2021

Strategies to Monitor and Deter Cyberloafing in Small Businesses: A Case Study

Veronica Pugh Dooly
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Veronica Dooly

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. Jodine Burchell, Committee Chairperson, Information Technology Faculty
Dr. Jose Feliciano, Committee Member, Information Technology Faculty
Dr. Gary Griffith, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2021

Abstract

Strategies to Monitor and Deter Cyberloafing in Small Businesses: A Case Study

by

Veronica Pugh Dooly

MS, University of Maryland University College, 2005

BA, King University, 2001

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2021

Abstract

Some information technology (IT) managers working for small businesses are struggling to monitor and deter cyberloafing. Strategies are needed to help IT practitioners to discourage cyberloafing and improve productivity while maintaining employee satisfaction. Grounded in adaptive structuration theory, the purpose of this qualitative multiple-case study was to explore strategies some small business IT managers use to monitor and deter cyberloafing. The participants were nine IT managers who successfully implemented cyberloafing monitoring and deterrence strategies in the United States. Data were collected via semistructured interviews and organization employee policy handbooks (*n* = 4) provided by the participants. Data were analyzed using thematic analysis. The major themes were using tools, policy, and procedures to monitor cyberloafing and using tools, trust, and policies as strategies to deter cyberloafing. One recommendation for practitioners is to incorporate hardware and software tools to monitor and deter cyberloafing early when hiring employees for a small business. The implications for positive social change include the potential to foster greater economic stability in the community while promoting a healthy working environment.

Strategies to Monitor and Deter Cyberloafing in Small Businesses: A Case Study

by

Veronica Pugh Dooly

MS, University of Maryland University College, 2005

BA, King University, 2001

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2021

Dedication

I dedicate this study to my parents, Donald Edwin Pugh and Mary Louise Pugh. From an early age, they taught me the value of hard work and to be a lifelong learner. I wish you both were here to see it finished.

Acknowledgments

First, I want to thank my chair, Dr. Jodine Burchell. Her voice was full of song every time I spoke with her. She worked with me through some deep personal setbacks and never gave up on me. I also want to thank my committee members, Dr. Jose Feliciano, and Dr. Gary Griffith, for their time and energy in helping me get the study completed.

Thank you to my husband, Mark Dooly. You never lost faith even when mine faltered. Thanks for taking over the cooking and the laundry. Thank you also for trying very hard on the other housework.

I need to thank my daughter, Katherine Dooly Jones, and friend, Brenda McFarland, for letting me call anytime to vent. To my sister, Paula Pugh, thank you for the hugs with the tears and the celebrations of the major accomplishments of getting three pages written in a single day.

Also to the friends, family, and church members who are too many to mention. Thank you for the thoughts and prayers throughout this process.

Lastly, I need to thank my Lord, Jesus Christ, for gifting me with the ability to persevere.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Background of the Problem

When employees have access to the internet on the job, there is a temptation to access it for personal reasons. Accessing company internet resources during working hours is known as *cyberloafing* (Lim, 2002). Cyberloafing increases risk to business by threatening the efficiency and security of the information technology (IT) system (Koay, 2018). There is also employee compensation for work undone due to time diverted to nonproductive internet activities. IT managers seek to minimize the risks inherent in employee cyberloafing (Mercado et al., 2017). One way to do so is to reduce nonproductive behavior.

Businesses and other organizations need strategies in place to reduce nonproductive behavior (Jiang et al., 2020). Workers will sometimes shy away from sending confidential personal email more because they are afraid that the network is not secure than because of the time wasted (Spence, 2002). However, more specific strategies need to be in place to reduce and potentially eliminate cyberloafing (Akbulut et al., 2017). Small businesses need monitoring and deterrence strategies.

Any IT project comes with a cost. The implementation of strategies to monitor and deter cyberloafing can be a significant cost to an organization (Mercado et al., 2017). Smaller businesses must often be creative in developing strategies on a much more limited budget than large organizations (Curry et al., 2017). A practical model for monitoring and deterring cyberloafing can help IT managers cost-effectively reduce risk with the limited resources of small businesses.

Problem Statement

Employees using the internet for personal tasks, known as cyberloafing, threatens security, company privacy, and employee productivity (Koay, 2018). Up to 62% of American employees use the internet for reasons other than work, thus participating in cyberloafing (Mercado et al., 2017). Although cyberloafing may occur in any organization regardless of type or size, larger organizations are more likely to have the requisite resources to handle issues related to cyberloafing than smaller businesses are (Curry et al., 2017). The general IT problem is that cyberloafing is prevalent in organizations and needs to be countered for productivity and security. The specific IT problem is that some IT managers lack strategies to monitor and deter cyberloafing in small businesses.

Purpose Statement

The purpose of this qualitative, multiple case study research was to explore the strategies used by IT managers to monitor and deter cyberloafing in small businesses. The classification of a small business varies by industry, with 100 to 200 employees usually being the defined maximums (Small Business Administration, 2017). The population for this study was IT managers of small businesses who reported strategies to monitor and deter cyberloafing and were located in the United States. In addition to interviews, I conducted document reviews of policy and kept a journal of the research process, as I served as the main data collection tool in my role as the researcher. This study has implications for positive social change, in that it may contribute to greater economic stability in the community as small businesses increase productivity and reduce risk through strategies to control cyberloafing behavior while increasing employee satisfaction in the workplace.

Nature of the Study

Although several methods of study could be proper for the topic of cyberloafing, I chose a qualitative method. Qualitative research occurs in natural settings, with the researcher as a key instrument, using complex reasoning to interpret data (Cruz, 2015). These features and the need for an in-depth exploration led to the choice of a qualitative design for this study. Quantitative design requires the development of hypotheses and provides statistical support in research (Xia, 2017). Statistical significance is not needed in the observation of a phenomenon to understand why or how it happens, so the quantitative method was not appropriate for this study. The mixed methodology uses a combination of both qualitative and quantitative data collection and analysis (Baškarada & Koronios, 2018). Because I did not collect quantitative data for this study, a mixed methodology was not appropriate. In-depth understanding, a natural setting, and the researcher as a key instrument were characteristics of this study leading to the choice of qualitative design.

