2018

Organizational Information Security: Strategies to Minimize Workplace Cyberloafing for Increased Productivity

Hawazin Al Abbasi
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Hawazin Al Abbasi

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Anthony Lolas, Committee Chairperson, Management Faculty
Dr. Teresa Lao, Committee Member, Management Faculty
Dr. Raghu Korrapati, University Reviewer, Management Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Organizational Information Security: Strategies to Minimize Workplace Cyberloafing for Increased Productivity

by

Hawazin Al Abbasi

MSc, Coventry University, 2009

BSc, Al Mansour University College, 1994

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

February 2018

Abstract

Productivity loss occurs in organizations that experience high levels of personal Internet use by employees on company time, which includes employees using smartphones to surf without needing the firm's Internet connection. The purpose of this qualitative phenomenological study was to explore reliable ways for organizational leaders to monitor or limit their employees' use of smartphone technology for personal use (*cyberloafing*) while on the job to minimize wasted work time. Social cognitive theory, which includes an emphasis on human behavioral changes based upon the environment, people, and behavior, served as the conceptual framework. The general research question was as follows: How can managers minimize wasted work time by limiting the personal Internet activity of employees who use personal mobile devices while on the job? Data collection involved gathering information from interviews with 20 frontline supervisors, human resource managers, and information technology managers and specialists in 2 U.S. industries: education and telecommunications. Data analysis included examining word frequencies, keyword coding, and identifying themes. Four management themes emerged: create mobile device usage policy, enforce monitoring technology, create a deterrence strategy, and customize monitoring and tracking technology. This study may be important because the analysis revealed effective ways to prevent or minimize employees from Internet surfing and wasting time at work. The findings could lead to positive social change through increased employee productivity and responsibility by providing managers with information to control or limit cyberloafing activities and by fostering an increased commitment to comply with an organization's Internet use policy.

Organizational Information Security: Strategies to Minimize Workplace Cyberloafing for Increased Productivity by

Hawazin Al Abbasi

MSc, Coventry University, 2009

BSc, Al Mansour University College, 1994

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

February 2018

Dedication

After an intensive period of seven years, today is the day: writing this note of thanks is the finishing touch on my dissertation. I want to thank my Dad who motivated me to follow my heart and keep learning throughout my life. His encouragement allowed me to reach this point in my academic journey. I dedicate this study to my loving and patient husband, Mustafa, and my lovely sons, Ali and Mohammad, who provide unending inspiration. I look forward to continuing our dreams together. Many thanks for you all!

Acknowledgments

I am very grateful to Dr. Anthony Lolas for his dedication and guidance throughout this journey. His constant encouragement kept me focused on my goal. I would like to acknowledge my committee member Dr. Teresa Lao, for her valuable guidance and suggestions contributed significantly to my study.

Table of Contents

Chapter 1: Introduction to the Study

The topic of this study is the misuse of the Internet by employees and managers while on the job. Internet misuse in the workplace can be a significant violation of company policy and exposes organizations to serious risk. Internet misuse can also reduce employee productivity (Boxall & Macky, 2014). Organizational leaders need to determine ways to improve job performance and reduce the risks of not complying with organizational security policies. Surfing the Internet during work hours results in lost productivity for organizations. Saraç and Çiftçioğlu (2014) found that web surfing costs U.S. employers more than $50 billion each year in lost productivity.

Careless employees misusing the Internet not only present serious threats to their organizations when they fail to follow information security and Internet use policies, but also such misuse could lead to reduced job quality and lost productivity (Donahue & Rahman, 2012). As a clear guide to handling Internet use for personal activity is necessary, this study is important for leaders, human resources staff, and administrative managers because the findings include ways to prevent surfing during work hours to avoid wasting time at work and to prevent virus risks resulting from visiting untrusted websites. A possible positive social change implication of this study is improved employee productivity because these findings could lead to organizational savings by preventing or limiting employees from spending their working hours browsing, chatting, and texting instead of focusing on their job (Kral, 2011). Organizational leaders may use the results of this study to protect their organizations from facing potential legal consequences of employees violating Internet policies, such as displaying or e-mailing pornographic materials and being noncompliant with sexual harassment law. The subsequent major sections of Chapter 1 include the background, problem statement, purpose, research questions, conceptual framework, nature of the study, definitions, assumptions, scope and delimitations, limitations, significance, and summary of the chapter.

Background of the Study

Because of the increase in Internet misuse in the workplace (Saraç & Çiftçioğlu, 2014), organizational leaders face serious threats to their daily operation. Internet misuse in the workplace is a violation of company policy and may result in adverse consequences to organizations, such as wasted work hours and a reduction in employee productivity. More important, misuse of the Internet could expose organizations to serious security risks and financial penalties (Grover, 2014).

End users may engage in behaviors that violate their organization's policy. Policy violation may lead to serious security breaches and result in adverse financial consequences. Employers are responsible by law for violations when employees misuse the Internet during work time. Misuse can include harassing other employees or creating an uncomfortable work environment by displaying or e-mailing pornographic material (Grover, 2014).

Many employees do not follow the security policy of their organization, even though they are aware of the risks to their organization's business systems because of these violations (Donahue & Rahman, 2012). Insider threats to organizations can range from exploring organizational information to releasing sensitive information accidentally or deliberately that exposes an organization’s infrastructure. Insider threats may originate from employees, managers, or anyone working in a company who gains access to the information.

Cyberloafing is the unauthorized use of the Internet for nonwork or personal activities during the workday and is a growing and costly problem for organizational leaders (Coker, 2011). Grover (2014) found that 64% of a sample of 1,000 workers in the United States surfed the Internet for personal activity during work hours. Employees tended to transfer the negative news among their group membership by texting or posting through social media, e-mails, and chat rooms (Grover, 2014). Therefore, many organizational business leaders need to ensure there is no gap or vulnerability in their monitoring strategy regarding personal Internet use during business hours (Král, 2011). The most popular procedure or strategy for ensuring a secure environment is monitoring employees’ activities to discourage them from committing violations or misusing an organization’s resources (Donahue & Rahman, 2012).

Researchers have suggested using various policies and technologies to control Internet use at work by employees for personal activity, but there is a lack of research literature regarding the topic of employee Internet misuse using personal phones and tablets while at work (Saraç & Çiftçioğlu, 2014). This study fills the gap in the literature regarding employee Internet use via smaller technology devices, such as smartphones and personal tablets. Organizational leaders need a reliable way to control or monitor employee Internet misuse through smaller personal devices to protect their company and increase employee productivity.

Problem Statement

Despite the many advantages of using the Internet in organizations, (cyberloafing) is a potentially serious problem for organizational leaders. Saraç and Çiftçioğlu (2014) estimated that web surfing costs U.S. employers more than $50 billion a year in lost productivity. The most common issues researched on non-work-related Internet use are productivity loss, Internet cost, and Internet security issues (Saraç & Çiftçioğlu, 2014). The general problem is that employees and managers can waste work time by using their own mobile devices while on the job, so organizational resources are not necessary for employees to access the Internet for personal use while on company time (Saraç & Çiftçioğlu, 2014). The specific problem is that leaders in educational organizations have not found a reliable way to limit or monitor employees' personal use of the Internet through their personal smartphones or tablets while on the job. This research fills the gap in the literature regarding this topic through a focus on the personal opinions of frontline supervisors, human resource managers, and information technology (IT) managers to find ways to make organizations' policies more effective with respect to limiting or preventing employee Internet use for personal activity while on the job.

Purpose of the Study

The purpose of this qualitative phenomenological study was to find reliable ways for organizational leaders to monitor or limit employees' personal use of the Internet through their mobile devices and smartphone technology while on the job. In addition to wasted work time, other major organizational concerns include security threats, policy violations, and the misuse of the Internet during work time, especially when employees use their smartphone to connect to the organization’s Internet system, thereby increasing the risk for viruses from visiting untrusted websites (Saraç & Çiftçioğlu, 2014). This study involved exploring ways to limit (cyberloafing) employees use through their personal smartphones while on the job, not only to minimize wasted work time, but also to prevent potential viruses from infecting company information systems as well as compromising confidential files. The approach used to address the study purpose was a qualitative research methodology with interviews. In this study, I collected data via LinkedIn from 20 individuals who were frontline supervisors, human resource managers, or IT managers and specialists representing U.S. educational or telecommunications institutions.

Research Questions

The general research question was as follows: How can managers minimize wasted work time by limiting the personal Internet activity of employees who use personal mobile devices while on the job?

The following were the research subquestions:

RQ1: What effective strategies can managers use to ensure employees are not wasting work time by cyberloafing and sending text messages from their personal mobile devices?

RQ2: How can managers prevent authorized employees from unauthorized access to an organization’s database system?

RQ3: How effective are disciplinary plans designed to punish employees for computer-use policy violations in changing employees' behavior and increasing their commitment to organization policy?

RQ4: How effective are the technology tools that limit or monitor employees' Internet use through their mobile devices while on the job?

Conceptual Framework

The conceptual framework for this qualitative study was Bandura's (1986) social cognitive theory (SCT), which is applicable to media attendance and mobile technology (LaRose & Eastin, 2004). The focus of SCT is human behavior in individuals and their environment, as the basis of SCT is the concept that the results people expect from their current behavior depend on their experiences or the experiences of others who had similar behaviors in the past (LaRose & Eastin, 2004). The aim of applying SCT) in research is to analyze human behavioral changes based upon specific environmental factors. Changing employees' behavior by limiting or controlling their personal Internet activity during work hours and preventing them from wasting work time is the major objectives in the use of this theory (Harris, Marett, & Harris, 2013). The theory provides the process or framework for designing, implementing, and evaluating programs related to research phenomena (Bandura, 1986).

SCT depends on three interrelated factors: (a) environment, (b) people, and (c) behavior (Bandura, 1986). For this study, *environment* referred to the workplace environment design, such as an open or closed office for frontline supervisors; technology environments, including software or hardware used to control Internet use for personal activities; or legal environments involving policy and legal punishments. *People* in this study referred to staff, frontline supervisors, and managers. Finally, *behavior* referred to managers' behaviors toward employees who violated organizational rules and policies.

Nature of the Study

This was a qualitative phenomenological study with interviews that shed light on the research problem. Qualitative research involves studying a connection between a story and ideas developing at a specific site. Qualitative methodology is a way to transform the world through a sequential process that includes interviews, conversations, recordings, and writing memos to self (Aluwihare-Samaranayake, 2012). The focus of qualitative phenomenological research is to record the everyday experiences of participants as they relate to a phenomenon. Researchers use open-ended interview questions to interpret a phenomenon by talking directly to the people and observing their behavior and action, as well as to conduct face-to-face interactions over time (Ballaro & O'Neil, 2013). Open-ended interview questions were suitable for this study.

The focus of the qualitative methodology is a single phenomenon and using text and images to develop an inquiry strategy (Chikweche & Fletcher, 2012). The qualitative tools for collecting the research data can include researchers' eyes and ears, as there are benefits from using casual conversations and accidental observations to collect data. Nevertheless, it is important for researchers to know which approach adds value to their research (Maxwell, 2013). Researchers can conduct qualitative research by exploring and comparing ideas to identify the relationship between them; however, researchers should not try to anticipate the relationships among the ideas from the beginning of a study to avoid bias (Marshall, Cardon, Poddar, & Fontenot, 2013).

I considered a quantitative method for this study. However, quantitative research is deductive and includes hypotheses and research questions (Frels & Onwuegbuzie, 2013). Furthermore, the focus of quantitative research is examining the cause-and-effect relationship between factors and rejecting or failing to reject the study hypotheses (Bansal & Corley, 2012). As the aim of this study is to understand how managers can control cyberloafing by employees during work time, close-ended, deductive questions were not suitable to address the aim of this research or to provide responses to the posited research questions to resolve the problem. Moreover, the sample size for this study was small to reflect participants' experiences of a phenomenon, so the quantitative research method was not appropriate.

I also considered mixed-method research, which involves using quantitative and qualitative research methods to answer the research questions. Researchers use mixed-method research to confirm study outcomes (Wisdom, Cavaleri, Onwuegbuzie, & Green, 2012). However, this study involved exploring reliable ways organizational leaders monitor or limit their employees' personal use of smartphone technology while on the job; therefore, mixed-method research was not appropriate.

Definitions

There were several operational terms associated with this study. The definitions provided reflect the most popular definitions in use in other academic studies and the meaning that served the objective of this study.

Cyberloafing: Cyberloafing is the unauthorized use of the Internet for nonwork or personal activities during work time (Coker, 2011; Ugrin & Pearson, 2013).

Self-control: Self-control refers to an individual's fundamental ability to direct feelings, thoughts, emotions, and behavior (Inzlicht & Schmeichel, 2012).

Self-efficacy: Self-efficacy refers to "individuals' beliefs in their capacity to exercise control over challenging demands and over their own functioning" (Gökçearslan, Mumcu, Haşlaman, & Çevik, 2016, p. 642).

Self-esteem: Self-esteem refers to "the degree to which people perceive themselves to be capable, significant, and worthy" (Wang, Tian, & Shen, 2013, p. 273).

Self-regulation: Self-regulation refers to "self-generated thoughts, feelings, and actions that are planned and cyclically adapted to the attainment of personal goals" (Gökçearslan et al., 2016, p. 641).

Assumptions

In qualitative studies, assumptions refer to researchers' philosophy and conceptions regarding certain issues that researchers use to interpret the results in a way that meets the study goals (Marshall & Rossman, 2015). The assumptions for this study were as follows:

1. I assumed the employees were aware of any Internet policies in place and had signed agreements related to obeying the policies.
2. I assumed the Internet policies applied to all staff regardless of authority or position and that employees would comply if they realized the policies applied fairly to all staff.

3. I assumed the employees could make phone calls or browse the Internet using a personal device during breaks and at lunchtime.
4. I assumed the employees could use their mobile device to make emergency calls and would leave the workroom to go to the staff room for such calls.

These assumptions were necessary because I explored the effective ways to limit the amount of personal Internet activity employees use through personal smartphones while on the job to minimize wasted work time and to minimize the risk of viruses infecting the network from visiting untrusted websites while connected to the organization's Internet system.

Scope and Delimitations

The scope of a study is a parameter that prevents researchers from conducting research in specific areas or under certain conditions (Marshall & Rossman, 2015). The scope of this study included organizations in two U.S. industries: education and telecommunications. I interviewed 20 individuals from two industries who held positions as frontline supervisors, human resource managers, or IT managers and specialists who had at least 2 years of experience in the management field to obtain data regarding the implementation of effective technologies to prevent the waste of work time. Because it is difficult to find effective ways to limit or monitor Internet use by employees during work time consistently, policies and technology need frequent reviews and updates (Saraç & Çiftçioğlu, 2014).

The term *delimitation* refers to the boundaries of a study defined by a researcher to ensure the achievement and accomplishment of study goals (Marshall & Rossman, 2015). Individuals who had held their position for less than 2 years were not eligible to participate. The participants had at least a bachelor's degree in human resources or a technical certification in IT. The participants worked in the education or telecommunications industries only. Only managers and IT professionals who worked in education or the telecommunications industry received an invitation to participate. The conceptual framework for this qualitative study was Bandura's (1986) social cognitive theory (SCT). Data collection involved conducting e-mail, phone, Skype, or face-to-face interviews.

Limitations

Marshall and Rossman (2015) defined the limitations of qualitative research as possible weaknesses that may affect the study outcome, including biased and limited knowledge. This study included some limitations. First, there were no guarantees that at least 15 participants would be able and willing to participate. Second, it could have been difficult to find IT managers and specialists who had the required knowledge and experience with the mobile security applications used to limit or monitor Internet use by employees on their cell phone devices during the workday. Another limitation was my unfamiliarity with the qualitative research method; therefore, I worked closely with my chair and committee member and followed their instructions to conduct my research.

Significance of the Study

This study could add value to businesses for two reasons. First, the study involved exploring effective policies and technologies to control or monitor Internet use by employees for personal activity during the workday. Second, the study includes policy and technology data that contribute to saving work time and increasing employee productivity.

Significance to Practice

Policy violations may cause an organization to face serious security risks and financial losses (Grover, 2014). Employees surfing the Internet during work time can result in billions of dollars of lost productivity for companies. For example, Kim (2012) estimated losses of productivity from cyberloafing in the United States to be $5,000 per employee annually, which amounts to $178 billion across companies nationwide. Even in a sophisticated IT environment, there does not appear to be a practical way to apply these policies to ensure employees comply with organizational policies on the use of personal devices, such as smartphones or tablets (Saraç & Çiftçioğlu, 2014). Consequently, many organizational leaders regularly adopt an improvised approach to ensure Internet activity is proper. This study may be important to organizational leaders because it involved exploring ways to limit the amount of personal Internet use by employees while on the job to prevent wasted work time and to minimize the risk of viruses infecting work networks from visits to untrusted websites (Saraç & Çiftçioğlu, 2014).

Significance to Theory

SCT includes an emphasis on human behavioral changes based on environment, people, and behavior. According to cognitive theory, employees anticipate what will happen depending on their experiences or others' experiences (Piscotty, Martindell, & Karim, 2016). SCT served as the framework to explore reliable ways to control or limit cyberloafing by employees during work time. This study fills the gap in the literature related to limiting or monitoring Internet use by employees through their smartphones while on the job to prevent them from wasting work time. Organizational leaders must be able to enforce established policies and technologies to control personal Internet activity during working hours, prevent wasted work time, and minimize the risk of uploading viruses from untrusted websites (Saraç & Çiftçioğlu, 2014).

Significance to Social Change

This study could contribute to social change because it may lead to improvements in employee productivity and responsibility, cause employees to feel like they are an important part of their organization's success, and increase their commitment through compliance with their organization's Internet use policy. A positive relationship between frontline supervisors and employees may develop by establishing a strategy and identifying technology to control employees' Internet use for personal purposes while on the job. The findings of this study could also lead to an increase in employee productivity by saving work time through controlling or limiting cyberloafing. This study could include means of reducing employee stress, increasing productivity, and achieving a balance between employees' job responsibilities during work time and family commitment by providing a critical strategy to control or limit cyberloafing.

Summary and Transition

Chapter 1 included a general overview of the importance of exploring how to limit the level of personal Internet use by employees during working hours. Surfing the Internet during work time can result in billions of dollars of lost productivity for companies (Saraç & Çiftçioğlu, 2014). Many organizational leaders have created policies related to using the Internet while on company time, but many employees violate these policies by browsing, conducting personal business, downloading inappropriate material, and conducting other activities that waste work time (Grover, 2014).

Chapter 1 also included the background of the problem, problem statement, purpose of the study, research questions, and nature of study. Furthermore, the chapter included the significance of the study and the effects the study may have on practice, theory, and social change. Chapter 2 includes a synthesis of past and current conceptual literature related to the misuse of the Internet by employees while on the job, legal punishment, and strategies leaders have used to solve policy violation situations. Chapter 3 includes information about the participants; research method; data collection; data organization; data analysis plan; research design, data collection, data organization, issues of trustworthiness, ethical procedures, and a summary. Chapter 4: includes the data analysis of the study, description of the participants level of education, the interview environment, demographic data, interview and data collection timeline, and unexpected circumstances experienced during data collection. Chapter 5 includes a restatement of the purpose of the study and the implications of the findings placed in the context of the conceptual framework. Chapter 5 also includes recommendations for additional research and action, as well as implications for a social change, and compare findings to the literature review.

Chapter 2: Literature Review

Despite the many advantages of using the Internet in organizations, the misuse of the Internet in the workplace is a potentially serious problem for organizational leaders. Saraç and Çiftçioğlu (2014) estimated that web surfing cost U.S. employers more than $50 billion a year in lost productivity. The most common issues researched on non-work-related Internet use are productivity loss, Internet cost, and Internet security issues (Saraç & Çiftçioğlu, 2014). Organizational leaders have not found a reliable way to limit or monitor employees' personal use of the Internet through their smartphones or personal tablets while on the job. The purpose of this study was to explore ways to limit the amount of personal Internet activity conducted by employees through their personal smartphones while on the job to minimize wasted work time, prevent viruses from infecting company information systems, and avoid compromising confidential files when employees connect to their organization's Internet system.

This chapter begins with a presentation of the literature review strategies used, followed by a discussion of the conceptual framework and related elements applied to efforts to control cyberloafing behaviors. The chapter also includes a synthesis of past and current conceptual research with a focus on Internet misuse by employees while working, various strategies organizational leaders may use to control the cyberloafing phenomenon, and various perspectives on cyberloafing and smartphone addictions that include details regarding cyberloafing from security perspectives and security challenges. The chapter ends with a summary and conclusion.

