Mora, C. A. (1989). Clinical evaluation of a measure to assess combat exposure. *Psychological Assessment: A Journal of Consulting and Clinical Psychology*, *1*(1), 53-55. https://doi.org/10.1037/1040-3590.1.1.53

Kennedy, J., Eberhart, R. C., & Shi, Y. (2001a). Humans—actual, imagined, and implied. In *Swarm intelligence* (pp. 187-259). Morgan Kaufmann. https://doi.org/10.1016/B978-155860595-4/50005-X

Kennedy, J., Eberhart, R. C., & Shi, Y. (2001b). *Swarm intelligence*. Morgan Kaufmann Publishers. https://books.google.com/books?id=vOx-QV3sRQsC

Keysar, B., Lin, S., & Barr, D. J. (2003). Limits on theory of mind use in adults. *Cognition*, *89*(1), 25-41. https://doi.org/10.1016/S0010-0277(03)00064-7

Kim, H.-W., & Pan, S. L. (2006). Towards a process model of information systems implementation: the case of customer relationship management (CRM). *SIGMIS Database*, *37*(1), 59-76. https://doi.org/10.1145/1120501.1120506

Kopan, T. (2015). *CIA Director John Brennan 'outraged' by hack of his emails*. Retrieved February 12. 2021 from http://www.cnn.com/2015/10/27/politics/john-brennan-email-hack-outrage/

Krishnamurthy, B., & Wills, C. E. (2009). On the leakage of personally identifiable information via online social networks. *Proceedings of the 2nd ACM workshop on Online social networks*, 7-12. https://doi.org/10.1145/1592665.1592668

Krombholz, K., Hobel, H., Huber, G. P., & Weippl, E. (2013). Social engineering attacks on the knowledge worker. *Proceedings of the 6th International Conference on Security of Information and Networks*, 28-35. https://doi.org/10.1145/2523514.2523596

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

Ku, Y.-C., Chen, R., & Zhang, H. (2013). Why do users continue using social networking sites? An exploratory study of members in the United States and Taiwan [Article]. *Information & Management*, *50*(7), 571-581. https://doi.org/10.1016/j.im.2013.07.011

Lawshe, C. H. (1975). A quantitative approach to content validity [Article]. *Personnel Psychology*, *28*(4), 563-575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

Lee, D.-J., Ahn, J.-H., & Bang, Y. (2011). Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection [Article]. *MIS Quarterly*, *35*(2), 423-A428. https://doi.org/10.2307/23044050

Lee, J. K. (2016). Invited Commentary—Reflections on ICT-enabled Bright Society Research. *Information Systems Research*, *27*(1), 1-5. https://doi.org/10.1287/isre.2016.0627

Leslie, A. M. (1987). Pretense and representation: The origins of "theory of mind.". *Psychological Review*, *94*(4), 412-426. https://doi.org/10.1037/0033-295X.94.4.412

Lewis, M. (2017). *The undoing project: A friendship that changed our minds*. W.W. Norton & Company.

Linstone, H. A., & Turoff, M. (1975). *The Delphi method: Techniques and applications* (Vol. 29). Addison-Wesley Reading, MA.

Luo, X. R., Brody, R., Seazzu, A., & Burd, S. (2013). Social engineering: The neglected human factor for information security management. *Managing Information Resources and Technology: Emerging Applications and Theories: Emerging Applications and Theories*. https://doi.org/10.4018/irmj.2011070101

Maar, M. C. (2013). *An examination of organizational information protection in the era of social media: A study of social network security and privacy protection* [Ph.D., Capella University]. ProQuest Dissertations & Theses Global. Ann Arbor.

Maeterlinck, M. (1930). Life of the white ant.