After considering several research designs, I chose a multiple case study. Researchers use case study design in real-life settings that are bounded to explore and understand complex issues (Yin, 1981). I studied cyberloafing monitoring and deterring within the bounds of small business organizations in the southeastern United States. Other qualitative designs that I considered but dismissed were ethnography, action research, and phenomenology. Ethnographic research focuses on describing the culture of a group (Friberg, 2016), which was not the intent of this research. Action research involves an effort to solve a logical problem with which the researcher is actively involved (Yang et al., 2017). As the researcher, I was not actively involved in the organizations of the multiple case study, so action research was not appropriate. In phenomenology, researchers focus on individuals' lived experiences, often regarding a specific event (Danielsson & Rosberg, 2015). Phenomenology was not chosen because the study did not focus on individual perceptions of a specific event. The characteristics of a bounded system, the use of multiple sites for greater data gathering and analysis, and a complex set of "how" and "why" questions were within this study, which led me to choose a multiple case study design.

Research Questions

The primary research questions for this study were as follows:

Q1: What strategies do IT managers use to successfully monitor cyberloafing in small businesses, so that inappropriate usage is discovered?

Q2: What strategies do IT managers use to successfully deter cyberloafing in small businesses, so that inappropriate usage is minimized?

Interview Questions

1. How have you observed users using the internet or other resources for personal use?
2. What policies do you have that address the restriction of computer usage, particularly the internet and email, to only business purposes?

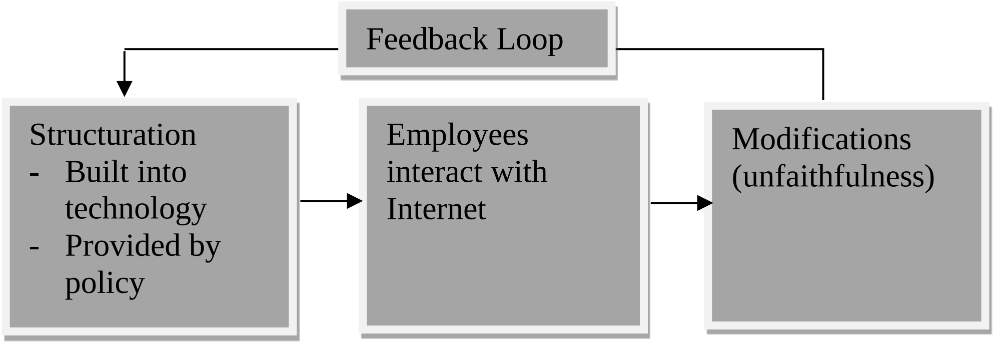
3. How do you update policies if you discover a violation or deviation by the users?
4. What monitoring software do you use to observe user interaction with the computers?
5. How do you monitor computer usage in addition to monitoring software?
6. What deterrence mechanisms do you have in place to prohibit personal usage of computer resources and the internet?
7. What happens if an employee misuses computer resources or the internet?
8. What happens if the misuse is repeated?
9. How successful are your mechanisms to deter cyberloafing?
10. What, if anything, would you have done differently when implementing your cyberloafing monitoring and deterrence program?
11. Is there any other information you can share that would be useful in understanding cyberloafing in your organization?

Conceptual Framework

Poole and DeSanctis (1990) introduced adaptive structuration theory (AST) as an information systems extension of structuration theory. DeSanctis and Poole (1994) used the theory to explain technology usage within the following constructs: (a) structure is designed into technology and created by the organization, (b) the structure defines how the technology should be used, and (c) groups will modify the structure to either use the technology more efficiently or to misuse it. Misusing a technology is being unfaithful to the structuration (Chin et al., 1997). Understanding how employees may be unfaithful to technology leading to cyberloafing helps in the monitoring and deterrence decisions of IT managers. According to AST, the organization creates structure, and this should be observed within the defined usage policies for the internet and monitoring technologies. Employees will then modify the structure. IT can observe the modifications that indicate unfaithfulness to the structure through monitoring and use this information to update deterrence policies. Figure 1 is a representation of the extension of AST to provide feedback to IT managers.

Figure 1

Graphical Model for Adaptive Structuration Feedback



Definition of Terms

Cyberloafing: Use of an organization’s internet access for personal purposes during work hours (Lim, 2002).

Electronic monitoring: Tool for fighting cyberloafing by tracking employee internet activity with mechanisms to track websites visited and record browsing history (Askew & Buckner, 2017).

Emergent structure: New definition of the usage of a system after users have modified the intended structure (Stoffregen & Pawlowski, 2018).

Policy: Framework of cyberloafing for an organization (Yang et al., 2016).

Procedure: Steps required to complete a task (Maymi et al., 2017).

Structure: Definition of how employees should use the technology (DeSanctis & Poole, 1994).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are ideas that a researcher accepts as truth, which may not have concrete proof and are documented to reduce misunderstanding (Ellis & Levy, 2009). For this research, the first assumption was that there were small businesses with good strategies in cyberloafing monitoring and deterrence to include as participants in the study. A second assumption was that there would be at least one IT manager in each business to interview, and that person would provide valuable data to inform the study. It was possible that due to the nature of small businesses, the person wearing the IT hat might not be an IT professional. A third assumption was that participants would answer the interview questions truthfully.

Limitations

A limitation is a potential problem or weakness that could threaten internal validity (Ellis & Levy, 2009). A key limitation was that as an instructor in the computer IT field, I might have bias concerning how monitoring should occur and what should be monitored in the workplace. I had to process the potential bias during the data analysis so that any potential bias did not affect interpretation. A second limitation was the small sample size. With a small group of cases, I needed to find enough sites to reach saturation. The estimated number needed for saturation was eight to 10 small businesses. A third limitation was the small geographical area of the study. Case studies are not generalizable due to their focus on a small population, further limiting the study. By completing a multisite case study at various sites, I increased generalizability.

Delimitations

Delimitations refer to the bounds of a study as defined by factors, constructs, or variables included or excluded from the study (Ellis & Levy, 2009). One delimitation was that IT managers were the only managers included in the study. Other management might have valuable insight into the monitoring and deterrence needs of the organization. The population was a delimitation because it was bound by the geographical area, which was two states in the southeastern portion of the United States. The research questions were also delimitations. I chose the research questions to help in understanding the process of monitoring and deterring cyberloafing on systems within the organization. I did not consider the ramifications of bring your own device (BYOD) items in this study.