Conceptual Framework

The conceptual framework for this qualitative study was SCT (Bandura, 1986), which can apply to media attendance and mobile technology (LaRose & Eastin, 2004). The theory depends on three factors integrated into a whole as the environment affects a person’s behavior: (a) the environment, (b) people, and (c) behavior. Therefore, a study of the environment and the situation may provide an understanding of individuals’ behavior concerning a specific phenomenon, such as the personal use of the Internet while at work. SCT served as the framework for exploring reliable ways to control or limit cyberloafing by employees during work time.

Grover (2014) confirmed that employees are likely to react positively to a policy when the policy applies to everyone and there is no difference regarding the power or authority one has, such as staff versus managers. However, when a policy does not appear to be equitable, some employees may feel disgruntled and may become an insider threat to their company by not complying with the company’s policy. Insider threats can come from employees, staff, managers, or on-site contractors. Hence, there is a need to understand human behavior to explore the issues that cause employees to commit violations, especially when the intent is to harm an organization (Humphreys, 2008). Although most organizations have policies related to using the Internet while on company time, employees frequently violate these policies by browsing, conducting personal business, downloading inappropriate material, and participating in other activities that waste work time, even though they may risk losing their job for the violation (Askew et al., 2014; Hassan, Reza, & Farkhad, 2015).

SCT is suitable for explaining the phenomenon of behaviors, such as violating company policy and the factors related to the behavior. Several factors related to individual behavior can explain a phenomenon, including self-control, self-regulation, and emotional coping responses (LaRose & Eastin, 2004). Self-control and self-regulation refer to the personal regulation of goal-directed behavior or performance (Dang, Dewitte, Mao, Xiao, & Shi 2013; LaRose & Eastin, 2004). Emotional coping responses are strategies or tactics a person uses to cope with emotional stimuli (LaRose & Eastin, 2004; RuningSawitri, 2012).

From a social cognitive perspective, excessive use of the Internet by employees during work time can be an addiction as well as the result of deficient self-regulation. Employees are aware that the time they spend online is excessive and disruptive for their productivity, especially during work time. Employees are also cognizant that they are wasting their work time and could face legal consequences for policy violations, but they prefer to continue their misconduct (Baumeister, 2014; LaRose & Eastin, 2004).

Therefore, the intent of this study was to explore effective ways to limit personal Internet and mobile technology use on the job, which might include policy and technical tools. Applying SCT could contribute to changing employees' behavior and could assist them in limiting their personal Internet use while on the job, which could improve productivity, prevent wasted work time, and minimize the risk of uploading viruses from untrusted websites. Furthermore, a need exists to understand the behavior of employees who commit violations of company policy, especially when the intent is to cause harm to their organization via the Internet (Vitak, Crouse, & LaRose, 2011).

The Internet and e-mail technology are significant assets to an organization if used for supporting work, but the Internet and its accompanying technology are like a double-edged sword, and organizational leaders should be careful when using it (Askew et al., 2014; Otto, Wahl, Lefort, & Frei, 2012). Furthermore, cyberloafing has serious negative implications for organizations related to nonwork activities during working time and presents serious challenges to organizational leaders (Rahimnia & Karimi Mazidi, 2015). Loafing or slacking refers to deviant behavior, and cyberloafing is the main factor that contributes to minimizing productivity (Kuschnaroff & Bayma, 2014). Human resources personnel need to create a balance between cyberloafing and productivity (König & Caner de la Guardia, 2014). The term cyberloafing refers to many activities, such as non-work-based computer use, Internet abuse, wasting work time, junk computing, online gaming, online shopping, chatting, cellphone texting, and more, but cyberloafing is mainly recognized as four activities: (a) personal communications, (b) accessing personal information, (c) personal downloads, and (d) personal e-commerce (Jia, Jia, & Karau, 2013).

There are four perspectives on cyberloafing, and the first one is lower task performance through work time spent surfing the Internet instead of on work, which results in lower productivity (Achakul & Yolles, 2013; Kuschnaroff & Bayma, 2014). Hence, the relationship between cyberloafing and job performance is negative (Moody & Siponen, 2013; Vitak et al., 2011). The second perspective includes a focus on a particular type of cyberloafing, such as gaming and social media, as it becomes difficult for employees to return to work if they use both types during working hours because these types of cyberloafing bring pleasure (Weatherbee, 2012). The result is neglected job responsibilities and decreased productivity (Lim, Teo, & Loo, 2002; Vitak et al., 2011). The third perspective on cyberloafing is that the relationship between cyberloafing and productivity can be positive when employees' reason for cyberloafing is for a work-related task, such as finding ways to market the organization's products (Coker, 2011; Collet, Hine, & du Plessis, 2015). The fourth perspective is the issue of employees' cyberloafing after they are done with their work duties (Askew, 2012). Not all staff are the same in terms of productivity, and if one depends on this last perspective, there would be no relationship between cyberloafing and task performance. The fourth perspective could also serve as confirmation that cyberloafing can be harmful when it becomes addictive (Klotz & Buckley, 2013).

Ugrin and Pearson (2013) focused on the cyberloafing problem and suggested using an appropriate policy with a deterrence mechanism to control and monitor the violations of employees. A deterrence model can help to overcome various types of cyberloafing. For example, threats of termination and detection mechanisms are practical ways to solve cyberloafing problems, including employees viewing pornography, managing personal finances, and doing personal shopping. Although IT innovations continue to grow and change business, social life, and technology, these changes also result in increased opportunities to violate company Internet policies by cyberloafing during work time, which leads to lower work quality and quantity (Jian, 2013; Ugrin & Pearson, 2013).

Rahimnia and Karimi Mazidi (2015) researched various ways to control cyberloafing, including blocking access and web monitoring, but there was a lack of dependence on a theory with which to make the model successful, so the attempt to control cyberloafing failed. In the study, only 40% of the managers believed that policy alone was sufficient for deterring cyberloafing and the deterrence factors did not help with tracking violators (Rahimnia & Karimi Mazidi, 2015). The result was that because the organizational leaders did not have the technology tools to track cyberloafing, they used firing as the solution to punish cyber loafers (Rahimnia & Karimi Mazidi, 2015).

Ugrin and Pearson (2013) noted that different models can serve as a deterrent to cyberloafing, but no specific data showed how to use organizational and individual controls to stop cyberloafing. Organizational leaders need to be able to identify the types of cyberloafing and know what types are more frequent to control or monitor it (Askew et al., 2014). For example, companies such as Xerox and Hewlett-Packard warn their employees about using Internet for personal activity during work time, but regardless of the warning, several employees violated the policy and were fired as a consequence (Piscotty et al., 2016). Many companies have security concerns with cyberloafing, in addition to lost productivity (Coker, 2011).

The cyberloafing phenomenon has appeared in the health care industry regarding nurses using smartphones for personal purposes and has led to several concerns (Piscotty et al., 2016). The concerns included issues such as personal smartphone use causing patient care interruptions, contributing to possible errors, and violating the Health Insurance Portability and Accountability Act, especially when they answered personal calls during a work shift. However, a limitation of the study was the inability to determine the reasons nurses used their smartphones during working hours, as it was unclear if they were using their personal devices to contact patients. Piscotty et al. (2016) noted the need for further research to address this limitation.

Literature Search Strategy

The literature search strategy I implemented was a standard approach for retrieving information regarding (SCT), cyberloafing, cyber slacking, smartphone addiction, organizational control mechanisms, Internet use for personal activity, monitoring strategy, and security technology. Specifically, to select relevant information, I began by searching various databases for peer-reviewed articles, books, and scholarly journal articles through the Walden University library online database system and Google Scholar. The databases included Business Source Complete, EBSCOhost, *Computers in Human Behavior*, and Science Direct. The searches involved keywords related to this study, such as *Internet violation policy, Internet, cyberloafing, job satisfaction, social cognitive theory (SCT), cognition, Internet addiction, problematic mobile phone use, daily cognitive failures, self-control, self-regulation, self-esteem, workplace deviance, bring-your-own-device, privacy, monitoring, employee privacy,* and *personal web use in work contexts*. The literature review contains more than 100 sources, most of them consisting of peer-reviewed articles published in or after 2013.

Concepts on Internet Use for Personal Activity

Using the Internet at work serves as a way to increase productivity, but researchers want to study the cyberloafing phenomenon because employees' using the

Internet for personal purposes during business hours negatively affects work productivity (Hassan et al., 2015). Researchers have also focused on cyberloafing for various other reasons, such as the negative effects on network security and possible bandwidth lost (Coker, 2011), as well as the effect cyberloafing may have on the work environment, task management, and employee performance (Coker, 2011; Ugrin & Pearson, 2013).

In many situations, there appear to be no boundaries between work time and personal time (Garczynski, Waldrop, Rupprecht, & Grawitch, 2013). For example, some employers expect employees to respond to work e-mails after regular working hours; therefore, the employees think it is acceptable to check their e-mails during work time (König & Caner de la Guardia, 2014).

Karaoğlan Yılmaz, Yılmaz, Öztürk, Sezer, and Karademir (2015) confirmed that using smartphone technology during work time for personal purposes affects work productivity and wastes work time. Employees who engage in social media activities during their work time tend to be less productive than those who do not engage in social networking (Andreassen, Torsheim, & Pallesen, 2014b). However, some researchers adopted the view that cyberloafing acts as a break for employees' brains from busy workday routines and may increase employee productivity (Coker, 2011; Paulsen, 2013). Nevertheless, cyberloafing represents a threat to organizational productivity and information security, especially with online services, as it may lead to the loss of customers and an organization's reputation (Zoghbi-Manrique-De-Lara, 2012).

Most researchers agree about the negative effect cyberloafing has on work productivity and thus have focused on employees' cyberloafing behaviors and reasons that employees may engage in cyberloafing as the means to solve this problem (Wang et al., 2013). Researchers have employed different models and theories to understand human behavior related to cyberloafing, including the self-regulation model, deterrence model, theory of planned behavior, and justice theory (Harris et al., 2013; Inzlicht & Schmeichel, 2012; Wagner, Barnes, Lim, & Ferris, 2012). Researchers have also focused on *cyberloafers'* characteristics, age, and gender (Borrero, Yousafzai, Javed, & Page, 2014). Other factors that may cause cyberloafing to become an addiction include self-control, self-regulation, self-efficiency, and self-esteem (Zoghbi-Manrique-De-Lara, 2012).

Self-control. Self-control is an important part of controlling cyberloafing or smartphone addiction in the workplace (Ajzen & Sheikh, 2013). Employees with weak self-control easily engage in cyberloafing, especially when there is an opportunity to do so, whereas individuals with strong self-control tend not to practice cyberloafing, even if given the opportunity (Inzlicht & Schmeichel, 2012; Wagner et al., 2012). Additionally, the work environment has a significant effect on employee behavior regarding cyberloafing and may increase self-control. For example, an open-office design makes employees feel exposed to a supervisor. From the employees' perspective, the supervisor's proximity may represent a threat to continuing undesirable behavior, such as cyberloafing, within the organization (Karimi, Gilbreath, Kim, & Grawitch, 2014; Murphy, Wayne, Liden, & Erdogan, 2003). In general, researchers consider cyberloafing the costliest threat to organizations, and in 2005, cyberloafing became the most popular way workers could waste their time in the workplace (Gökçearslan et al., 2016).

Self-regulation. Self-regulation covers both emotions and feelings and represents a model of thoughts and behaviors applied by humans to achieve a specific goal. Self-regulation also covers feelings and thoughts related directly to addiction theory, Internet addiction, media addiction, and smartphone addiction (van Deursen, Bolle, Hegner, & Kommers, 2015). Cyberloafing is an activity that employees must avoid by practicing self-regulation and staying on task (Cheng, Li, Zhai, & Smyth, 2014). The term self-regulation refers to the individual thoughts and feelings that lead people to practice something over time (Inzlicht & Schmeichel, 2012). Past studies show that failure in self-regulation leads individuals to increase their use of social media and be at risk for addictions such as smartphone addiction (Jeong, Kim, Yum, & Hwang, 2016).

Self-esteem. In addition to self-control and self-regulation, researchers have focused on self-esteem, which includes self-acceptance, self-liking, and self-respect. A person with a high level of self-esteem tends to engage in cyberloafing to a very low degree and, conversely, a low level of self-esteem indicates a high propensity toward cyberloafing and misbehavior (Cheng et al., 2014; Köpetz, Lejuez, Wiers, & Kruglanski, 2013). Employees with a positive self-concept, strong self-control and self-regulation, and high levels of esteem perform their jobs more effectively because they have a positive view and strong motivation (Gökçearslan et al., 2016; Wang et al., 2013). Positive employees tend to follow organizational rules and Internet use codes, especially when they know they must comply with organizational policy, avoid cyberloafing, and focus on their job to maintain their positive image in front of their supervisor (Askew et al., 2014; Hertzum & Holmegaard, 2013).

Self-efficiency. Self-efficiency refers to individuals' belief in their own capabilities to control phenomena (Köpetz et al., 2013). Self-efficiency provides humans power and belief in their skills and abilities and can help people overcome their stress (Köpetz et al., 2013). Some researchers confirmed a medium level of relationship between general self-efficiency and cyberloafing (Buckner, Castille, & Sheets, 2012; Lim et al., 2002). However, others found a positive high level of relationship between general self-efficiency and cyberloafing (Coker, 2013; Köpetz et al., 2013; Ugrin & Pearson, 2013). If individuals have high self-efficacy, they have strong computer and technology skills that could lead them to participate in cyberloafing (Hosie, Jayashree, Tchantchane, & Lee, 2013).

Concepts of Smartphone Addiction

Gökçearslan et al (2016) showed that there were 4.55 billion cell phone users in the world in 2014, and 1.75 billion of them were using smartphones (Gökçearslan et al., 2016). A smartphone can be more than a communication device and affects human life in many ways, specifically allowing individuals to contact and communicate with each other easily (Lee, Chang, Lin, & Cheng, 2014). Smartphone addiction can cause many serious problems within domestic, academic, occupational, and social spheres (Demirci, Orhan, Demirdas, Akpınar, & Sert, 2014). Smartphone addiction means using a smartphone continuously and desiring to continue using it. Smartphones may cause serious health problems and push addicted users to feel stress because they did not get enough rest and continue using their phones (Borrero et al., 2014).

Smartphone addiction may contribute to academic or work problems, including students failing classes or employees' productivity decreasing (Inzlicht & Schmeichel, 2012; Wagner et al., 2012). Smartphone addiction may cause users to ignore their responsibilities, tasks, and duties and to waste their work time (Borrero et al., 2014). Also, smartphone addiction may cause users to lose the desire to stay active in work or the classroom (K. Harris et al., 2013; Kibona & Mgaya, 2015; Lanaj, Johnson, & Barnes, 2014). Smartphone addicts develop user habits, such as needing check their text messages and e-mails continuously or whenever new notifications appear on the screen; smartphone devices fully control smartphone addicts (van Deursen et al., 2015).

Health care researchers Black, Light, Paradise Black, and Thompson (2013) studied social media use through smartphones and confirmed that the health care staff studied spent 12 minutes per hour on Facebook. Social media use increased in correlation with increasing patient numbers in the hospital under study (Black et al., 2013). Many online organizations are losing their customers' satisfaction and productivity because of their employees' cyberloafing behavior (Langfred, 2013; Zoghbi-Manrique-De-Lara, 2012). Users in another study spent 74 minutes per day on the web surfing sites such as LinkedIn, Twitter, and Facebook and 81 minutes per day with mobile apps (MacCormick, Dery, & Kolb, 2012).

Borrero et al. (2014) explored social media use among college students and the ways it affects academic progress. Data came from 214 participants, and analysis took place through the lens of the unified theory of acceptance and use of technology. The results showed that students' behavior regarding social media use affected effort expectancy, social influence, and performance expectancy. Additionally, there were differences between males and females in their intent to use the technology. The findings revealed that individuals facing pressure in their life or work are more likely to use social media at the same time (O'Neill, Hambley, & Bercovich, 2014). For male students and students with self-reported high levels of technology readiness, social factors strongly influenced the relationship (Baturay & Toker, 2015; Borrero et al., 2014; Hystad, Mearns, & Eid, 2014).

Having an effective policy to restrict Internet use in organizations is important (Koch & Nafziger, 2016). Employees with high levels of reciprocity are more likely to do their work, even when the Internet is available in the workplace, whereas workers with a low-level interchange are most likely to be less productive if the Internet is active. Koch and Nafziger suggested turning off the Internet to increase employee productivity. Two options were available for employees during the study: raising wages or keeping Internet access during working time. Twice as many employees selected increasing their salary and removing Internet access compared those who selected using the Internet and reducing wages (Koch & Nafziger, 2016). Charness, Cobo-Reyes, Jiménez, Lamcomba, and Lagos (2012) suggested turning on Internet technology in the workplace and letting employees make the decision to access the Internet or not, as this could increase employee loyalty and responsibility to their work.

With a focus on the role of smartphone addiction with respect to two important factors, self-regulation and self-efficacy, Gökçearslan et al. administered an online survey and received 589 responses from students in a public university in Ankara. Participants indicated cyberloafing had a positive relationship with smartphone addiction, and there was a negative effect for self-regulation with respect to smartphone addiction. There was no effect on self-regulation and general self-efficacy regarding cyberloafing among students. The conclusion was that the pleasure provided by smartphones may lead users to become smartphone addicts and to be disruptive to others (Gökçearslan et al., 2016).

Security Perspective on Cyberloafing

Even if there is a policy in place, security tools are necessary to prevent staff from cyberloafing. Many organizations permit their employees to use their own devices, such as smartphones and tablets, to research corporate data. The employees can use their own devices to connect online without using organizational networks by using their mobile network. In this type of situation, organizational leaders need to adopt monitoring and security strategies, such as blocking websites, tracking e-mails, and reviewing browsing history (Harris & Patten, 2014).

Several organizational leaders have used a new plan to control employee cyberloafing via a personal device, data streaming, texting, and voice messages. Organizational leaders can use mobile device management systems to monitor and control nearly all functions of personal employee devices and to collect private data (Lee, Crossler, & Warkentin, 2016). Nevertheless, it is difficult to estimate the security risks faced by employees without having real knowledge about a security concept related to the information stored in their smartphones (Lee et al., 2016).

The use of smartphones in daily life and at work can lead to increased risks from attacks and breaching opportunities. Although a smartphone is personal property, employees can use it to access personal and work information according to the bring-your-own-device strategy. Many organizational leaders confirmed that using smartphones to access organizational databases reduced operating costs (Harris & Patten, 2014). However, although approximately 75% of large businesses allow employees to connect to the organization’s system from personal smartphones, many of these smartphones lack passwords or any security application that could mitigate potential risk (Harris & Patten, 2014). There needs to be a secure system to protect an organization’s information and to save working time, especially when employees connect their smartphones to the system directly or through the organization’s computer desktop. This study reveals solutions that could control or limit the use of mobile technology during work time using strategies and hardware or software technology. The findings also indicate the effectiveness of having direct communications between human resource managers, system administrators, and IT specialists regarding protecting organization systems and applying an effective mobile usage policy successfully. IT security risks continue to increase as hackers create tools to hack or breach any system not protected adequately, including smartphones, tablets, or computers. Rakes, Deane, and Rees (2012) noted a secure IT environment is critical for government institutions, and system protection becomes more difficult because attackers have more knowledge.

Thalmann, Bachlechner, Demetz, and Manhart (2014) made several points about establishing a successful Internet security policy and ensuring an organization’s system is secure. Managers must identify productivity measurement and security issues. Managers must also measure user satisfaction with the security information and Internet use policy, as users’ security awareness has a significant effect on information security procedures (Bettini, Cheyney, Wang, & Leko, 2015). Monitoring information system security is difficult if an attack is occurring. Avoiding the security risks and finding the perfect solution are also difficult. The high cost of a security system means organizational leaders might ignore the need for one, especially if they do not understand the real value of a system. Additionally, the leaders of many organizations set security as a low-priority goal and prefer to hire security services externally (Cheng et al., 2014). External security can have some negative effects, as service providers might not understand the importance and value of the information. Challenges might arise related to losing security control when applying the security system. Lastly, organizational leaders need to develop a security process along with an Internet use policy (Thalmann et al., 2014).

Security Challenges

Internet misuse in the workplace can be a significant violation of company policy because it may bring serious security and financial risks to a business and may reduce employee productivity (Andreassen, Torsheim, & Pallesen, 2014a). To ensure a company has a secure information system environment, leaders should be aware of the challenges that face the business and its security process. Managers classify the main challenges that face businesses whose leaders are building an effective security information system to control Internet use by employees during working time into three parts: (a) human, (b) organizational, and (c) technical (Thalmann et al., 2014).