Mamonova, S., & Koufaris, M. (2016). The impact of exposure to news about electronic government surveillance on concerns about government intrusion, privacy self-efficacy, and privacy protective behavior. *Journal of Information Privacy & Security*, *12*(2), 56-67. https://doi.org/10.1080/15536548.2016.1163026

Marczak, W. R., & Paxson, V. (2017). Social engineering attacks on government opponents: Target perspectives. *Proceedings on Privacy Enhancing Technologies*, *2*, 152-164. https://doi.org/10.1515/popets-2017-0019

Martin, K. E. (2015). Ethical issues in the big data industry. *MIS Quarterly Executive*, *14*(2), Article 4. https://doi.org/10.4324/9780429286797-20

Maynard, D., Greenwood, M. A., Roberts, I., Windsor, G., & Bontcheva, K. (2015). Real-time social media analytics through semantic annotation and linked open data. *Proceedings of the ACM Web Science Conference*, 1-2. https://doi.org/10.1145/2786451.2786500

McCallister, E., Grance, T., & Scarfone, K. (2010). *Guide to protecting the confidentiality of personally identifiable information (PII)*. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/nist.sp.800-122

Meguerdichian, S., Koushanfar, F., Qu, G., & Potkonjak, M. (2001). Exposure in wireless ad-hoc sensor networks. *Proceedings of the 7th annual international conference on Mobile computing and networking*, 139-150. https://doi.org/10.1145/381677.381691

Mertler, C. A., & Reinhart, R. V. (2013). *Advanced and multivariate statistical methods: Practical application and interpretation* (5th ed.). Pyrczak Publishing.

Minkus, T., Liu, K., & Ross, K. W. (2015). Children seen but not heard: When parents compromise children's online privacy. Proceedings of the 24th International Conference on World Wide Web, Florence, Italy. https://doi.org/10.1145/2736277.2741124

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mohaisen, A., Al-Ibrahim, O., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). *Rethinking information sharing for actionable threat intelligence* [Conference Paper]. Proceedings of the fifth ACM/IEEE Workshop on Hot Topics in Web Systems and Technologies, San Jose, California. https://doi.org/10.1145/3132465.3132468

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers [Article]. *Journal of Consumer Research*, *26*(4), 323-339. https://doi.org/10.1086/209566

Mouton, F., Leenen, L., Malan, M. M., & Venter, H. (2014). Towards an ontological model defining the social engineering domain. IFIP International Conference on Human Choice and Computers, https://doi.org/10.1007/978-3-662-44208-1_22

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186-209. https://doi.org/10.1016/j.cose.2016.03.004

Neupane, A., Rahman, M. L., Saxena, N., & Hirshfield, L. (2015). A multi-modal neuro-physiological study of phishing detection and malware warnings. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 479-491. https://doi.org/10.1145/2810103.2813660

Norman, G. (2010). Likert scales, levels of measurement and the "laws" of statistics [journal article]. *Advances in Health Sciences Education*, *15*(5), 625-632. https://doi.org/10.1007/s10459-010-9222-y

O'keefe, D. J. (2002). *Persuasion: Theory and research* (Vol. 2). Sage Publications, Inc.

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, *57*(6), 1701-1777.

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. *Pew Research Center*, *26*, 311-327. assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf

Oltmann, S. M. (2010). Katz out of the bag: The broader privacy ramifications of using Facebook. *Proceedings of the American Society for Information Science and Technology*, *47*(1), 1-4. https://doi.org/10.1002/meet.14504701250

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. *Proceedings of the 5th conference on Information technology education*, 177-181. https://doi.org/10.1145/1029533.1029577

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, *2*(1), 1-28. https://doi.org/10.4135/9781849209687.n4

Orman, H. (2013). The Compleat Story of Phish. *IEEE Internet Computing*, *17*(1), 87-91. https://doi.org/10.1109/MIC.2013.16

Palen, L., & Dourish, P. (2003). *Unpacking "privacy" for a networked world* [Conference Paper]. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Ft. Lauderdale, Florida, USA. http://www.dourish.com/publications/2003/chi2003-privacy.pdf https://doi.org/10.1145/642611.642635

Parrish, J. L., & Nicolas-Rocca, S. (2012). Toward better decisions with respect to IS security: Integrating mindfulness into IS security training. Proceedings of the Seventh Pre-ICIS Workshop on Information Security and Privacy,

Pavlou, P. A. (2011). State of the Information Privacy Literature: Where are we and where should we go? [Article]. *MIS Quarterly*, *35*(4), 977-988. https://doi.org/10.2307/41409969

PCI Security Standards Council. (2016). *Payment Card Industry (PCI) Data Security Standard, v3.2*. PCI Security Standards Council, LLC. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

Peer, E., & Acquisti, A. (2016). The impact of reversibility on the decision to disclose personal information. *Journal of Consumer Marketing*, *33*(6), 428-436. https://doi.org/10.1108/jcm-07-2015-1487

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Electronic data processing audit, control and security newsletter*, *33*(8), 1-13. https://doi.org/10.1201/1079.07366981/45802.33.8.20060201/91956.1

Perloff, R. M. (2010). *The dynamics of persuasion: Communication and attitudes in the twenty-first century* (Second ed.). Routledge.