Significance of the Study

Contribution to Information Technology Practice

Cyberloafing threatens the efficiency and security of an IT system. IT managers are charged with providing support to an organization that is efficient and secure. Therefore, IT managers seek to minimize the risks inherent in employee cyberloafing. These risks include lower production and the possibility of malware or other security issues. This study is significant to IT practice in that it may provide a practical model for IT managers to establish monitoring and deterrence policies in small businesses. A significant practical model can help IT managers cost-effectively reduce risk with the limited resources of small businesses.

Implications for Social Change

This study has implications for positive social change in that it may contribute to greater economic stability in the community while promoting a healthy working environment. Employees need work-life balance (Soh et al., 2017). Greater economic stability is accomplished through controlling cyberloafing by increasing productivity and reducing risk. Economic stability can lower the stress level of employees. Reducing stress reduces burnout (Kim & Christensen, 2017). Productivity may increase due to less time spent on cyberloafing by employees, which can result in fewer working hours on specific projects as wasted time is eliminated. Small businesses can also reduce the risk of loss due to security issues that could ensue with inappropriate internet usage, such as visiting harmful websites. This study may contribute to positive social change by gathering strategies to help small businesses to succeed in monitoring and deterring cyberloafing while maintaining work-life balance for employees.

A Review of the Professional and Academic Literature

Prevalence of cyberloafing at work exists where personal use of technology takes away from business uses (Kim & Christensen, 2017). Managers need to ensure that cyberloafing behavior does not become counterproductive or detrimental to the company (Sampat & Basu, 2017). Cyberloafing increases the risk to business by threatening the efficiency and security of IT systems when, instead of working, employees go to websites that could introduce malware to their system (Koay, 2018). The purpose of this study was to explore how small businesses use strategies to monitor and deter cyberloafing activities. I developed two research questions for this study. First, what strategies do IT managers use to monitor cyberloafing in small businesses successfully, so that inappropriate usage is discovered? What strategies do IT managers use to deter cyberloafing in small businesses successfully, so that inappropriate usage is minimized?

This literature review begins with an explanation of the conceptual framework of the study, AST. AST is a framework used to explain how employees modify working procedures to cyberloaf (Barrett, 2018). The discussion includes an analysis of the framework, along with an analysis of supporting and contrasting frameworks and theories. After the discussion of the framework is an analysis of the themes/phenomena discovered in the review of the literature. The first theme is why cyberloafing occurs. The second is the importance of dealing with cyberloafing as viewed through organizational and personal risk management and ethical considerations. The third theme is dealing with cyberloafing in terms of monitoring, change management, compliance, policy, and procedures. The final theme is the defining characteristics of small businesses, the population of the research. After the themes, there is a discussion of the relationship of this study to previous research. Last, there is a transition and summary section.

The research strategy for the literature review was to access materials via the Walden University Library database-launching page. The results yielded articles from the EBSCOhost, ProQuest, SAGE Premier, Business Source Complete, Emerald Management, and Science Direct databases. Keywords used in the searches included *cyberloafing*, *cyberslacking*, *risk management*, *risk mitigation*, *monitoring*, *deterrence*, *compliance*, *counterproductive work behaviors*, *neutralization*, *internet abuse*, *small business*, *computer policy*, *usage policy*, *adaptive structuration theory*, and *structuration*.

There are 114 articles and one book referenced in this literature review. Of the articles, 93% were peer reviewed, and 85% were published in 2017 or later. Five of the older articles, 4% of the total articles, and the book are seminal in their fields.

Application to the Applied Information Technology Problem

The purpose of this research study was to explore the strategies used by IT managers to monitor and deter cyberloafing in small businesses. In this study, small businesses were those with fewer than 100 employees. The population for this study was IT managers of eight small businesses that had strategies to monitor and deter cyberloafing in the southeastern United States. I used interviews, review of policy documents, and a journal of the research process to conduct the research. The purpose of this literature review is to identify the conceptual framework, key themes, and current trends in the research on cyberloafing.

Conceptual Framework: Adaptive Structuration Theory

A conceptual framework aids in the understanding of a topic by providing a language to illustrate concepts (Bicket et al., 2019). AST was chosen for this study because it helps in explaining how users take IT and make it their own, for good or bad. Poole and DeSanctis (1990) introduced AST as an information systems extension of structuration theory. AST is widely used in the study of collaborative systems to account for the system and the individuals using the system (Bresciani & Comi, 2017). According to AST, an organization creates structure, and this structure is observable within the defined usage policies for the internet and monitoring technologies. DeSanctis and Poole (1994) used the theory to explain technology usage within the following constructs: (a) structure is designed into technology and created by the organization, (b) the structure defines how the technology should be used, and (c) groups will modify the structure either to use the technology more efficiently or to misuse it. Misusing a technology is being unfaithful to the structure designed into the technology (Chin et al., 1997). Understanding how employees may be unfaithful to the technology in a manner that leads to cyberloafing helps in the monitoring and deterrence decisions of IT managers.

AST in Recent Research

AST developed as a method to explain how social interactions of groups can lead to changes in how employees use technology and resulting changes in rules. Early research focused entirely on groups and social interactions when working with technology. This early research included group decision making with group decision support systems and helped define the parameters of AST (DeSanctis & Poole, 1994). Chin et al. (1997) developed AST further by adding a measurement for faithfulness to the original structure of technology by studying groups using electronic meeting systems. AST guided studies of business software that helped groups of people interact with each other. This usage of AST continued but is now evolving.