Human challenges. Several human challenges face the IT security system. The first is how well the employees in an organization understand the concept of policy and information security and how they will communicate the information system effectively (Werlinger, Hawkey, Botta, & Beznosov, 2009). Human communications have an important effect on the security management process, as they can help to provide a daily security report about the security status for the system that will help solve security problems in the future. The human communication challenges are as follows:

- Lack of security training: Security knowledge is the most important factor for preventing security accidents. Security training helps employees to understand the security goals and the importance of following security and policy rules. Providing employees with the security training they need will lead to a balance between organizational needs and individual capabilities.
- Lack of a security culture: It is difficult to change the security culture in an organization. However, there needs to be privacy all the time. Many organizations' security departments have a lack of regard for the privacy of information; for instance, staff may use the same passwords in more than one department.
- Communication of security issues: It is important to maintain communications with stockholders and prevent breakdowns with stakeholders. Such communication can lead to a discussion of different security issues and an understanding of security goals (Werlinger et al., 2009).

Organizational challenges. Organizational challenges have an important effect on breaking down system security (Werlinger et al., 2009). Werlinger et al. (2009) noted the organization challenges as follows:

- Risk estimation: It is difficult to estimate the security risks to businesses without having good security knowledge, so it is necessary to have security training and good security experience. Some important points to consider when management aims to estimate the security risk include the level of user satisfaction with information security procedures and the level of user information security awareness.
- Open environment and academic freedom: It is difficult to monitor the information system if any attack occurs in an open environment. It is also difficult to limit the risks and find the perfect solution.
- Lack of budget: The high cost of the security systems might lead organizational leaders to ignore the importance of having a secure system, especially if they do not understand the real value of these systems and the losses they will experience if they ignore them.
- Security as a secondary priority: Many organizational leaders set security as a low-priority goal, especially when they outsource services or contract with external vendors. It is important for organizational leaders to set security as a main part of their strategies. It is also important to set penalties if any gap exists in security services or security software.
- Business relationships with other organizations: Each organization has a specific policy and its security rules differ from others. The conflict in security rules and policy may appear when organizations combine or merge with others or when there are differences in the security levels or security

strategies between them. Therefore, there needs to be a solution to this conflict and a shared security strategy.

- Distribution of IT responsibilities: In many cases, different departments share networks, depending on an organization's strategies. In multiple academic departments, different departments share networks, so each department assigns separate administrators to manage the department's network. The network-sharing design prevents the application of IT security controls on networks because they use a decentralized system.
- Access control to sensitive data: It is necessary to restrict access to sensitive data, especially to organizations with a decentralized system. Sensitive data need to move through different networks to stakeholders.
- Size of the organization: The size of an organization has a significant effect on managing the organization's security system. It is difficult to understand how to control an organization's security when the organization consists of multiple networks, branches, and databases.
- Top management support: Management needs to understand the importance of security systems and consider the security process a high-priority solution that will protect the organization's system effectively (Werlinger et al., 2009).

Technical challenges. It is difficult for vendors to understand organizations' requirements or needs because of the complexity of system technology and the organization's networks (Werlinger et al., 2009). An organization's networks may use different technologies to manage the data system and restrict access to network devices, such as routers, switches, and firewalls.

- Vulnerabilities and application: Network system protection is a complex task, so it is necessary for practitioners to align security updates to protect their networks by using different protection programs that provide a high level of system security for the organization's systems.
- Mobile and distributed access: It is difficult to control user access from unprotected networks, especially if users are using their laptops and smartphones without technical expertise outside the organization (at home) that might result in infections of malicious software in their laptops or smartphones during such use.
- Lack of efficient security tools: Some of the participants complained about the effectiveness of security tools. The participants noted the tools did not support the security system, and it was difficult to use them due to network scanners and intrusion detection systems (Werlinger et al., 2009).

Managers must select the right policy and security solution for an organizational system in terms of whether to use security software or hardware to limit Internet use for personal activity during work time. It is also necessary to update security software when vendors are reporting new threats and vulnerabilities. Separating staff duties and keeping staff up to date are necessary to maintain an efficient security system in an organization (Donahue & Rahman, 2012). Furthermore, leaders need to engage employees to comply with organizational policy to prevent wasting work time and protect the organizational system from viruses due to employees visiting untrusted websites. Additionally, Wilson (2012) noted a need exists to understand human behavior and then design a high-security system for it. Leaders of corporations can use different security strategies to protect their systems against insider threats.

Users' experience has a significant effect on designing security control strategies. Users' experiences come from having worked at a job site for an extensive amount of time and are helpful for determining the privileges to access a system or applications (Spears & Barki, 2010). The information collected regarding organizational security requirements came from organizations or business users. Many organizational leaders set their policies regarding Internet use during work time according to their business mission and ask employees to follow the rules blindly without explaining the benefits from complying and the risks for violating the security policy (Donahue & Rahman, 2012). Involving users in the security process increases their awareness of the vulnerabilities and makes them aware of sensitive information, so the security process will help protect the system and make it more secure (Donahue & Rahman, 2012).

Donahue and Rahman (2012) reported different levels of security training for users, managers, patients, and IT and information assurance. Providing the information assurance team with different training courses creates a secure information system. Furthermore, Donahue and Rahman confirmed that using security risk management is an effective strategy for facing security challenges and policy violations.

To select an effective security policy for an organization, it is important to identify the quality of the information that already exists in the system and the risk that will result from losing this information (Donahue & Rahman, 2012). Managers must know how to apply effective security control strategies to protect the information. The security control process should reduce security risk and protect system information. Selecting the best security control depends on the level of data sensitivity, and the security control selected should be compatible with the mission and objectives of a business (Donahue & Rahman, 2012). Viruses, worms, and other malware; data leakage; phishing; pharming; identity theft; malicious attacks; and software bugs can lead to security incidents (Ng & Rebeiro, 2010).

Although organizational security is the responsibility of everyone in a business, it is the main responsibility of senior managers. Specifically, the responsibility of senior managers is to keep information private and support the security process. Senior managers are also responsible for ensuring the staff complies with security policy, laws, and regulations to protect information privacy (Donahue & Rahman, 2012). The most effective way to avoid different security threats is to manage the threats efficiently instead of ignoring them. The managers need to observe, monitor, and report the system status at all times and try to determine the security gaps. Company leaders must create an intermediate layer between human–computer interfaces and management. Company leaders cannot rely on security technology only to face security risks, so it is better that they combine security technologies and social-organizational resources as an effective security strategy (Král, 2011). Leaders also need to balance system security to ensure information privacy and have a good level of monitoring for their systems. Company leaders must ensure there is no gap or vulnerability in their monitoring systems or the system could break down completely (Král, 2011).

The most popular procedure or strategy for ensuring a secure environment is the monitoring strategy, which involves monitoring employees' activities to prevent them from committing any violations or misusing an organization's resources (Dhillon, Samonas, & Etudo, 2016). Another effective security strategy is to enroll users into a security risk management system to improve the security process and thus reduce data breaches. Security risk management is a system that includes policies, strategies, rules, procedures, and the people managing the security risks. Enrolling users in the security process and providing them perfect security information is an effective security strategy to protect the information system for a business (Dhillon et al., 2016; Spears & Barki, 2010).

Werlinger et al. (2009) reported that many security incidents occur because of flaws in the software. A software patch that comes directly from a vendor may include more than 20,000 flaws per line (Werlinger et al., 2009). Consequently, there is a need for a set agreement with vendors and a need to establish penalty conditions if employees find any defects in the security products later. An assessment of the current business security system is necessary to decide the appropriate security tools to use to protect the system. For example, performance system management can be an effective way to evaluate the security level of a business system. Performance system management involves monitoring business goals and performance as well as evaluating the security level of an information system. Changing to router access control lists to ensure a system is secure is an effective security solution for many organizations (Humphreys, 2008). The leaders of many government and commercial companies use the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) standards as an optimal security choice because they share a common language for the leaders of all company types to implement their information security system. Lastly, the separation of duties is necessary to gain an effective security system and prevent security errors and fraud. Leaders should distribute security duties and privileges among multiple users according to business needs (Donahue & Rahman, 2012).

Management responsibilities should involve reviewing and monitoring the security management process to avoid security risks, as this is one of the most effective strategies (Dhillon et al., 2016). Furthermore, there needs to be positive feedback. Positive feedback can include a reward system for all business activities, such as a recording system and network use, risk reports, handling of incidents, security issues, network weaknesses, and security gaps, and a plan for development (Dhillon et al., 2016).

Information assurance should include an effective security policy to protect sensitive data with a complete guide that helps users to protect information efficiently (Donahue & Rahman, 2012). Information assurance should also include a model for policy direction and details of the laws, benefits, and penalties of compliance or noncompliance to company policy, which will support the efficiency of business system security. A need exists to identify the security risk and threats, set the security policy, and provide an assessment. It is also important to monitor user compliance to the security challenges and security risks based upon the knowledge and awareness of security risks that come from users' training and education (Donahue & Rahman, 2012).

The cost of security control is a crucial factor, so there is a need to calculate the cost effectively and evaluate the quality of the information that needs protection to ensure information confidentiality, integrity, authentication, and availability (Donahue & Rahman, 2012). The optimal security control selected and implemented will protect information according to a specific security plan that is compatible with the business purposes of a company. Furthermore, a secure configuration and assessment for the system is necessary. The assessment serves to ensure whether the security control is achieving its objectives and if it is cost effective. A system that receives approval has authorization for use and the leaders trust the security features (Donahue & Rahman, 2012).

Using multiple security tools to protect the same system will decrease opportunities for breaches and will help to cover security defects or weaknesses in software by using additional software or hardware that does not have the same gap or defect. However, the need exists to check the positive and negative security features for each security software or hardware and then to cover the negative points by combining the current software with another software or hardware that does not have the same weakness (M. Harris & Patten, 2014). For example, many government departments and commercial companies use the ISO/IEC standards as the optimal choice for providing effective security specifications for a system, as ISO/IEC is a general security language for all company types (Humphreys, 2008). The ISO/IEC standards can help to handle insider threats that would cause vulnerabilities in an organization’s system, as it is important to achieve balance in information security systems and to have a good level of monitoring for changes in the system and security risks (Král, 2011). In many cases, employees have authorization to access the system, but they use the information for unauthorized or illegal purposes. The surveys conducted indicated 35% of security problems in the United States and the United Kingdom were about insider threats, such as fraud (Humphreys, 2008). These threats are a serious problem and may have a negative effect on businesses (Humphreys, 2008). Leaders must check candidates’ backgrounds before providing security assignments, as the leaders need to know if an employee has any criminal intent that might lead to the destruction of the information system or cause the employee to sell information to competitors (Spears & Barki, 2010).

Cyberloafing and Data Breach

Another important issue in this study was data breach consequence policy violation and poor system protection. To manage security risks, it is necessary to determine the cost of security breaches. Methods used to calculate data breach costs include calculating the long-term and short-term costs, as well as the tangible and intangible costs (Humphreys, 2008). Some of the estimated data breach cost methods depend on the market value or the market theory. Leaders need to analyze vulnerabilities to manage security risks by using different tools that depend on the situational details and causes of risk (Dhillon et al., 2016). Managing security risks involves transferring technical tools to engineering managers to provide a more secure environment (Humphreys, 2008).

A risk assessment indicates the probability of risk occurring and how much harm it may do to a business system (Humphreys, 2008). The aim of risk assessment is to identify the risk and the level of damage to a company. Some security risks affect some parts of a business and others may affect several companies, but both lower customer confidence. Therefore, leaders should have different strategies and techniques to cope with security risks.

Leaders may use many active security tools to reduce security risk, such as firewalls, antivirus systems, or a complete security policy such as blocking ports (Humphreys, 2008). Transferring security responsibility to outsourcing services or insurance agencies is an effective security risk management strategy within the right conditions and with solid agreements. Accepting the security risk as part of the investment and deciding on a specific budget for security issues is also important. Furthermore, it is important to select which security level is necessary for a business and to realize no system is fully secure. Thus, identifying a security level for a business system is one of many difficult tasks. Before choosing any security tools, it is necessary to understand the security situation and estimate the data value in the system. Data protection tools must be effective and should not cost more than the cost of data breaches (Cullinane, Bosak, Flood, & Demerouti, 2013).

Rakes et al. (2012) developed a model to block or mitigate security attacks. The model, when examined with respect to the most widespread threats and worst security cases, indicated that the security environment is a top concern for leaders of corporations and government entities. Breaches are significant problems for business leaders and have a catastrophic effect on them. Rakes et al. “developed a model for optimally choosing countermeasures to block or mitigate security attacks in the presence of a given threat level profile” (p. 1).

Rakes et al. (2012) examined the 2010 *Data Breach Investigations Report* prepared by the Verizon Business RISK Team and the U.S. Secret Service, submitted 47 threats they considered the most significant security threats, and posted a larger problem in their research that consisted of 50 threats with the remaining one accounting for less than 1% of breaches and affected records. The purpose of the study was clear, and Rakes et al. explained the problem adequately. However, while the results might be helpful in developing a framework for security systems, there was no real problem in the study and no data for the survival matrices.

Spears and Barki (2010) focused on the effect of security awareness for the staff on the development of organizational security control by examining the effect of user participation on the development of IT security risk management. The tools used to collect data were questionnaires from 228 professionals with experience in IT risk management. Spears and Barki examined the “user participation in information systems security risk management and its influence in the context of regulatory compliance via a multi-method study at the organizational level” (p. 500). Nine semistructured interviews took place with representatives from five companies in three industries. The first set of interviews was with a senior risk officer, a risk manager, and a deputy chief information security officer at a large national bank. The second set of interviews was with internal audit and information systems managers at a manufacturing firm. The third set of interviews was with a financial comptroller, internal audit director, and information systems director at another manufacturing company. The final set of interviews was with managers of accounting and internal audits at a third manufacturing company (Spears & Barki, 2010).

The development of the model was successful, and the research results indicated that the participants had a positive effect on improving security control (Spears & Barki, 2010). The interview data showed an alignment between information systems security risk management and the business environment. Furthermore, the participants added value to the IT security management system. Nevertheless, a review of the literature indicated that users have a weak link in IT security system development, but the findings in Spears and Barki's (2010) research revealed the inverse: users may have a strong effect on developing IT security systems through their working business knowledge. The qualitative and quantitative findings indicated the users' awareness of security risks and controls improves control development and performance (Spears & Barki, 2010).

Spears and Barki (2010) confirmed the positive effect of users on developing IT security systems. The efforts in the study contributed to developing a security model. However, the research had several limitations, including an inadequate sample, because it included only people in the United States. Also, the research result did not include the level of security knowledge of the participants. Another important limitation related to the weak responses to the study questionnaires and the answers did not fit the target (Spears & Barki, 2010).

Lajevskis, Dorogovs, and Romanovs (2009) provided several recommendations for achieving the maximum-security awareness, such as training administration specialists or technical staff to face security threats. Although Lajevskis et al. defined the development of the IT security system in precise steps, they did not include the technological process. The technological process should include a description and demonstration of what would happen in each phase of the process, and the lack of this information was a limitation of the research. Hence, the current study includes recommendations about making critical decisions to create a safe environment for a business's information system. The study findings could also lead to starting or maintaining effective communication rules between IT specialists and human resource managers to ensure the application of some effective tools to limit Internet or mobile use for personal activity during work time.

Cyberloafing Controlling Mechanisms

Because cyberloafing connects to the many negative effects on employees' productivity, researchers tend to focus on understanding human behavior related to cyberloafing and the reasons employees engage in cyberloafing using various social theories to explain this phenomenon (Richards, 2012). Wang et al. (2013) noted cyberloafing affects employee productivity and increases security threats. Hence, managers use several mechanisms to control cyberloafing, including organizational control, prevention strategies, and monitoring strategies (Piscotty et al., 2016).

Organizational control mechanism. Organizational control has an association with terms such as managerial control, system control, policy control, and behavior control and represents the possible procedures used to control employees' behavior and engage them to comply with an organization's policies and goals (Piscotty et al., 2016). Employees generally comply with organizational rules and policy when managers force them to do it and when the employees realize there are punishments in place. This strategy depends on employing various types of formal punishments and applying these punishments to employees who violate the rules. If employees realize there is a punishment in place and that punishers will practically apply it to others who commit or violate organizational policy, they will try to avoid repeating undesirable behavior (Piscotty et al., 2016). Leaders can control or minimize employees' undesirable behavior by making them expect various formal punishments if they continue cyberloafing during working hours. Although there need to be effective strategies to control cyberloafing in the workplace, including a control strategy and punishment strategy to control the cyberloafing phenomenon, supervisors must be near the employees, understand their behavior in depth, and monitor and apply punishments if any violations happen (Piscotty et al., 2016).

Kidwell (2010) focused on cyberloafing in the workplace and the ways it can lower job efforts by considering (a) low-cost operators, (b) global competitors, and (c) high-involvement firms and the ways they relate to each other. Cyberloafing hides lack of effort in a virtual team; therefore, Kidwell proposed a model to examine the cyberloafing phenomenon and the ways a work ethic and a leisure ethic could improve the productivity and creativity of the job. Kidwell indicated that the monitoring software was able to control the keyboard, the Internet, and e-mails. Also, the software could track virtual teams' steps by saving images that appear on employees' screen, games, or chatrooms, as well as e-mails sent and received. Organizational managers can use software for controlling and monitoring. Using such software may create trust issues among some employees, but it does lower operator costs (Kidwell, 2010).

Kidwell (2010) submitted alternative methods for managing and controlling cyberloafing during work time. Setting an effective policy related to Internet use is important for employees to have clear rules related to using an organization's computers for personal purposes. Internet policy restriction is efficient, especially when applied to coworkers and employees at the same time (Kidwell, 2010).

Prevention strategy. Many companies adopt a strategy to control employees' policy violations (Eivazi, 2011). The prevention strategy is important for deterring employee policy violations. Using preventative technology may help with growing a business, but the technology could cause business owners to lose their reputation and customers due to employees' misuse of the technology in the workplace (Eivazi, 2011).

Organizational leaders should follow several steps to start an effective prevention strategy. The first step is to ensure the online policy includes clear points related to an organization's rules and policies (Glassman, Prosch, & Shao, 2015). It is difficult for employers to estimate the risks faced by employees without having real knowledge about a security concept. Therefore, there needs to be training for managers regarding knowledge of security risks and threats possibly associated with violating organizational policy (Drouvelis & Nosenzo, 2013; Bartariya & Rastogi, 2016). Employees also need to have security training and experience in this area before they can identify the risks from using an online service in the workplace (Glassman et al., 2015).

Electronic monitoring strategy. One study conducted in the United Kingdom showed that computer users spend an average of 31.4 hours per month Internet browsing and 5.4 hours using their mobile devices for web browsing (Ofcom, 2015). The same report indicated that people use their smartphone 61% more than their desktop computer, as smartphones provide people the freedom to surf wherever and whenever (Ofcom, 2015). However, despite the many advantages related to using e-mail and Internet tools, misuse at work has created new financial and legal challenges for employers (Piscotty et al., 2016). Employers have many concerns regarding the misuse of online services from their employees and therefore tend to adopt an electronic monitoring strategy to protect their business interests and minimize or prevent potential risks to online services at work by employees (Piscotty et al., 2016).

Some concerns related to the misuse of employees' personal information when employers monitor their employees' Internet activities include employee data storage and the retrieval of the data for review from time to time to ensure the level of employee productivity as well as to avoid any financial liability that employee misuse of an Internet monitoring strategy may have in terms of changing the work environment and worker behavior (Gökçearslan et al., 2016; Wang et al., 2013). Additional concerns center on the prospect of making employees feel uncomfortable, even though organizational leaders have the right to monitor employees when they are using organizational resources, such as computers and devices (Glassman et al., 2015). Sarpong and Rees (2014) focused on the big-brother effect in the workplace. The qualitative study involved exploring any fears, discomfort, and stress caused by using a monitoring system during working hours. Managers can use monitoring systems to have an overview of their employees' activities during work hours. In Sarpong and Rees's (2014) study, the 73 managers and nonmanagers who participated in this study confirmed that they did not have any concerns regarding the electronic monitoring strategy.

