2020

SNS Use, Risk, and Executive Behavior

Andrew Green

SNS Use, Risk, and Executive Behavior

By

Andrew Green

A dissertation 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
2020

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

James L. Parrish, Ph.D.
Chairperson of Dissertation Committee

4/30/2020
Date

Jason Thatcher, Ph.D.
Dissertation Committee Member

4/30/2020
Date

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

30 April 2020
Date

Approved:

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

04/30/2020
Date

College of Computing and Engineering
Nova Southeastern University

2020

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

SNS Use, Risk, and Executive Behavior

by
Andrew Green
April 2020

Personal social networking sites (SNS) are popular outlets for people to share information about themselves, their family and friends, and their personal and professional lives. On the surface, the information shared may seem to be innocuous or nonthreatening. However, prior studies have shown that cybercriminals can take information shared via personal SNS and use it to conduct attacks against organizations. Organization executives are of particular interest to cybercriminals because they have access to sensitive data, and they also have the ability to command actions from their subordinates. The purpose of this study was to explore what executive personal SNS behaviors pose financial risks to an organization.

This study utilized grounded theory method (GTM) to interview nine information security professionals to discover their perceptions regarding executives' personal SNS behaviors that could pose a financial risk to an organization. The researcher used a semi-structured interview process in order to collect thick, rich data for analysis. Respondents came from a diverse array of industries, thus providing data from multiple perspectives.

The resulting data analysis revealed four overarching dimensions: *Loss of Intellectual Property or Sensitive Data; Compliance Violations; Harm to Reputation,* and *Fraudulent Transaction Loss.* These overarching dimensions were supported by multiple themes, which were built on concepts identified from respondent interview data. These overarching dimensions were used to build an emergent theoretical model to explain what personal executive SNS behaviors pose financial risks to an organization.

Acknowledgments

I would like to thank several people for their invaluable support and encouragement during this long, winding process.

First, thank you to my committee chair, Dr. James Parrish. He has pushed me to become a more focused researcher, a more critical thinker, and a better academic. He has said “no” to me so many times during this process, that I eventually took to opening discussions with “I realize you will probably say ‘no’ to this, but…”. I realized both then and now that without that “no,” I would not be where I am today, and I am deeply grateful for his unwavering support and friendship throughout this endeavor.

Thank you to my committee members, Dr. James Smith, and Dr. Jason Thatcher. Without Dr. Smith’s early help on my proposal, I would most likely still be stuck in the weeds. In particular, I would like to thank him for our extended conversations in San Francisco during ICIS 2018, as well as the many “hey, have you got a minute?” telephone calls that turned into 45-minute sessions, which took him away from family and other work. Additionally, I would like to thank Dr. Jason Thatcher for his assistance with framing my research question appropriately and forcing me to dig into the deeper issues around my original research ideas. Dr. Thatcher has a world-class mind, and I am a better researcher and person for his observations, critiques, and criticisms.

Thank you to my work colleagues at Kennesaw State University, who were so gracious with their time and efforts to help me during this process. You know who you are, and I want you to know how much I appreciate everything you did to help me cross this finish line.

Thank you to my family and friends who put up with me being absent from events, being distracted while thinking about this dissertation instead of being present in the moment, and for offering support when I doubted myself.

Finally, thank you to my sweet Rebeccah. You mean everything to me. You have been unwavering in your support, sacrificing time together to allow me to finish this project. Your understanding as I worked at all hours of the night contributed so much to me reaching this milestone. I love you with all of my heart.

“So, what’s next?”

Table of Contents

Chapters

Appendices

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Cybercriminals direct social engineering attacks at organizational employees as a means to secure access to sensitive data (Conteh & Royer, 2016; Gardner & Thomas, 2014; Greitzer et al., 2014; Wilcox, Bhattacharya, & Islam, 2014). Adversaries collect and use intelligence to engage in organizational attacks through various vectors. For example, cybercriminals use pretexting, a form of social engineering (SE), to create scenarios that convince victims to perform the desired action (Brody, Brizzee, & Cano, 2012; Greitzer, et al., 2014; Luo, Brody, Seazzu, & Burd, 2011). Cybercriminals can employ pretexting in many attack vectors, including phishing (Conteh & Royer, 2016; Symantec, 2015; Verizon Enterprises, 2016), spear phishing (He, 2012; Heartfield & Loukas, 2015; Laszka, Lou, & Vorobeychik, 2015; Teplinsky, 2013), vishing via telephone, voice over IP (VoIP), or short message service (SMS) messages (Gardner & Thomas, 2014; Shahriar, Klintic, & Clincy, 2015).

Frequently, cybercriminals collect data used in these attacks through personal social media channels which belong to an employee, such as community-based platforms (Facebook, Twitter, LinkedIn), discussion boards, blogs, and wikis (Greitzer, et al., 2014; He, 2012; Kim, 2012). Collectively, these channels are called social network sites, or SNS (boyd & Ellison, 2007). Data collected about an employee via SNS may seem harmless to an organization. However, like Humphreys, Gill, and Krishnamurthy (2014, p. 846) noted, when aggregated, this type of data "…may tell a deeper, more intimate story" about an individual.

Data gathered from SNS users can be used to design SE attacks (Constantiou & Kalinikos, 2015; Palmer, 2020; Social-Engineer LLC, 2019). SNS users share personal information for various reasons, such as developing or maintaining personal relationships or general knowledge acquisition (Krasnova, Veltri, Eling, & Buxmann, 2017; Wakefield & Wakefield, 2016), as well as perceived benefits to job performance (Ali-Hassan, Nevo, & Wade, 2015). Such data, collected from employees' personal SNS, helps cybercriminals to design realistic pretexting scenarios (Greitzer, et al., 2014; He, 2012; Kim, 2012).

Once cybercriminals collect SNS data, they next look to use it for SE attacks against organizations (Greitzer, et al., 2014). Email account compromise (EAC) is one such type of SE attack. With an EAC attack, cybercriminals can use SNS data to hijack or impersonate executives' accounts and use the authority of the executives' position to direct employees to initiate an EFT or wire transfer to a bank account that they control (Burch, Taylor, & Yeung, 2015; Federal Bureau of Investigation, 2017; Kemp, 2016). Upon receipt of the funds, the cybercriminal then disperses the funds to other accounts, for obfuscation and making recovery of those funds for the victim organization difficult, if not impossible (Burch, et al., 2015; Meinert, 2016).

Organization executives are frequent targets of EACs because of their access to sensitive data, as well as their ability to command actions from subordinates (Bullée, Montoya, Pieters, Junger, & Hartel, 2017; Federal Bureau of Investigation, 2017; Sharp, 2017; Trustwave, 2017). Executives make these attacks easier for cybercriminals by sharing data on SNS (Burch, et al., 2015). Such breaches put organizations at risk in three primary areas: monetary losses, corporate liability, and credibility (Cavusoglu, Cavusoglu, & Raghunathan, 2004). Kemp (2016) noted a 270% increase in this type of attack since January 2015, with an estimated loss of 2.3 billion dollars in 2014-2015. The Federal Bureau of Investigation (2017) reported a 2,370% increase in identified losses between January 2015 and December 2016, with instances occurring in each of the 50 states in the United States of America, as well as 131 countries. As these numbers demonstrate, successful attacks can have a direct impact on the organization's financial well-being, ranging from inconvenient to catastrophic.

Categorizing the types of data being accessed by cybercriminals to engage in EAC attacks has proven to be difficult, due to the lack of a seminal definition. For example, the literature shows that there is a tendency to use the phrase personally identifiable information (PII) interchangeably with personal information (PI) and sensitive information (SI) (Baker & Hostetler LLP, 2017; Humphreys, et al., 2014; Peppet, 2014; Schwartz & Solove, 2014) to describe essentially the same data points. Social data is data collected from social media platforms (Constantiou & Kalinikos, 2015; Krombholz, Hobel, Huber, & Weippl, 2015; Mukkamala, Vatrapu, & Hussain, 2013). This study will use the term social data to describe the data shared by organization executives via their personal SNS.

Problem Statement

Executives' use of personal SNS makes organizations more vulnerable to attacks. In one such attack which took place for several months in 2018, a group of cybercriminals known as London Blue developed a list of over 50,000 finance executives to target (AGARI Data, 2018). Of those potential targets, 71% carried the title of Chief Financial

Officer (CFO) (AGARI Data, 2018). In March 2018, Pathe Cinemas lost more than 19 million euros after cybercriminals targeted both their CFO and Chief Executive Officer (CEO) for attack (Grooten, 2018). After being fired by Pathe Cinemas, the CFO successfully sued his former employer for back wages for improper termination, resulting in an even more significant loss for the organization (Grooten, 2018). In December 2018, the "Save the Children" charity organization disclosed they lost $1 million as the result of a business email compromise (BEC) attack (Wallack, 2018). Industry professionals have made calls for corporate security teams to help senior executives improve their cyber hygiene because they unknowingly leak information via SNS and other means (Grunwitz, 2018).

Extant literature sheds little light on the financial risks organizations face from their executives' personal use of SNS. Studies have explored the general need for social engineering training in the organizational context (Buckley, Nurse, Legg, Goldsmith, & Creese, 2014; Molok, Chang, & Ahmad, 2013), as well as the effectiveness of social engineering awareness training in general (Gardner & Thomas, 2014; Korpela, 2015; Rocha Flores & Ekstedt, 2016). Also, existing literature has examined organizational issues associated with the surveillance of personal SNS (Uldam, 2016). Furthermore, existing literature has explored steps organizations can take to minimize the potential damage from social engineering attacks in general (Rocha Flores & Ekstedt, 2016; Vaast & Kaganer, 2013), as well as to understand the legalities surrounding organizational policies regarding employees use of their personal social media channels in non-work related situations (Sánchez Abril, Levin, & Del Riego, 2012). To date, there has not been a systematic study that ties social engineering, organizational information security risk assessment, and information security policies to better, more secure use of personal SNS by organizational executives. The first step in that direction is understanding what executive SNS behaviors place organizations at risk.

Dissertation Goal

The goal of this research study was to explore the types of executive SNS behaviors that might pose a financial risk to an organization.

Research Question

This study answered the following research question:

RQ1: What executive personal SNS behaviors pose financial risks to an organization?

Relevance and Significance

This study advanced current research by gaining a deeper understanding of what executives' behaviors on SNS can post financial risks to an organization. Organizations continue to be susceptible to attacks via the human element (Social-Engineer LLC, 2017). Documented incidents involving senior organizational management are plentiful (Atkins & Huang, 2013; Rivera, 2018). Existing literature has explored the risks organizations face by way of their executives, as well as the roles they can play in helping to mitigate those risks (Brody, et al., 2012; Bronk, 2014; Buckley, et al., 2014; Burch, et al., 2015; Hsu, Shih, Hung, & Lowry, 2015). This study helped inform academia as well as practitioners by offering an emergent theoretical model that explores the financial risks organizations face from executives' use of their personal SNS.

Barriers and Issues

One barrier for this study was getting Institutional Review Board (IRB) approval to interview study respondents. Since this research involved collecting potentially sensitive or embarrassing information, the researcher had to develop trust with respondents, demonstrate data safekeeping processes, and how the data collected would not put the respondent or the researcher at risk (Creswell & Creswell, 2018). Another potential barrier to the study was the population size needed to complete the study. As Creswell and Creswell (2018) noted, researchers must purposefully choose respondents for qualitative studies in order to help the researcher understand both the problem and the research question.

Assumptions, Limitations and Delimitations

Assumptions

The study has some assumptions. One assumption is that that all respondents answered questions truthfully and honestly. Another assumption is that respondents chosen to participate are representative of the overall population. Yet another assumption is that the respondents possessed the necessary insight to provide valid responses.

Limitations

The study has some limitations. One limitation is the availability of respondents for recorded interviews. To counter this limitation, the researcher was very flexible in scheduling interviews both in place and time. Most interviews were done remotely via WebEx, but the researcher also traveled to conduct one interview in-person. Another limitation is the dearth of extant research available about organization executives' use of SMS.

Delimitations

The study has some delimitations. One delimitation is that all respondents came from the United States. As a result, conducting the same study in a different country could yield different findings. A second delimitation is the work experience level of the respondents. By requiring a minimum of five years of work experience, the study does not include data from respondents who may have valid insights but fail to meet the minimum experience threshold.

Definition of Terms

Email Account Compromise (EAC) – A form of social engineering attack which targets employees who are authorized to perform EFT or wire transfer payments (Federal Bureau of Investigation, 2017)

Information security – A well-informed sense of assurance that information risks and technical, formal and informal controls are in dynamic balance (Torres, Sarriegi, Santos, & Serrano, 2006)

Pretexting – A form of social engineering involving the creation of scenarios designed to convince the victim to perform the desired action (Brody, et al., 2012; Greitzer, et al., 2014; Luo, et al., 2011)

Risk – the possibility of an undesired outcome which results from an incident or occurrence, as determined by the likelihood and relevant consequences (Department of Homeland Security Risk Steering Committee, 2010)

Social data - data which has collected from social media platforms (Constantiou & Kalinikos, 2015; Krombholz, et al., 2015; Mukkamala, et al., 2013)

Social engineering (SE) – deceptive practices designed to entice individuals to aid attackers in achieving their goals (Atkins & Huang, 2013)

Social network site(s) (SNS) – Web-based services that allow users to build a public or semi-public profile within a bounded system; create a list of other users they share a connection with; view their list as well as others (boyd & Ellison, 2007)

List of Acronyms

BEC – Business email compromise

CEO – Chief executive officer

CFO – Chief financial officer

EAC – Email account compromise

IS – Information systems

PI – Personal information

PII – Personally identifiable information

SE – Social engineering

SI – Sensitive information

SNS – Social network site(s)

Summary

This chapter discussed the background for the research topic, describing various information security threats to the organization, and how executive behaviors can pose a financial risk to the organization. This chapter also laid out the foundation for the justification of the proposed study and described the research question to be studied.

Additionally, the relevance and significance of the study were discussed, as well as barriers and issues, which may affect the study. Finally, definitions for specific terms used in the study were defined.

Chapter 2

Review of the Literature

Introduction

This section will explore literature specific to information security as a defined concept, ways to classify organizations, organization executives, and how they differ from rank-and-file employees, organizational information disclosure, and organizational risk. The literature search focused primarily, but not exclusively, on the Association for Information Systems (AIS) Senior Scholars' Basket of Journals list (Association for Information Systems, 2011). The literature review supports the researcher's position that a gap in the literature exists at the intersection of executive SNS behaviors and the potential financial risks they pose to an organization.

Information Security definition

Based on a review of the literature, the term information security, while frequently used, lacks a seminal definition or explanation. Existing literature observed that the term is a concept that lacks a clear-cut definition (Anderson, 2003; Torres, et al., 2006). Dlamini, Eloff, and Eloff (2009) found that the concept of information security predates the invention of the computer. Interestingly, there are numerous articles (Crossler et al., 2013; Johnston, Warkentin, & Siponen, 2015; Lowry, Posey, Bennett, & Roberts, 2015; Rocha Flores & Ekstedt, 2016) which use the term information security without ever supplying a definition, thus leaving it to the reader to interpret its meaning through their lenses and experiences.