In the last 5 years, AST has been prevalent in education and healthcare studies along with business functions. Additionally, researchers are beginning to use AST to explain how individuals can modify a system’s structure. Bondarouk et al (2017) partially applied AST to explain the adoption of electronic human resource management, which is a business application. Bresciani and Comi (2017) used AST to study group meetings but added the element of a culturally diverse group. In healthcare, Barrett (2018) used AST to explain the integration of electronic health records and showed that mandated technologies are more useful when employees modify them to fit their needs. In education, Stoffregen and Pawlowski (2018) used AST to study e-learning in massive open online courses (MOOC) for business training. Sun et al. (2020) used AST to study MOOCs in a university setting. These studies on MOOCs focused on groups modifying structures to improve learning (Stoffregen & Pawlowski, 2018). Zha et al. (2019) used AST as a framework to study innovative information seeking through digital libraries. In business research, Turner et al. (2019) discussed the relevance of AST in human resource development. Janson et al. (2020) used AST for their framework when studying problem solving training. Schmitz et al. (2016) expanded AST to consider the individual as a change agent for structure in a system. This addition of AST as an application to an individual relates directly to this study on cyberloafing.

Analysis of AST

The purpose of AST is to determine how users contribute to the evolution of technology. Users adapt technology and processes so that the technology better suits their preferences or working habits (Barrett, 2018). Over time, users reshape technology through their interactions with it, the social structure of the organization, and human factors (Stoffregen & Pawlowski, 2018). It is the act of transforming the rules of the structure that is the social element of structuration (Turner et al., 2019). Employees will modify a task to better use technology or modify the technology to accomplish the task more efficiently (Barrett, 2018). When a new technology is introduced, employees will begin to modify the technology itself, along with any workplace rules and environments affected by the technology.

Introducing a technology will trigger employees to change how resources and rules within an organization best serve their own needs (DeSanctis & Poole, 1994). Users can work with technologies, make judgments about them, or display different attitudes toward them, leading to adaptions in technology usage (Bondarouk et al., 2017). People may, therefore, use a technology faithfully as created, adapt it to better suit their needs and workflow, or ignore the technology or some of its features (Barrett, 2018). Adaptations not only change how technology functions, but also affect workplace tasks that involve technology (Schmitz et al., 2016). Adaptation in this form is an appropriation of technology.

In appropriation, employees modify technology with the hope of improving it (Barrett, 2018). Users shape and reshape technology from development to everyday usage (Stoffregen & Pawlowski, 2018). This reshaping is being unfaithful to the designed structure of the technology (Chin et al., 1997). However, unfaithfulness can lead to positive or negative consequences. This unpredictability of technology implementation and use is why AST provides a viable framework for studying appropriation (Barrett, 2018). As users interact with technology, modification of the technology is part of the adoption process. How the modification takes place is through structuration.

Structuration. Structuration is the main precept of AST. Structuration is the process that groups use to create and maintain order within a social system (Chin et al., 1997). Through the structuration process, users or user groups shape norms, values, and resources (Stoffregen & Pawlowski, 2018). Over time, groups using the technology create emergent structures that deviate from the base structure envisioned by the organization (Stoffregen & Pawlowski, 2018). The emergent structures can improve workflow for the user or lead to practices, such as cyberloafing, that are detrimental to the organization.

When users are working with technology, their actions create modifications to organizational structure (Iyamu, 2017). Allowing users to adapt structure might lead to a better workflow (Barrett, 2018). Managers need to make sure that adaptations are positive. One method to help employees increase the contribution of adaptation is to give them freedom of decision-making authority (Schmitz et al., 2016). Structuration, as a stand-alone theory, involves the interplay between structure and the user (Iyamu, 2017). Learning is essential early in the structuration process but has diminishing returns (Schmitz et al., 2016). Structures and their adaptation give meaning to the technology in its everyday use.

AST usually involves the assumption that structuration is a group function. Schmitz et al. (2016) noted that AST is extendable to study how individuals adapt technology. In this study, I used AST to examine how individuals modify the usage of web access technologies, such as the internet, to serve their own needs.

Application to the Applied Information Technology Problem

Analysis of Supporting Theories

I considered many alternative frameworks for this study before choosing AST. Some theories that I explored had names with terms that were suggestive of this study's topic, such as *deterrence*, *consequences*, and *disruption*. Researchers used other theories in previous cyberloafing research, leading to consideration of those theories for this research. An analysis of some of these theories and explanations for why they were not chosen for this study are presented in this section. I begin with supporting theories followed by contrasting theories.

Technology Acceptance Model (TAM)

TAM supports the research in this study as it explains how users accept technologies. TAM is one of the most used models for determining technology acceptance (Fedorko et al., 2018). Researchers utilize TAM as a framework in many fields. TAM serves as the basis for research in areas such as education (Anni, 2018; Deslonde & Becerra, 2018; Joo et al., 2018), crowdfunding (Thaker et al., 2018), health (Rönnby et al., 2018), banking (Marakarkandy et al., 2017), e-commerce (Fedorko et al., 2018), and the car industry (Koul & Eydgahi, 2018). TAM's prevalent usage makes it a logical choice for consideration as a framework for any research.

The ability of TAM to predict acceptance of new technology is the reason for its extensive use. TAM explains the acceptance of technology in terms of perceived usefulness and perceived ease of use (Nawaz et al., 2017). Perceived usefulness reflects the degree to which users see the technology as helpful in completing a task or increasing performance (Fedorko et al., 2018). Perceived use predicts the degree to which users see themselves using technology without difficulty (Joo et al., 2018). The basis of TAM is the theory of reasoned behavior, which posits that beliefs and attitudes predict intention to perform a behavior (Fedorko et al., 2018). These beliefs and attitudes form external variables that affect perceived usefulness and perceived ease of use (Joo et al., 2018). When a user believes a technology to be easy to use and useful to a task, the user adopts the technology. Adoption is not adaption. Cyberloafing behaviors form with the adaptation of the technology for personal use. This study was on misuse rather than acceptance of the internet as a technology. TAM does not address misuse, so TAM was not suitable as a framework.

Punctuated Social-Technical Information System Change Model (PSIC)

PSIC posits that technology acceptance is a change that includes both the technology and social elements of the users (Luna-Reyes et al., 2005). Reimers et al. (2014) added the elements of task and organizational structure when determining the deep structure of a system. Deep structure is the fundamental structure and usage of a system (Romanow et al., 2018). PSIC is like TAM in that it seeks to explain technology acceptance but adds the structuration found in AST (Luna-Reyes et al., 2005).

Technology acceptance is a result of change or is a catalyst for change in a system. PSIC models change in the system.