Organizational policy should include discussing the monitoring system with employees before applying it. Employers can block websites, monitor e-mails, and retrieve browsing histories; however, monitoring personal mobile devices has two opposing views (Glassman et al., 2015). One view is an employer's right to monitor employees' use of personal devices, especially for measuring job performance and protecting organizational data for security purposes (Glassman et al., 2015; Kidwell, 2010; Lee et al., 2016). Another view is employees' right to reject a monitoring strategy that includes their own devices because the aim of monitoring is to control and monitor employees' personal data (Lim et al., 2002).

A monitoring strategy is a control mechanism used to control or monitor employees' information during working hours. Controlling employee information privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Lee et al., 2016, p. 5). However, the agreement needed is a contract between employees and organizational leaders that serves as confirmation of employees' acceptance of a monitoring strategy and relinquishment of their mobile privacy to their organizational leaders (Glassman et al., 2015; Kidwell, 2010; Lee et al., 2016).

A monitoring strategy may save work time and improve job performance (Carnevale & Smith, 2013). The foundation of performance expectancy is the adoption of a specific technology that will improve job performance, as organizational leaders must monitor and control personal devices to keep organizational data safe and to save work time (Carnevale & Smith, 2013). However, a balance is necessary between the monitoring system and employee privacy (Lee et al., 2016).

In contrast, Glassman et al. (2015) focused on analyzing the countermeasures of cyberloafing by using a multitheoretical perspective to explain the phenomenon. Glassman et al. discussed a monitoring and filtering strategy as a solution to the problem and noted that a control plan alone is not an effective way to control cyberloafing, as there needs to be an effective Internet use policy signed by the employees that confirms their understanding of the policy, rules, and consequences for violating the current policy. Glassman et al. recommended using several factors, including various justice avenues and social norms, to support compliance with an Internet use policy. Other factors that may affect employees' reactions to the cyberloafing phenomenon include an organization's Internet use policies, user training, culture, and managerial orientation (Glassman et al., 2015).

Summary and Conclusions

The most common issue researched with respect to non-work-related Internet use is productivity loss. Thirty to 40% of lost worker productivity is due to web surfing, which costs U.S. employers more than $50 billion yearly (Saraç & Çiftçioğlu, 2014). Therefore, selecting the right security solution for an organizational system, whether security software or hardware tools, is important to limit Internet use for personal activity during work time. It is also necessary to update security software when vendors report new threats and vulnerabilities. Separating staff duties and keeping the staff up to date are necessary to maintain an efficient security system in organizations (Saraç & Çiftçioğlu, 2014). Leaders need to engage employees to comply with organizational policy, prevent wasted work time, and protect organizational systems from visits to untrusted websites (Piscotty et al., 2016).

This chapter included an overview of cyberloafing and smartphone addiction and the ways they affect employee productivity. The literature reviewed on cyberloafing and social cognitive theory (SCT) comprised a sound basis for this study. The chapter also included an in-depth literature review to support this study. This study fills the gap in the literature. Organizational leaders in business organizations had not found a reliable way to limit or monitor employees' personal use of the Internet through their smartphones or personal tablets while on the job (Saraç & Çiftçioğlu, 2014). Chapter 3 includes the purpose of the study, details of the role of the researcher and participants, research method, research design, data collection, data organization, issues of trustworthiness, ethical procedures, and a summary.

Chapter 3: Research Method

The purpose of this qualitative phenomenological study was to explore reliable ways for organizational leaders to monitor or limit their employees' use of smartphone technology for personal use while on the job. In addition to wasted work time, other major organizational concerns are security threats, policy violations, and the misuse of the Internet during work time, especially when employees use their smartphone and connect to the organization's Internet system, thereby increasing the risk of viruses from visiting untrusted websites. Chapter 3 includes the research design and rationale; the role of the researcher; information about the participants; research method; data collection; data organization; pilot study; data analysis plan; and issues of trustworthiness that include credibility, transferability, dependability, and confirmability. Additionally, this chapter includes a discussion of the ethical procedure for the study. The focus of Chapter 3 is on the controlling strategies in the literature that organizational leaders may use to control personal Internet use by employees on the job.

Research Design and Rationale

For this study I used a qualitative research methodology with interviews to shed light on the research problem. Qualitative research involves making a connection between a story and ideas that develop at a site. Researchers can use different methodologies to conduct a study on the same topic to enhance validity and reliability (Hayes, Bonner, & Douglas, 2013; Maxwell, 2013). The participants included frontline supervisors, human resource managers, and IT managers and specialists. The responses to the interview questions helped me gain insight into the following central research question and the subsequent subquestions: How can managers minimize wasted work time by limiting the personal Internet activity of employees who use personal mobile devices while on the job?

RQ1: What effective strategies can managers use to ensure employees are not wasting work time by cyberloafing and sending text messages from their personal mobile devices?

RQ2: How can managers prevent authorized employees from unauthorized access of an organization’s database system?

RQ3: How effective are disciplinary plans designed to punish employees for computer-use policy violations in changing employees’ behavior and increasing their commitment to organization policy?

RQ4: How effective are the technology tools that limit or monitor employees’ Internet use through their mobile devices while on the job.

Role of the Researcher

It is important for researchers conducting interviews to understand the human instrument. To collect data correctly, researchers must have certain skills. For example, researchers need excellent communication skills to conduct interviews to collect data and must be able to structure the questions clearly and effectively to maintain a relationship with the participants (Marshall & Rossman, 2015). Researchers also need to be able to establish rapport with the respondents using humor and humility (Maxwell, 2013). Furthermore, interpersonal skills are important for researchers conducting interviews and collecting data, as sometimes they must ask probing questions to understand an issue

(Marshall & Rossman, 2015). If a question makes a respondent feel uncomfortable, a researcher needs to change the question and try to obtain the same answer in a different way to make the participants feel comfortable (Maxwell, 2013).

Another important issue was how I managed my relationship with the participants during the research study. For example, if I were to conduct research in my company or with someone I have a relationship with, I would need to inform the readers about that relationship. It is important that researchers not exploit their job position or relationship with participants to obtain information without permission from the site owner or the manager (Maxwell, 2013). Researchers must control any negative feelings toward participants and avoid any bias or assumptions before conducting interviews. Researchers can solve issues of bias easily by using member checking during the data collection process to serve as a second set of eyes and ears for the researcher. Member checking is a technique used to clarify the accuracy of data collected from participants during an interview. Bias may exist for different reasons, including experiences related to specific cultures or situations, and member checking is an appropriate way to avoid bias (Maxwell, 2013). Member checking serves to verify the accuracy of data interpretations and minimize researcher bias (Houghton, Casey, Shaw, & Murphy, 2013). I sent participants an invitation by e-mail to conduct a member check, so they could review my interpretation of their responses, correct any mistakes, and ensure the accuracy of the information.

Finally, researchers must be objective and understand their role as a researcher. Researchers who cannot be objective on one topic must find another topic in order to avoid distorting the facts. I wrote a brief introduction of the study and submitted it to the participants, so they would understand the aim of my study and the reason I was conducting the research. Participation was voluntary, and there was no coercion to participate. The participants could withdraw from the interview at any time without penalty. Also, participants' names and contact information remained in a secure place to protect their privacy.

Methodology

Qualitative research methodology is a way to transform the world through a sequential process that includes interviews, conversations, recordings, and writing memos to self (Korhonen, 2014). The focus of qualitative phenomenological research is recording the everyday experiences of participants as they relate to a phenomenon (Moustakas, 1994). The strength of the qualitative methodology was my use of interviews to formulate a deeper understanding of the phenomenon. The use of open-ended interview questions is appropriate to qualitative research, as researchers can interpret a phenomenon by talking directly to people involved and observe their behaviors, actions, and face-to-face interactions over time (Maxwell, 2013). The rest of this chapter includes a rationale for participant selection, instrumentation, recruitment procedures, and issues related to ethics and trustworthiness. The focus is on providing details so other researchers can duplicate or extend this research. This chapter also includes an overview of the data analysis process.

Participant Selection Logic

Researchers must select a sample correctly and ensure it relates to the study and adds value to the research (Koning & Waistell, 2012). This study included interviews with 20 individuals who were frontline supervisors, human resource managers, or IT managers and specialists from two U.S. industries: education and telecommunications. I selected a small sample size related directly to the phenomenon under study, as Maxwell (2013) noted that the sample for qualitative studies should be between five and 25 interviewees.

I used a purposive sampling strategy to select a sample consisting of frontline supervisors, human resource managers, and IT managers and specialists, all with least 2 years of experience in the field, because these participants would understand the research problem and add value to the research. Researchers conduct phenomenological studies to provide a deep understanding of a phenomenon, but must carefully select participants who have experienced the phenomenon to fit the sample requirements (Steelman, Hammer, & Limayem, 2014). Sample selection also depends on a researcher understanding the phenomenon and the specific criteria that relate to participants' education and experience (Trotter, 2012; Walker, 2012). Frontline supervisors and human resource managers were suitable because they had experience with established policies, rewards, and legal punishments, as well as knowledge about staff behavior toward organizational policies and whether employees comply with or violate the policies. The IT managers and specialists were suitable because of their knowledge and experience with strategies used to control or limit Internet use and could therefore provide appropriate information related to selecting the best software or hardware to deter cyberloafing by employees.

Individuals in a selected sample must have in-depth knowledge and experiences with the phenomenon under study, and researchers can stop conducting interviews when saturation occurs (Petty, Thomson, & Stew, 2012). Saturation can occur after 10 interviews, but researchers should continue the interview process until three interviews do not add any value to the research (Francis et al., 2010). The interview process should continue until data saturation occurs, which ensures the quality of the outcomes (Onwuegbuzie & Byers, 2014). Saturation takes place when no new information or evidence can add value to the research (Fusch & Ness, 2015; Onwuegbuzie & Byers, 2014). To ensure saturation, I continued past 10 until I conducted 20 interviews.

Instrumentation

In qualitative studies such as this one, the primary instrument for collecting, analyzing, and coding the data is the researcher (Condie, 2012; Pezalla, Pettigrew, & Miller-Day, 2012; Sarker, Xiao, & Beaulieu, 2013). Data collection involved using Skype, e-mails, or phone calls interviews. I used a sensitive microphone to make audio recordings of the interviews. Audio recording provided enough time to focus on the participants' answers and listen to them adequately, as well as to write some comments about the interviewees' behavior during the interview. The observation method is beneficial to researchers because they can note how the participants behave directly and can interpret their attitudes or behaviors (Bernard, 2013).

For this study, I used a semistructured method to conduct interviews because this method provides rich details related to a phenomenon and engages participants, so they feel comfortable sharing their experiences freely (Marshall & Rossman, 2015). The interview protocol consisted of open-ended questions that included subquestions related to limiting or controlling cyberloafing while on the job.

The data collection process requires a good relationship between the researcher and the participants to collect the data from the interviewees (Aguirre & Bolton, 2014; Comi, Bischof, & Eppler, 2014). The relationship between the interviewer and the interviewee needs to be opening to allow free dialogue between both individuals regarding the research problem (Collins & Cooper, 2014). Researchers must collect data from the participants through free discussions in questioning, interpreting, and reporting. Furthermore, researchers must avoid being a receiver in terms of only collecting the data or making the participants a source for the data (Collins & Cooper, 2014). It is better to collect the data in different ways to ensure the data are reliable and to develop the research theory (Camfield & Palmer-Jones, 2013).

Setting an exact time to conduct interviews and informing the participants how long interviews will take are important aspects of the interview process. For this study, the length of the interviews depended on participants' discussions, but interviews were no longer than 60 minutes. I offered a safe and comfortable environment to the participants and was flexible with my questions during the interviews. Furthermore, the participants chose the interview place and time.

Procedures for Recruitment, Participation, and Data Collection

The study involved searching for potential participants using the LinkedIn search tool. I listed specific requirements for the candidates, which included having at least 2 years of experience in the human resources or IT field and having at least a bachelor's degree in human resources or a technical certification in IT, and then I reviewed the prospective participants' profiles. If they matched, then I sent an invitation to connect. Interested individuals needed to contact me via e-mail, through LinkedIn, Skype, or by phone. I used screening questions to verify that prospective participants were working within educational or telecommunications institutions in a managerial role and had done so for a minimum of 2 years. Those who responded affirmatively to the screening questions received an informed consent form to sign and return prior to scheduling the interview. I provided a consent form and the interview questions to the participants before starting the interviewing process (see Appendix A). Upon receipt of the signed informed consent form, the potential participant chose the format of the interview (phone, Skype or face-to-face) and scheduled it. Additionally, participants received open-ended questions through mail or e-mail to prepare for the interview.

This study included a semistructured method to conduct Skype, or phone interviews with frontline supervisors, human resource managers, and IT managers and specialists. A semistructured approach can provide rich details related to a phenomenon, and researchers can engage participants to share their experiences freely (Marshall & Rossman, 2015). The focus of the unstructured approach is the phenomenon, and researchers aim to achieve generalizability and internal validity and may obtain specific results and determine local causality (Maxwell, 2013). Each interview took approximately 30 minutes, but some were longer if the participant agreed. Participants received a reminder prior to beginning the interview that they may refuse to answer a question or stop the process at any time without question or consequence. Participants also gave permission to record the interview prior to beginning the interview. I digitally audio recorded participants' answers using Dragon Naturally Speaking voice recognition software and took notes during the interviews to ensure accuracy.

At the close of the interview, after recording had stopped, I asked the participants to forward my contact information to anyone who may be interested in participating in the study. Such snowball sampling can serve as a way to recruit more participants (Maxwell, 2013) if the initial response does not lead to a sufficient number of participants. After the transcripts were complete, the participants received a copy of their interview by e-mail or mail for member checking. Upon return of the participant-approved transcripts, the next step was to download the data to a secure file on a password-protected computer for analysis. I used My Cloud or Mirror Cloud to save the data, as they had a security feature that would not allow others access to the data.

Data Analysis Plan

New knowledge results from accurate data and by following the protocol of data analysis and validating data sourcing (Yin, 2014). Member checking is the best method to enhance the validity and accuracy of a study (Bekhet & Zauszniewski, 2012). Researchers use the member-checking strategy to interpret data, identify themes, and validate results (Denzin & Lincoln, 2011).

Accuracy is a significant factor in research, so analyzing data critically is important. Immediately following each interview, I listened to the recorded data carefully and transcribed the voice responses verbatim for later analysis using Dragon Naturally Speaking voice recognition software. Mistakes may occur from using a voice recognition program; therefore, reviewing the recording and transcripts repeatedly and correcting any errors is important, as is noting the tone of the participants.

Because peer review can be an important role in research, particularly with respect to analyzing, organizing, interpreting, and coding data (Lawrence & Tar, 2013), I used software programs for analyzing and coding the data to ensure a high degree of accuracy. Using NVivo qualitative software also led to a new theory derived from the data instead of following the grounded theory guide. I used the software's auto-coding features to code data, derive themes, and compare themes.

To organize the data, I used a matrix with several fields, including participant names, coding, questions, answers, position, comments, added value, corporation, themes, subthemes, emergent themes, and participant suggestions. I used different strategies to analyze the data, including manual data manipulation, data analysis computer program, word processing, and electronic spreadsheets. I also used data reduction processes to narrow the data collected before starting the coding process. Determining word frequency reveals similar answers related to the same question to organize themes (Folta, Seguin, Ackerman, & Nelson, 2012). The interview protocol supported social cognitive theory (SCT), as the study involved collecting data from the participants and analyzing the data based on the three important factors: (a) self-control,

(b) self-regulation, and (c) self-esteem. Member checking helps to ensure correct data interpretation and to avoid bias (Grossoehme, 2014; Harper & Cole, 2012).

Issues of Trustworthiness

Credibility

Credibility refers to internal validity and whether the instruments employed achieved what the researcher intended (Guba & Lincoln, 1994). Trustworthiness is another way to validate data, and establishing the trustworthiness of a study is important to ensure credibility (Lehmann-Willenbrock, Grohmann, & Kauffeld, 2013). Therefore, it was necessary to use the qualitative research method to identify a specific line of questioning to collect the data effectively, without misunderstanding. I identified the sequence of the questions and organized them to collect the data to solve the research problem. In the interviews, I asked the questions clearly and used simple words to help the participants understand.

Transferability

Transferability refers to the ability to apply the result of a study to other settings to assess external validity (Guba & Lincoln, 1994). I selected participants who could provide data to solve the research problem. The three types of participants who helped to find a solution for the problem were frontline supervisors, human resource managers, and IT managers and specialists. Frontline supervisors described the behavior of employees related to the cyberloafing phenomenon during work time based upon their direct contact with the employees. Human resource managers provided evidence related to employee violations of the Internet control policy and ways to handle such violations. IT specialists or managers helped identify the appropriate technology, including hardware, software, or both, to control cyberloafing during work hours. The participants must have at least 2 years of experience in their field. Future researchers may be able to use the results of this study and apply them to other institutions.

Dependability

Dependability means researchers can use the alternative to assess reliability and trustworthiness (Guba & Lincoln, 1994). The two strategies that affect the dependability of a qualitative study are member checking and triangulation (Guba & Lincoln, 1994). Triangulation involves comparing data from interviews and documents provided by participants (Denzin, 2012). In this study, I used the member-checking technique to achieve credibility. For the member-checking process, participants can review the transcript of their interview to correct mistakes or include additional information (Houghton et al., 2013).

Confirmability

Confirmability is a way to achieve reliability and trustworthiness that refers to the neutrality of findings (Guba & Lincoln, 1994; Tufford & Newman, 2012). My strategy was to establish confirmability using memos, field notes, and transcripts. It was my responsibility to interpret the data responsibly and accurately and to enhance confirmability by reflectively journaling during the study as well as by connecting the data with the literature review. Yin (2014) stated there needs to connect the data, literature review, conclusion and findings to enhance the confirmability.

Ethical Procedures

A design and plan regarding ethics issues are necessary to conduct research. Ethical issues can arise when collecting data from participants. Researchers must respect participants' privacy, keep their personal information private, and keep their answers secure and safe. Researchers should code participants' names and places of employment (Pollock, 2012). The participants had the right to withdraw from the research at any time. Any participants who withdrew from an interview would have received the notes and the record related to their interview, as well as any documentation they submitted. I e-mailed the consent form with the interview questions to the participants to give them an idea about the research study and to obtain written permission to conduct the interviews. The participants and I signed the consent forms. Further, data collection took place in a way that did not exploit the participants.

The research did not begin without first receiving written permission from the participants. I explained the aim of this research and potential benefits. A brief proposal submitted to the participant provided a complete perspective of the research. Additionally, I obtained Institutional Review Board (IRB) approval prior to collecting data, and I complied with the IRB rules and policies of Walden University.

In the reporting stage, it was important to be honest in the inquiry, not to plagiarize other works, to keep the information about the participants safe, and not to publish something that may harm the participants. In the publishing stage, I protected the information related to the participants by masking their names, jobs, and places of employment. Using a coding strategy protects the identity and privacy of participants.

The data organization tool was a critical component in this study. The data remained in a separate and secure place. A separate storage device helps to protect data if a researcher's computer crashes (Lohle & Terrell, 2014). My Cloud or Mirror Cloud was suitable for storing the data. These methods are effective ways to store data because the data remain within a personal cloud (Unluer, 2012). Each participant's data remained in a separate folder coded by an alphanumeric code such as HRM-P1, AMU-P2, ITM-P3, and so on.

Summary

Chapter 3 included an explanation of the quality indicators and research activity for this study. The research method selected was a qualitative phenomenology. The open-ended questions were suitable for obtaining a solid and complete interpretation of the phenomenon. This chapter included a discussion of my role as the researcher on developing a rapport with the participants and the ethical procedures used to collect the data from the participants, which included obtaining agreement from the onsite owner to conduct the research. The chapter also included the process for selecting the participants, the number of participants, the interviews steps, and a description of the consent form that participants signed before starting the interview process. Additional topics discussed were ways to keep participants' information safe, how to protect participants' privacy, and issues of trustworthiness.

Chapter 4: Results

Introduction

The purpose of this study was to explore ways to limit the amount of personal Internet activity (cyberloafing) employees use through their personal smartphones while on the job, not only to minimize wasted work time, but also to prevent potential viruses from infecting company information systems as well as compromising confidential files. This chapter includes the data analysis of the study, organized into the following descriptive sections: (a) introduction, (b) research setting, (c) demographics, (d) data collection, (e) data analysis, and (f) qualitative results. The section on the setting includes a description of the participants' education level and experiences that explain the reasons for their selection. Also included are the interview environment, demographic data, interview and data collection timeline, and unexpected circumstances experienced during data collection. Data analysis includes the data gathering approach, reaching saturation, and in vivo and descriptive coding method. Data analysis also includes the evidence of trustworthiness. The qualitative results section includes a description of the research question results through emergent themes, categorical findings, and theoretical results. The general research question was as follows: How can managers minimize wasted work time by limiting the personal Internet activity of employees who use personal mobile devices while on the job?