Anderson (2003) observed that previous attempts to define information security were overly broad. Subsequently, Anderson (2003, p. 310) offered his definition of information security as being "…A well-informed sense of assurance that information risks and controls are in balance". Torres, et al. (2006, p. 532) offered a definition similar to that offered by Anderson (2003), "Information security is a well-informed sense of assurance that information risks and technical, formal and informal controls are in dynamic balance."

Further complicating the issue of defining information security is the increasing use of the terms cybersecurity or cyber security. Agresti (2010) and von Solms and van Niekerk (2013) both noted that these terms might be viewed by some as having the same meaning, thus making their usage interchangeable. Agresti (2010) also went on to note that the use of the term cybersecurity is increasingly replacing information security as the default term. Bronk (2014) observed that the term cyber security could have different meanings to different market sectors, as well as to nation-states when considering national defense concerns. von Solms and van Niekerk (2013) explored the differences between the terms information security and cyber security/cybersecurity, concluded there is a difference between the terms, and thus not interchangeable. Similar to the observation made previously, numerous articles used the term cybersecurity or cyber security without defining it (Carlton & Levy, 2015). This study will use the definition of information security as offered by Torres, et al. (2006). By extension, we will define an information security risk as any activity that could potentially disrupt the aforementioned dynamic balance.

Social Networking Sites (SNS)

Existing literature has explored several different themes related to SNS. This section will cover some of those themes, including challenges and benefits of enterprise SNS usage; benefits of SNS data available to organizations; personal risks associated with information shared via SNS; emotional benefits and challenges associated with SNS; SNS privacy policy impact on users' willingness to share personal information; and employee benefits from using SNS.

Leonardi (2015) examined the benefits of organizationally restricted SNS, focusing on the benefits of ambient knowledge gained by employee SNS interaction. According to Leonardi (2015), employees using SNS to interact internally can gain a degree of ambient awareness, which he described as an understanding of who knows what (also described as organizational metaknowledge) within an organization. Choudrie and Zamani (2016) explored the challenges of organizationally restricted SNS use within the workplace. Choudrie and Zamani (2016) found that the implantation of SNS software in the workplace can be challenging. In order to benefit from SNS software usage, the organization must take the proper steps to highlight the benefits associated with its usage (Choudrie & Zamani, 2016). Forsgren and Byström (2017) explored the benefits associated with organizationally restricted SNS usage by conducting a case study of a Scandinavian software company. By exploring the environment through the lens of activity theory, Forsgren and Byström (2017) discovered that SNS usage within the organization made work-related activities more coherent, even in environments where the

SNS was not optimized.

Pike, Bateman, and Butler (2017) explored how organizations use information from external SNS to assist in the hiring process of job candidates. Pike, et al. (2017) found that while information collected on job candidates via SNS can be beneficial, hiring managers must be careful to evaluate the quality of the information collected holistically. Specifically, information collected from sources which evidenced a high degree of context collapse may increase the amount of ambiguity in the decision-making process, as opposed to reducing it.

Wakefield (2013) examined how user affect impacted the desire to disclose information online. Wakefield (2013) found that when users had a pleasant experience using a website, privacy concerns decreased, and their perception of trust increased. As a result of the pleasant experience, users were more likely to share personal information with the website (Wakefield, 2013). Chen, Lu, Chau, and Gupta (2014), as well as Heravi, Mubarak, and Choo (2018) explored how personal risks associated with information shared via SNS help shape user intent to use SNS. Both Chen, et al. (2014) and Heravi, et al. (2018) confirmed that perceived cyber risks from sharing information played a critical role in user determination about SNS usage. Hu, Kettinger, and Poston (2015) examined the role that perceived information risk played in user decision-making regarding the use of SNS. Hu, et al. (2015) found that users believed the benefits associated with SNS usage outweighed the risks associated with sharing their personal information. Gerlach, Widjaja, and Buxmann (2015) explored the impact of SNS privacy policies on user intention to share personal information. Gerlach, et al. (2015) found that the permissiveness of a SNS privacy policy negatively impacted a user’s desire to share personal information. However, Gerlach, et al. (2015) also found that the perceived risks associated with the privacy policy served as a mediating factor in user desire to share personal information. Gao, Liu, Guo, and Li (2018) explored issues of ubiquitous connectivity to SNS via mobile devices. According to Gao, et al. (2018), ubiquitous connectivity to SNS can result in negative psychological impacts on users, as well as inadvertent leakage of personal information.

Matook, Cummings, and Bala (2015) examined how personal SNS usage impacted user perceptions of loneliness. Matook, et al. (2015) found that employees who travel frequently may suffer greater feelings of loneliness and that organizations may benefit from encouraging SNS usage in these cases. Additionally, Matook, et al. (2015) recommended that organizations should focus on creating policies which encourage positive outcomes from employee use of SNS. Ali-Hassan, et al. (2015) examined employee use of personal SNS in the workplace and the associated impact on the organization. Ali-Hassan, et al. (2015) found that hedonic use of personal SNS in the workplace had mixed results, with a negative impact on employee productivity, but a positive impact on employee creativity as well as an increase in employee social capital. Ali-Hassan, et al. (2015) also recommended organizations encourage the use of personal SNS during work hours, and to allow the line between work and personal social activities to blur, to have a positive impact on overall job performance. Turel and Qahri-Saremi (2016) probed the problematic issues associated with SNS usage concerning undergraduate student academic performance. Turel and Qahri-Saremi (2016) supported the idea that educational institutions should focus on helping students find ways to control problematic information systems (IS) usage while enrolled, and beyond.

Wakefield and Wakefield (2016) explored the impact of user passion and affect on SNS usage. Surprisingly, one finding in the Wakefield and Wakefield (2016) study was there was no relationship between user excitement about an event and SNS usage at the event. However, Wakefield and Wakefield (2016) found that while excitement may not directly induce SNS usage at an event, it may contribute to a belief that the event is conducive to meet some need, which would lead to SNS usage.

As the literature shows, SNS presents both benefits and challenges to employees and organizations. Employees can benefit both personally and professionally from SNS usage, and so are inclined to use it. The literature also shows that organizations can be put at risk from SNS usage. What is unexplored in the literature is the financial risk that organizations can face as a result of their executives' use of personal SNS.

Organization classification

Existing literature reveals that various criteria can be used to classify organizations in different ways. As Flack (2016) noted, the classification of organizations can occur across multiple considerations such as the number of employees, annual revenue, as well as the number of locations, and these considerations can vary by industry. National Institute of Standards and Technology (2011) published a report that focused on the management of information security risk from the organizational view. National Institute of Standards and Technology (2011) outlined different sectors for organizational groupings, such as legal, finance, information technology, and regulatory compliance, among others, and stated that managing information security risks required expertise specific to that particular sector.

Buonanno et al. (2005) explored different ways in which organizations could be classified by exploring existing IS literature through the lens of enterprise resource planning (ERP) adoption. Buonanno, et al. (2005) found discussed classification criteria for organizations, such as company size, market area, membership in an industrial group, the presence of branch offices, diversification level, and the degree of functional extension. Flack (2016) echoed some, but not all, of these same criteria.

J. W. Lee, Seong, and Lee (2012) explored the ways organizations can be classified through the lens of human resources management. J. W. Lee, et al. (2012) explored existing taxonomy for organization classification by way of literature review and discovered it was lacking. According to J. W. Lee, et al. (2012), existing organization taxonomy literature failed to scientifically group organizations, thus exposing a gap in the literature.

According to DeSalvo, Limehouse, and Klimek (2016), the United States Census Bureau classified organizations by industrial sector, the legal form of the organization, as well as federal tax status. Quttainah and Paczkowski (2014) explored the ways privately held organizations could be classified while undergoing valuation for potential purchase. As Quttainah and Paczkowski (2014) noted, rational business owners will choose to seek the highest value for their organization at the time of sale, but if both parties cannot agree on a price, they may call an appraiser in to offer input. As part of this process, appraisers may classify an organization based on criteria such as cash flow, the effectiveness of current management, and the uncertainty associated with the span of control to be held by the owner post-sale (Quttainah & Paczkowski, 2014).

Extant literature showed multiple methods by which organizations can be classified. The literature also showed that the management of information security risks required expertise specific to that classification. Thus, it is important to research financial risks for organizations across a diverse set of organizational classifications in order for the results to be both rigorous and generalizable.

Organization executives

Existing literature has explored organization executives through multiple lenses. As early as Hambrick (1981), literature explored the impact that executives had on the success of their organization. The seminal work of Hambrick and Mason (1984), which offered the Upper Echelons perspective model, served as a foundation for exploring various ways to predict organizational outcomes. According to Hambrick and Mason (1984), organizational outcomes are reflections of top managers and their values. Hambrick and Mason (1984) also argued that the behavior and characteristics of executives mattered as it related to organizational outcomes. Hambrick and Mason (1984) theorized that top managers made strategic choices that would impact the performance of the organization. According to Hambrick and Mason (1984), the success or failure of these choices could be partially predicted based on observable criteria such as age, functional tracks, prior career experiences, education level, socioeconomic background, financial position, and group characteristics.

Hambrick and Mason (1984) referenced existing literature with conflicting findings. Notably, Hall (1977) argued that organizations effectively run themselves in the form of inertia and are mostly immune to executive behaviors. Additionally, Hannan and Freeman (1977) used an ecological lens to examine organizational behavior and found that organization executives fail to substantially impact outcomes due to both internal and external pressures which impact the organization, and are outside of executive control.

As Finkelstein and Hambrick (1990) noted, researchers attempted to bridge the gap between these two competing views by offering a contingency approach. According to Finkelstein and Hambrick (1990), the concept of managerial discretion was a theory to bridge this gap. Building on prior literature, Finkelstein and Hambrick (1990) refined the Upper Echelons perspective model, by offering managerial discretion as a moderating variable. Finkelstein and Hambrick (1990) described managerial discretion as the degree of freedom available to top executives to make decisions. According to Finkelstein and Hambrick (1990), in situations where managerial discretion was low, executive effectiveness was limited, and the Upper Echelons perspective model did not hold up well and was unable to explain the situation adequately. However, Finkelstein and Hambrick (1990) observed that in situations where managerial discretion was high, executive effectiveness was not limited, and the Upper Echelons perspective model held up well and was able to explain the situation adequately. Hambrick, Finkelstein, and Mooney (2005) further refined the Upper Echelons perspective model by introducing executive job demands as an additional moderating variable. According to Hambrick, et al. (2005), executives who faced heavy job demands would take mental shortcuts, and rely on solutions they had seen work successfully in the past, so their backgrounds and prior experiences effectively colored their decisions. However, Hambrick, et al. (2005) found that executives with lighter job demands had the flexibility and freedom to be more comprehensive in their analyses and were ultimately better positioned to make a decision that more objectively addressed the situation at hand.

Building on Hambrick and Mason (1984), Hambrick, et al. (2005) argued that senior executives are of specific interest because they serve as an interface between the organization and its environment, and wield sufficient power to impact the organization. According to Hambrick, et al. (2005), executive-level work is qualitatively different from work found at other levels of the organization. Hambrick, et al. (2005) also found that executive leadership behaviors could impact both the vitality and performance of their organization and thus warranted further examination.

Organization executives are of particular interest to adversaries, because of the level of access and oversight they have. Krombholz, et al. (2015) outlined whaling attacks, a type of phishing attack, which targets organization executives explicitly. Adversaries can use whaling attacks to achieve different goals. For example, Hong (2012) described whaling attacks targeting chief operating officers (CEOs) with fake subpoenas as email attachments, which had malware installed. In 2016, a finance executive at Mattel was the victim of a whaling attack, nearly resulting in a loss of $3 million via EFT (Associated Press, 2016). Holland, Amado, and Marriott (2018) reported on cybercriminals offering access to executive email accounts for as little as $150.

Organizational information disclosure

A review of the literature regarding organizational information disclosure revealed the presence of multiple themes in the space. This section will review some of those themes, which include organizational challenges in responding to customer privacy concerns, challenges present in protecting organizational data, and the possible market reactions organizations face when they suffer from unauthorized disclosure of information.

Greenaway and Chan (2013) proposed a framework that organizations could use to create a customer data privacy policy. Greenaway, Chan, and Crossler (2015) were able to utilize a case study methodology to provide six lessons learned to assist organizations in overcoming challenges associated with maintaining their customer data privacy initiatives. Wakefield (2013) studied the effect of user affect in the disclosure of personal information on commercial websites. Among the findings, Wakefield (2013) observed that users were more likely to disclose personal information to a website if their initial experience with the website was enjoyable, even if the user was not familiar with any organizational policies regarding the safekeeping of users personal information. The impact of user affect on personal information disclosure was explored by Kehr, Kowatsch, Wentzel, and Fleisch (2015). Similar to the findings in the Wakefield (2013) study, Kehr, et al. (2015) found that users were more likely to disclose personal information when in a positive affective state while using an information system. Greenaway, et al. (2015) proposed a conceptual framework to help organizations reconcile their legal and ethical responsibilities to customers concerning their personal data, and organizational responsibilities to adhere to internal information management objectives. Among their findings, Greenaway, et al. (2015) observed that organizations need to make a fundamental determination as to whose interests they are operating in, how they will use the information collected, and to what degree they should extend beyond any legal requirements in order to provide a higher degree of protection for their customer's personal data.

Organizations also face challenges in regards to protecting corporate data. Conger, Pratt, and Loch (2013) explored the challenges organizations face in protecting corporate data. Among their findings in this area, Conger, et al. (2013) noted that data collection and sharing among organizations, combined with the growing number of methods to customer data, pose a significant challenge to organizations in their efforts to protect data collected. Hsu, et al. (2015) studied the effectiveness of extra-role behaviors exhibited by organization workers as they relate to information security policy effectiveness. Defined as employee behaviors that extend beyond those described in organizational security policies, Hsu, et al. (2015) found that when combined with in-role behaviors, extra-role behaviors have a positive impact on organizational security policy effectiveness. Lowry and Moody (2015) proposed a new model which examined employee motivations, in an attempt to determine employee intent to comply with new organization security policies. This model, which combined control theory with reactance theory, found that organizational controls were a positive predictor of an employee's intent to comply with new security policy, while perceived threats to personal freedom resulted in employee reactance to new security policy. Lowry, et al. (2015) explored how organizations could leverage fairness theory and reactive theory to increase the likelihood that employees would adhere to organizational security policies. Among their findings, Lowry, et al. (2015) discovered that employees were more likely to adhere to organizational security policies if an atmosphere of organization trust existed. Lowry, et al. (2015) found that one method to increase the level of organizational trust was through the implementation of explanation adequacy, used to inform employees of the underlying reason and subsequent importance of organizational security policy. C. H. Lee, Geng, and Raghunathan (2016) examined the impact of mandatory standards on the effectiveness of organizational information security. Among their findings, C. H. Lee, et al. (2016)

reported that the implementation of a higher security standard does not necessarily lead to an increase in security for an organization.