Pew Research Center. (2019). *Social networking fact sheet*. Pew Research Center. Retrieved February 12, 2021 from pewinternet.org/fact-sheets/social-networking-fact-sheet/

Premack, D., & Woodruff, G. (1978). Does the chimpanzee have a theory of mind? *Behavioral and Brain Sciences*, *1*(04). https://doi.org/10.1017/s0140525x00076512

Privacy Rights Clearinghouse. (2018). *Data Breaches*. Retrieved January 01, 2018, January from https://www.privacyrights.org/data-breaches

Prosch, M. (2008). Protecting personal information using generally accepted privacy principles (GAPP) and continuous control monitoring to enhance corporate governance. *International Journal of Disclosure and Governance*, *5*(2), 153-166. https://doi.org/10.1057/jdg.2008.7

Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, *2*(1), 122-136.

Raskar, R., Agrawal, A., & Tumblin, J. (2006). Coded exposure photography: motion deblurring using fluttered shutter. *ACM Trans. Graph.*, *25*(3), 795-804. https://doi.org/10.1145/1141911.1141957

Richey, R. C., & Klein, J. D. (2005). Developmental research methods: Creating knowledge from instructional design and development practice. *Journal of Computing in Higher Education*, *16*(2), 23-38. https://doi.org/10.1007/BF02961473

Rivard, S., & Lapointe, L. (2012). Information technology implementers' responses to user resistance: Nature and effects [Article]. *MIS Quarterly*, *36*(3), 897-A895. https://doi.org/10.2307/41703485

Rogers, T. B., Kuiper, N. A., & Kirker, W. S. (1977). Self-reference and the encoding of personal information. *Journal of Personality and Social Psychology*, *35*(9), 677-688. https://doi.org/10.1037/0022-3514.35.9.677

Rosenbaum, M. H. (2015). Identifying unethical personally identifiable information (PII) privacy violations committed by IS/IT practitioners: A comparison to computing moral exemplars.

Ross, R., Viscuso, P., Guissanie, G., Dempsey, K., & Riddle, M. (2016). *Protecting controlled unclassified information in nonfederal systems and organizations*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-171r1

Ross, R. S., Katzke, S. W., & Johnson, L. A. (2006). *Minimum security requirements for federal information and information systems*. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/nist.fips.200

Russell, M. A. (2013). *Mining the social Web* (Second Edition ed.). O'Reilly Media, Inc.

Ryan, W. M., & Loeffler, C. M. (2010). Insights into cloud computing. *Intellectual Property & Technology Law Journal*, *22*(11), 22-28.

Salkind, N. J. (2012). *Exploring research* (8th ed.). Pearson Education.

Sanders, S. D. (2012). Privacy is dead: The birth of social media background checks. *Southern University Law Review*(39), 243-264.

Sawilowsky, S. S. (2009). New Effect Size Rules of Thumb. *Journal of Modern Applied Statistical Methods*, *8*(2), 597-599. https://doi.org/10.22237/jmasm/1257035100

Saxe, R., Schulz, L. E., & Jiang, Y. V. (2006). Reading minds versus following rules: Dissociating theory of mind and executive control in the brain. *Social Neuroscience*, *1*(3-4), 284-298. https://doi.org/10.1080/17470910601000446

Schmider, E., Ziegler, M., Danay, E., Beyer, L., & Bühner, M. (2010). Is it really robust? *Methodology*.

Schneier, B. (2000). *Secret and Lies*.

Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *New York University Law Review*, *86*(6), 1814-1894.

Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill-building approach* (6th ed.). John Wiley & Sons LTD.

Shapiro, S. L., Carlson, L. E., Astin, J. A., & Freedman, B. (2006). Mechanisms of mindfulness. *Journal of Clinical Psychology*, *62*(3), 373-386. https://doi.org/10.1002/jclp.20237

Simpson, M. D. (2016). All your data are belong to us: Consumer data breach rights and remedies in an electronic exchange economy. *University of Colorado Law Review*, *87*(2), 669-709.