The following were the research subquestions:

RQ1: What effective strategies can managers use to ensure employees are not wasting work time by cyberloafing and sending text messages from their personal mobile devices?

RQ2: How can managers prevent authorized employees from unauthorized access of an organization’s database system?

RQ3: How effective are disciplinary plans designed to punish employees for computer-use policy violations in changing employees’ behavior and increasing their commitment to organization policy?

RQ4: How effective are the technology tools that limit or monitor employees’ Internet use through their mobile devices while on the job?

Research Setting

The participants held managerial roles in IT, human resources, and administration in educational and telecommunications organizations in the United States. Several participants held management and IT positions in educational and telecommunications organizations in and outside the United States. Some of the participants held Project Management Professional (PMP) certification or IT security certification. Potential education and telecommunications participants received invitations through LinkedIn to take part in the research study to address the problem of employees’ cyberloafing on personal mobile devices. The specific focus was how the problem leads to a decrease in employee productivity in education organizations and leads organizational leaders to face security threats to their organization system because employees are visiting untrusted websites during working hours. The participants described their experiences with mobile usage limitation policies for personal activity in their past and current positions that included managerial and IT responsibilities. Some of participants' lived experiences with Internet or mobile usage limitation policies occurred in previous jobs outside the United States. Some also had newer experiences related to unrestricted mobile usage policies for activity on personal devices during working hours at educational organizations in the United States.

Demographics

The participants worked in educational and telecommunications organizations, including schools and colleges in the United States. Participant recruitment took place through LinkedIn groups, including IT, human resources, and PMP groups. Participants held master's degrees in management, business or human resources or PMP certificates with at least 2 years of experiences in the field. The IT security specialist participants held bachelor degrees in computer science, information system management, or software engineering, with one or more IT certificates, including Cisco Certified Network Associate Routing & Switching certification (CCNA) or Certified Information Systems Security Professional certification (CISSP) with at least 2 years of experiences in the IT field. Although the focus of this study was the phenomenon of cyberloafing in educational organizations in the United States, I invited several participants from telecommunications companies to take part in this study because of their extensive knowledge and experience in mobile software tracking and monitoring technology that added significant value to the study. I interviewed four individuals from the telecommunications industry and 16 interviewees from educational industry. Participants included both men and women at managerial and IT security specialist levels (see Appendix B).

Data Collection

The 20 managers and IT security specialists who participated had experience with cyberloafing in educational and telecommunications organizations inside and outside the United States. Some participants were under contract with educational or telecommunications companies in the United States and were not permanent staff. Participant interviews took place over a period of 3 to 4 weeks during late June 2017 and late July 2017. To accommodate participants' schedules, phone interviews took place on weekends and holidays. I asked follow-up and clarification questions to refine my understanding of the information provided, especially some of participants' preference to conduct the interviews offline followed by phone calls to confirm the accuracy of data. Although the plan was to record the interviews, the interviews took place in accordance with the participants' preference. Transcribing the participants' phone conversations involved using Microsoft Word, Microsoft Excel, and NVivo software. The initial plan had been to use Dragon Naturally Speaking software for the transcription process, but this was not possible for all participants, as some of participants asked to be interviewed offline. I sent invitations to the participants with my research questions and consent letter by e-mail. In the consent letter, I asked participants to respond to the email with the words "I consent" if they agreed to participate and then to schedule an appointment to conduct offline or online interviews. Some of participants provided conditional consent that included setting an appointment for offline interviewing due to their busy schedule and an agreement to follow up by phone as needed. The interviews were taking place offline or online included follow-up phone calls to obtain more details when needed. During phone calls with the participants, I wrote down notes related to participants' answers. The participants answered the questions in detail through e-mails followed by phone calls to ensure I understood the information provided. I transcribed the phone conversation and reviewed the transcriptions several times with the participants through e-mails.

The interviews went smoothly, and I allowed the participants to express their thoughts freely regarding the problem. I avoided interrupting the interviewees during phone calls. The interview was an open conversation between participants and me in which the participants presented their thoughts freely. I made every attempt to ensure participants answered each question and covered the topic completely.

Data Analysis

The interviews took place offline, online and subsequent phone calls to the participants ensured that there was no misinterpretation of participants' answers. Reviewing each interview involved copying the text to Microsoft Word and rereading each interview to ensure clarity and accuracy. I was careful not to use any of my own thoughts or words. The participants answer quotes presented are verbatim to ensure that they retain the true meaning the participants intended; therefore, the quotes include all errors as written by the participants. The themes started emerging after I transcribed the interviews. I noticed developing themes as I reread the e-mails, written memos, written theoretical notes, and written journal notes. Reading the transcribed interviews multiple times was important to obtaining the essence of each participant's response. After becoming more familiar with the data, I was able to generate themes. I compiled the themes into a template that I used to compare the responses of each participant to make it easier to read and code in the software program. I masked participants' names by assigning the letter *P* to each participant and giving each participant a number instead of providing participant name. I labeled each participant's position and industry. The first part of coding involved identifying the position and industry, while the second part involved assigning the participant number (see Appendix B). During the phone conversations, I inserted my notes into a comment field displayed on one side of the transcription page. I reached saturation of the themes with P10 and P11, but I continued the interview process until I completed the final interview with P20.

After writing my notes, I compared and contrasted the answers of the participants using mixed analysis techniques, including in vivo and descriptive analysis strategies. For in vivo analysis, a researcher uses the participants' language to assign words to the data by using a short phrase, whereas descriptive coding involves assigning the data to the words or short phrase (Maxwell, 2013). Four major themes and 12 subthemes emerged from the participants' responses. I used Microsoft Word, Microsoft Excel, and NVivo software to import, store, organize, and code data into manageable files. NVivo helped me to identify themes and to relate each research question to each participant's experience. Researchers should not use just one coding strategy, but should use a mix of strategies when appropriate (Miles & Huberman, 2014).

Evidence of Trustworthiness

Credibility

I posed the questions in a clear way to help the participants answer easily. The interviews took place offline or online, followed by phone calls. There are no recordings of the calls for offline interviews, in accordance with participants' requests. I sent the questions to participants via e-mail and received their responses through e-mails as well. I made phones calls after each e-mail I received from each participant to ensure the credibility of the data. The participant set up an appointment for the phone calls to review the answers on the phone. I reviewed the answers for each question with the participant and added my notes for each question. I transcribed their calls, added new information to their answers, and sent the final transcript back to the participants for their confirmation. I used a member-checking technique to review the data with participants four times to achieve credibility. The participants reviewed their answers and I received confirmation from them after several communications by e-mail and phone. I provided sufficient time for the member check so that the participants could review, update, or add more information to their answers to achieve credibility.

Transferability

Transferability refers to the degree to which a result can apply to other environments to evaluate the external validity (Guba & Lincoln, 1994). The transferability of results relates to readers' ability to identify transferability of the study. I wrote detailed descriptions to provide readers with comprehensive information that they can use to identify the transferability of the findings in this study.

Dependability

I used member checking to verify the accuracy of the data and my interpretations. Participants reviewed my interpretation of their responses, and they revised and added data to their responses. I updated the interpretations three or four times according to the participants' revisions. I had the opportunity to correct mistakes and clarify information until all participants agreed that my analysis reflected an accurate interpretation of their statements during the interviews.

Confirmability

I kept a reflective journal throughout the study. I wrote down my thoughts, and I made an effort to avoid including my own reflections and making my own assumptions. Researchers should consider all interpretations of data to achieve reliability. My report included detailed descriptions and an objective analysis of the documentation to ensure transparency. I connected the conclusions, data, and literature review to enhance confirmability (Yin, 2014).

Themes and Results

Four themes emerged from this phenomenological study: enforce cyberloafing control policy, enforcing monitoring technology, and create deterrence strategies. The main research question was as follows: How can managers minimize wasted work time by limiting the personal Internet activity of employees who use personal mobile devices while on the job?

The themes and subthemes were supported and answered by the following sub questions:

RQ1: What effective strategies can managers use to ensure employees are not wasting work time by cyberloafing and sending text messages from their personal mobile devices?

RQ2: How can managers prevent authorized employees from unauthorized access of an organization's database system?

RQ3: How effective are disciplinary plans designed to punish employees for computer-use policy violations in changing employees' behavior and increasing their commitment to organization policy?

RQ4: How effective are the technology tools that limit or monitor employees' Internet use through their mobile devices while on the job?

Theme 1: Create Mobile Device Usage Policy

Participants from educational organizations confirmed that no clear policy limits or restricts the use of personal mobile devices for personal activity during work time in educational organizations in the United States. Employees can use their mobile devices at any time. Employees may not conduct voice calls, but they can use their mobile devices for texting and surfing, as it is not necessary to connect their phones to their organization's Wi-Fi. Some employees do not like to use their mobile device data because the plans are limited, and the provider may charge them if they exceed the data limitations. Furthermore, no organizational policies prevent employees from connecting their mobile devices to company networks during working hours. Sixteen participants from the education industry confirmed the need to create and enforce a mobile policy to limit mobile device use for security purposes, to improve employees' work quality, and to protect educational organizations from security threats.

For instance, HRM-P1 stated,

> The employees don’t like to work very hard without take mandatory break such as using their mobile devices at least ten minutes every one hour to check text messages, emails or social media. There is no limit or deny mobile usage in my company, but from my view there is need to set one to limit the usage of internet accessing or mobile usage to increase employees’ productivity and protect employees and students’ information. I believe that private employee information, such as addresses, personal information, social security numbers, and bank information are considered high threats to organizations. Let me tell you something, some employees in my department connect the organization system through their mobile devices for easy access and retrieve the information. I am the manager here, but I don’t have the right to prevent employees from using their mobile devices during working hours especially if it is not a busy day. Sometimes, I have to do a conference outside my office, however, my room is next door from my employees’ room. Many times, I notice several employees are busy with their mobile devices during working day but when they notice me attend the room, they embarrass and try to hide their mobiles. As I mentioned, there is no policy prevents them from using their mobile, even that is correct, but employees realize they are doing something wrong, and waste working time.

AMU-P2 and ITS-P6 also reported that they had mobile usage policies in previous jobs outside the United States. They worked in administrative and IT security fields in higher education in Dubai, and they noted that such policies depend on the business culture and work environment. At the time of the study, ITS-P6 worked as an IT software specialist with a telecommunications company in the United States, and AMU-P2 worked in administrative management at a university in the United States. The participants described the rules in their previous company as "strict" and noted that policy enforcement prevents employees from violating mobile usage policies at their workplace.

For instance, ITS-P6 stated,

> With regards to Internet or mobile device use policies, in my previous job we did have such policy and it was strict (no social media access, no radio stations, limited you tube viewing, IP calls, etc.). University technology strategy was not working on mobile devices data plan, it only works on company WIFI services, so anyone with data plan on his mobile can access whatever he wants but employee cannot use their mobile devices during working hours because there is a clear rule prohibits employees using their mobile devices anytime except in break or lunch time.

AMU-P2, ITM-P12, ITS-P13, and ITM-P14 supported applying the policy to everyone. The participants confirmed the importance of showing the employees that the manager is a model of good conduct. The participants also confirmed the importance of the manager being the first to comply with organizational policy to engage the employees to follow the rules. Employees feel a sense of satisfaction when they comply with organizational policy because the policy applies to everyone.

For instance, AMU- P2 stated,

> During my past work, there is no violation for using mobile devices limiting policy or trying to access to restricted websites were reported. However, do you know why this policy was success in my past work? Because it was applied on everyone, there is no exception. There is a consent must sign by us, it comes under tittle “Managers and Employees” that’s mean there is no differences between powers, and the policy are enforcing on everyone.

ITM-P3, HRM-P19, and ITS-P20 reported they already had a policy at their workplace. HRM-P19 and ITS-P20 worked at the same telecommunications company, and they both noted the importance of organizational leaders allowing their IT security team to find the gaps in the security system to support the organizational policy and to apply the right technology to protect the information system and save work time.

HRM-P19 stated, “Internet policies are applied at the time we release new laptop or desktop the employees since everything is pushed using one click technology and every employee machine imaged with the defined policies by the organization.” ITS-P13 stated,

> Bosses are equally responsible for low morale of employees, so how about "Boss tracking”? I agree about the sharing responsibility with my employees. However, in my current job, there is no policy for mobile devices usage limitation and no monitoring technology.

Theme 2: Enforce Monitoring Technology

Participants believe that creating a mobile devices usage policy for personal activity during working hours is not enough to ensure all employees follow it. Enforcing specific technology by installing software or hardware is necessary to prevent policy violations. All participants confirmed the importance of having software or hardware in place to control cyberloafing, including having cameras in place or installing tracking software on employees' mobile devices to track employees' performance. Participants' considered having monitoring or tracking software installed on company mobile devices and prohibiting employees from bringing their devices to work as effective strategies. Monitoring or tracking software on employees' mobile devices provided by the company can track employees' activity during working hours and after working hours to prevent authorized employees from accessing unauthorized information through monitoring user login and logout time. Employees may have access to some information during working hours, but not have access after working hours without authorization.

For instance, ITM-P3 stated,

> In my organization, we have very strict Internet usage policies that also my company provided mobile devices. Using the personal mobiles are not allowed in the company. All the security and tracking applications are installed via Technology team at the company and we have full control over the devices during working hours and after working hours. No one is allowed to install anything on the company machines and everything has to go the manager of the person requesting new software or any kind of exception. We also do not allow anyone to bring his or her own devices to work. It is strictly enforced, and anyone finds in violation gets reported to the Ethics and Compliance."

ITS-P6 also stated,

> In my past job in Emirates, IT specialist can use company mobile devices to access the database or connect to organization computers for maintenance purposes during working time. But we deny any access to organization database or connect to operating system even by IT staff after working hours, the database is shout down after 6:00 pm, and there is no one can connect the system after this time for any reason. Also, IT specialist cannot copy anything or install anything without department manager written permission to protect information privacy and increase organization system security.

AMS-P7 responded,

> Well, monitoring without consent is not appropriate, although the owner of the company, the investors, and/or shareholders could put a certain employee(s) under surveillance by court order. This means if I am the owner, I have the ability to ask my employees to sign a form that says I can read your emails, texts, snail mail, etc., to protect my organization, but as administrative manager at school district I cannot do that because there is no policy allows me to do that.

ITM-P8 replied,

> Policy is not enough to protect the organization due to the ease of access. Increased security and tighter restrictions to internet access is needed to help keep organizations safe. There are various technologies that monitoring, or tracking employees' activity should be used by organizations managers for security reasons or for ensuring quality assurance with having consent from employees

> there is no problem with any type of monitoring or tracking. Allowing employees free access causes issues with security and other external threats.

HRM-P9 noted,

> There needs to have a professional IT staff to control cyberloafing in the organization. About my company we hired a private contractor that can observe what employees do on the computer but on mobile devices, there is limitations on carry the personal mobile devices or using during working time. I suggested that personal mobiles are keeping in employees' lockers, and employees can get their mobiles during lunch or break time only. About monitoring strategy, I would support employees and managers to join our monitoring program. I have participated in the program and was a member of the board about 10 years ago. My company has a good monitoring program, but in my opinion, it is not as strong as it used to be, especially the monitoring system is not cover personal mobile devices during working hours.

ITM-P14 stated,

> A resource (Time, Money, Opportunity to do more tasks) wasted is clearly a loss. Proficiency is linked with resource efficiency. You compute Efficiency by computing the work done on a task in given time. If it is on track and visible progress is there it is good. If you see more breaks, then you know the resource is underutilized or he is too smart for the task and finished it fast. If it is a misfit, then there would be negative impacts on the timeline and quality of work.

> Monitor and Control needs to be bettered if you are facing project or work proficiency issues.

Theme 3: Create Deterrence Strategy

The participants noted the need to enforce employee compliance with mobile device usage policies and to control cyberloafing. All participants confirmed the need to take action when employees knowingly violate the organizational policy. It is also important that organizational leaders improve security knowledge and awareness for their employees. Security training and education must increase employees' understanding of the aim of the mobile usage policy and the security threats that led to enforcing the policy. Participants confirmed the necessity of taking some action toward employees who lack commitment to organizational policy, including legal punishment, threat of termination, and loss of payment due to noncompliance. Protecting an organization's system and ensuring employees comply with organization policy is everyone's responsibility. It is important for staff to remind each other about the importance of complying with company policy, that any violation is not acceptable in the working environment, and that staff will report violations to managers.

For instance, ITS-P6 stated,

> I would prefer to start soft then get tougher and tougher until a harsher punishment in place. Employees would not violate the mobile usage policy if they completely aware the serious outcomes from their actions, such as termination, and there needs to provide employees by deep security and awareness training. In addition to the cameras in place (as a big brother), an employee must sign a

> consent to comply with mobile usage policy for security reasons and ensure quality assurance for their services. Finally, in my past job at Higher Colleges of Technology in Emirates, if an employee violates the policy, the company terminates employee contract and charges him $5,000US, also there is a rule that punish any employee may notice the violation and not reports it to the direct manager, you can find this rule when you sign a job contract with most educational organizations in Emirates.

AMS-P7 replied,

> The employees are expected to protect the organization, including assets, reputation, and representation of the organization to the public. My philosophy is: once employees are hired, they should have ownership of the organization, no matter what title they hold. The contribution is what counts in day-to-day operations. The most difficult organization to work with/for is one without quality and quantity in production (i.e., work by following intuition or "go with the flow" are not my favorites). Managers have to set a clear policy and formal punishment rules to punish those who violate the company policy.

HRM-P9 responded,

> It would help to show employees problems that could arise if they became relaxed and did not continue to follow company policy. This could be done in the online mandatory training course. Building security awareness among the employees is contribute avoiding the policy violation, for instance remind each other the important to follow the rules and commit to organizational policy. Everyone has a

> certain level of responsibility and when they notice something wrong tell management.

Some participants noted that the only way to stop cyberloafing during working hours and to ensure employees comply with organization policy is to put punishments in place, such as immediately punishing an employee who is violating the policy and letting others know about the punishment. Other employees might choose not to violate the policy knowing they will face the same result.

For instance, AMU- P2 noted,

> Job is a security factor for person life, knowing they are able to take care of themselves and their families by keeping this job. If they think they are losing the only way that support their lives and their family, they never think about policy violation or commit any negative behave that cause losing their jobs and paycheck.

ITM-P8 stated,

> I believe the only effective way to prevent an employee from hurt or violate his organization is threat of termination or loss of pay due to non-compliance. If one of employee got a punishment for policy violation, the others will scare and will never do the same violation because they realize they will face the same punishment if they try to do the same violation.

Other participants had different views related to cyberloafing and the ways managers can stop it. Managers can encourage employees to commit to their organization by building trust between managers and their employees. Employees must have a goal when they are doing their job. By implementing a reward system, managers encourage their employees to control negative behaviors or feelings to look good in front their managers. Managers confirmed they need to allow their employees to deal with their emotions in the right way. Some participants indicated encouraging employees to be hard workers and to comply with organizational policy by activating a reward system is an effective way to comply with a mobile usage policy. Employees should know that those who provide good service quality, either by working hard or by demonstrating positive behavior in committing to organizational policies and rules, will receive a reward.

HRS-P1 stated,

> I believe that happy employees equal a happy environment. Keeping employees in the know; to the extent of what may directly affect them; may leave room for them to breathe in; the concepts of dealing with any organizational change. Employees must have a goal engage them to keep their jobs healthy and stay focus on task such as a good salary, skills development, great benefits, good manager, etc. From my view, this may increase their commitment to organization policy, increase responsibility feeling toward their organization, therefore, they can control their emotions from doing any violation to company policy or rules. It is important for managers to reward employees for any positive achievement that helps organization improvement. It is not acceptable to inform the employees there is a punishment in place for violating company policy, and no reward for your commitment or for doing your job very hard, managers must hold the stick

> from the middle. From my view rewarding strategy engage employees to deal with their emotions, follow the rules, and try to be at the best at the workplace.

ITM-P3 noted,

> In my humble opinion, I would say building TRUST within the team is the best way to mitigate such issues. Employees needs to be empowered by the work competition within the team where they are busy in a very productive manner. Sometime, I have given each employee some break where they allowed to look into new technology that has benefited company in many ways.

ITS-P13 responded,

> The solution for controlling cyberloafing during working hours is to have a chat with the employees, tell them one on one what's happening and how it's affecting the company's productivity and offer assistance to help them improve. Beyond all this, you just have to trust your employee to deliver the goods and support them in whatever way you can through mentoring, coaching and training.