Existing literature has also explored the marketplace consequences organizations can face after suffering a data breach. Wang, Kannan, and Ulmer (2013) examined the impact organizations may face when publicly disclosing a data breach event. Wang, et al. (2013) found no significant difference in marketplace reaction when an organization disclosed a data breach in financial reporting documents, but that the marketplace did respond differently when an organization announced a breach outside the release of financial reporting documents.

Summary

Overall, the review of the literature revealed a gap in the understanding of the financial risks that organizations face from executives' use of personal SNS. This gap merited further exploration and supported the justification for this study. The literature review showed that the actions of their executives' impact organizations. Specifically, the literature review showed that executives merit specific scrutiny because they interface between the organization and its environment and are powerful enough to impact the organization. Furthermore, executive-level work is different from the work done by others in the organization. Next, the literature review showed that executive behaviors could impact the performance of their organization, and thus warranted further examination. Additionally, the literature review showed the lack of a seminal definition of information security, thus making it difficult for organizations to approach the concept in a coherent, organized manner. Finally, the literature review showed that organizations face challenges in protecting their data and that they can suffer negative financial impacts as a result.

Chapter 3

Methodology

Introduction

This chapter discusses the methodology used for this research study. This chapter also contains details about the research methodology employed and how the researcher developed and validated the research instrument. Additionally, population and sample size is discussed. Next, this chapter discusses how collected research data was analyzed. Finally, this chapter discusses the resources used to conduct this research study.

Overview of research methodology and design

According to Creswell and Creswell (2018), researchers should identify their worldview as a fundamental component of any study they conduct. Creswell and Creswell (2018) identify four distinct worldviews: Postpositivism, Constructivism, Transformative, and Pragmatism. Creswell and Creswell (2018) describe the constructivist worldview as an approach typically used with qualitative research. Constructivist researchers do not start with a theory, instead choosing to generate or develop a theory based on observations (Creswell & Creswell, 2018). Based on this description, Constructivist was the researcher’s worldview for this study.

Grounded theory methods (GTM) were first proposed by Glaser and Strauss (1967), although they have since split into two distinct camps after a public falling out between Glaser and Strauss over fundamental issues (Urquhart, Lehmann, & Myers, 2009). Matavire and Brown (2017) outlined subsequent advances in GTM, referring to the two camps as “classic” and “evolved.” According to Matavire and Brown (2017), the work of

Charmaz and others falls into the “evolved” faction of GTM, and are the methods used for this study. GTM can apply to both qualitative and quantitative research data (Charmaz, 1995). GTM emphasizes theory development and allows researchers to aim at various levels of theory when conducting research (Denzin & Lincoln, 1994). The use of GTM allows the researcher to discover concepts that are grounded in collected data, as well as determining their underlying sources (Corbin & Strauss, 1990). Glaser and Strauss (1967) argued that GTM could be used to develop new theory by focusing on the differences between daily realities of behaviors and how those behaviors are interpreted by those who engage in those behaviors (Suddaby, 2006). When used correctly, GTM can produce high-level theories that are generalizable and useful (Urquhart & Fernández, 2013). Because there is little understanding of the degree of financial risk posed to an organization by way of executives’ use of SNS, the use of GTM provided an avenue to determine the answer to the research question for this study.

Research methods employed

This study of financial risks associated with executive use of SNS was qualitative. Data collection focused on the specific behaviors that executives can engage in via SNS usage, which could result in financial risks to an organization.

This study advanced current research by gaining a deeper understanding of how executives' behaviors on SNS impact financial risks to the organization. This deeper understanding came about as a result of collecting examples of executive behaviors from information security professionals, which they believe could pose a financial risk to the organization. The researcher conducted semi-structured interviews using open-ended questions to collect data about these behaviors. This study collected the perceptions of the respondents interviewed to answer the research question and to help build an emergent theoretical model to assist organizations in dealing with financial risks associated with executives' use of SNS.

A qualitative research approach was justified for this study, in part to help inform the emergent theoretical model for the study. Additionally, a qualitative research approach was needed to collect data about executive SNS behaviors that may pose a financial risk to the organization. The researcher used semi-structured interviews to collect the qualitative data needed for this study. Interviews do come with associated risks: artificiality of the interview, lack of trust; lack of time; level of entry; elite bias; Hawthorne effects, constructing knowledge, ambiguity of language, and interview abandonment by the interviewee (Myers & Newman, 2007).

Instrument development and validation

Boudreau, Gefen, and Straub (2001) observed, IS researchers should seek to ensure research is rigorous, by validating the instruments used to collect data. Venkatesh, Brown, and Bala (2013) noted that researchers should discuss the validity of design, analysis, and findings within the separate contexts of both qualitative and quantitative research. Straub, Boudreau, and Gefen (2004) offered a set of guidelines for ensuring research validity. According to Straub, et al. (2004), construct validity, internal consistency, inter-rater reliability, and statistical conclusion validity are mandatory.

The researcher used a list of open-ended interview questions for this study. The interview guide was first tested with two subject matter experts to assess the types of questions, validity, and reliability of the data, which resulted in minimal changes to the interview guide prior to use.

Descriptive demographic data about study respondents was collected prior to the interview by use of a Qualtrics survey instrument. Collected data included age range, education level, ethnicity, gender, household income, industry currently employed in, and details regarding their career to ensure they met population requirements for this study prior to being interviewed.

Population and sample

Creswell and Creswell (2018) identified the key aspects of population and sampling to describe a research plan adequately. Those aspects are described below and were applied to this study.

Population description

The population for this study consisted of individuals who identify as information security professionals currently working in-field or did so within the last 24 months. Additionally, the population had sufficient work experience in the information security field, such that it allowed them to speak from a place of authority as it related to executive SNS behaviors they have either witnessed directly or have heard related examples of executive SNS behaviors from others that they found to be credible. In order to meet this criterion, the population had a minimum of five years of information security-related work experience.

Sampling techniques

Single-stage sample design is appropriate when the researcher has access to the population and can sample them directly (Creswell & Creswell, 2018). Because of the researcher's direct and indirect access to the population, a single-stage sample design was the appropriate choice for this study. Creswell and Creswell (2018) described three types of sampling: random, systemic, and nonprobability. As Creswell and Creswell (2018) noted, obtaining a random sample may be difficult, if not impossible, to obtain. The ability to generate a systemic sample will also prove to be problematic, as well. Accordingly, the researcher used a nonprobability sample technique to select respondents for this study. While nonprobability sampling is not the optimal choice, Creswell and Creswell (2018) noted that it is a frequently used method to choose respondents. Sample size determination needed to be taken into account as well. As Creswell and Creswell (2018) observed, sample size determination is a tradeoff between more accuracy, time, and cost.

Qualitative research uses the concept of saturation to help determine sample size (Mason, 2010). Charmaz (2006) observed that reaching saturation can be a function of the aims of a study, thus making the sample size difficult to determine. Brinkmann and Kvale (2015) suggested that general interview studies need between 5 and 25 interviews. While the researcher anticipated data saturation at 15 respondents, data saturation occurred after the ninth respondent at which time the researcher discontinued interviews.

Data collection

Data collection initiated with the identification of subject matter experts in the field of information security. The researcher identified a total of 21 individuals as potential study respondents. Next, the researcher asked these individuals to participate in this study, with all of them agreeing to do so. Once the individuals agreed to participate, they were sent a link to a Qualtrics survey instrument used to collect demographic data. The researcher scheduled interviews after verifying the respondent submitted demographic data. The anticipated time for interviews was 30-45 minutes, with actual times ranging from 25-55 minutes. The researcher conducted interviews between February 2019 and March of 2020. The researcher conducted one interview in-person and the rest via WebEx online meeting software. Interviews were conducted only after obtaining informed consent from the respondent and were recorded with the respondent's permission. Interviews and initial coding were conducted in the same period, to minimize the amount of time needed to collect data and begin the initial coding process. When needed, follow-up questions were sent to respondents via email to gain further insight into topics.

Respondents ranged in age from mid-20s to mid-50s. All respondents had some level of college education, with most of them completing either a bachelor's or master's degree. The respondents were mostly male, and all had at least five years of information security work experience. Over half of the respondents reported having more than ten years of industry experience.

At the conclusion of each interview, the researcher reviewed the resulting audio file to ensure successful recording. Next, the researcher sent the audio file to a paid transcription service, which returned a transcript within one day. The researcher reviewed the transcripts for accuracy and allowed the respondent to do the same. After verification, the researcher imported the transcript into ATLAS.ti, a qualitative data analysis application. The use of ATLAS.ti allowed the researcher to code interviews, sort, and explore the data in order to discover themes, categories, and relationships.

The researcher interviewed a total of nine respondents. The first interview was a pilot in order to ensure the interview script would meet study objectives. The researcher sent the first transcript to an experienced academic researcher for validation that the research question was being addressed.

Data analysis

Data analysis should follow generally acceptable standards (Pratt, 2009; Romano Jr., Donovan, Chen, & Nunamaker Jr., 2003; Venkatesh, et al., 2013). Qualitative data is so rich that researchers should aggregate it into somewhere between five and seven distinct themes (Creswell & Creswell, 2018). Researchers should use qualitative software in order to ease the burden of data analysis (Bringer, Johnston, & Brackenridge, 2006; Creswell & Creswell, 2018; Peters & Wester, 2007; Romano Jr., et al., 2003). The use of qualitative software is especially appropriate when using GTM (Bringer, et al., 2006). Creswell and Creswell (2018) outline a five-step process to analyze qualitative data, which includes: organizing and preparing data for analysis; read or look at the data; data coding; generating a description and themes; representing the description and themes.

Interviews were electronically recorded and sent out for professional transcription in order to add validity to the process. Additionally, the researcher addressed trustworthiness and authenticity concerns by sending transcripts to the respondents to ensure the accuracy of the data before analysis. The researcher then imported transcripts into ATLAS.ti, a qualitative data analysis application.

Coding was done in three phases, as described by Charmaz (2006): initial coding, focused coding, and theoretical coding. Charmaz (2006) acknowledged the concept of axial coding, which exists in the Strauss and Corbin version of GTM but described it as optional. Coding is a non-linear process in GTM, and researchers should feel free to move between coding methods as needed (Thornberg & Charmaz, 2012). Coding allows researchers to begin understanding what is happening in the data and to understand what it means (Charmaz, 2006).

Initial coding is the process by which researchers begin to apply labels to data in order to allow further exploration. Initial coding allows researchers to gradually analyze and interpret respondents' concerns regarding the problem being explored (Thornberg & Charmaz, 2012). Focused coding is the process of taking codes generated in the initial coding process and using them to sift through large amounts of data (Charmaz, 1995). Theoretical coding allows researchers to highlight possible relationships between codes developed during the focused coding phase, and to help tell a story in a theoretical direction (Charmaz, 2006).

The researcher initially coded all interviews. Those initial codes revealed basic concepts that the researcher then compiled and reviewed to address redundancy and overlap. To address validity and reliability concerns, the researcher had a subject matter expert also engage in initial coding of all interviews, using a codebook developed by the researcher during his initial coding process. As McDonald, Schoenebeck, and Forte (2019) observed, agreement between coders is an important part of qualitative research. Agreement on codes by multiple people indicates consistency in the measurements (McDonald, et al., 2019). When disagreement amongst coders exists, there are multiple methods available to resolve the disagreement (MacPhail, Khoza, Abler, & Ranganathan, 2015; McDonald, et al., 2019; Wiesche, Jurisch, Yetton, & Krcmar, 2017). For this study, the researcher chose the meet/discuss/resolve approach as described in both McDonald, et al. (2019) and Wiesche, et al. (2017).

According to Creswell and Creswell (2018), researchers can measure intercoder agreement by using any reliability process checking present in qualitative data analysis applications. Process checking was available in the ATLAS.ti software used for this study, specifically Krippendorff's alpha. The use of Krippendorff's alpha is supported in studies where two coders are coding the same data, and the data are nominal (McDonald, et al., 2019). According to Krippendorff (2004), an alpha score of .800 or greater is needed to ensure minimal agreement amongst coders.

Once the initial coding of all interviews was completed, the researcher moved on to focused coding to develop themes that represented a common thread or idea. Finally, the researcher utilized theoretical coding to develop the overarching dimensions which were used to create the emergent theoretical model.

Resource requirements

Resources were needed to complete this study. Computing-based resources used included a computer, word processing software, citation management software, Internet connectivity, transcription services, video conferencing software, online survey tools, corresponding survey tool delivery mechanisms, and statistical analysis software. Human resources used included industry professionals in order to assist with instrument validation, as well a serving as respondents. Additionally, human resources were needed in the form of subject matter experts to assist with intercoder agreement of the results. The computing-based resources were owned by the researcher, or available to him at no charge because of his employment at a Georgia-based public university. The human resources were available as well, due to the numerous connections the researcher has to the metro Atlanta area information security community, as well as having a substantial global social media footprint via LinkedIn and Twitter.

Summary

This chapter provided an overview of the research methodology, which was used for this study. The research methodology for this study was discussed. Instrument development and validation for this study were also discussed. Population, sample size, and sampling techniques for this study were also discussed. Finally, the data analysis techniques used in this study were also discussed.

Chapter 4

Results

Introduction

This chapter discusses the results of data analysis and findings for this research study. The chapter explains the analysis method followed. Next, the chapter discusses the demographic analysis that was conducted. A discussion of the detailed results of the findings follows next. Finally, the chapter concludes with a summary of the results.

Data analysis

The researcher conducted data analysis on respondent interview data, respondent demographic data, and interview data coding. By using grounded theory methods (GTM), concepts and themes emerged from the data, which ultimately led to the discovery of overarching dimensions. The discovery of these overarching dimensions led to the creation of an emergent theoretical model to explain the results.

Data analysis began with the researcher commencing with the initial coding process, as described by Charmaz (2006). The researcher conducted initial data coding of each interview immediately after receiving the professionally transcribed recording and allowed the respondent to review it, thus addressing any concerns related to validity and reliability. This process allowed the researcher to analyze the data using GTM and code the interview data to discover relevant concepts, themes, and overarching dimensions. As a result, interviews and initial coding overlapped as the researcher both continued to engage in respondent interviews while also conducting initial data analysis. This overlap was necessary, as it allowed the researcher to discover relevant concepts more quickly, as well as to ascertain when data saturation occurred. Coding was done in three phases, as described by Charmaz (2006): initial coding, focused coding, and theoretical coding. Charmaz (2006) acknowledged the concept of axial coding, which exists in the Strauss and Corbin version of GTM but described it as optional.

The discovery of the overarching dimensions present in the data led to the development of an emergent theoretical model that may be used by future researchers and practitioners to assist with protecting organizations from financial risks associated with executives' use of their personal SNS channels.