PSIC predicts punctuated change, which has phases that are stable with interspersed periods that are rapid and/or drastic (Reimers et al., 2014). In addition to punctuation, change is multilevel. The levels are interdependencies within the work system, the building system, and the environment plus the temporal interactions (Salmimaa et al., 2018). PSIC also maintains that change is evolutionary while gradual (Reimers et al., 2014). As the system develops from a building system to a working system, it evolves at a steady pace with some punctuated activity. Although PSIC explains the building and acceptance of a system, the theory does not address the misuse of a system, which was the topic of this research.

Cyberloafing is misuse that occurs as new practices within the structure of the system. PSIC does not explain the appearance of new practices (Reimers et al., 2014). PSIC assumes random or chaotic behaviors of users (Iannacci et al., 2019). Cyberloafing is intentional and only random in timing. The inability of PSIC to explain new practices made it inappropriate as the framework of this study.

Analysis of Contrasting Theories

The analysis of contrasting theories is the topic of this section. Interestingly, theories that originally supported the research can turn out to be just the opposite. Such is the case with these theories: innovative work behavior and general deterrence theory.

Innovative Work Behavior (IWB)

Employees can be innovative in finding ways to use technology inappropriately at work. Although eventually discarded as not a proper fit, I considered IWB as a potential framework for this study. IWB posits that developing employee creativity will result in the organization being more innovative (Shah et al., 2020). The framework explains how organizations adapt to changing conditions through innovation. Innovation within this framework is beneficial to the organization.

Employee creativity helps in the adaptation to change. An organization performs better when the employees are innovative (Atitumpong & Badir, 2018). Innovation breeds the creativity needed for an organization to be effective (Theurer et al., 2018). The outcomes for the organization are new and improved methods to complete tasks (Woods et al., 2018). Innovative employees are doing more than the basic tasks required for their jobs and improve the organization in the process.

The creativity of innovation results in the improvement of processes. The employees generate new ideas that lead to better procedures or products (Woods et al., 2018). Employees then take their ideas and implement them (Atitumpong & Badir, 2018). IWB helps employers identify and build on characteristics of employees that promote innovation. The innovation that results improves the organization.

There are several characteristics of innovative employees. The predominant characteristic is creativity, which is the hallmark of an innovative person and necessary for idea generation (Theurer et al., 2018). IWB recognizes openness as a characteristic. Openness shows flexibility, curiosity, and imagination formed from the experience that comes from the job (Woods et al., 2018). Another characteristic is the lack of fear of the unknown that leads to experimentation (Atitumpong & Badir, 2018). Conscientiousness is a characteristic found through IWB that leads to reliability in job performance (Woods et al., 2018). Lastly, a desire to improve knowledge and skills is a characteristic of innovative people seen through the lens of IWB (Atitumpong & Badir, 2018). Highly innovative people exhibit these characteristics and organizational benefits. However, innovative people cannot benefit the organization without support.

Support from management is necessary to foster an innovative environment. Management recognizes that ideas take time to develop and implement (Woods et al., 2018). Management promotes the realization of the ideas created by innovative employees (Theurer et al., 2018). Stoffers and Van der Heijden (2018) demonstrated that supervisors' innovative behavior encourages employees' innovative behavior. Managers develop a culture of innovation to promote creativity. Within this culture, employers give credit to ideas that succeed and place no blame when ideas fail (Atitumpong & Badir, 2018). A culture of innovation produces greater creativity.

IWB posits that innovation is beneficial to an organization (Atitumpong, & Badir, 2018). Researchers consider cyberloafing counterproductive (Sampat & Basu, 2017) or a risk to business (Koay, 2018). Andel et al. (2019) argue that employees that cyberloaf are more innovative and perform at a higher level from them being more refreshed by taking a break from the work routine. Akar and Karabulut Coskun (2020) found that cyberloafing has a positive impact on behaviors including performance, scholarly, and artistic activities. Innovation is beneficial to the organization and a basic tenant of IWB.

However, IWB encourages idea creation and implementation not found in the behaviors associated with cyberloafing. IWB also does not address the monitoring of internet activities. For these reasons, IWB is not appropriate for this study.

General Deterrence Theory (GDT)

GDT posits that threats by authority will modify behavior (Bhattacherjee & Shrivastava, 2018). These threats work best if followed with a punishment of some sort. Punishment can be severe, including capital punishment for malicious, violent crime, as studied by Forst (1983). GDT assumes there is a correlation between the risk of punishment and the perception of the risk, although Nixon and Barnes (2018) did not find that to be true. GDT also assumes that individuals are rational and compare the cost of the crime to the expected benefits when choosing to commit the crime (Bhattacherjee & Shrivastava, 2018). Regarding cyberloafing behavior, the user would compare the risk of discovery to the benefit of acting upon the behavior.

The correlation between risk of punishment and perception of risk found in GDT was the reason I considered the theory for the framework of this study. However, GDT use for conflict and criminal activities is more appropriate. Additionally, modifying cyberloafing behavior through punishment may increase the behavior according to previous research (Kim, 2018). Although Hensel and Kacprzak (2020) found that both those that have and have not been punished will reduce cyberloafing. Basing this study on a framework that encourages only threats and punishments as deterrents is not desirable to me as the researcher.

Summary of Conceptual Frameworks

I presented an analysis of the chosen conceptual framework, AST, along with TAM, PSIC, IWB, and GDT. Several frameworks not included but considered for this study were consequentialism, contingency theory, the theory of planned behavior, and social learning theory. All these theories had aspects that were promising but did not match the study as well as AST does. AST provides the best framework for the observation of modifications to the system through cyberloafing and mechanisms to deter through policy.

Analysis of Potential Themes/Phenomena

There are several themes observable in the literature concerning this research study. Primary themes are why people choose to cyberloaf, ethical considerations, tools used to manage cyberloafing, and the definition of a small business. This section includes a discussion of each primary theme with any applicable subthemes.

Choosing Whether to Cyberloaf

Cyberloafing occurs when employees have access to use the internet on the job and access it for personal reasons (Lim, 2002). Cyberloafing can range from minor infractions such as sending emails or playing computer games to major infractions such as engaging in identity theft or taking company data hostage (Venkatraman et al., 2018). Cyberloafing is further complicated due to the intertwining boundary of work and private lives (Soh et al., 2017). Employees check work email at home and private email at work, for example. There are multiple reasons people choose to go from a quick check of email to wasting a large amount of time on the internet.