Theme 4: Effectiveness of Customizing Monitoring and Tracking Technology Tools

Participants agreed about the effectiveness of using monitoring technology as an effective strategy to control cyberloafing in the workplace. Participants focused on two types of monitoring technologies. The first one was to install various types and sizes of cameras to prevent employees from violating organization policy or committing undesirable behavior during work time. The second type of monitoring technology is mobile and computer tracking software technology. Organizational leaders should install type of technology on laptops, computers, or smart phones provided by the company to employees. Participants supported using mobile or computer tracking software as an effective tool to monitor virtual team performance and prevent virtual teams from wasting work time. P1-P20 all confirmed the effectiveness of installing cameras not only for monitoring employees' cyberloafing but also for making the workplace safer. The 20 participants preferred to install cameras in open places rather than to hide them, as they noted employees must see and realize there is a camera in place to be more responsible.

For instance, HRM-P9 stated,

> Monitoring technology improved its effectiveness by preventing any violation to company policy and rules, not just for the cyberloafing during work time, but also to increasing employees' commitment to do their work in the right way. For instance, you can see the cameras everywhere in the banks in the USA. I have a friend who works at [names bank] and she told me that she cannot use her mobile during working hours without permission from her supervisor, not because a policy enforces it, but because there are several cameras in the work area. She said her banks pays very well, so she does not want to lose her job for any reason. From my view, a camera is a good witness and may be with or against the employee during working hours. It all depends on employee choices and behavior during work time, that's why I support installing cameras in the workplace.

AMU-P2, HRM-P4 and ITS-P6 confirmed the importance of posting a clear policy that informs employees there are monitoring technologies in place in the workplace to ensure security and productivity. Participants noted that all employees should sign consents that include permission for their employers to monitor them for security or performance evaluation during working hours. Monitoring technology would be more effective when the employees know there are a policy, punishment, and technology to evaluate and monitor their performance. Monitoring technology transfers monitoring responsibilities from managers or supervisors to performance monitoring technology, which allows organizational leaders to focus on important tasks, instead of personally monitoring their employees and wasting their own work time. Installing camera in work areas may solve many problems and reduce the burden of administration.

AMS-P7 responded,

> If the district's leaders decide to install cameras in the workplace, this will keep managers from any embarrassing situations, such as asking their employees to focus on their job every time. The camera would be the responsibility of the electronic supervisor, and he or she could make the right decisions toward employees, depending on their behavior.

Monitoring technology, including cameras, will increase self-regulation and self-control for employees and prevent them from violating organizational policies and rules. ITM-P8 noted,

> When employees are aware they are being monitored by their managers or authorized persons, they will be careful and keep themselves focused on their job. However, I think monitoring technology is more effective in organizations with many employees. Sometimes because [of] the limitation of the budget, organizational managers are ignoring the need to have enough supervisors to

> control employees' behavior or monitor their performance, so placing the camera in the work area is great, especially in situations like that.

ITM-P3 stated,

> In my past job in Emirates, we had cameras everywhere, except in the bathroom and lunch room. I don't know who managed these cameras, but it was an effective tool to monitor employees' performance and behavior. Employees were thinking twice before they made any mistake or violated company policy. From my side, when I was manager there, I did not get any report regarding a violation of the mobile device policy because the employees were aware there was a camera in use. From my view, keeping a camera in the workplace is a good idea and could increase employees' productivity and support their commitment to the organization's rules and policy.

AMU-P2, ITM-P12, ITS-P13, AMS-P7, and ITM-P14 noted that mobile software tracking for personal mobile devices may violate personal privacy, especially in the United States. Therefore, organizational leaders prefer to install cameras in the workplace with signs that indicate cameras are in use. AMS-P7 replied,

> Well, I believe that installing a camera in the workplace is more effective than mobile tracking software because the software may be against the employees' privacy or something like that. We don't like to be involved in this anymore. Also, using a camera in the workplace is easier than installing mobile software tracking because it will not need employee permission and it will serve monitoring purposes in an effective way. The employer can install cameras in the

> workplace for many reasons, including monitoring employees' performance, security policy, customer satisfaction, and ensure the employees comply with the organization's policy etc.

HRM-P19 stated,

> We are having contracts with IT technicians who work with us from home [virtually], so we need to evaluate their work and pay them hourly. However, installing cameras in the workplace or in their home is not the [most] effective because they are working virtually. Instead, we use various software, including Time Doctor, and Phone Tracker, to monitor employees' performance, activity, and working hours. For instance, Time Doctor can take screen shot every 3 minutes; if the employee needs to take a break or do something personal, the employee can press the break button.

ITS-P13 and ITS-P20 recommended several types of mobile tracking software that work on iPhones, Androids, and iPads to track employees' personal activity during working hours by installing these types of software on organizations' mobile or tablet devices. IT specialists can install mobile tracking software such as Phone Tracker, Spy Bubble, Higher Mobile, and MSpy, depending on organizations' needs and selections. Mobile tracking software can record Voice Over Internet Protocol calls for Viber, WhatsApp, and Skype, and employers can receive SIM card change notifications. Tracking software can handle various tasks, including tracking social network chatting, e-mails, and browsing history. Monitoring technology can save organizations money and time, especially for virtual teams or online businesses.

HRM-P9 stated,

> If you own a business online or you depend on using computers in your business and your average employee is working 40 hours per week, if they only waste 1 hour a day, which is actually it is likely to be more, it is 5 hours a week or 20 wasted hours a month for each employee; therefore, tracking software is a very effective tool because it helps to automatically reduce wasted time and make sure everybody gets paid for the actual work done.

Summary

All of the participants had their own ideas and views about controlling cyberloafing. The participants indicated that cyberloafing is a serious problem that organizational leaders must control using various strategies and technologies. Creating and enforcing an effective cyberloafing strategy is the first step in using a security and productivity process to control cyberloafing in the workplace. Also, enforcing monitoring or tracking performance technology with consent is a common strategy to control cyberloafing and policy violations during working hours. Employers might use various strategies to enforce compliance to organizational policy. Punishments such as a loss of pay due to noncompliance and the threat of termination are normal consequences of violating organizational policy. Prohibits using personal mobile devices during working hours and provide employees by company mobile devices for working purpose with monitoring or tracking software on the device is another strategy. Building trust and implementing a reward system are other strategies to control cyberloafing. Chapter 5 includes a restatement of the purpose of the study and the implications of the findings placed in the context of the conceptual framework. I continue the discussion, present a conclusion, and compare findings to the literature review. Chapter 5 also includes recommendations for additional research and action, as well as implications for social change, with a review of current research as it relates to participants' views about finding ways to control cyberloafing problem in educational organizations in the United States.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

The purpose of this qualitative phenomenological study was to find reliable ways for organizational leaders to monitor or limit employees' personal use of the Internet through their mobile devices and smartphone technology while on the job. Data collection consisted of semistructured offline and online interviews followed by phone calls and e-mail messages with IT managers, human resource managers, administrative managers, and IT security specialists. In this chapter I will explain the four main themes emerged from the data: create a mobile usage policy, enforce monitoring technology, and create a deterrence strategy. The participants suggested various strategies to control cyberloafing in the workplace, which included enforcing mobile usage policies, installing cameras, prohibiting the use of personal mobile devices in the workplace, using performance tracking software, building trusting relationships between managers and employees, and implementing positive reward systems. Data revealed that managers represent a model of good conduct and ethics and they support enforcing mobile usage policies and applying monitoring technology as well.

Interpretation of Findings

I collected and analyzed data for this phenomenological research study using mixed methods, including in vivo and descriptive data analysis methods that support qualitative research. In vivo and descriptive data analysis methods supported the effort to understand participants' thoughts and suggestions to find ways to control the cyberloafing phenomenon. My goal was to capture words from the participants' language and use these words to represent participants' thoughts by selecting short phrases or statements (Maxwell, 2013). I transcribed each interview, reread the interviews several times, and used NVivo 11 and Excel software to analyze interview content. After the emerging themes were established, I analyzed and reviewed the content again. The four emergent themes were as follows: create a mobile device usage policy, enforce monitoring technology, and create a deterrence strategy. The following discussion is a summary of the findings.

Theme 1: Create Mobile Device Usage Policy

This study showed that there is no clear policy related to monitoring or limiting employees' personal use of mobile devices and smartphone technology while on the job in educational organizations in the participants educational organizations United States. The employees can use their mobile devices anytime and anywhere without any restriction or limitation. Employees may connect their mobile devices to organizational Wi-Fi to save their data plan on their personal mobile devices. Such use of mobile devices for personal activity during work time negatively affects productivity and bandwidth (Coker, 2011). Managers cannot prevent employees from connecting their mobile devices to organizations' Wi-Fi either for work or for personal activity when there is no clear policy to prohibit these actions in educational organizations. Employees are more likely to use their mobile devices for surfing or texting when their supervisor or manager does not share the same work room. Employees who believe they are doing something wrong might experience a decrease in productivity and may represent security threats to their organizations. Participants noted that employees feel embarrassed when managers notice them *cyberloafing* with their mobile devices during working hours. Employees believe supervisors or managers represent a threat and may prevent them from continuing their undesirable cyberloafing behavior (Karimi et al., 2014; Murphy et al., 2003). Participants noted a need to create and enforce mobile device usage policies for everyone. Managers must model good conduct in front of their employees for employees to want to follow them. Employees are willing to comply with a mobile usage limitation policy when they know the policy applies to everyone, regardless of whether a person is an employee, a supervisor, or a manager (Grover, 2014).

Theme 2: Enforce Monitoring Technology

Despite the importance of having a mobile device usage policy, participants stated that having a policy without enforcing it is not enough to control cyberloafing in the workplace. Combining a monitoring technology with the policy is necessary to control this phenomenon. Monitoring technologies, including both hardware and software, are effective solutions for controlling policy violations from most participants' viewpoint. Managers can use various technologies to limit or monitor employees' personal use of mobile devices during working hours. For instance, having cameras in place to track or monitor employees' performance is like having managers or supervisors in the same room as employees. Having an open office environment or a manager's desk in the same area with employees or installing cameras may help to control employees' cyberloafing behavior and improve self-control and self-regulation. Participants in this study noted that employees might not use their mobile devices in front of their managers or when they think their managers are watching them. Employees believe their managers have the power to track their performance or to make decisions related to their behavior at work, so it is better for them to look good and comply with organization rules in front their managers.

Employees share a common goal: to prove they fit their position and complete their tasks efficiently. Managers are responsible for evaluating employees' behavior and performance during work time and for determining if employees fit their position and deserve rewards, bonuses, violations, or punishments. Cameras provide a connection between employees' behavior and their supervisor. Installing cameras in work areas is a second eye for managers. Monitoring technologies, including hardware and software, can track employees' behavior, improve employees' commitment to organization policy, and improve employees' self-regulation and self-control. Monitoring technology serves to encourage employees to cope with their emotions and to practice self-regulation and self-control strategies. Using monitoring technology allows employees to demonstrate their commitment to organization policy to overcome mobile addictions and to improve their image in front of their managers to keep their job and their paycheck. Monitoring and tracking employees' activities is a best practice to prevent cyberloafing and enforce employees' compliance with organization policy (Dhillon et al., 2016).

According to the SCT, mobile devices can become an addiction due to weak or incomplete self-regulation (Baumeister, 2014; LaRose & Eastin, 2004). Therefore, individuals need to engage in self-regulation and self-control, so they need something, such as an open environment or a manager or camera in the same work room, to help them avoid addictive behaviors. Prohibiting employees' use of mobile devices in the workplace is an effective strategy to control cyberloafing. Participants stated that their companies provide employees mobile devices for work purposes and install monitoring or tracking performance software. Employees who bring personal mobile devices to the workplace may violate mobile usage policies, and participants preferred that employees keep their mobiles in a separate place, such as lockers, to improve employee productivity and to protect organization systems from viruses that result from visiting untrusted websites. Cyberloafing and slacking represent serious threats to employees' productivity and contribute to wasting work time (Kuschnaroff & Bayma, 2014).

Although organizational Wi-Fi is open to all staff members, and they can connect their mobile devices to various websites anytime during working hours, IT security specialists recommended denying access to many websites to help employees stay focused on their tasks and protect organization systems from serious security threats as well. One way to engage employees is by limiting Internet access or enforcing Internet restriction technology on many websites, including social media, gaming, dating, charting, and pornography sites. Internet policy restrictions are efficient strategies, especially when applied to managers and employees at the same time (Kidwell, 2010). Employees who are connecting their mobile devices to social media or online gaming during working hours may find it difficult to focus on their tasks after they return back to work, especially if they enjoy visiting those sites (Weatherbee, 2012).

IT security participants stated that technology is not strong enough to cover employees' mobile devices, in spite of monitoring technology in several educational organizations. Monitoring technology may cover office devices such computers, printers, scanners, and faxes only. Furthermore, monitoring strategies that apply to employees' personal mobile devices need to include an agreement between employees and their employer to confirm relinquishment of their mobile privacy to their employer (Glassman et al., 2015; Kidwell, 2010; Lee et al., 2016).

Many organizational leaders hire private contractors to protect organization systems against external security threats. However, these organizational leaders are ignoring the importance of setting the insider threat as a high priority. Managers need to improve monitoring systems and feedback to diagnose the security gap either in human behavior or in security technology (Král, 2011). External venders may not have the required information related to an organizational culture or environment to identify internal security threats; therefore, organizational leaders must consider insider security threats as a main part of their security strategies (Weatherbee, 2012). A frontline supervisor stated that employees might take several breaks during working hours and not complete their tasks in time, which negatively affects timelines and quality of work. Therefore, supervisors need to control and prevent this behavior by separating and distributing tasks to employees using a performance tracking strategy (Donahue & Rahman, 2012).

Theme 3: Create a Deterrence Strategy

A private conversation needs to occur between managers and employees who violate policies before managers apply a punishment, especially the first time an employee commits a violation or when an employee does not have enough information regarding organizational policy and security threats due to weak security training or education. Therefore, it is better for managers to provide employees security training at the beginning of their employment. Managers should note the aim and benefits of following the organization’s policy and ensure that employees sign a consent form before starting their actual job responsibilities. Many organizational leaders set a strict policy and try to enforce it among their employees without showing them the importance of following it. Organizational leaders push their employees to follow organization policy without having sufficient knowledge, and employees may violate policy as a consequence of misunderstanding the value of the policy (Donahue & Rahman, 2012). Security training is an important step to protect organization systems and to ensure employee compliance with organization policy. Organizational leaders must provide various security training levels to employees, IT staff, and managers and keep them up to date. Employees cannot be aware of security threats facing their organizations without involving them in the security process and making them aware of the value of the information they work with daily (Glassman et al., 2015).

Deterrence strategies, including threats of termination or loss of pay due to noncompliance, are a mandatory solution, especially if employees are aware of security policies and sign consent forms to indicate their agreement to comply with organizational policy and security rules. Organizational mechanisms, including policy and behavior violation control, are an effective deterrence to cyberloafing (Piscotty et al., 2016). Punishment strategies must apply to everyone who violates organizational policy, as employees are more likely to comply with the policy when they realize there are punishments in place (Piscotty et al., 2016). Everyone has a level of responsibility, and it is important for employees to remind each other about the importance of following security rules and organizational policies. Employees may report policy violations when a member of their team knowingly violates company rules or policies, especially when the violation may affect other employees' job or an organization's reputation. Reporting policy violations to ethics and compliance departments is an effective deterrence strategy, as such reporting represents a strong threat of termination or punishment and is likely to help improve employees' self-control and self-regulation by encouraging them to comply with organizational policy.

Supporters of SCT indicate that people expect outcomes from their current behavior based on their experiences or the experiences of others who exhibited similar behaviors in the past (LaRose & Eastin, 2004). According to SCT, punishing those who violate organizational policy and security rules might lead other individuals to reconsider their actions prior to committing such violations. Reward systems are another effective cyberloafing deterrence strategy in which employees must have a goal to do their job efficiently. Reward strategies such as motivate employees, keep them on task, and engage them to comply with organization policy. Managers must show their employees their trust and engage them to increase their achievement; employee performance reports should be available each month, as well as a reward list available to those who improve their efforts during the month. Keeping employees busy may improve their self-regulation and lead to their inclusion on the reward list. According to SCT, staff members realize that when they work hard, improve their skills, and commit to organization policy, they impress their managers and their evaluation report will be positive. Therefore, they might receive a bonus, a raise, a recommendation, or a promotion as a reward for their efforts, which leads to improved self-control, self-regulation, and compliance with organizational policy. Leaders of educational organizations in the United States have ignored the importance of mobile usage limitation policies that can improve security and productivity; therefore, the leaders of educational organizations have not made any efforts to have IT mobile security specialists or to use monitoring software technology to monitor or track employees' performance in their organizations.

Theme 4: Effectiveness of Customizing Monitoring and Tracking Technology

Using monitoring technology allows employees to demonstrate their commitment to organization policy to overcome mobile addictions and to improve their image in front of their managers to retain their job. Monitoring and tracking employees' activities is a best practice to prevent cyberloafing and enforce employees' compliance with organization policy (Dhillon et al., 2016). Monitoring technology may assist organizational leaders in their work and help them to evaluate their employees in the right way. Monitoring technology may also improve employees' self-regulation and self-control because cameras represent supervisors' presence in the work area. Employees work harder in front of their managers because they believe managers or supervisors represent a threat and may prevent them from keeping their job when managers notice their cyberloafing or policy violation behaviors (Karimi et al., 2014; Murphy et al., 2003).

Employees are more likely to comply with policy when it applies to everyone (Grover, 2014). Therefore, installing monitoring technology such as a camera in each work room means that monitoring technology applies to everyone, so there are no differences in power in this regard between managers and employees. Therefore, it is easy for employees to accept monitoring technology and comply with organization policy because it applies on everyone. It is important for organizational leaders to customize monitoring technology usage according to the organization needs. A camera in the work place may improve employees' commitment to organization policy. However, using a camera in the work place is only possible when the employees are physically working on site at the office (Dhillon, Samonas, & Etudo, 2016). Performance tracking software either installed on organizations' computers or mobile devices can be used to monitor or evaluate employees' performance especially when employees are working virtually. Monitoring or tracking software has two buttons, one to start recording employees' activities and other to stop the recording process. When an employee starts a task by using a computer or mobile device, the employee must press the start button to turn on the tracking software and start recording activity, which then sends the information to the manager or team leader automatically. The manager can see the employee's computer screen or mobile device screen and track all employees' activities when tracking software is on.

Limitations of the Study

The study included some limitations. I limited the information security specialist for mobile software to three participants due to difficulties recruiting them. The small sample size of security software specialists limited the ability to obtain more details on mobile tracking software. The rest of the sample included human resource managers, administrative managers, IT managers, and frontline supervisors. Another limitation was the insufficient data regarding mobile usage restriction policies and mobile security software, as most of the participants did not have such a policy in their current jobs. However, some of the participants had relevant experience based on prior international experience. The focus of the study was also on the knowledge of participants and not necessarily their positions in U.S. organizations at the time of the study.

Recommendation for Action

Cyberloafing is a serious problem for educational organizations in the United States. Despite the high costs and low productivity of employees as a consequence of mobile usage addiction and the absence of mobile usage limitation policies during working hours, educational leaders in the United States have not made any effort to overcome this problem. Many educational leaders continue ignoring the importance of enforcing a mobile usage policy and technology to handle cyberloafing. Organizational leaders should be providing managers and employees mandatory security training, showing them the importance of creating mobile usage limitation policies, and enforcing the application of monitoring technology on everyone to protect organization systems and to improve employee productivity (Grove, 2014). Involving information security specialists in security control and monitoring processes will help to maintain direct channels with human resources staff, administrative management, frontline supervisors, and IT security specialists to ensure employees comply with mobile device usage policies (Harris & Patten, 2014). Installing monitoring and performance tracking software on employees' personal mobile devices in case the employees bring their mobile devices to work is an effective strategy to ensure employees comply with organization policy. Employees must sign a consent form or an agreement for their employer to monitor their mobile devices for security purposes when they bring their mobile devices to work. It is important for organizational leaders to assign phone lockers to each employee during working hours and to allow them access during breaks or lunch hours or with permission from managers to conduct emergency calls. Installing a camera in every work room and in halls is necessary to ensure employee productivity remains high and for security purposes; an exception would be lunch rooms and restrooms. Internet restriction plans are an effective way to minimize or control cyberloafing during working hours.