Demographic analysis

Demographic data was collected prior to the interview by use of a Qualtrics survey tool. Prior to analysis, data accuracy was checked by ensuring that no respondent had left any portion of the survey blank. Once the data was verified, analysis commenced. Table 1 provides a breakdown of descriptive statistics for all respondents. Respondents' ages ranged from the mid-20s to early 60s. Eight of the respondents identified their gender as male, and one identified as female. Two respondents had some level of college education but did not complete a degree of any type. Three respondents had a bachelor's degree, and four respondents had a master's degree. Respondents reported working in various industries, including educational services, financial services, and information services.

This sample is reflective of the information security industry in terms of gender, ethnicity, educational level, and industry verticals. The sample for this study was 89% male and 11% female. These numbers are similar to the 80% male and 20% female gender breakdown reported by The United States Census Bureau (2020a) for information security analysts in 2017. The sample is also reflective of the information security industry in terms of race and ethnicity. The ethnicity breakdown for the sample was 78% White, 11% Asian, and 11% Black or African American. The United States Census Bureau (2020c) reported the 2017 race and ethnicity breakdown for information security analysts as 73.9% White, 9.52% Asian, and 12.5% Black. Next, the sample is reflective of the information security industry in terms of educational level. 77% of the sample reported having a bachelor's degree or higher. This is similar to The Occupational Information Network (2019) finding that 76% of information security analysts have a Bachelor's degree or higher. Finally, the sample is reflective of the information security industry in terms of the representation of industry verticals. The industry breakdown for the sample was 11% educational services, 11% financial services, 33% information-related services, and 44% professional, scientific or technical services. These numbers closely relate findings reported by The United States Census Bureau (2020b) of 10% educational services, 18% financial services, 33% information-related services, and 44% professional, scientific or technical services. The single noteworthy exception here is the difference in the information-related services field, but otherwise, the sample is reflective of the information security industry.

Table 1

Descriptive Statistics for the Population (N=9)

Characteristic	**N**	**Percentage (%)**
Age		
25-34	2	22%
35-44	3	33%
45-54	2	22%
55-64	2	22%
Gender		
Female	1	11%
Male	8	89%
Ethnicity		
White	7	78%
Asian	1	11%
Black or African American	1	11%
Education		
Some college, no degree	2	22%
Bachelor's degree	3	33%
Master's degree	4	44%
Industry		
Educational services	1	11%
Financial services	1	11%
Information	3	33%
Professional, scientific or technical services	4	44%
Industry experience		
5-6 years	2	22%
7-8 years	2	22%
Longer than 10 years	5	56%

Respondent interview data analysis

Using ATLAS.ti for data analysis, the researcher engaged in the process of initial coding on each interview immediately after being transcribed. As Charmaz (2006) noted, the use of initial coding allows the researcher to compile data into categories and discover the existence of any processes that are present in the data. While engaged in the initial coding process, the researcher also applied constant comparative methods, as described by Charmaz (2006). When using constant comparative methods, researchers begin to establish distinctions in the data, which allows the researcher to make comparisons at each coding level (Charmaz, 2006).

The researcher recruited a subject matter expert to engage in initial coding of all interviews in order to ensure the validity and reliability of the results. This process took place in batches of two interviews at a time, whereby the researcher engaged in initial coding of two interviews, which were then handed off to the subject matter expert for them to initially code. The researcher supplied the codebook for the subject matter expert use, which was generated from the researcher's initial codes. Having agreement between coders is an important component of any qualitative research effort (McDonald, et al., 2019; Wiesche, et al., 2017). This iterative process allowed for the resolution of any differences in coding, which is needed to ensure reliability in the results (MacPhail, et al., 2015).

When coding conflicts occurred, the researcher and the subject matter expert would meet via telephone, or remote messaging services like Microsoft Teams or Signal, to discuss the conflict and reach consensus. Coding conflicts occurred in three rounds of interview coding, resulting in the researcher and the subject matter expert meeting for a total of approximately 90 minutes across three separate meetings. In total, 169 codes were identified during the initial coding phase, and are shown in Appendix D. The resulting initial coding process identified the existence of basic concepts that respondents identified during their interviews.

Researchers can measure intercoder agreement by using reliability process checking tools that are present in qualitative data analysis applications (Creswell & Creswell, 2018). Such a reliability process checking tool was available in ATLAS.ti, namely Krippendorff's alpha. Krippendorff (2004) stated that an alpha score of .800 or greater is needed to ensure minimal agreement between coders. The Krippendorff's alpha score of .874 was calculated after the initial coding and conflict resolution process, thus confirming intercoder agreement in the initial coding process.

From there, the researcher moved on to focused coding of the data. Focused coding allows the researcher to begin data synthesis and understanding larger segments of data (Charmaz, 2006). The comparison of data against data is what allows for the creation of focused codes (Charmaz, 2006). The resulting output of focused codes allowed the researcher to identify themes that encompassed the concepts identified during the initial coding process.

Once focused coding was complete, the researcher began the process of theoretical coding analysis. Theoretical codes highlight possible relationships between the themes identified during the focused coding process (Charmaz, 2006). The resulting theoretical code analysis resulted in the discovery of overarching dimensions in the data, which became the elements of the emergent theoretical model.

Using GTM, the researcher presents the concepts, themes, and overarching dimensions that emerged from the data collection and analysis process, as shown in Figure 1.

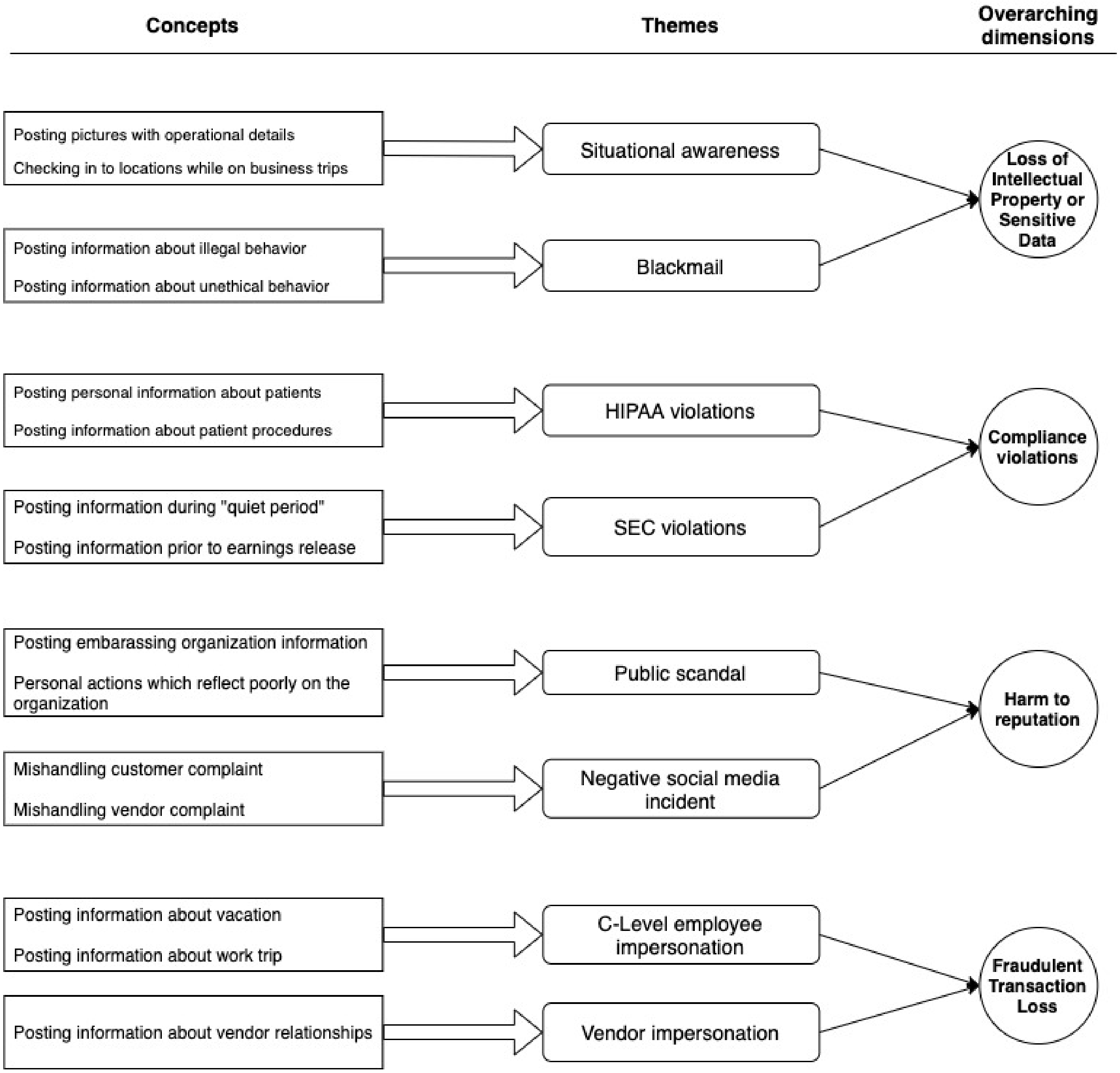

Concepts
Themes
Overarching dimensions
Posting pictures with operational details
Checking in to locations while on business trips
Situational awareness
Posting information about illegal behavior
Posting information about unethical behavior
Blackmail
Loss of Intellectual Property or Sensitive Data
Posting personal information about patients
Posting information about patient procedures
HIPAA violations
Posting information during "quiet period"
Posting information prior to earnings release
SEC violations
Compliance violations
Posting embarassing organization information
Personal actions which reflect poorly on the organization
Public scandal
Mishandling customer complaint
Mishandling vendor complaint
Negative social media incident
Harm to reputation
Posting information about vacation
Posting information about work trip
C-Level employee impersonation
Posting information about vendor relationships
Vendor impersonation
Fraudulent Transaction Loss

Figure 1. Emergent concepts, themes, and overarching dimensions

Findings

Loss of Intellectual Property or Sensitive Data

The researcher found that loss of intellectual property or sensitive data included situational awareness and blackmail. These themes and representative data are presented in Appendix E.

Situational Awareness

Situational awareness is defined in the seminal Endsley (1995) article as "…the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (p. 36). Organizations are right to be worried about the risk associated with employees disclosing confidential information (Fuduric & Mandelli, 2014). Working from the Endsley (1995) definition, executives need to be aware of the possibility of financial risk to the organization, which can result from the sharing of data (text or images) via their personal SNS. As respondent #4 observed:

> "We talk about we want to share pictures and share how great and wonderful it is to work there, but we also want to be very aware of the surroundings when we take pictures, of what we post that someone might be able to see pseudocode in the background, or those types of things…"

As a result of these types of behaviors, organizations face a financial risk due to the exposure of intellectual property or sensitive data.

Blackmail

(Merriam-Webster, n.d.) defines blackmail as "extortion or coercion by threats especially of public exposure or criminal prosecution." Respondents emphasized the financial risk that organizations face as a result of their executives being blackmailed as a result of something they posted on their personal SNS. Respondent #3 offered this observation regarding the financial risk to the organization associated with executive blackmail scenarios:

> “The business is higher profile, more prone to any sort of blackmail, ransom, anything like that, and my belief is that they've got to be a little bit more careful about what they post, how it's posted, when it's posted, and things like that.”

Compliance violations

The researcher found that compliance violations included HIPAA and SEC concerns. These themes and representative data are presented in Appendix E.

HIPAA violations

U.S. lawmakers created The Health Insurance Portability and Accountability Act of 1996 (HIPAA) to protect the privacy and security of certain types of health information (U.S. Department of Health and Human Services, n.d.). The act empowers the U.S. Department of Health and Human Services Office of Civil Rights (OCR) to enforce the act by conducting complaint investigations as well as conducting compliance reviews (U.S. Department of Health and Human Services, n.d.). Organizations that violate HIPAA face potentially substantial fines (Green, 2007; Parks, Xu, Chu, & Lowry, 2017; Solove, 2013). Organizations can face financial risk from executives sharing information on their personal SNS, which violates HIPAA. As respondent #10 described, an executive can share patient information in the act of attempting to show organizational competence, thus creating a HIPAA violation:

> “Imagine an executive tweets something to the tune of ‘we're so good at what we do, Beyonce chose our hospital for her healthcare.’ Unless this was very clearly approved by Beyonce, this is a HIPAA violation at minimum.”

SEC violations

The Securities and Exchange Commission (SEC) is the federal agency charged with overseeing publicly traded organizations and can initiate civil action against lawbreakers, or can also work with the Justice Department to initiate criminal actions (U.S. Securities and Exchange Commission, n.d.). Organizations can face financial risk from executives sharing information that violates securities law.

As respondent #10 described:

> ‘[For publicly traded organizations] there’s a lot of rules around what you can say that is material to the business and how that is disseminated, so they've got to be very careful. I think that, that from a financial risk perspective, that could cause fines and loss of business, and potential, other legal lawsuit issues if they aren't careful about what and how they say things that are material to the business.’

Harm to reputation

The researcher found that harm to reputation included public scandal and negative social media incidents. These themes and representative data are presented in Appendix E.

Public scandal

Public scandal can cause financial risk to an organization (Drew, Kelley, & Kendrick, 2006). An executive can cause a public scandal when they share information on their personal SNS, which draws negative attention to the executive, and by extension, the organization. As respondent #5 offered:

> “We've seen it go well, and we've seen it go horrifically wrong. The guy who shot the rhino, right? The founder of Jimmy John's posed with big game, and it went on his Facebook, and it went viral, and the company damn near went bankrupt because people were, you know, like, ‘The guy's a horrible human being.’”

Respondent #1 offered this observation about executives having to balance the desire to share information against the potential financial risk it can bring to the organization:

> “I think you can do whatever you want to do; you just have to be careful and set some boundaries with how you're going to use that media to influence, right? So you don't want your personal life too much influencing the business life so-to-speak, if that makes any sense”

<u>Negative social media incident</u>

Negative social media incidents can occur when an organization executive engages with a customer, employee, vendor, or the public at large via their personal SNS. The organization faces financial risk from these types of interactions, even when the incident occurs on an executive’s personal SNS.

Respondent #5 described this situation, in which an executive participated in a negative social media incident with someone:

> “’Well, that must mean clearly, we think that's what the company says.’ I'm like, ‘Wait a second. Time out. This is on my own time.’ And they're like, ‘Yeah, but

> you don't get to do that.' And so that was a harsh realization, I think, for me is that there is no off time."

In another example of a negative social media incident, respondent #8 described a situation where an organization executive shared a negative experience involving an organization customer while on vacation:

> "Person went on vacation talked about the bad experiences they had at this resort. Turns out, that that resort was one of their biggest clients and that resulted in some interesting conversations".

Fraudulent Transaction Loss

The researcher found that fraudulent transaction loss included C-level employee impersonation and vendor impersonation. These themes and representative data are presented in Appendix E.