There are a variety of potential reasons, to cyberloafing identified in the literature. The possible reasons to cyberloaf are referred to as antecedents, including gender, age, pleasure, internet skill level, rationalization, and organizational justice (Banerjee, & Thakur, 2016). Understanding the antecedents is necessary when looking for ways to discourage employees from cyberloafing (Sampat, & Basu, 2017) and managing behaviors that may lead to poor security (Hadlington, & Parsons, 2017). The reasons users choose not to cyberloaf are also varied. These reasons include self-control, fear of discovery, and fear of punishment (Mercado et al., 2017). Some of the factors could be an influence for or against the choice to cyberloaf depending on the person. There are two general groups of factors, organizational factors, and personal factors.

Organizational Factors That Affect the Choice to Cyberloaf. Organizational factors that affect the choice of whether to cyberloaf is the lesser studied of the two groups. Examining organizational factors gives insight into the choices of the users. Understanding these choices aids in understanding why productivity fails during working hours (Sampat, & Basu, 2017). Users will sometimes cyberloaf during office hours to enhance work-life balance (Soh et al., 2017). Organizational factors are part of the neutralization process in which users will justify the benefits of cyberloafing over the perceived discipline (Cheng et al., 2014). Some users will choose to cyberloaf because they feel the organization owes them something while others do not have these feelings or choose not to act upon their feelings.

Organizational Justice. Organizational justice is often an antecedent for cyberloafing, as found by one of the earliest researchers on the topic of cyberloafing

(Lim, 2002). For example, giving higher wages will often lead to more productivity by those that felt their pay was too low (Rojas-Fallas & Williams, 2020). Perceived unfairness in wages led to a lack of productivity through cyberloafing and other activities. A perceived imbalance in treatment will lead employees to find ways to redistribute justice (Lim, 2002). For example, a worker feeling workplace ostracism will cyberloaf in part to set things right (Koay & Soh, 2018). Organizational justice is positively related to organizational trust, which increases productivity when trust is high (Oosthuizen et al., 2018). Organizational justice is not the only factor that contributes to the choice of whether to cyberloaf.

Organizational Attributes. Organizational structure, climate, culture, and size may also be factors to varying degrees. Structure, in this case, refers to private or public institutions. Employees at public organizations are more likely to cyberloaf due to a perception of lesser penalties (Huma et al., 2017). Banerjee and Thakur (2016) defined climate as working hours and organizational ethics, finding that cyberloafing takes place in organizations with long working hours but on a small scale. Gorenc et al. (2016) describe the organizational climate in terms of remuneration, career development, and satisfaction. Gorenc et al. (2016) found that organizational climate does not serve as an antecedent to cyberloafing at all. Cultures, including organizational cultures, can be either feminine or masculine. Feminine cultures are more cooperative, display empathy, and highly interested in the quality of life, while masculine cultures value success and are more assertive (Ugrin et al., 2018). These feminine and masculine qualities describe societies but apply to organizational cultures as well. Cyberloafing occurs more often in feminine cultures (Ugrin et al., 2018). The size of the organization does not serve as a predictor of cyberloafing behavior is (Banerjee & Thakur, 2016). Based on the current research, organizational factors are not overwhelming antecedents to cyberloafing. Personal factors tend to predict cyberloafing behavior better than organizational factors.

Personal Factors That Affect the Choice to Cyberloaf. Researchers have studied personal factors that affect the choice of whether to cyberloaf more often than organizational factors. Personal factors and emotional responses are related to personal attributes (Wu et al., 2018), such as those studied as demographic information (Toker & Baturay, 2021). Attitude and engagement are two such personal attributes that affect the tendency to cyberloaf (Soh et al., 2018). Personal factors sometimes exhibit themselves as compulsive internet use even to the point of addiction (Hadlington, & Parsons, 2017). Understanding these factors will help in understanding cyberloafing.

***Personal Gratification*.** Gratification is an emotional response that may cause a user to participate in cyberloafing activities (Ugrin et al., 2018). Entertainment pleasure found in cyberloafing activities will lead some employees to choose to cyberloaf (Koay & Soh, 2018). However, those with high self-control can put off gratification and are less likely to cyberloaf (Ugrin et al., 2018). Thus, a personality trait like self-control can override an emotional response such as gratification.

***Boredom*.** It is not unusual for loyal, hardworking employees to be tempted to communicate online, check the news, play a game, shop, or watch videos when there is a perceived spare time at work (Hartijasti & Fathonah, 2015). Boredom results from work under- load, which is the lack of tasks necessary to fill an entire workday (Pindek et al., 2018).

Structuring jobs to optimally use human resources will result in fewer opportunities to cyberloaf (Fakoor Saghih, & Nosrati, 2021). Boredom also results from the under stimulation (Mercado et al., 2017). Students report boredom due to the communication style of instructors (Varol & Yildirim, 2018). In the workplace, boredom results from overqualification, real or perceived (Cheng et al., 2020). Filling downtime with nonwork activity seems to be a natural response to a lack of work. Cyberloafing due to boredom is a coping mechanism that results in interest-enhancement (Pindek et al., 2018). Cyberloafing is an easy activity to fill that time when an internet connection is handy.

Job Burnout. Greater strain and lower motivation will lead to the burnout that causes cyberloafing activity (Kim & Christensen, 2017). In their study on workload and cyberloafing, Aladwan et al. (2021) determined a large psychological workload would affect cyberloafing. However, Varghese and Barber (2017) stated that role ambiguity and role overload are not significant indicators of cyberloafing. How employees manage the stress of the job may lead to cyberloafing (Ghani et al., 2018). Both work related and personal stress will lead to cyberloafing (Koay, et al., 2017). Stress from using technology itself, known as technostress, also contributes to cyberloafing (Güğerçin, 2019). Employees with high adversity intelligence reduce the impact of stress by channeling outside difficulties into learning opportunities (Rahayuningsih & Putra, 2018). Employers can teach techniques to manage that stress and reduce the possibility of cyberloafing behaviors. Strain is a part of most jobs, but employees can control the strain with proper techniques.