Recommendation for Further Research

In further research, it will be important to know the result of combining a mobile device usage policy, monitoring technology, and a reward and punishment model to control employees' cyberloafing by using their mobile devices while on job. The proposed model may improve self-regulation and self-control in employees and may therefore improve employee compliance with mobile device usage policies during working hours. Future researchers should test the effectiveness of tracking or monitoring employees' performance thorough personal mobile devices to limit or control cyberloafing by employees during working hours. By using monitoring or tracking software, researchers can collect information regarding which websites employees visit most often during working hours, control security threats that may face educational organizations by analyzing information obtained from tracking software, and block all websites that may lead to decreases in employee productivity, increases in security threats, and wasted work time.

Implications

Information security and employee productivity must be a priority in organizations and evolve as a core competency for managers and employees. Whereas employees are part of the problem, they are also part of the solution. Organizational leaders who create their mobile usage limitation strategy, enforce the use of monitoring technology, and plan for a deterrence strategy to meet established core competencies may increase their commitment to their organizations.

Manager as a Model of Good Conduct

The findings from this study yielded multiple outcomes. First, the findings revealed that managers serve as models of good conduct by confirming their agreement to apply mobile usage limitation policies and monitoring technologies on themselves as well as their employees. Enforcing mobile usage limitations on managers and employees supports equity theory and improves relationships between managers and employees. Employees may feel satisfied complying with mobile usage policies and monitoring technologies when the strategies applied to everyone are equal (Grove, 2014). Organizational security is everyone’s responsibility, and managers share the responsibility with employees. Monitoring strategies save work time and serve to encourage employees to commit to organizational rules and policies, especially if they apply to their managers as well.

Rewards and Punishment Efficiency

A reward and punishment strategy can serve to improve self-control and self-regulation and to develop a spirit of positive competition among employees. Employees want to look good in front of their managers, so they comply with organization policy and work hard to achieve this goal. Rewards serve to encourage employees to do better and be responsible during working hours and by continuing to receive their managers' praise, while punishment increases their commitment to organizational policies and rules.

Internet Restriction Plan Efficiency

An Internet restriction plan has a positive effect on employee productivity and reduces stress by protecting staff from gossip and unexpected news received through social media or texting, which affects their productivity during working hours. Installing performance monitoring software on employees' mobile devices may lead to important information regarding the websites employees visit most frequently during working hours. Therefore, managers can evaluate employees' productivity and ensure they are not wasting work time by blocking those websites, especially if they include security threats to the organization's system.

Benefits of Denying Personal Devices on Work

The study showed great benefits from denying employees the use of their personal mobile devices on job. Providing employees mobile devices for their job is a practical way to save work time and protect organization systems from security threats that occur from employees surfing during working hours.

Effectiveness of Monitoring Technology

The study showed a benefit from using either hardware such as a camera or software such as computer or mobile tracking software as forms of monitoring technology. Monitoring technology represents an effective deterrence tool that prevents employees from cyberloafing behavior or from trying to violate company policy. Monitoring technology represents a real threat that may lead employees to face formal punishment if they commit unacceptable violations, especially if they sign a consent that acknowledges they are aware of the cyberloafing policy.

Training and Education Benefits

The training and education available in various levels for both employees and managers indicate they represent an important part of organization success. Employees cannot protect their organization system without understanding the value of the information they are working with, and training and education help employees and managers understand the aim of complying with mobile usage limitation policies and the importance of enrolling managers and employees in various types of security training according to their job roles.

Potential Implications for Social Change

Study results included both practical and theoretical knowledge applicable to leaders in academia, industry, and government organizations. This study involved original research. I tried to cover most known issues that may appear as a consequence of cyberloafing on personal mobile during working hours. Enforcing mobile device usage policies and monitoring technologies improves employee productivity and protects organization systems from security threats. I used a social cognitive theory (SCT), to study employees' thoughts, beliefs, emotions, and behaviors to push my research beyond theoretical boundaries to practical and real life. The study showed organizational leaders might use practical and effective solutions to control employees' cyberloafing behavior. The study showed a positive relationship might develop between employees and managers when both sides comply with organizational policy and represent an important part of an organization's success. Organizational leaders who apply the findings from this study might save organizational resources, including a loss of productivity and lost bandwidth costs, and might protect organization systems from the cost of security threats if information breaches or hacking occurs after visiting untrusted websites.

Conclusions

The findings of this study indicated that educational organization managers do not mind sharing responsibilities with employees regarding mobile usage limitation policies and monitoring technologies and they do so regularly. Managers seemed intent on being a model of good conduct for their employees and on developing a sense of responsibility among employees and managers toward their organizations to control cyberloafing and protect organization systems. Cyberloafing affects employees' productivity negatively, and participants agreed that monitoring technology, applying Internet and mobile usage restrictions, activating a reward and punishment system, and increasing employees' security knowledge and awareness are effective strategies to control cyberloafing during working hours.

References

Achakul, C., & Yolles, M. (2013). Intrinsic and extrinsic motivation in personality: Assessing knowledge profiling and the work preference inventory in a Thai population. *Journal of Organizational Transformation & Social Change, 10*(3), 196-217. doi:10.1179/1477963312Z.0000000005

Aguirre, R. T., & Bolton, K. W. (2014). Qualitative interpretive meta-synthesis in social work research: Uncharted territory. *Journal of Social Work, 14,* 279-294. doi:10.1177/1468017313476797

Ajzen, I., & Sheikh, S. (2013). Action versus inaction: Anticipated affect in the theory of planned behavior. *Journal of Applied Social Psychology, 43,* 155-162. doi:10.1111/j.1559-1816.2012.00989.x

Aluwihare-Samaranayake, D. (2012). Ethics in qualitative research: A view of participants' and researchers' world from a critical standpoint. *International Journal of Qualitative Methods, 11*(2), 64-81. Retrieved from http://ejournals.library.ualberta.ca/index.php/IJQM

Andreassen, C. S., Torsheim, T., & Pallesen, S. (2014a). Predictors of use of social network sites at work: A specific type of cyberloafing. *Journal of Computer-Mediated Communication, 19,* 906-921. doi:10.1111/jcc4.12085

Andreassen, C. S., Torsheim, T., & Pallesen, S. (2014b). Use of online social network sites for personal purposes at work: Does it impair self-reported performance? *Comprehensive Psychology, 3,* 1-21. doi:10.2466/01.21.CP.3.18

Askew, K. (2012). *The relationship between cyberloafing and task performance and an examination of the theory of planned behavior as a model of cyberloafing* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses database. (UMI No. 3519206)

Askew, K., Buckner, J. E., Taing, M. U., Ilie, A., Bauer, J. A., & Coovert, M. D. (2014). Explaining cyberloafing: The role of the theory of planned behavior. *Computers in Human Behavior*, *36,* 510-519. doi:10.1016/j.chb.2014.04.006

Ballaro, J., & O'Neil, M. (2013). Transformational and transactional leadership behaviors: A phenomenological study of women executives in major league sports. *International Leadership Journal, 5,* 45-69. Retrieved from http://www.tesu.edu/business/leadership-journal.cfm

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory.* Englewood Cliffs, NJ: Prentice Hall.

Bansal, P., & Corley, K. (2012). Publishing in AMJ--Part 7: What's different about qualitative research? *Academy of Management Journal, 55,* 509-513. doi:10.5465/amj.2012.4003

Bartariya, S., & Rastogi, A. (2016). Security in wireless sensor networks: Attacks and solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, *5*, 214-220. doi:10.17148/IJARCCE.2016.5352

Baturay, M. H., & Toker, S. (2015). An investigation of the impact of demographics on cyberloafing from an educational setting angle. *Computers in Human Behavior, 50,* 358-366. doi:10.1016/j.chb.2015.03.081

Baumeister, R. F. (2014). Self-regulation, ego depletion, and inhibition. *Neuropsychologia*, *65*, 313-319. doi: 10.1016/j.neuropsychologia.2014.08.012

Bekhet, A. K., & Zauszniewski, J., A. (2012). Methodological triangulation: An approach to understanding data. *Nurse Researcher, 20,* 40-43. doi:10.7748/nr2012.11.20.2 .40.c9442

Bernard, H. R. (2013). *Social research methods: Qualitative and quantitative approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Bettini, E. A., Cheyney, K., Wang, J., & Leko, C. (2015). Job design: An administrator's guide to supporting and retaining special educators. *Intervention in School and Clinic, 50,* 221-225. doi:10.1177/1053451214532346

Black, E., Light, J., Paradise Black, N., & Thompson, L. (2013). Online social network use by health care providers in a high traffic patient care environment. *Journal of Medical Internet Research, 15*(5), e94. doi:10.2196/jmir.2421

Borrero, J. D., Yousafzai, S. Y., Javed, U., & Page, K. L. (2014). Expressive participation in Internet social movements: Testing the moderating effect of technology readiness and sex on student SNS use. *Computers in Human Behavior, 30,* 39-49. doi:10.1016/j.chb.2013.07.032

Boxall, P., & Macky, K. (2014). High-involvement work processes, work intensification and employee well-being. *Work, Employment & Society, 28,* 963-984. doi:10.1177/0950017013512714

Buckner V, J. E., Castille, C. M., & Sheets, T. L. (2012). The five-factor model of personality and employees' excessive use of technology. *Computers in Human Behavior, 28,* 1947-1953. doi:10.1016/j.chb.2012.05.014

Camfield, L., & Palmer-Jones, R. (2013). Improving the quality of development research: What could archive qualitative data for reanalysis and revisiting research sites contribute? *Progress in Development Studies, 13,* 323-338. doi:10.1177 /1464993413490481

Carnevale, A. P., & Smith, N. (2013). Workplace basics: The skills employees need and employers want. *Human Resource Development International, 16,* 491-501. doi:10.1080/13678868.2013.821267

Charness, G., Cobo-Reyes, R., Jiménez, N., Lacomba, J. A., & Lagos, F. (2012). The hidden advantage of delegation: Pareto improvements in a gift exchange game. *American Economic Review, 102,* 2358-2379. doi:10.1257/aer.102.5.2358

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior, 38,* 220-228. doi:10.1016/j.chb .2014.05.043

Chikweche, T., & Fletcher, R. (2012). Undertaking research at the bottom of the pyramid using qualitative methods: From theoretical considerations to practical realities. *Qualitative Market Research: An International Journal*, 15, 242-267. doi:10.1108/13522751211231978

Coker, B. L. S. (2011). Freedom to surf: The positive effects of workplace Internet leisure browsing. *New Technology, Work & Employment, 26,* 238-247. doi:10.1111/j.1468-005X.2011.00272.x

Coker, B. L. S. (2013). Workplace Internet leisure browsing. *Human Performance, 26,* 114-125. doi:10.1080/08959285.2013.765878

Collet, C., Hine, D., & du Plessis, K. (2015). Employability skills: Perspectives from a knowledge-intensive industry. *Education + Training, 57,* 532-559. doi:10.1108 /ET-07-2014-0076

Collins, C. S., & Cooper, J. E. (2014). Emotional intelligence and the qualitative researcher. *International Journal of Qualitative Methods, 13,* 88-103. Retrieved from http://ejournals.library.ualberta.ca/index.php/IJQM

Comi, A., Bischof, N., & Eppler, M. J. (2014). Beyond projection: Using collaborative visualization to conduct qualitative interviews. *Qualitative Research in Organizations and Management, 9,* 110-133. doi:10.1108/QROM-05-2012-1074

Condie, J. (2012). Beyond rationalizations: Improving interview data quality. *Qualitative Research in Accounting & Management, 9,* 168-193. doi:10.1108/ 11766091211240379

Cullinane, S. J., Bosak, J., Flood, P. C., & Demerouti, E. (2013). Job design under lean manufacturing and its impact on employee outcomes. *Organizational Psychology Review, 3,* 41-61. doi:10.1177/2041386612456412

Dang, J., Dewitte, S., Mao, L., Xiao, S., & Shi, Y. (2013). Adapting to an initial self-regulatory task cancels the ego depletion effect. *Consciousness and Cognition*, *22*, 816-821. doi:10.1016/j.concog.2013.05.005

Demirci, K., Orhan, H., Demirdas, A., Akpınar, A., & Sert, H. (2014). Validity and reliability of the Turkish version of the smartphone addiction scale in a younger population. *Bulletin of Clinical Psychopharmacology, 24*, 226-234. doi:10.5455 /bcp.20140710040824

Denzin, N. K. (2012). Triangulation 2.0. *Journal of Mixed Methods Research*, *6*(2), 80-88. doi:10.1177/1558689812437186

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2011). *The SAGE handbook of qualitative research* (4th ed.). Thousand Oaks, CA: Sage.

Dhillon, G., Samonas, S., & Etudo, U. (2016). Developing a human activity model for insider IS security breaches using action design research. In *IFIP International Information Security and Privacy Conference* (pp. 49-61). doi:10.1007/ 978-3-319-33630-5_4

Donahue, K., & Rahman, S. M. (2012). Healthcare IT: Is your information at risk? *International Journal of Network Security & Its Applications, 4*(5), 97-109. doi:10.5121/ijnsa.2012.4508.

Drouvelis, M., & Nosenzo, D. (2013). Group identity and leading-by-example. *Journal of Economic Psychology*, *39*, 414-425. doi:10.1016/j.joep.2013.06.005

Eivazi, K. (2011). Computer use monitoring and privacy at work. *Computer Law & Security Review*, *27*, 516-523. doi:10.1016/j.clsr.2011.07.003

Folta, S. C., Seguin, R. A., Ackerman, J., & Nelson, M. E. (2012). A qualitative study of leadership characteristics among women who catalyze positive community change. *BMC Public Health, 12*, 383-394. doi:10.1186/1471-2458-12-383

Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., & Grimshaw, J. M. (2010). What is an adequate sample size? Operationalizing data saturation for theory-based interview studies. *Psychology & Health*, *25*, 1229-1245. doi:10.1080/08870440903194015

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development*, *91*, 184-194. doi:10.1002/j.1556-6676.2013.00085.x

Fusch, P., & Ness, L. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*, 1408-1416. Retrieved from http://tqr.nova.edu/

Garczynski, A. M., Waldrop, J. S., Rupprecht, E. A., & Grawitch, M. J. (2013). Differentiation between work and nonwork self-aspects as a predictor of presenteeism and engagement: Cross-cultural differences. *Journal of Occupational Health Psychology*, *18*, 417-429. doi:10.1037/a0033988

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

Gökçearslan, S., Mumcu, F. K., Haşlaman, T., & Çevik, Y. D (2016). Modelling smartphone addiction: The role of smartphone usage, self-regulation, general self-efficacy and cyberloafing in university. *Computers in Human Behavior Students*, (30), 639-649. doi:10.1016/j.chb.2016.05.091

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care Chaplaincy, 20*, 109-122. doi:10.1080/08854726.2014.925660

Grover, S. L. (2014). Fair workplace regulation of Internet usage. *Asia Pacific Management Review*, *19*, 99-115. doi:10.6126/APMR.2014.19.1.06

Guba, E. G., & Lincoln, Y. L. (1994). Competing paradigms in qualitative research. In N. K. Dezin & Y. S. Lincoln (Eds.), *The SAGE handbook of qualitative research* (pp. 105-117). Thousand Oaks, CA: Sage.

Harper, M., & Cole, P. (2012). Member checking: Can benefits be gained similar to group therapy? *The Qualitative Report*, *17*, 510-517. Retrieved from http://www.nova.edu/ssss/QR

Harris, K. J., Marett, K., & Harris, R. B. (2013). An investigation of the impact of abusive supervision on technology end-users. *Computers in Human Behavior*, *29*, 2480-2489. doi:10.1016/j.chb.2013.06.008

Harris, M., & Patten, K. (2014). Mobile device security considerations for small-and medium-sized enterprise business mobility. *Information Management & Computer Security, 22*, 97-114, doi:10.1108/IMCS-03-2013-0019

Hassan, H. M., Reza, D. M., & Farkhad, M. A. A. (2015). An experimental study of influential elements on cyberloafing from general deterrence theory perspective case study: Tehran subway organization. *International Business Research*, *8*(3), 91-98. doi:10.5539/ibr.v8n3p91

Hayes, B., Bonner, A., & Douglas, C. (2013). An introduction to mixed methods research for nephrology nurses. *Renal Society of Australasia Journal*, *9*, 8-14. Retrieved from http://www.renalsociety.org/RSAJ/index_nl.html

Hertzum, M., & Holmegaard, K. D. (2013). Perceived time as a measure of mental workload: Effects of time constraints and task success. *International Journal of Human-Computer Interaction*, *29*, 26-39. doi:10.1080/10447318.2012.676538

Hosie, P., Jayashree, P., Tchantchane, A., & Lee, B. S. (2013). The effect of autonomy, training opportunities, age and salaries on job satisfaction in the South East Asian retail petroleum industry. *International Journal of Human Resource Management*, *24*, 3980-4007. doi:10.1080/09585192.2013.829517

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case study research. *Nurse Researcher*, *20*, 12-17. doi:10.7748/nr2013.03.20.4.12.e326

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Journal of Information Security Technical Report, 13*(4), 247-255. doi:10.1016/j.istr.2008.10.010

Hystad, S. W., Mearns, K. J., & Eid, J. (2014). Moral disengagement as a mechanism between perceptions of organizational injustice and deviant work behaviors. *Safety Science*, *68*, 138-145. doi:10.1016/j.ssci.2014.03.012

Inzlicht, M., & Schmeichel, B. J. (2012). What is ego depletion? Toward a mechanistic revision of the resource model of self-control. *Perspectives on Psychological Science*, *7*, 450-463. doi:10.1177/1745691612454134

Jeong, S. H., Kim, H., Yum, J. Y., & Hwang, Y. (2016). What type of content are smartphone users addicted to? SNS vs. games. *Computers in Human Behavior, 54,* 10-17. doi:10.1016/j.chb.2015.07.035

Jia, H., Jia, R., & Karau, S. (2013). Cyberloafing and personality: The impact of the big five traits and workplace situational factors. *Journal of Leadership & Organizational Studies*, *20*, 358-365. doi:10.1177/1548051813488208

Jian, G. (2013). Understanding the wired workplace: The effects of job characteristics on employees' personal online communication at work. *Communication Research Reports*, *30*, 22-33. doi:10.1080/08824096.2012.746221

Karaoğlan Yılmaz, F. G., Yılmaz, R., Öztürk, H. T., Sezer, B., & Karademir, T. (2015). Cyberloafing as a barrier to the successful integration of information and communication technologies into teaching and learning environments. *Computers in Human Behavior*, *45*, 290-298. doi:10.1016/j.chb.2014.12.023

Karimi, L., Gilbreath, B., Kim, T.-Y., & Grawitch, M. J. (2014). Come rain or come shine: Supervisor behavior and employee job neglect. *Leadership & Organization Development Journal*, *35*, 210-225. doi:10.1108/LODJ-05-2012-0066

Kibona, L., & Mgaya, G. (2015). Smartphones' effects on academic performance of higher learning students. *Journal of Multidisciplinary Engineering Science and Technology*, *2*, 777-784. Retrieved from http://www.jmest.org/wp-content/uploads/JMESTN42350643.pdf

Kidwell, R. E. (2010). Loafing in the 21st century: Enhanced opportunities—and remedies—for withholding job effort in the new workplace. *Business Horizons*, *53*, 543-552. doi:10.1016/j.bushor.2010.06.001

Kim, P. T. (2012). The piper lecture: Electronic privacy and employee speech. *The Chicago-Kent Law Review, 87*, 901. Retrieved from http://studentorgs.kentlaw.iit.edu/cklawreview/

Klotz, A. C., & Buckley, M. R. (2013). A historical perspective of counterproductive work behavior targeting the organization. *Journal of Management History*, *19*, 114-132. doi:10.1108/17511341311286222

Koch, A. K., & Nafziger, J. (2016). Gift exchange, control, and cyberloafing: A real-effort experiment. *Journal of Economic Behavior & Organization, 131*, 409-426. doi:10.1016/j.jebo

König, C. J., & Caner de la Guardia, M. E. (2014). Exploring the positive side of personal Internet use at work: Does it help in managing the border between work and nonwork? *Computers in Human Behavior*, *30*, 355-360. doi:10.1016/j.chb.2013 .09.021

Koning, J., & Waistell, J. (2012). Identity talk of aspirational ethical leaders. *Journal of Business Ethics*, *107*, 65-77. doi:10.1007/s10551-012-1297-3

Köpetz, C. E., Lejuez, C. W., Wiers, R. W., & Kruglanski, A. W. (2013). Motivation and self-regulation in addiction a call for convergence. *Perspectives on Psychological Science, 8*, 3-24. doi:10.1177/1745691612457575