C-Level executive impersonation

BEC attacks were responsible for losses of more than $1.7 billion in 2019 (Federal Bureau of Investigation, 2020). Executives potentially expose their organizations to this type of attack when they share information via their personal SNS. In this situation, the ability of a cybercriminal to impersonate a C-Level executive is essential, as they rely on the natural pressures a subordinate would feel to keep the executive happy or the fear of losing their job if they do not carry out the instructions of the C-Level executive. As respondent #10 described:

“…if they know a senior executive is going to be, perhaps, out of comms for a weekend, maybe that's a good time to start spoofing them, because they know that the real person can’t be reached…”

When an organization executive shares details about their travel plans via their personal SNS, that information can be used by a cybercriminal to make their attack feel more authentic. As respondent #8 described:

> “For example if a chief marketing officer just posted ‘hey, I'm going to be in Bahamas next week,’ I know the location. Now, I know that that person is out of office and I can use that information for let's say, social engineering…”

Vendor impersonation

Another form of BEC occurs when a cybercriminal impersonates a vendor to entice an accounts payable employee to pay a fraudulent invoice being presented. One possible scenario was described by respondent #1:

> “Let's say the CFO's on vacation. The secretary or the office manager for the finance department has some bills to pay. Suddenly somebody calls up and, ‘Hey. This is an urgent bill. If you don't pay this bill today, by X time, we're going to turn the lights out, or we're going to turn your internet connection off.’ Whatever that scenario is, and she can't get in touch or he can't get in touch with the CFO, suddenly now you've got people pressured to make a decision for the benefit of the company without the oversight, and they were able to be socially engineered because somebody got that information off of a public social media site…”

Summary of Results

The results of the data analysis conducted for this study generated an emergent theoretical model that is grounded in the evidence found in the data. The emergent theoretical model (Figure 2) indicates the overarching dimensions that present financial risks to organizations from executives' use of their personal SNS.

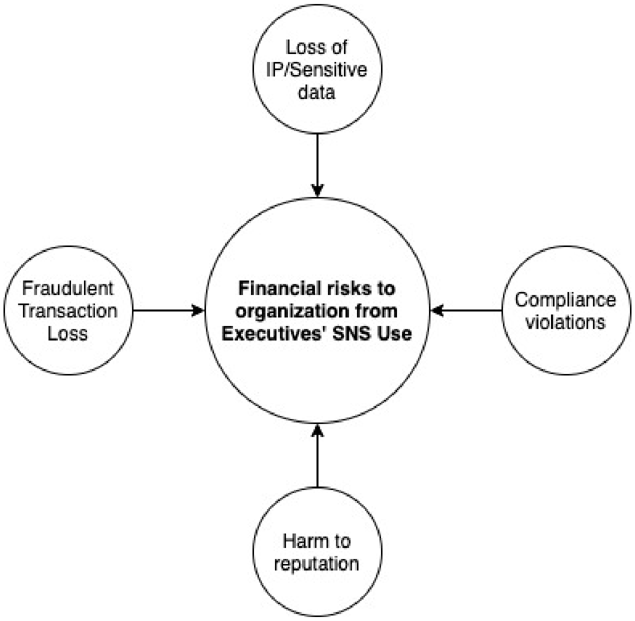

Loss of IP/Sensitive data
Fraudulent Transaction Loss
Financial risks to organization from Executives' SNS Use
Compliance violations
Harm to reputation

Figure 2. Emergent theoretical model

Loss of Intellectual Property or Sensitive Data

The analysis of information provided by respondents resulted in the discovery of this overarching dimension and is grounded in the discovery of two themes: Situational awareness and Blackmail. The discovery of these themes is grounded in the information provided by respondents during their interviews. Respondents offered multiple observations of incidents in which organizations were faced with situations where their intellectual property or other sensitive data was exposed through information shared by executives' personal SNS, this creating a financial risk to the organization. Additionally, respondents were able to offer scenarios in which executives could expose intellectual property or sensitive data via their personal SNS, and thus expose their organization to financial risk as a result.

Compliance violations

The analysis of information provided by respondents resulted in the discovery of this overarching dimension and is grounded in the discovery of two themes: HIPAA violations and SEC violations. The discovery of these themes is grounded in the information provided by respondents during their interviews. Respondents offered multiple instances of executives engaging in behavior on their personal SNS that resulted in SEC investigations, thus exposing their organizations to financial risk. Additionally, respondents were able to offer various scenarios where things executives share via their personal SNS could result in either HIPAA or SEC violations, thus exposing their organizations to financial risk.

Harm to reputation

The analysis of information provided by respondents resulted in the discovery of this overarching dimension and is grounded in the discovery of two themes: Public scandal and Negative social media incident. The discovery of these themes is grounded in the information provided by respondents during their interviews. Respondents offered multiple instances of executives sharing information via their personal SNS, which resulted in either a public scandal for the organization or a negative social media incident, which resulted in financial risk to the organization. Additionally, respondents were able to envision multiple scenarios in which something an executive shared via their personal

SNS could result in either a public scandal or negative social media event, which could potentially result in financial risk to the organization.

Fraudulent Transaction Loss

The analysis of information provided by respondents resulted in the discovery of this overarching dimension and is grounded in the discovery of two themes: C-Level employee impersonation or Vendor impersonation. The discovery of these themes is grounded in the information provided by respondents during their interviews. Respondents were able to offer multiple instances of executives sharing information via their personal SNS, which resulted in adversaries being able to impersonate a C-Level executive, resulting in a successful BEC attack, thus exposing the organization to financial risk. Respondents were also able to provide multiple instances where information shared by an executive via their personal SNS allowed a cybercriminal to impersonate a vendor that did or potentially did business with the organization. These impersonations resulted in a successful BEC attack, which also exposed the organization to financial risk. Furthermore, respondents were able to offer multiple scenarios wherein information shared by an executive on their personal SNS could lead to successful BEC attacks, thus potentially exposing the organization to financial risk.

Summary

This chapter provided a detailed overview of the methodological framework, data coding, analysis, and interpretation used in this study. Four overarching dimensions were identified through data analysis: *Loss of Intellectual Property or Sensitive Data; Compliance violations; Harm to reputation;* and *Fraudulent Transaction Loss.* The respondents' quotes that were related to their statements in each of the four overarching dimensions were also presented. Next, this chapter discussed the findings of the study, showing how respondent data were grouped into themes, which ultimately led to the discovery of the overarching dimensions for this study. Finally, this chapter presented the four overarching dimensions in an emergent theoretical model that answered the research question for this study.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Introduction

This chapter presents the conclusions reached in this study. The research question will be outlined and answered, and implications for the study will be discussed. Finally, this chapter concludes with recommendations for future study.

Conclusions

The goal of this study was to explore what financial risks organizations face from executives' use of their personal SNS. This study addressed the research question proposed in this study: What executive personal SNS behaviors pose financial risks to an organization? In this study, the researcher interviewed nine information security professionals to uncover their perceptions and experiences in order to provide answers to the research question.

The study met its overall goal of answering the research question and generating an emergent theoretical model. This study utilized a grounded theory approach to collect qualitative data by interviewing nine information security professionals regarding their personal experiences, beliefs, and perceptions of financial risks that organizations face from executives' use of their personal SNS. The data analysis conducted for this study resulted in the discovery of overarching dimensions, themes, and concepts that addressed the research question for this study. The results of this study revealed four overarching dimensions of executives' behavior on their personal SNS that pose financial risks to organizations: Loss of Intellectual Property or Sensitive Data; Compliance Violations;

Harm to Reputation; and Fraudulent Transaction Loss. Furthermore, these overarching dimensions were grounded in underlying themes. A summary of these dimensions and themes are presented in Table 2.

Table 2

Summary of Overarching Dimensions and Themes

Overarching Dimensions	**Themes**
Loss of Intellectual Property or Sensitive Data	
	Situational Awareness
	Blackmail
Compliance Violations	
	HIPAA violations
	SEC violations
Harm to Reputation	
	Public Scandal
	Negative Social Media incident
Fraudulent Transaction Loss	
	C-level Employee impersonation
	Vendor impersonation

The discovery of these items led to the creation of an emergent theoretical model that explains the financial risks that organizations face from executives' use of their personal SNS and thus addressed the research question for this study.

This study has strengths. One strength is the researcher's years of industry experience. This experience allowed the researcher to understand industry jargon used by the respondents in the interview process and allowed the researcher to easily grasp the significance of respondents' statements about how a particular given example was important in answering the study's research question. Another strength of this study is the use of grounded theory to explore the study's research question. The researcher's use of grounded theory allowed him to collect ground truth from industry experts without relying on a theoretical lens through which to view the data, and thus avoid bias. The grounding of concepts found in the reality of the data collected is key to the use of grounded theory, as it helps the researcher guard against internal bias (Corbin & Strauss, 1990). Yet another strength is the diversity of the industry verticals reflected in the demographic, and how closely their percentages mirror the data reported by The United States Census Bureau (2020b). The generalizability of this study's findings is increased as a result of this diversity and percentage of individual industry representation.

This study has weaknesses. The previously mentioned researcher's industry experience could be considered a weakness as it opened the possibility of researcher bias due to prior firsthand experiences. To counter the potential bias, the researcher made every attempt to discard previously held assumptions and engage in active listening to respondents' answers with an open mind. Another weakness is the potential for elite bias to influence the data collection process. The researcher countered the potential bias by interviewing respondents of varying statuses to capture a broader understanding of the phenomenon being studied. Another weakness is not testing the emergent theoretical model created in this study. While a weakness, the lack of testing of the emergent theoretical model is also an avenue for future research.

Lastly, this study has limitations. One limitation was the access to information security professionals who would commit to sitting for an interview due to time constraints or general availability issues. Another limitation was the researcher's available time to conduct interviews and subsequent data analysis. Yet another limitation relates to the generalizability of the results. The respondents were all located in the same geographical area of one major city in the southeast United States. As a result, the results found in this study may not apply to other geographical regions in the United States or foreign countries. Another limitation of the study relates to some of the data collected for the Compliance violations overarching dimension. While the industries represented in the study are varied, all respondents pointed to two types of compliance violations in their interviews – HIPAA and SEC. As a result, the associated themes are inferences based on interview data. While regulatory violations apply to all market verticals, some verticals are more directly impacted by these particular regulations than others.

Implications

No known published qualitative research exists that presents findings of the financial risks organizations face from executives' use of their personal SNS. These behaviors create financial risk for organizations because of the information executives sometimes share, which cybercriminals then leverage for use in attacks (Palmer, 2020; Social-Engineer LLC, 2019). Cybercriminals attacking organizations is not a new or novel idea. What is novel, and thus worthy of study, is understanding the financial risks organizations may face as a result of information executives share in their personal SNS.

This study has implications for the information security personnel tasked with protecting their organization from threats, as this newly discovered threat vector may require a change in operational procedures. This study also has implications for organization risk management personnel who may not have been aware of the threats which come from their executives' use of their personal SNS and thus have not factored this newly discovered threat vector into their overall risk management process. Finally, this study also has implications for organization policy, human resources, and legal personnel who may not have been aware of the threat from this newly discovered vector and may now have to craft new management policies or employment contracts.

Recommendations

This study was a grounded theory research effort designed to discover financial risks that organizations may face from executives' use of their personal SNS. Future research is needed to test the emergent theoretical model put forth in this study. Future research should also be done to confirm the overarching dimensions and themes discovered in this study, possibly using a different research method such as Delphi panel or quantitative survey instrument. Future research should also explore the possibility of cues being present that could help organizations minimize the financial risks they face when executives use their personal SNS. Once such research possibility is a retrospective inspection of the information executives share, in order to develop guidelines for executives regarding what they share via their personal SNS. Another such research possibility is to explore proactive steps executives can use to minimize financial risks to their organization when they do share information via their personal SNS. For example, exploring personal circumstances such as the use of a personal device for work and personal matters, device exposure when personal, intimate relationships end, or children's use of the executive's personal or corporate computing assets are all areas that warrant future research.

Recommendations for information security, legal, and human resources practitioners include using the overarching dimensions and themes discovered in this study to conduct a risk assessment to determine the extent to which their organization may be at risk. If supported by risk assessment findings, organization information security personnel should explore processes to monitor their executives' personal SNS channels. If also supported by risk assessment findings, organizations human resources and legal personnel should explore the creation of new organization policies that specifically target executives' use of their personal SNS. Such policies may seek to create boundaries around what executives can share or may even seek to prohibit such behavior. Next, human resources and legal practitioners may seek to prohibit executives' use of personal SNS as a term of employment by including appropriate language in employment contracts. Finally, information security practitioners, in collaboration with human resources and legal practitioners, may seek to create a security education, training, and awareness (SETA) program that specifically targets executives and their use of personal SNS, to educate and raise overall awareness for this special group of employees with a specific threat vector.

Summary

This study addressed the research question: what executive personal SNS behaviors pose financial risks to an organization. The study was relevant due to the lack of extant literature on the research question being asked. The study explored the research question through the use of GTM. The researcher chose GTM because the nature of the research question being asked required the collection of ground truth based on the observations and experiences of qualified information security professionals.

The researcher developed a semi-structured interview question guide to answer the research question. The questions were open-ended and designed to elicit thick, rich data for analysis. The researcher developed the question guide and then had two subject matter experts vet it in order to assess the questions and to ensure the validity and reliability of the data to be collected. The researcher collected demographic data from respondents before conducting interviews. The researcher interviewed all respondents either in-person or via meeting-at-distance software and recorded all interviews after obtaining permission.

Before commencing full data collection, the researcher conducted a pilot interview with a respondent to ensure the question guide would ensure the collection of the data needed to meet study objectives. The researcher conducted initial coding of the interview, then had the coding and interview data reviewed for validity by an experienced academic researcher. After receiving positive feedback on the initial coding and interview data collected, the researcher commenced with full data collection.

Respondents responded to the questions asked, with the researcher having the flexibility to ask probing or follow-up questions as needed throughout the interview. Once the researcher concluded the interview, the audio recording was sent out for transcription. The researcher allowed each respondent to review the transcribed file to ensure validity and authenticity. The researcher commenced with the initial coding of the interview immediately afterward. The researcher engaged a subject matter expert to code each interview as well. The researcher provided the interviews to the subject matter expert in groups of two, and also provided a codebook developed by the reviewer during his initial coding process, to use in their coding process. Coding conflicts occurred in three rounds of interview coding, which resulted in the researcher and the subject matter expert meeting three separate times for a total of approximately 90 minutes, in order to reach a consensus on all conflicts. Once the initial coding process was completed, the researcher calculated a Krippendorff's alpha to ensure intercoder agreement. The Krippendorff's alpha score was .874, thus confirming intercoder agreement in the initial coding process. The initial coding process allowed the researcher to identify basic concepts present in the data, and the initial codes were the output needed for the next step in the coding process.