Singh, B., Bansal, D., & Sofat, S. (2014). An approach of privacy preserving based publishing in Twitter. *Proceedings of the 7th International Conference on Security of Information and Networks*, 39-42. https://doi.org/10.1145/2659651.2659733

Smith, A. (2015, April 2015). *U.S. smartphone use in 2015*. Pew Research Center. http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review [Article]. *MIS Quarterly*, *35*(4), 980-A927. https://doi.org/10.2307/41409970

Solove, D. J. (2006). A taxonomy of privacy [Article]. *University of Pennsylvania Law Review*, *154*(3), 477-560. https://doi.org/10.2307/40041279

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types

of organizations. *Journal of Applied Psychology*, *68*(3), 459-468. https://doi.org/10.1037/0021-9010.68.3.459

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems*, *13*(1), 380-426. https://doi.org/10.17705/1cais.01324

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, *13*(2), 147-169. https://doi.org/10.2307/248922

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users [Article]. *MIS Quarterly*, *37*(4), 1141-A1145. https://doi.org/10.25300/misq/2013/37.4.07

Sweeney, L. (1997). Weaving technology and policy together to maintain confidentiality. *The Journal Of Law, Medicine & Ethics: A Journal Of The American Society Of Law, Medicine & Ethics*, *25*(2-3), 98-110. https://doi.org/10.1111/j.1748-720x.1997.tb01885.x

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, *32*(10), 1014-1023. https://doi.org/10.1080/0144929X.2013.763860

Tversky, A., & Kahneman, D. (1975). Judgment under uncertainty: Heuristics and biases. In *Utility, probability, and human decision making* (pp. 141-162). Springer. https://doi.org/10.1007/978-94-010-1834-0_8

U.S. Department of Justice. (2018). *Nine Iranians charged with conducting massive cyber theft campaign on behalf of the Islamic Revolutionary Guard Corps*. https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

Van den Akker, J., Branch, R. M., Gustafson, K., Nieveen, N., & Plomp, T. (2012). *Design approaches and tools in education and training*. Springer Science & Business Media. https://doi.org/10.1007/978-94-011-4255-7

von der Gracht, H. A. (2012). Consensus measurement in Delphi studies: Review and implications for future quality assurance. *Technological Forecasting and Social Change*, *79*(8), 1525-1536. https://doi.org/10.1016/j.techfore.2012.04.013

Wenyin, L., Huang, G., Xiaoyue, L., Min, Z., & Deng, X. (2005). *Detection of phishing webpages based on visual similarity* [Conference Paper]. Special interest tracks and posters of the 14th international conference on World Wide Web, Chiba, Japan. https://doi.org/10.1145/1062745.1062868

Wilkerson, W. S., Levy, Y., Kiper, J. R., & Snyder, M. (2017). Towards a development of a Social Engineering eXposure Index (SEXI) using publicly available personal

information. Conference on Cybersecurity Education, Research and Practice, Kennesaw State University, USA. https://digitalcommons.kennesaw.edu/ccerp/2017/research/5/

Wolff, J. (2016). Perverse effects in defense of computer systems: When more Is less [Article]. *Journal of Management Information Systems*, *33*(2), 597-620. https://doi.org/10.1080/07421222.2016.1205934

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, *16*(6), 315-331. https://doi.org/10.1080/10658980701788165

Workman, M. (2008). Wisecrackers: A theory‐grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662-674. https://doi.org/10.1002/asi.20779

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42-52. https://doi.org/10.1016/j.dss.2010.11.017

Youssef, N. A., Green, K. T., Dedert, E. A., Hertzberg, J. S., Calhoun, P. S., Dennis, M. F., Research, E., Clinical Center Workgroup, M.-A. M. I., & Beckham, J. C. (2013). Exploration of the influence of childhood trauma, combat exposure, and the resilience construct on depression and suicidal ideation among U.S. Iraq/Afghanistan era military personnel and veterans. *Archives of Suicide Research*, *17*(2), 106-122. https://doi.org/10.1080/13811118.2013.776445

Zhang, B., Wu, M., Kang, H., Go, E., & Sundar, S. S. (2014). Effects of security warnings and instant gratification cues on attitudes toward mobile websites. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto Ontario Canada. https://doi.org/10.1145/2556288.255734710.1145/2556288.2557347