Personal gratification, boredom, and job burnout are emotional responses that may lead employees to cyberloaf. There are also personal attributes that may lead to a tendency to cyberloaf. In the next section, I deliberate personal attributes that may influence cyberloafing tendencies. These attributes include gender, age, generational ideas, and personal attitudes.

Gender. Gender is an attribute that researchers disagree about the ability to predict cyberloafing behavior. Toker and Baturay (2021) found that males were more likely to cyberloaf than females. The finding that males are more likely to cyberloaf is in line with the findings of Akbulut et al. (2017) as well as some of the earliest cyberloafing researchers Teo and Lim (2000). Gorenc et al. (2016) found that gender has no bearing on whether an employee chooses to cyberloaf in the workplace. Gökçearslan et al. (2018) found no difference based upon gender also. Tosuntaş (2020) showed that men tend to prefer individual cyberloafing behaviors as opposed to group cyberloafing. It is quite complex to pin down one attribute that predicts cyberloafing behavior.

Age. Age is another attribute that may be predictor of the inclination to cyberloaf. In organizations, older employees tend to cyberloaf more, as shown in the results of Banerjee and Thakur (2016). Banerjee and Thakur posited older employees tend to be managers that can indulge more in nonproductive activities. Toker and Baturay (2021) found that younger users tend to cyberloafing more. The findings of Gorenc et al. (2016) refute the findings of others by showing no connection between age and the number of cyberloafing activities in an organization. If older employees are indeed managers indulging in counterproductive activities, it may prove difficult to counteract employees doing so as well. This study aims to find ways to deter cyberloafing, which may prove difficult if cyberloafing is a practice among organizational leaders.

Generational Cohort. Related to the attribute of age is that of generation. Baby Boomers are less likely to cyberloaf, according to Hartijasti and Fathonah (2015). Either the older employees identified by Banerjee and Thakur (2016) were not Baby Boomers, or this is once again disparate findings. Hartijasti and Fathonah (2015) identified Gen X as the group that began integrating the personal use of the internet with work purposes. Gen Y, also known as Millennials, have their identity tied to technology use and feel it right to use technology as they want (Kim, 2018). Gen Y is the most excessive cyberloafing generation (Hartijasti & Fathonah, 2015). Personal use of technology is part of their work values (Kim, 2018). Understanding the differences in generational cyberloafing can help in building deterrence activities. Adding challenge to work activities with a pay-for-performance system is an idea for promoting productivity with younger employees (Hartijasti & Fathonah, 2015). Each generation brings its own set of experiences and values to the workplace, which also affects the tendency to cyberloaf.

Attitude. The intention to cyberloaf is based on the attitude of the user (Askew, & Buckner, 2017). When an opportunity is present, the user will cyberloaf if the desire to do so is high enough (Koay, 2018). Users that have greater access to the internet and more devices are more inclined to cyberloaf (Rahman & Muldoon, 2020). Other employees will try to cheat the system due to a low sense of work obligation (Agarwal & Avey, 2020). When employees that feel they are overqualified for a position have been found to cyberloaf (Zhang et al., 2020). Employees that consider themselves successful are more likely to cyberloaf (Saygin & Güvenç, 2019). Attitude is personal and varies with each employee.

Attitude is an intrinsic part of the person. Intrinsic motivation correlates with productivity (Hur, et al., 2018). A fundamentally motivated employee will perform better and avoid cyberloafing. Yılmaz, and Yurdugül, (2018) showed that increased motivation in students will reduce cyberloafing to an extent. Supervisors can increase motivation by shaping meaningful work for employees (Usman et al., 2021). Employees cyberloaf because they want to, and they do not evaluate potential consequences as part of the decision process (Khansa et al., 2017). If there is an attitude within the employee that will lead to cyberloafing, the person will choose to cyberloaf.

Risk Management. Cyberloafing increases the risk to businesses and threatens the efficiency and security of the information technology (IT) system (Koay, 2018). Managing security risk begins with impact analysis and risk analysis (Yang et al., 2016). Cyberloafing is a security risk, so these analyses are important to small businesses. A thorough analysis should show actions necessary to reduce the consequences of the risk (Che Pa et al., 2017). Part of the impact analysis and risk analysis includes finding vulnerabilities, threat sources, and the actions needed to mitigate the risks (Yang et al., 2016). Mitigation of the risks is necessary for successful operation (Che Pa et al., 2017). For this study, cyberloafing is an identified risk, so businesses need to take the next steps of naming the threat sources and vulnerabilities.

Management may play a significant role in managing risks. In small organizations, managers or owners need to understand the mitigation of risk by making risk decisions that mitigate the identified risk (Che Pa et al., 2017). The mitigation of risks aids managers to understand the mutual relationships among the enablers of risk mitigation and provides a suitable metric to quantify these risks. In risk mitigation, management makes risk decisions to mitigate the identified risks. Managers can encourage the mitigation of risk by creating an environment of shared responsibility (Yang et al., 2017). Managers can enlist the aid of the employees to reduce the risk inherent in cyberloafing. There are guidelines managers and employees can follow to recognize and reduce risk.

The primary guideline is that risk assessment needs to be a continuous process (Vijayakumar & Arun, 2017). When viewed as a continuous process, leaders analyze risks and mitigate those risks continuingly. Fully integrating and supporting a framework for risk assessment aids management in the ability to manage risk continually (Vijayakumar & Arun, 2017). Risk mitigation should be the best practice of everyone in the company.

Another consideration is that cyberloafing is a misalignment risk in that participation in this behavior is not in alignment with organizational goals. By recognizing cyberloafing as a misalignment risk, managers identify variables that can cause the misalignment so that the risk is mitigated (Ching-Chiu et al., 2019). Those employees that take part in cyberloafing behaviors need to understand why it is detrimental. Employee policy may help in this understanding. Well-edited policies provide a reference framework that becomes vital guidelines for the organization (Yang et al., 2016).

Risk Mitigation. Mitigating the risk of cyberloafing is necessary for an organization. Costs of such risks can have a financial impact, cause operational disruptions, and potential liabilities (Koay, 2018). A small business may reduce the risk by identification and analysis, leadership involvement in risk mitigation, and incorporating policies and procedures to address cyberloafing.