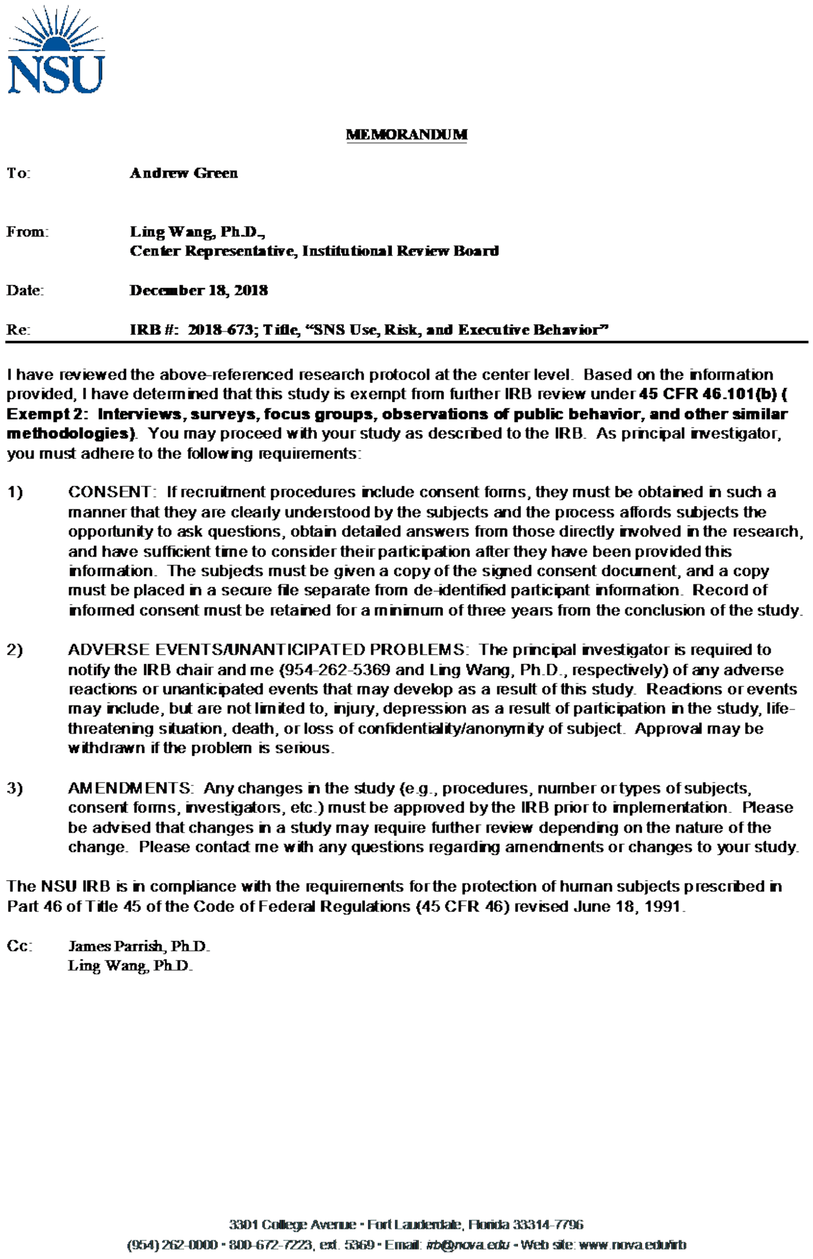
Next, the researcher commenced focused coding of the data, using the initial codes identified in the previous step. Focused coding allows the researcher to synthesize and understand larger chunks of data, as Charmaz (2006) explained. By comparing data against data, the researcher was able to create the focused code output that was needed for the next step in the coding process and allowed the researcher to identify themes that encompassed the concepts identified in the initial coding phase.

The final step in the coding process was theoretical coding. Theoretical coding highlights relationships between themes identified during the focused coding process (Charmaz, 2006). Theoretical coding relied on the output of focused codes from the previous step and resulted in the identification of the overarching dimensions in the data, which helped form the emergent theoretical model that addressed the study's research question.

Appendices

Appendix A

IRB approval



NSU

MEMORANDUM

To: **Andrew Green**

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

Date: **December 18, 2018**

Re: **IRB #: 2018-673; Title, "SNS Use, Risk, and Executive Behavior"**

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

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

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 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: James Parrish, 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

Interview Guide

Research Question - What executive social networking site (SNS) behaviors pose financial risks to an organization?

Introduction:

My name is Andy Green, and I am a Ph.D. candidate who is studying how executives' use of their personal social networking sites could pose financial risks to their organization, for my dissertation to finish my degree. I appreciate you taking the time to talk with me so that I can get your thoughts on the area I am researching.

Before we begin, I want to let you know that I will treat this interview confidentially. I will take the necessary steps to anonymize your responses so that they cannot be traced back to you. I will also be using a couple of voice recorders so that I can transcribe this interview for use in my analysis. One device is the primary, and the other is a backup in case some type of problem happens with the primary. After ensuring there was no recording problem with the primary, I will immediately delete the recording on the backup recorder.

If at any point I ask a question that you're not comfortable answering, just say so and I can skip it. Also, you have the right to end this interview at any time, for any reason, no explanation needed.

After we finish our interview, I will provide the recording to a professional transcription service so they can turn our interview into a text document I can use for my analysis.

I will encrypt both the interview recording and the associated transcription, so as to keep them from being accessed by unauthorized individuals. I will only decrypt them when I have to access them for work on my research.

Before we begin the interview and I start recording, do you have any questions for me?

Questions:

1. Let's start with you telling me a little bit about yourself? Your name, where you work, your job title, how long you've worked for your current organization, and how long you've worked in information security overall?

2. How would you describe your day-to-day workload and responsibilities?

3. What are your overall thoughts about social media in general?

4. Do you use social media yourself?

    a. Probe - Can you share any stories about your own social media experiences that were noteworthy for you in some way?

5. What are your overall thoughts about how employees use social media?

    a. Probe – Can you share any stories about situations you've seen or heard about, involving a co-worker's use of social media that was noteworthy to you in some way for them, or their organization?

6. What are your overall thoughts about organization executives who use social media in a personal capacity?

    a. Probe – Not just CEO "persona" – focus more on the entire C-suite, not just the "face" of the organization (CTO, CIO, CISO, CFO, CMO, etc.)

7. Do you think organization executives' use of social media in a personal capacity could pose a risk to their organization?

    a. Probe – Why or why not?
    b. Probe – How so?
    c. Probe – Financial risks?

8. Can you share any examples of situations where you thought that an executive's use of social media in a personal capacity may have exposed their organization to risk?

    a. Probe – How do you think that situation actually exposed the organization to financial risk?

9. Do you think that executive use of social media in a personal capacity is a risk to your organization?

    a. Probe – Why or why not?
    b. Probe - How so?

10. Are you concerned about organizational risks stemming from third party use of personal social media?

    a. Probe – Who are you worried about?
    b. Probe – Why do they concern you?

11. Are there ways for an organization to minimize any risk exposure it may face from one of its executives using social media?

    a. Probe - What might those be?

12. Are there any advantages to an organization which arise from an executive's use of social media in a personal capacity?

    a. Probe - What might those be?

13. Thinking about your industry; What are your thoughts on the effect of personal SNS usage by executives on their companies value?

14. If an executive were to come to you and ask, “What are some things I should or shouldn’t do on my social media accounts”, what guidance would you give them?

    a. Probe – Why?

15. Is there anything else you’d like to talk about that I haven’t asked?

16. Is there some question you think I should have asked, that I didn’t?

17. Would you mind if I contact you about this interview again, if I have follow-up questions?

Appendix C

Demographics Questions

Demographics questions

All questions are optional in nature.

1. What is your age in years?
    a. Under 21
    b. 22-24
    c. 25-34
    d. 35-44
    e. 45-54
    f. 55-64
    g. 65-74
    h. 75 or older
2. What is the highest degree or level of school you have completed? (If you're currently enrolled in school, please indicate the highest degree you have received.)
    a. Less than a high school diploma
    b. High school degree or equivalent (e.g. GED)
    c. Some college, no degree
    d. Associate degree (e.g. AA, AS)
    e. Bachelor's degree (e.g. BA, BS)
    f. Master's degree (e.g. MA, MS, MEd)
    g. Professional degree (e.g. MD, DDS, DVM)
    h. Doctorate (e.g. PhD, EdD)
3. Are you of Hispanic, Latino, or of Spanish origin?
    a. Yes - Hispanic
    b. Yes - Latino
    c. Yes - Spanish
    d. No
4. How would you describe yourself (select all that apply)?
    a. White
    b. Black or African American
    c. American Indian or Alaska Native
    d. Asian
    e. Native Hawaiian or Pacific Islander
    f. Other (Text box)
5. What is your gender?
    a. Female
    b. Male
    c. Non-binary/third gender
    d. Prefer to self-describe (Text box)
6. What is your total household income?
    a. Less than $60,000

b. $60,000 to $69,999
c. $70,000 to $79,999
d. $80,000 to $89,999
e. $90,000 to $99,999
f. $100,000 to $109,999
g. $110,000 to $119,999
h. $120,000 to $129,999
i. $130,000 to $139,999
j. $140,000 to $149,999
k. $150,000 or greater

7. Which of the following industries most closely matches the one in which you are employed?
   a. Forestry, fishing, hunting or agriculture support
   b. Real estate or rental and leasing
   c. Mining
   d. Professional, scientific or technical services
   e. Utilities
   f. Management of companies or enterprises
   g. Construction
   h. Admin, support, waste management or remediation services
   i. Manufacturing
   j. Educational services
   k. Wholesale trade
   l. Health care or social assistance
   m. Retail trade
   n. Arts, entertainment or recreation
   o. Transportation or warehousing
   p. Accommodation or food services
   q. Information
   r. Other services (except public administration)
   s. Finance or insurance
   t. Unclassified establishments
8. Are you currently employed in an information security or cyber security related position?
   a. Yes
   b. No
9. How long have you worked in the information security or cyber security field?
   a. Less than 1 year
   b. 1-2 years
   c. 3-4 years
   d. 5-6 years
   e. 7-8 years
   f. 9-10 years

g. Longer than 10 years

10. How long have you worked at your current employer?

a. Less than 1 year
b. 1-2 years
c. 3-4 years
d. 5-6 years
e. 7-8 years
f. 9-10 years
g. Longer than 10 years

11. How long have you worked in your current position?

a. Less than 1 year
b. 1-2 years
c. 3-4 years
d. 5-6 years
e. 7-8 years
f. 9-10 years
g. Longer than 10 years

12. What is your current job title? (Text box)

13. Which of the following best describes your current job level?

a. Owner/Executive/C-Level
b. Senior management
c. Middle management
d. Intermediate
e. Entry-level
f. Other (please describe) (Text box)

14. About how many employees work for your current organization

a. 99 or fewer
b. 100-499
c. 500-999
d. 1000-4,999
e. 5,000+

15. About how much revenue does your current organization generate each year?

a. Less than $1M
b. $1M-$9M
c. $10M-$49M
d. $50M-$99M
e. $100M-$249M
f. $250M-$499M
g. $500M-$999M
h. $1B-$9B
i. $10B+

Appendix D

List of Initial Codes

"persona" social media account content vetted ahead of time	keep followers on personal social media to a small number	Prior job title	social media positive value to user
avoid personal life social media posts impacting business	keep work life off social media	private group conversations can damage future employment chances	social media sharing can provide details about organization employees
balance employee free speech rights against risk	kidnap attack scenario	private group conversations can damage the organization	Social media training for employees
be careful when posting pictures taken in the workplace	lack of employee SETA	provide social media usage training to all employees	social media use can be a bad habit
BEC attack scenario	lack of executive social media use had no impact on brand growth	provide social media usage training to senior executives	social media use causes risk to a business client
block social media access at work	lack of organizational ethics	public social media comments can impact future employment opportunities	social media use depends on employee rank in organization
block social media access on corporate assets	lack of social media policies	Rank and file employees may be more successful at maintaining "personal" vs. "work" social media accounts	social media use has become second nature
broad targeting of organizations	leadership team creates value in the marketplace	Reason for leaving prior job	social media used as a temporary distraction
company Facebook page run by marketing staff	little benefit from executive use of personal social media	receiving positive feedback via personal social media	social media used for intelligence gathering
conduct a risk assessment for social media concerns	Location data used as OSINT	restrict employee social media use through contract	social media used for personal branding

create more restrictive social media policies for senior executives	loss of company devices could lead to negative social media postings	resume details leak details about an organization	social media used to acquire personal knowledge
Current job description	loss of employment over personal social media posts	risk from compromised social media account	social media used to build a personal following
Current job title	monitor senior executive accounts for policy violations	Risk tied to market sector	social media used to build corporate reputation
Data classification	network attack scenario	risk to competitive advantage	Social media used to connect with others
develop incident response plan for social media incidents	No separation between personal and professional persona on social media	risk to intellectual property	Social media used to educate friends
different social media platforms used for different objectives	only negative consequences from executive use of personal social media	sales people using social media inappropriately to make sales connections	social media used to for information gathering
differing risk profiles	organization can get sued for senior executives personal social media comments	seeing co-workers engage in negative interactions on social media	social media used to maintain personal relationships
difficult to calculate value of executive social media use	organization culture towards social media	Senior executive awareness of content shared via social media	social media used to maintain professional relationships
discloses upcoming new product release on social media	organization employee listing available on linkedin	Senior executive awareness of timing of shared content on social media	social media used to monitor college student behavior
Driven by different motivations	organization size factor in employee sharing of company information on social media	Senior executive belief that policies don't apply to them	social media used to sell corporate products

Employee fear of reprisal from leadership	organization use of social media for publicity purposes	senior executive creates personal risk by announcing personal plans ahead of time	social media used to stay updated on current events
employee feels pressured to make decision during social engineering attack	organization use of social media to boost employee morale	Senior executive making inappropriate comments on social media	social media users engage in negative interactions
employee leaking credentials	organization uses social media for publicy announcements	senior executive personal trip details used for social engineering attack against the organization	social media users post without thinking
employee leaking credentials via twitter	organizations have to balance employee private time against company risk	Senior executive should avoid discussing business on personal social media channels	spouse usage of social media
Employee rank in organization	organizations need social media sharing policies	Senior executive social media usage negatively impacts stock price	time spent with on social media with no organizational benefit
employees bypassing technical controls	Organizations use internal social media to keep employee conversations internal	Senior executive successfully avoid negative social media interactions	time spent with on social media with no personal value
employees inappropriately sharing company details	organizations use social media for branding themselves as experts in field	Senior executive usage negatively impacts organization value	use controls to stop others from posting on your Facebook page
employees leaking credentials via facebook	organizations use social media for corporate branding	senior executive use personal social media to promote brand	use employee social media conversations for social engineering attacks

employees posting normal events can positively impact organization financial standing	organizations use social media for relationship building with customers	senior executive use personal social media to share knowledge	use employee social media details to break in to home
Employees should have "work" and "personal" social media accounts	oversharing personal details on social media	senior executives at high risk organization should avoid social media use	use multifactor authentication
Employees spread rumors about organization via social media	personal social media usage can impact relationships with business clients	senior executives attending public events will be publicized by other means	use risk assessment to drive policy creation
employees talk negatively about the organization	personal social media usage giving details about organization security tools used	senior executives avoid using social media for fear of job loss	use social media platform's privacy controls
employees tweeting network diagrams	personal social media used for mass dissemination of information to friends	senior executives create organizational risk by announcing personal trips ahead of time	user discretion in what to share online
Employees with marketing background will avoid social media posts that reflect negatively on the company	personal social media used for problem solving	senior executives fired for personal social media postings	users avoiding negative interactions
examples of personal social media usage causing business risk	personal social media used for resume sharing	Senior executives make a deliberate choice to not use social media	users pay more attention to their professional tweets than personal tweets
executive should consider adversarial usage of their tweets	personal social media used to attract potential customers	senior executives need to think about negative impact of information shared on social media	uses senior executive personal details to time an attack

executive social media use can positively impact company value	personal social media used to connect with others	senior executives set boundaries for types of information to be shared on their social media accounts	value from social media use depends on if company is private or public
executive social media use provides intel for use in an attack	personal social media used to Identify current trends	Senior executives should avoid disclosing personal trips ahead of time	what value do they place on the organization
executives not allowed to express personal opinions on social media	personal social media used to monitor children's activity	Senior executives should avoid disclosing work trips ahead of time	which personal social media platforms are used
executives required to take media training before speaking to the public	personal social media used to share Information	shared company specifics used in social engineering attack (Glassdoor, etc.)	younger generation social media overuse
hard to distinguish between personal and work-related achievements	personal social media used to share resume	sharing job postings via social media accounts	
have staff post on behalf of senior executives in personal accounts	policy prohibits employees from discussing company via social media	size of organization as factor in nature of response to negative social media interactions	
Hired by competing organization to target them	Prior job description	social media contacts causing work disruption	