Korhonen, J. J. (2014). Big data: Big deal for organization design? *Journal of Organization Design*, *3*, 31-36. doi:10.146/jod.3.1.13261

Král, D. (2011). Information security in small and medium-sized companies. *Economic Studies & Analyses/Acta VSFS, 5*, 61-73. doi:10.1145/2925995.2926003

Kuschnaroff, F. C., & Bayma, F. O. (2014). Critical analysis of cyberslacking in organizational structures. *Journal of Human Resource and Sustainability Studies*, *2*, 70-90. doi:10.4236/jhrss.2014.22007

Lajevskis, V., Dorogovs, P., & Romanovs, A. (2009). IT security system development for state institution. *IT and Management Science*, *40,* 27-32. doi:10.2478/v10143-010-0003-0

Lanaj, K., Johnson, R. E., & Barnes, C. M. (2014). Beginning the workday yet already depleted? Consequences of late-night smartphone use and sleep. *Organizational Behavior and Human Decision Processes*, *124*, 11-23. doi:10.1016/j.obhdp.2014.01.001

Langfred, C. W. (2013). To be or not to be autonomous: Exploring why employees want more autonomy. *North American Journal of Psychology*, *15*, 355-366. Retrieved from http://najp.8m.com

LaRose, R., & Eastin, M. S. (2004). A social cognitive theory of Internet uses and gratifications: Toward a new model of media attendance. *Journal of Broadcasting and Electronic Media, 48*, 358-377. doi:10.1207/s15506878jobem4803_2

Lawrence, J., & Tar, U. (2013). The use of grounded theory technique as a practical tool for qualitative data collection and analysis. *Electronic Journal of Business Research Methods*, *11*, 29-40. Retrieved from http://www.ejbrm.com

Lee, J. L., Jr., Crossler, R. E., & Warkentin, M. (2016). Implications of monitoring mechanisms on bring your own device (BYOD) adoption. *Journal of Computer Information Systems, 3,* 1-10. doi:10.1080/08874417.2016.1184032

Lee, Y. K., Chang, C. T., Lin, Y., & Cheng, Z. H. (2014). The dark side of smartphone usage: psychological traits, compulsive behavior and technostress. *Computers in Human Behavior*, *31,* 373-383. doi:10.1016/j.chb.2013.10.047

Lehmann-Willenbrock, N., Grohmann, A., & Kauffeld, S. (2013). Promoting multifocal citizenship behavior: Time-lagged effects of procedural justice, trust, and commitment. *Applied Psychology: An International Review*, *62*, 454-485. doi:10.1111/j.1464-0597.2012.00488.x

Lim, V. K. G., Teo, T. S. H., & Loo, G. L. (2002). How do I loaf here? Let me count the ways. *Communications of the ACM*, *45*, 66-70. doi:10.1145/502269.502300

Lohle, M. F., & Terrell, S. R. (2014). Real projects, virtual worlds: Coworkers, their avatars, and the trust conundrum. *The Qualitative Report, 19*(8), 1-35. Retrieved from http://nsuworks.nova.edu/tqr/

MacCormick, J. S., Dery, K., & Kolb, D. G. (2012). Engaged or just connected? Smartphones and employee engagement. *Organizational Dynamics, 41*, 194-201. doi:10.1016/j.orgdyn.2012.03.007

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? A review of qualitative interviews in is research. *Journal of Computer Information Systems*, *54*, 11-22. Retrieve from http://www.iacis.org/jcis/jcis.php

Marshall, C., & Rossman, G. B. (2015). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage.

Maxwell, J. A. (2013). *Qualitative research design: An interactive approach* (3rd ed.). Thousand Oaks, CA: Sage.

Miles, M. B., Huberman, A. M., & Saldaäna, J. (2014). *Qualitative data analysis: A methods sourcebook* (Third edition.). Thousand Oaks, California: SAGE Publications, Inc.

Moody, G. D., & Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information & Management*, *50*, 322-335. doi:10.1016/j.im.2013.04.005

Moustakas, C. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage.

Murphy, S. M., Wayne, S. J., Liden, R. C., & Erdogan, B. (2003). Understanding social loafing: The role of justice perceptions and exchange relationships. *Human Relations, 56*, 61-84. doi:10.1177/0018726703056001450

Ng, V., & Rebeiro, J. (2010). Information security issues, strategies and spending in 2010. *Network World Asia*, *6,* 10-13. Retrieved from http://www.networksasia.net

Ofcom. (2015). *The communications market report 2015*. Retrieved from https://www.ofcom.org.uk/research-and-data

O’Neill, T. A., Hambley, L. A., & Bercovich, A. (2014). Prediction of cyberslacking when employees are working away from the office. *Computers in Human Behavior*, *34*, 291-298. doi:10.1016/j.chb.2014.02.015

Onwuegbuzie, A. J., & Byers, V. T. (2014). An exemplar for combining the collection, analysis, and interpretations of verbal and nonverbal data in qualitative research. *International Journal of Education*, *6*, 183-246. doi:10.5296/ije.v6i1.4399

Otto, S. C., Wahl, K. R., Lefort, C. C., & Frei, W. H. P. (2012). Exploring the impact of multitasking in the workplace. *Journal of Business Studies Quarterly*, *3*(4), 154-162. Retrieve from http://jbsq.org

Paulsen, R. (2013). Non-work at work: Resistance or what? *Organization. 22,* 351-367. doi:10.1177/1350508413515541

Petty, N. J., Thomson, O. P., & Stew, G. (2012). Ready for a paradigm shift? Part 2: Introducing qualitative research methodologies and methods. *Manual Therapy*, *17*, 378-384. doi:10.1016/j.math.2012.03.004

Pezalla, A. E., Pettigrew, J., & Miller-Day, M. (2012). Researching the researcher-as-instrument: An exercise in interviewer self-reflexivity. *Qualitative Research*, *12*, 165-185. doi:10.1177/1468794111422107

Piotrowski, C. (2012). Cyberloafing: A content analysis of the emerging literature. *Journal of Instructional Psychology*, *39*, 259-261. Retrieved from http://www.projectinnovation.biz/index.html

Piscotty, R., Martindell, E. & Karim, M. (2016). Nurses' self-reported social media and mobile device use in the work setting. *Online Journal of Nursing Informatics*, *20*(1). Retrieved from http://www.ojni.org

Pollock, K. (2012). Procedure versus process: Ethical paradigms and the conduct of qualitative research. *BMC Medical Ethics*, *13*, 25-31. doi:10.1186/1472-6939-13-25

Rahimnia, F., & Karimi Mazidi, A. R. (2015). Functions of control mechanisms in mitigating workplace loafing: Evidence from an Islamic society. *Computers in Human Behavior, 48*, 671-681. doi:10.1016/j.chb.2015.02.035

Rakes, T. R., Deane, J. K., & Rees, L. P. (2012). IT security planning under uncertainty for high-impact events. *Omega, 40*, 79-88. doi:10.1016/j.omega.2011.03.008

Richards, J. (2012). What has the Internet ever done for employees? A review, map and research agenda. *Employee Relations*, *34*, 22-43. doi:10.1108/01425451211183246

RuningSawitri, H. S. (2012). Role of Internet experience in moderating influence of work stressor on cyberloafing. *Procedia: Social and Behavioral Sciences*, *57*, 320-324. doi:10.1016/j.sbspro.2012.09.1192

Saraç, M., & Çiftçioğlu, A. (2014). What do human resources managers think about the employee's Internet usage? *Anadolu University Journal of Social Sciences*, *14*(2), 1-12. doi:10.18037/ausbd.51987

Sarker, S., Xiao, X., & Beaulieu, T. (2013). Qualitative studies in information systems: A critical review and some guiding principles. *MIS Quarterly*, *37*, 3-18. Retrieved from http://www.misq.org/

Sarpong, S., & Rees, D. (2014). Assessing the effects of "big brother" in a workplace: The case of WAST. *European Management Journal*, *32*, 216-222. doi:10.1016/j.emj.2013.06.008

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*, 503-A5. Retrieved from http://www.misq.org

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data collection in the digital age: innovative alternatives to student samples. *MIS Quarterly, 38*, 355-A20. Retrieved from http://www.misq.org

Thalmann, S., Bachlechner, D., Demetz, L., & Manhart, M. (2014). Complexity is dead, long live complexity! How software can help service providers manage security and compliance. *Computers & security*, *45*, 172-185. doi:10.1016/j.cose.2014.05.012

Tirgari, V. (2012). Information technology policies and procedures against unstructured data: A phenomenological study of information technology professionals. *Academy of Information & Management Sciences Journal*, *15*(2), 87-106. Retrieved from http://alliedacademies.org/aimsj_public.php

Trotter, R. T. (2012). Qualitative research sample design and sample size: Resolving and unresolved issues and inferential imperatives. *Preventive Medicine*, *55*, 398-400. doi:10.1016/j.ypmed.2012.07.003

Tufford, L., & Newman, P. (2012). Bracketing in qualitative research. *Qualitative Social Work*, *11*, 80-96. doi:10.1177/1473325010368316109

Ugrin, J. C., & Pearson, J. M. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior*, *29*, 812-820. doi:10.1016/j.chb .2012.11.005

Unluer, S. (2012). Being an insider researcher while conducting case study research. *The Qualitative Report*, *17*(29), 1-14. Retrieved from http://www.nova.edu/ssss/QR

van Deursen, A. J., Bolle, C. L., Hegner, S. M., & Kommers, P. A. (2015). Modelling habitual and addictive smartphone behavior: the role of smartphone usage types, emotional intelligence, social stress, self-regulation, age, and gender. *Computers in Human Behavior, 45*, 411-420. doi:10.1016/j.chb.2014.12.039.

Vitak, J., Crouse, J., & LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, *27*, 1751-1759. doi:10.1016/j.chb .2011.03.002

Wagner, D. T., Barnes, C. M., Lim, V. K. G., & Ferris, D. L. (2012). Lost sleep and cyberloafing: Evidence from the laboratory and a daylight saving time quasi-experiment. *Journal of Applied Psychology*, *97*, 1068-1076. doi:10.1037 /a0027557

Walker, J. L. (2012). The use of saturation in qualitative research. *Canadian Journal of Cardiovascular Nursing*, *22*(2), 37-46. Retrieved from http://www.cccn.ca

Wang, J., Tian, J., & Shen, Z. (2013). The effects and moderators of cyber-loafing controls: An empirical study of Chinese public servants. *Information Technology and Management*, *14*, 269-282. doi:10.1007/s10799-013-0164-y

Weatherbee, T. G. (2012). Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. *Human Resource Management Review*, *20*, 35-44. Retrieved from https://www.journals.elsevier.com/human-resource-management-review

Werlinger, R., Hawkey, K., Botta, D., & Beznosov, K. (2009). Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies, 67*, 584-606. doi:10.1016/j.ijhcs.2009.03.002

Wilson, C. V. (2012). *Postimplementation planning and organizational structure of enterprise resource planning systems* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 3512581)

Wisdom, J. P., Cavaleri, M. A., Onwuegbuzie, A. J., & Green, C. A. (2012). Methodological reporting in qualitative, quantitative, and mixed methods health services research articles. *Health Services Research*, *47*, 721-745. doi:10.1111/j .1475-6773.2011.01344.x

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Los Angeles, CA: Sage.

Zoghbi-Manrique-De-Lara, P. (2012). Reconsidering the boundaries of the cyberloafing activity: The case of a university. *Behaviour & Information Technology*, *31*, 469-479. doi:10.1080/0144929X.2010.549511

Appendix A: Informed Consent Form

My name is Hawazin Al Abbasi, and I am a PhD candidate in information system management at Walden University. You are invited to take part in a research study on exploring reliable ways organizational leaders and managers use to control cyberloafing behaviors among their employees. I am conducting a doctoral study to explore ways to limit the amount of personal Internet activity (cyberloafing behavior) among employees on their personal smartphones while on the job to minimize wasted work time and to prevent viruses from infecting company information systems and compromising confidential files connected to organizations' Internet system.

In this letter, I am requesting your permission to participate in the research study that will involve an attempt to describe the most effective management strategies to prevent employees from using personal mobile devices for personal activity during work time to increase employees' productivity. This research will form part of my dissertation. This study is being conducted by me, Hawazin Alabbasi, a doctoral student at Walden University. The purpose of this study is to explore reliable ways for organizational leaders to monitor or limit their employees from using smartphone technology for personal use while on the job.

This research project will involve conducting phone, Skype, or face-to-face interviews with you after I send the questions to you via e-mail. Although no computer is fully protected, reasonable efforts will be made to protect your personal information and privacy. I will be the only person to read the transcript of your interview, and if you want to withdraw from this research, you can do so, and I will delete the data immediately. Your participation is voluntary, and there are no feasible risks, but if you want to withdraw from this study, you can do so at any time and for any reason. The information you are providing will remain in a secure location. I will mask your name, your answers, and all identity information will not mention in the study. Data will be kept secure by using a password-protected flash drive that remains in a locked cabinet when not in use. Data will be kept for a period of at least 5 years, as required by the university.

I am doctoral student, and this form is part of a process called informed consent to help you to understand the study before deciding whether to take part. If you have any questions related to this form, please contact me through e-mail at hawazin.alabbasi@waldenu.edu. I am working under Dr. Anthony Lolas's supervision. If you have any concerns regarding your rights or privacy, please contact Dr. Lolas through e-mail at anthony.lolas@waldenu.edu or you can call him on his cell phone: XXX-XXX-XXX. The approval number for this study is……………… and it expires on ……………., 2018.

The researcher will provide you a copy from this form to keep for your records.

Thank you!

Sincerely

Hawazin Alabbasi

I have read and understand the consent form above and the aim of this study, and I am willing to participate in this research voluntarily.

Name of the Participant …...………………………………………….

Date of the Consent ……….…………………………………………….

Participant Signature ………..………………………………………..

Researcher Signature ...……………………………………………….

Hawazin Al Abbasi

CONSENT FORM

You are invited to take part in a research study about "Organizational Information Security Minimizing cyberloafing activity While on the Job"." Cyberloafing is a term refers to any non-work-related activity perform during work hours, and leads to waste working time and minimize employees' productivity. Saraç and Çiftçioğlu (2014) estimated that web surfing costs U.S. employers more than $50 billion a year in lost productivity. The most common issues researched on non-work-related Internet use are productivity loss, Internet cost, and Internet security issues (Saraç & Çiftçioğlu, 2014). Careless employees present serious threats to their organizations when they fail to follow information security and Internet use policies, and such employees lead to reduced job quality and lost productivity (Donahue & Rahman, 2012). Employers are responsible by law for violations when employees misuse the Internet during work time. Misuse can include harassing other employees or creating an uncomfortable work environment by displaying or e-mailing pornographic material (Grover, 2014).

The researcher is inviting participants at Managerial level or IT Managerial and some general understanding of cyberloafing to participant in the study. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part. This study is being conducted by a researcher named Hawazin Al Abbasi doctoral student at Walden University.

Background Information:
The purpose of this research is to explore ways to limit the amount of personal Internet activity (cyberloafing behavior) among employees on their personal smartphones while on the job to minimize wasted work time and to prevent viruses from infecting company information systems and compromising confidential files connected to organizations' Internet system.

Procedures:
If you agree to be in this study, you will be asked to:

- Complete an Informed Consent Form (10 minutes or less to complete.)
- Eligibility is defined as the participant must be in IT Management or at Managerial Professional level, 2-5 years of professional experience and must have a general understanding of cyberloafing problem.
- If deemed eligible, participate in an offline(email) or online (skype or phone) or in person interview that will not exceed 30 minutes to answer the questions.

- Note, the participant is under no circumstances required to complete the interview.
- Once the interview is completed, the researcher will be given the $20.00 gift card if participants asking for it.
- The researcher may need to follow-up with the participant if additional questions arises from the interview. Follow-up interview will be completed in 20 minutes or less.
- Sample interview questions include:
    - What was your experience with cyberloafing in as a department manager or at any managerial level?
    - When you notice a team member texting or surfing several times during working hours or team meeting, how you react?

Voluntary Nature of the Study:
This study is voluntary. You are free to accept or turn down the invitation. No one at Walden University will treat you differently if you decide not to be in the study. If you decide to be in the study now, you can still change your mind later. The researcher will not use your personal information for any purpose outside of this research project." Please note, all volunteers that meets the criteria of possessing a Management knowledge or certification, 2-5 years of Department management or IT management experience and a general understanding of cyberloafing will be invited to participate in the study. Volunteers that do not meet all three criteria's will not be invited to participate in the study.

Risks and Benefits of Being in the Study:
Being in this type of study involves some risk of minor discomforts that can be encountered in daily life, such as fatigued, stress, or boredom.
The proposed study may shed light on ways to improve team behavior and minimize or limit cyberloafing, which could improve team productivity and lead to more positive relationships between team leader and team members.

Privacy:
Reports coming out of this study will not share the identities of individual participants. Details that might identify participants, such as the location of the study, also will not be shared. The researcher will not use your personal information for any purpose outside of this research project. Participants will receive a copy of the transcribed notes the interview via a secure email with a password for entry. The researcher will take precautions to maximize security, and will keep all data for the study secured and safe. Data will be stored in an electronic cabinet that only the researcher can access. The password for this data will use 23 characters with a mix of letters, numbers, and special characters. The researcher will keep all physical data (e.g. informed consent forms, printed transcripts, interview protocol, notes and/or audiotape) in a fire-protected safe in my home office. The researcher will keep all data in its original form and in the safe for 5 years as required by Walden University. After the 5-year period, the researcher will

cross-shred files, burn the physical data, and wipe all electronic data from the electronic file cabinet.

Contacts and Questions:

You may ask any questions you have now. Or if you have questions later, you may contact the researcher via email at hawazin.alabbasi@gmail.com.If you want to talk privately about your rights as a participant, you can contact Dr. Leilani Endicott e-mail at irb@mail.waldenu.edu. The approval number for this study is 06-12-17-0263671 and it expires on June 11th, 2018.

For online research or when consent is done via e-mail, use: Please print or save this consent form for your records.

Obtaining Your Consent

If you feel you understand the study well enough to make a decision about it, please indicate your consent by replying to this email with the words, “I consent.”

Appendix B: Participants Demographics

Participant Code	Position	Certificates	Gender	Years of Experience	Interview Method	Industry
HRM-P1	Human Resource Manager	Master degree in business administration(MBA)	F	5	E-mail	Education
AMU-P2	Administrative Manager @University	Master degree in business administration(MBA), PMP	M	17	E-mail	Education
ITM-P3	Information Technology Manager	Cisco Certified Network Associate (CCNA) security	M	8	Skype Call	Telecommunication
HRM-P4:	Human Resource Manager	Master degree in human resource (MHR)	M	5	Skype Call	Education
HRM-P5	Human Resource Manager	Master degree in human resource (MHR)	M	8	Cell phone Call	Education
ITS-P6	Information Technology Specialist	Certified Information Systems Security Professional (CISSP)	M	10	E-mail	Telecommunication
AMS-P7	Administrative Manager @School	Master degree in business administration (MBA), PMP	F	5	Skype Call	Education
ITM-P8	Information Technology Manager	BSc. in information system management	M	10	Skype Call	Education
HRM-P9	Human Resource Manager	Master degree in business administration(MBA)	F	15	Skype Call	Education
ITM-P10	Information Technology Manager	Bachler degree in computer science, CCNA security	M	6	Cell phone Call	Education
ITM- P11:	Information Technology Manager	MSc. in computer science, A+	M	6	Skype Call	Education
ITM- P12	Information Technology Manager	MSc. in information system management.	M	6	Cell phone Call	Education
ITS-P13	Information Technology Specialist	BSc. in computer science, A+	M	5	Cell phone Call	Education
ITM-P14	Information Technology Manager	MSc. in information system (MIS), PMP	M	5	E-mail	Education
HRM-P15	Human Resource Manager	Master in human resource(MHR)	M	9	Cell phone Call	Education
FLS-P16	Frontline Supervisor	Bachler degree in business administration (BBA)	M	5	Cell phone Call	Education

FLS-P17	Frontline Supervisor	Bachler degree in business administration (BBA)	M	6	Cell phone Call	Education
AMS-P18	Administrative Manager School	Master degree in business administration (MBA)	M	12	Skype Call	Education
HRM-P19	Human Resource Manager	Master degree in human resource (MHR)	M	10	Skype Call	Telecommunication
ITS-P20	Information Technology Specialist	MSc. in Information System management (MIS)	M	5	E-mail	Telecommunication