Appendix E

Illustrative supporting data for overarching dimensions

Overarching Dimensions	Themes	Concepts
Loss of Intellectual Property or Sensitive Data		
	Situational Awareness	• ‘We talk about we want to share pictures and share how great and wonderful it is to work there, but we also want to be very aware of the surroundings when we take pictures, of what we post that someone might be able to see…’ • ‘I've seen some folks tweet some pictures of their network diagrams’ • ‘I’ve seen some folks… accidentally putting credentials up on Facebook’ • ‘And, he had their YouTube credentials on a sticky note, on his monitor’ • ‘…but now it happens a lot on Twitter too, and I've seen organizations post passwords’ • ‘[Executives]… be very aware of the surroundings when we take pictures, of what we post that someone might be able to see pseudocode in the background’
	Blackmail	• 'The business is higher profile, more prone to any sort of blackmail, ransom, anything like that, and my belief is that they've got to be a little bit more careful about what they post, how it's posted, when it's posted, and things like that' • ‘what happens in their private lives could certainly be used to gain leverage over them in a business capacity, so blackmailing them for ...’ • ‘I could easily see it as a future possibility that an executive could post something either without realizing its importance or accidently posting something that could be used as blackmail against them.’ • ‘Executive being blackmailed as a result of something they post is real. Jeff Bezos is a prominent example of this.’

		• ‘It’s more likely to occur when execs use a social media platform to privately message and disclose things they shouldn’t or behave in a manner that puts that individual in a compromising position either morally or ethically.’ • ‘Let's just say that they are very active, and things that are done within social media that are not necessarily, you know, ethical in the sense of like what happens in their private lives could certainly be used to gain leverage over them in a business capacity, so blackmailing them for ... You know, if they access pictures, or something along those lines, because the potential damage for that kind of information and getting it out to the public has its damages to the company, as well.’
Compliance Violations		
	HIPAA violations	• ‘Imagine an executive tweets something to the tune of "we're so good at what we do, Beyonce chose our hospital for her healthcare". Unless this was very clearly approved by Beyonce, this is a HIPAA violation at minimum.’ • ‘One could even argue that executive's [sic] shouldn't even know about the individual patients because they aren't directly involved in patient care.’ • ‘The funny thing [when thinking about HIPAA violations] about inference is that you never know what seemingly innocent piece of information is harmful.’ • ‘Certainly, you could see a health care exec talking about a patient, naming a name…’
	SEC violations	• ‘I would envision the possibility that executives may get overly excited about big “deals” or huge “issues” with customers and tweet or post in instagram about things that would violate SEC. this may fall under “manipulating market prices” or “insider trading” by sharing too much or confidential information with followers who in turn react

		to this with information with buying/selling stocks based on the post.’
		• ‘Elon Musk is a great example of that where he gets himself in trouble all the time by talking about things that aren't the way the SEC wants him to release that information.’ • ‘[For publicly traded organizations] there’s a lot of rules around what you can say that is material to the business and how that is disseminated, so they've got to be very careful. I think that, that from a financial risk perspective, that could cause fines and loss of business, and potential, other legal lawsuit issues if they aren't careful about what and how they say things that are material to the business.’ • ‘Publicly traded companies have to be very careful because obviously C-level people, many of them are on the board of directors and they are privy to information that's not necessarily for public consumption, and if it gets out there aside from the normal channels where the stockholders are informed about these decisions, about these things, it could impact the stock price.’
Harm to Reputation	*Public Scandal*	• ‘It has ended people's careers. Do you support... Who was it? The gentleman that was a part of Mozilla. Was there... The CEO at the time? Who supported... who tweeted that he was not in favor of some boycott against some company. I don't want to say it was Chick-fil-A. It was something like that, where he expressed support for some organization, and he was labeled a bigot, and all sorts of things. And he got run out of his own company. I think it was Mozilla…’

		• ‘We've seen it go well, and we've seen it go horrifically wrong. The guy who shot the rhino, right? The founder of Jimmy John's posed with big game, and it went on his Facebook, and it went viral, and the company damn near went bankrupt because people were, you know, like, "The guy's a horrible human being."’ • ‘Your personal profile is really not, right? You always can be tied back to the company that you represent, especially if the bigger company you work for... You know, the bigger, the bigger the problem.’ • ‘I think you can do whatever you want to do; you just have to be careful and set some boundaries with how you're going to use that media to influence, right? So you don't want your personal life too much influencing the business life so-to-speak, if that makes any sense’
	Negative Social Media incident	• ‘"Well, that must mean clearly, we think that's what the company says." I'm like, "Wait a second. Time out. This is on my own time. And they're like, "Yeah, but you don't get to do that." And so that was a harsh realization, I think, for me is that there is no off time.’ • ‘Person went on vacation talked about the bad experiences they had at this resort. Turns out, that that resort was one of their biggest clients and that resulted in some interesting conversations.’ • ‘You had somebody talk about a bad experience at a hospital, turns out their company sells software to the hospital. And, they were talking about that on their personal Facebook account, except they didn't really have good privacy settings on that. And, some of the people that are friends with were actually at the hospital too so, it became interesting.’
Fraudulent Transaction Loss		

C-level Employee impersonation	• ‘…if they know a senior executive is going to be, perhaps, out of comms for a weekend, maybe that's a good time to start spoofing them, because they know that the real person can’t be reached…’ • ‘If you say, hey, I'm going to Cancun for the weekend, and then the bad actor starts emailing the CFO saying, hey, I'm stuck in Cancun, but I need you to transfer this money. That now is a more credible email and that doesn't help the organization defend itself.’ • ‘[Executives] have to be careful about putting too much of their personal information out there because it may be the piece of the puzzle that someone malicious might need to be able to penetrate the organization through an email not against them personally necessarily, but against their assistant or against someone that works for them.’ • ‘[Penetration testers] have typically created, very, very precise attacks that have penetrated the network, and that was because people gave too much information.’ • ‘For example if a chief marketing officer just posted hey, I'm going to be in Bahamas next week, I know the location. Now, I know that that person is out of office and I can use that information for let's say, social engineering…’
Vendor impersonation	• ‘Let's say the CFO's on vacation. The secretary or the office manager for the finance department has some bills to pay. Suddenly somebody calls up and, "Hey. This is an urgent bill. If you don't pay this bill today, by X time, we're going to turn the lights out, or we're going to turn your internet connection off." Whatever that scenario is, and she can't get in touch or he can't get in touch with the CFO, suddenly now you've got people pressured to make a decision for the benefit of the company

without the oversight, and they were able to be socially engineered because somebody got that information off of a public social media site…'

• '…the company gets a random invoice from a person saying, "Hey, so and so said to go ahead and pay this." That the person who sends the email, and the invoice, knows that the executive is on a plane or somewhere, that they are just not reachable, and the company doesn't do their checks and balances, and pays a fraudulent invoice…'
• 'They're finding those kind of things online and then … embezzling your money from your accounts in ways that they have convinced other people to do it.'

References

AGARI Data. (2018). London blue: Uk-based multinational gang runs bec scams like a modern corporation.

Agresti, W. W. (2010). The four forces shaping cybersecurity. *IEEE Computer Magazine, 43,* 101-104.

Ali-Hassan, H., Nevo, D., & Wade, M. (2015). Linking dimensions of social media use to job performance: The role of social capital. *The Journal of Strategic Information Systems, 24*(2), 65-89. doi: https://doi.org/10.1016/j.jsis.2015.03.001

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(4), 308-313. doi: https://doi.org/10.1016/S0167-4048(03)00407-3

Associated Press. (2016). Mattel vs. Chinese cyberthieves: It's no game. Retrieved from https://www.cbsnews.com/news/mattel-vs-chinese-cyberthieves-its-no-game/

Association for Information Systems. (2011). Senior scholars' basket of journals, from http://aisnet.org/?SeniorScholarBasket

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences, 1*(03), 23-32.

Baker & Hostetler LLP. (2017). State data breach law summary, from https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *Management Information Systems Quarterly, 25*(1), 1-16.

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

Bringer, J. D., Johnston, L. H., & Brackenridge, C. H. (2006). Using computer-assisted qualitative data analysis software to develop a grounded theory project. *Field Methods, 18*(3), 245-266.

Brinkmann, S., & Kvale, S. (2015). *Interviews: Learning the craft of qualitative research interviewing* (Third ed.). Thousand Oaks, California: SAGE Publications, Inc.

Brody, R. G., Brizzee, W. B., & Cano, L. (2012). Flying under the radar: Social engineering. *International Journal of Accounting & Information Management, 20*(4), 335-347. doi: 10.1108/18347641211272731

Bronk, C. (2014). Corporate risk, intelligence and governance in the time of cyber threat. *Risk Governance & Control: Financial Markets & Institutions, 4*(1), 16-22.

Buckley, O., Nurse, J. R. C., Legg, P. A., Goldsmith, M., & Creese, S. (2014). *Reflecting on the ability of enterprise security policy to address accidental insider threat.* Paper presented at the 2014 Workshop on Socio-Technical Aspects in Security and Trust, Vienna, Austria.

Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2017). On the anatomy of social engineering attacks—a literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*, 1-26. doi: 10.1002/jip.1482

Buonanno, G., Faverio, P., Pigni, F., Ravaini, A., Sciuto, D., & Tagliavini, M. (2005). Factors affecting erp system adoption : A comparative analysis between smes and large companies. *Journal of Enterprise Information Management*(4), 384. doi: 10.1108/17410390510609572

Burch, G., Taylor, A., & Yeung, C. (2015). Wire transfer email fraud and what to do about it. *Intellectual Property & Technology Law Journal, 27*(1), 13-15.

Carlton, M., & Levy, Y. (2015, 9-12 April 2015). *Expert assessment of the top platform independent cybersecurity skills for non-it professionals.* Paper presented at the SoutheastCon 2015, Fort Lauderdale, Florida.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of itsecurity management: Four improvements to current security practices. *Communications of the Association for Information Systems, 14*, 65-75.

Charmaz, K. (1995). Grounded theory. In J. A. Smith, R. Harre & L. Van Langenhove (Eds.), *Rethinking methods in psychology*. London, United Kingdom: Sage Publishing.

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Thousand Oaks, CA: Sage Publishing.

Chen, A., Lu, Y., Chau, P. Y. K., & Gupta, S. (2014). Classifying, measuring, and predicting users' overall active behavior on social networking sites. *Journal of Management Information Systems, 31*(3), 213-253. doi: 10.1080/07421222.2014.995557

Choudrie, J., & Zamani, E. D. (2016). Understanding individual user resistance and workarounds of enterprise social networks: The case of service ltd. *Journal of Information Technology, 31*(2), 130-151.

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal, 23*(5), 401-417. doi: 10.1111/j.1365-2575.2012.00402.x

Constantiou, I. D., & Kalinikos, J. (2015). New games, new rules: Big data and the changing context of strategy. *Journal of Information Technology, 30*(1), 44-57.

Conteh, N. Y., & Royer, M. D. (2016). The rise in cybercrime and the dynamics of exploiting the human vulnerability factor. *International Journal of Computer, 20*(1), 1-12.

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. [journal article]. *Qualitative Sociology, 13*(1), 3-21. doi: 10.1007/bf00988593

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (Fifth ed.): SAGE Publications, Inc.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101. doi: http://dx.doi.org/10.1016/j.cose.2012.09.010

Denzin, N. K., & Lincoln, Y. S. (1994). *Handbook of qualitative research*. Thousand Oaks: Sage Publications.

Department of Homeland Security Risk Steering Committee. (2010). *Dhs risk lexicon*. Retrieved from https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf.

DeSalvo, B., Limehouse, F. F., & Klimek, S. D. (2016). *Documenting the business register and related economic business data*. Washington, D.C.: Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755723.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security, 28*(3), 189-198. doi: https://doi.org/10.1016/j.cose.2008.11.007

Drew, S. A., Kelley, P. C., & Kendrick, T. (2006). Class: Five elements of corporate governance to manage strategic risk. *Business Horizons, 49*(2), 127-138. doi: 10.1016/j.bushor.2005.07.001

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), 32-64. doi: https://doi.org/10.1518/001872095779049543

Federal Bureau of Investigation. (2017). Business e-mail compromise; e-mail account compromise; the 5 billion dollar scam, from https://www.ic3.gov/media/2017/170504.aspx

Federal Bureau of Investigation. (2020). *2019 internet crime report*. Washington, D.C.: Retrieved from https://pdf.ic3.gov/2019_IC3Report.pdf.

Finkelstein, S., & Hambrick, D. C. (1990). Top-management-team tenure and organizational outcomes: The moderating role of managerial discretion. *Administrative Science Quarterly, 35*(3), 484-503.

Flack, C. K. (2016). *Is success model for evaluating cloud computing for small business benefit: A quantitative study.* Doctor of Business Administration, Kennesaw State University, Kennesaw, Georgia. Retrieved from http://digitalcommons.kennesaw.edu/dba_etd/20

Forsgren, E., & Byström, K. (2017). Multiple social media in the workplace: Contradictions and congruencies. *Information Systems Journal*, 1-23. doi: 10.1111/isj.12156

Fuduric, M., & Mandelli, A. (2014). Communicating social media policies: Evaluation of current practices. *Journal of Communication Management, 18*(2), 158-175. doi: doi:10.1108/JCOM-06-2012-0045

Gao, W., Liu, Z., Guo, Q., & Li, X. (2018). The dark side of ubiquitous connectivity in smartphone-based sns: An integrated model from information perspective. *Computers in Human Behavior, 84*, 185-193. doi: https://doi.org/10.1016/j.chb.2018.02.023

Gardner, B., & Thomas, V. (2014). *Building an information security awareness program: Defending against social engineering and technical threats*: Elsevier.

Gerlach, J., Widjaja, T., & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The Journal of Strategic Information Systems, 24*(1), 33-43. doi: https://doi.org/10.1016/j.jsis.2014.09.001

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. New Brunswick, New Jersey: AldineTransaction.

Green, A. (2007). *Management of security policies for mobile devices.* Paper presented at the InfoSecCD '07, Kennesaw, Georgia.

Greenaway, K. E., & Chan, Y. E. (2013). Designing a customer information privacy program aligned with organizational priorities. *MIS Quarterly Executive, 12*(3), 137-150.

Greenaway, K. E., Chan, Y. E., & Crossler, R. E. (2015). Company information privacy orientation: A conceptual framework. *Information Systems Journal, 25*(6), 579-606. doi: 10.1111/isj.12080

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). *Analysis of unintentional insider threats deriving from social engineering exploits.* Paper presented at the 2014 IEEE Security and Privacy Workshops.

Grooten, M. (2018). Cinema chain sees bad movie script play out as it loses millions in email scam, from https://www.forbes.com/sites/martijngrooten/2018/11/12/cinema-chain-sees-bad-movie-script-play-out-as-it-loses-millions-in-email-scam/#73050e4b6af9

Grunwitz, K. (2018). Raising executive awareness. *Computer Fraud & Security, 2018*(12), 20.

Hall, R. H. (1977). *Organizations: Structures, processes and outcomes* (2nd ed.). Englewood Cliffs, New Jersey: Prentice-Hall.

Hambrick, D. C. (1981). Strategic awareness within top management teams. *Strategic Management Journal, 2*(3), 263-279.

Hambrick, D. C., Finkelstein, S., & Mooney, A. C. (2005). Executive job demands: New insights for explaining strategic decisions and leader behaviors. *Academy of Management Review, 30*(3), 472-491. doi: 10.5465/AMR.2005.17293355

Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: The organization as a reflection of its top managers. *Academy of Management Review, 9*(2), 193-206. doi: 10.5465/AMR.1984.4277628

Hannan, M. T., & Freeman, J. (1977). The population ecology of organizations. *American Journal of Sociology, 82*(5), 929-964. doi: 10.1086/226424

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology, 14*(2), 171-180. doi: doi:10.1108/13287261211232180

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

Heravi, A., Mubarak, S., & Choo, K.-K. R. (2018). Information privacy in online social networks: Uses and gratification perspective. *Computers in Human Behavior, 84*, 441-459. doi: https://doi.org/10.1016/j.chb.2018.03.016

Holland, R., Amado, R., & Marriott, M. (2018). Pst! Cybercriminals on the outlook for your emails, from https://resources.digitalshadows.com/digitalshadows/cybercriminals-on-the-outlook-for-your-emails

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research, 26*(2), 282-300. doi: 10.1287/isre.2015.0569

Hu, T., Kettinger, W. J., & Poston, R. S. (2015). The effect of online social value on satisfaction and continued use of social media. *European Journal of Information Systems, 24*(4), 391-410.

Humphreys, L., Gill, P., & Krishnamurthy, B. (2014). Twitter: A content analysis of personal information. *Information, Communication & Society, 17*(7), 843-857. doi: 10.1080/1369118X.2013.848917

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

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

Kemp, T. (2016). Social engineering fraud: A case study. *Risk Management, 63*(6), 8-9.

Kim, H. J. (2012). Online social media networking and assessing its security risks. *International Journal of Security and Its Applications, 6*(3), 11-18.

Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective, 24*(1-3), 72-77. doi: 10.1080/19393555.2015.1051676

Krasnova, H., Veltri, N. F., Eling, N., & Buxmann, P. (2017). Why men and women continue to use social networking sites: The role of gender differences. *The Journal of Strategic Information Systems, 26*(4), 261-284. doi: https://doi.org/10.1016/j.jsis.2017.01.004

Krippendorff, K. (2004). *Content analysis: An introduction to its methodology*. Thousand Oaks, California: SAGE Publications.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113-122. doi: https://doi.org/10.1016/j.jisa.2014.09.005

Laszka, A., Lou, J., & Vorobeychik, Y. (2015). *Multi-defender strategic filtering against spear-phishing attacks.* Paper presented at the Twenty-Ninth AAAI Conference on Artificial Intelligence, Austin, TX.

Lee, C. H., Geng, X., & Raghunathan, S. (2016). Mandatory standards and organizational information security. *Information Systems Research, 27*(1), 70-86. doi: 10.1287/isre.2015.0607

Lee, J. W., Seong, J. Y., & Lee, J. H. (2012). A new perspective on human resource management research: An organizational systematics approach. *Business and Management Research, 1*(1), 77-88.

Leonardi, P. M. (2015). Ambient awareness and knowledge acquisition: Using social media to learn "who knows what" and "who knows whom". *MIS Quarterly, 39*(4), 747-762.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (crcm) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal, 25*(5), 433-463. doi: 10.1111/isj.12043

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193-273. doi: 10.1111/isj.12063

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. *Information Resources Management Journal, 24*(3), 1-8. doi: 10.4018/irmj.2011070101

MacPhail, C., Khoza, N., Abler, L., & Ranganathan, M. (2015). Process guidelines for establishing intercoder reliability in qualitative studies. *Qualitative Research, 16*(2), 198-212. doi: 10.1177/1468794115577012

Mason, M. (2010). Sample size and saturation in phd studies using qualitative interviews. *Forum: Qualitative Social Research, 11*(3).

Matavire, R., & Brown, I. (2017). Profiling grounded theory approaches in information systems research. *European Journal of Information Systems, 22*(1), 119-129. doi: 10.1057/ejis.2011.35

Matook, S., Cummings, J., & Bala, H. (2015). Are you feeling lonely? The impact of relationship characteristics and online social network features on loneliness. *Journal of Management Information Systems, 31*(4), 278-310. doi: 10.1080/07421222.2014.1001282

McDonald, N., Schoenebeck, S., & Forte, A. (2019). Reliability and inter-rater reliability in qualitative research. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), 1-23. doi: 10.1145/3359174

Meinert, M. C. (2016). Social engineering: The art of human hacking. *ABA Banking Journal, 108*(3), 49.

Merriam-Webster. (n.d.). Blackmail, from https://www.merriam-webster.com/dictionary/blackmail

Molok, N. N. A., Chang, S., & Ahmad, A. (2013). *Disclosure of organizational information on social media: Perspectives from security managers.* Paper presented at the Pacific Asia Conference on Information Systems, Jeju Island, Korea.

Mukkamala, R. R., Vatrapu, R., & Hussain, A. (2013). Towards a formal model of social data: IT-Universitetet i København.

Myers, M. D., & Newman, M. (2007). The qualitative interview in is research: Examining the craft. *Information and Organization, 17*(1), 2-26. doi: https://doi.org/10.1016/j.infoandorg.2006.11.001

National Institute of Standards and Technology. (2011). *Managing information security risk: Organization, mission, and information system view*. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

Palmer, D. (2020). Ceos are deleting their social media accounts to protect against hackers, from https://www.zdnet.com/article/ceos-are-deleting-their-social-media-accounts-to-protect-against-hackers/

Parks, R., Xu, H., Chu, C.-H., & Lowry, P. B. (2017). Examining the intended and unintended consequences of organisational privacy safeguards. *European Journal of Information Systems, 26*(1), 37-65. doi: 10.1057/s41303-016-0001-6

Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review, 93*(85), 85-176.

Peters, V., & Wester, F. (2007). How qualitative data analysis software may support the qualitative analysis process. *Quality and Quantity, 41*(5), 635-659.

Pike, J. C., Bateman, P. J., & Butler, B. S. (2017). Information from social networking sites: Context collapse and ambiguity in the hiring process. *Information Systems Journal*, 1-30. doi: 10.1111/isj.12158

Pratt, M. G. (2009). For the lack of a boilerplate: Tips on writing up (and reviewing) qualitative research. *Academy of Management Journal, 52*(5), 856-862. doi: 10.5465/AMJ.2009.44632557

Quttainah, M., & Paczkowski, W. (2014). Linking business owners' choice of organizational form to appraisers' determination of value: An agency theory perspective. *Journal of Management Policies and Practices, 2*(4), 77-96.

Rivera, R. (2018). Person pretending to be ceo steals info from charleston co. Aviation authority, from http://www.live5news.com/story/37681721/person-pretending-to-be-ceo-steals-info-from-charleston-co-aviation-authority

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44. doi: http://dx.doi.org/10.1016/j.cose.2016.01.004

Romano Jr., N. C., Donovan, C., Chen, H., & Nunamaker Jr., J. F. (2003). A methodology for analyzing web-based qualitative data. *Journal of Management Information Systems, 19*(4), 213-246.

Sánchez Abril, P., Levin, A., & Del Riego, A. (2012). Blurred boundaries: Social media privacy and the twenty-first-century employee. *American Business Law Journal, 49*(1), 63-124. doi: 10.1111/j.1744-1714.2011.01127.x

Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the united states and european union. *California Law Review, 102*(4), 877-916.

Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile phishing attacks and mitigation techniques. *Journal of Information Security, 6*(3), 206-212. doi: 10.4236/jis.2015.63021

Sharp, A. (2017). Fbi warns of surge in wire-transfer fraud via spoofed emails, from http://www.reuters.com/article/us-cyber-fraud-email-idUSKBN1811QH

Social-Engineer LLC. (2017). The 2017 social engineering capture the flag report.

Social-Engineer LLC. (2019). The verizon dbir — the c-suite is under attack, from https://www.social-engineer.com/the-verizon-dbir-the-c-suite-is-under-attack/

Solove, D. J. (2013). Hipaa: Mighty and flawed. *Journal of AHIMA, 84*(4), 30-31.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for is positivist research. *Communications of the Association for Information Systems, 13*(24), 380-427.

Suddaby, R. (2006). From the editors: What grounded theory is not. [Editorial]. *Academy of Management Journal, 49*, 633-642. doi: 10.5465/AMJ.2006.22083020

Symantec. (2015). *Internet security threat report*. Retrieved from http://know.symantec.com/LP=1123.

Teplinsky, M. J. (2013). Fiddling on the roof: Recent developments in cybersecurity. *American University Business Law Review, 2*(2), 225-322.

The Occupational Information Network. (2019). Custom report for: 15-1122.00 - information security analysts (education), from https://www.onetonline.org/link/result/15-1122.00?n_tk=10&e_tk=1&c_tk=50&s_tk=IM&n_tc=10&s_tc=s&n_tl=10&s_tl=s&n_kn=10&c_kn=50&s_kn=IM&n_sk=10&c_sk=50&s_sk=IM&n_ab=10&c_ab=50&s_ab=IM&n_wa=10&c_wa=50&s_wa=IM&n_dw=10&a_iw=g&a_iw=i&a_iw=d&a_iw=t&n_cx=10&c_cx=50&c=et&c_in=50&n_ws=10&c_ws=50&c_wv=50&n_cw=10&s_cw=CIP&n_ad=10&g=Go

The United States Census Bureau. (2020a). Information security analysts: Gender composition. *Information security analysts: Gender Composition*, from https://datausa.io/profile/soc/information-security-analysts#gender

The United States Census Bureau. (2020b). Information security analysts: Industries by share, from https://datausa.io/profile/soc/information-security-analysts#tmap_ind

The United States Census Bureau. (2020c). Information security analysts: Race & ethnicity, from https://datausa.io/profile/soc/information-security-analysts#ethnicity

Thornberg, R., & Charmaz, K. (2012). Grounded theory. In S. D. Lapan, M. T. Quartaroli & F. J. Riemer (Eds.), *Qualitative research: An introduction to methods and designs* (pp. 41-67). San Francisco, California: Jossey-Bass.

Torres, J. M., Sarriegi, J. M., Santos, J., & Serrano, N. (2006). *Managing information systems security: Critical success factors and indicators to measure effectiveness*. Paper presented at the 2006 International Conference on Information Security, Samos Island, Greece.

Trustwave. (2017). 2017 trustwave global security report.

Turel, O., & Qahri-Saremi, H. (2016). Problematic use of social networking sites: Antecedents and consequence from a dual-system theory perspective. *Journal of Management Information Systems, 33*(4), 1087-1116. doi: 10.1080/07421222.2016.1267529

U.S. Department of Health and Human Services. (n.d.). Summary of the hipaa security rule, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

U.S. Securities and Exchange Commission. (n.d.). What we do, from https://www.sec.gov/Article/whatwedo.html

Uldam, J. (2016). Corporate management of visibility and the fantasy of the post-political: Social media and surveillance. *New Media & Society, 18*(2), 201-219. doi: 10.1177/1461444814541526

Urquhart, C., & Fernández, W. (2013). Using grounded theory method in information systems: The researcher as blank slate and other myths. *Journal of Information Technology, 28*(3), 224-236. doi: 10.1057/jit.2012.34

Urquhart, C., Lehmann, H., & Myers, M. D. (2009). Putting the 'theory' back into grounded theory: Guidelines for grounded theory studies in information systems. *Information Systems Journal, 20*(4), 357-381. doi: 10.1111/j.1365-2575.2009.00328.x

Vaast, E., & Kaganer, E. (2013). Social media affordances and governance in the workplace: An examination of organizational policies. *Journal of Computer-Mediated Communication, 19*(1), 78-101. doi: 10.1111/jcc4.12032

Venkatesh, V., Brown, S., & Bala, H. (2013). Bridging the qualitative–quantitative divide: Guidelines for conducting mixed methods research in information systems. *Management Information Systems Quarterly, 37*(1), 21-54.

Verizon Enterprises. (2016). 2016 data breach investigations report.

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

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems, 22*(2), 157-174. doi: https://doi.org/10.1016/j.jsis.2013.01.003

Wakefield, R., & Wakefield, K. (2016). Social media network behavior: A study of user passion and affect. *The Journal of Strategic Information Systems, 25*(2), 140-156. doi: https://doi.org/10.1016/j.jsis.2016.04.001

Wallack, T. (2018). Hackers fooled save the children into sending $1 million to a phony account, *Boston Globe*. Retrieved from https://www.bostonglobe.com/business/2018/12/12/hackers-fooled-save-children-into-sending-million-phony-account/KPnRi8xIbPGuhGZaFmlhRP/story.html

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research, 24*(2), 201-218. doi: 10.1287/isre.1120.0437

Wiesche, M., Jurisch, M. C., Yetton, P. W., & Krcmar, H. (2017). Grounded theory methodology in information systems research. *MIS Quarterly, 41*(3), 685-701.

Wilcox, H., Bhattacharya, M., & Islam, R. (2014). *Social engineering through social media: An investigation on enterprise security.* Paper presented at the International Conference on Applications and Techniques in Information Security, Melbourne, Australia.