Ethics and Cyberloafing

The choice to cyberloaf brings a question of ethical behavior and decision-making, which organizations need to address. Cyberloafing is an unethical behavior (Arciniega et al., 2017). The company needs to shape its perspectives for information in such a way to protect data (Lobschat et al., 2021). Proper usage of data is an obligation to protect the customers and company assets by not allowing unethical behavior, including cyberloafing, to sites that could affect operations or compromise data. Ethical leadership is one mechanism to curb cyberloafing.

Since cyberloafing is an unethical behavior due to its time waste and endangerment of company resources, managers need to lead employees into making ethical decisions. Ethical leadership significantly decrease cyberloafing activity, as demonstrated by Zoghbi-Manrique-de-Lara and Viera-Armas (2017). Leaders with strong core values that can impart the values to employees send a loud and clear message (D. Lee et al., 2017) while abusive supervisors inadvertently encourage cyberloafing (Agarwal & Avey, 2020). Even leaders that communicate in an aggressive manner can be perceived as abusive leading to cyberloafing (Agarwal, 2019). The corporate culture defined by leadership creates an ethical context for employees to follow when choosing whether to cyberloaf (Zoghbi-Manrique-de-Lara & Viera-Armas, 2017). Managers that understand their ethical values can develop a culture that discourages cyberloafing. Managers can create this culture by modelling ethical behaviors (Zoghbi-Manrique-de-Lara & Viera-Armas, 2017). Ethical training is one of the tools for developing culture.

Training reduces computer misuse (Jafarkarimi et al., 2016). Values are complex and may change due to the situation (Arciniega et al., 2017). Training will help guide ethical decision making in differing situations. Accounting education includes ethical training (Miller & Shawver, 2018; Mubako et al., 2020) with specifics that can be adapted to cyberloafing.

When completing ethical training, it is important to be specific and relatable. The goal is to vaccinate employees from taking part in cyberloafing behaviors (Arciniega et al., 2017). Training programs and seminars need to focus on moral development (Jafarkarimi et al., 2016). Training should help employees develop moral reasoning skills along with the ability to voice values (Frémeaux et al., 2018). Training should include moral and ethical reflection (Lobschat et al., 2021; Michl et al., 2021). The use of examples helps in all these objectives (Jafarkarimi et al., 2016). Vignettes are beneficial in providing examples (Arciniega et al., 2017). Finally, the education must relate to moral issues and cultivate moral obligation to the public interest (Frémeaux et al., 2018). Once the training is completed, the policy reinforces ethical concepts through codes of conduct and monitoring. The Change Management and Compliance section includes a discussion on policy, while Monitoring is discussed more fully in the Monitoring section.

Monitoring

Monitoring is a primary mechanism for controlling cyberloafing behaviors within an organization (Gorman, 1998). Specifically, monitoring discourages internet usage that is not work-related (Gorenc et al., 2016). Monitoring software tracks usage of company computers for activities that are not work-related (Arciniega et al., 2017). The software records browsing history, keystrokes, and websites visited (Gorenc et al., 2016). Recording keystrokes tracks unallowed internet activity, which can be included as a reason to monitor.

Reasons to monitor employee computer usage vary but involve avoiding risk. One of the earliest articles on cyberloafing identified maintaining productivity, avoiding viruses, maintaining security, evading the exposure of the company network, eluding corporate espionage, and avoiding financial risks are all reasons to curb cyberloafing via monitoring (Gorman, 1998). These reasons are still valid today.

Some employees may cyberloaf regardless of the countermeasures used. For these employees, monitoring will not help deter behavior (Arciniega et al., 2017). For some users, cyberloafing behavior is habitual and part of their routine (Khansa et al., 2017). Other users consider cyberloafing or at least the information received when on the internet for personal reasons, as self-enhancement (Arciniega et al., 2017). Part of the issue is that increased connectedness has led to a blurring of the separation of work and personal time (Hagqvist et al., 2020). Users check work email at home; why not check personal email at work? Yet, monitoring can help with some employees.

Formal controls, such as monitoring, can help reduce cyberloafing intention (Khansa et al., 2017). Confirmation of policy via the monitoring software is one mechanism that may reduce cyberloafing (Arciniega et al., 2017). Formal training on proper usage of phones, the internet, and other communication is another useful control (Gorenc et al., 2016). One other formal control is the use of quota modules that allow a bit of personal usage while flagging the user upon reaching the quota (Jeong et al., 2020). Gorman (1998) suggests that exhibiting trust in employees to behave as adults may be enough to increase productivity. All these measures will work unless the employee initiates neutralizing behaviors.

Neutralization techniques will increase cyberloafing intent. Neutralization is an attempt to legitimize cyberloafing behavior (Lim, 2002). The announcement of formal control may trigger neutralization (Khansa et al., 2017). Employees may refer to rights such as privacy or free speech as legitimizing factors (Gorman, 1998). After the announcement of formal controls, employees begin to see themselves in unsatisfactory conditions and apply neutralizing techniques (Khansa et al., 2017). Monitoring is not useful in case of neutralization. Yet, monitoring is still the primary method of counteracting cyberloafing.

Managers must be deliberate when adding monitoring as a formal control for cyberloafing behavior. The purpose of monitoring is to enforce policy (Gorman, 1998). Compliance with policy is the goal (Hensel & Kacprzak, 2020). Monitoring must be appropriate for the situation and justifiable (Gorenc et al., 2016). A formal definition of who is watching the employees is necessary (Gorman, 1998). Employees should consent to the monitoring, according to Gorenc et al. (2016), yet monitoring is a legal right of the organization (Gorman, 1998). In the end, businesses must integrate monitoring as a control while still managing to cultivate an environment of trust, which is hard to balance.

Change Management and Compliance

Change management is essential to IT efficiency within an organization. Employees resist change regardless of the organization due in part to disruptions in routine or even fear of instability (Galli, 2015). Employees may see a forced changed as an injustice. The resistance to the change may lead some to cyberloaf as a mechanism to overrule a perceived injustice (Akbulut et al. (2017)). Change is more likely accepted when there is respect and trust in management (Veridiana et al., 2019). Managing change is essential for employees to understand compliance with policies and procedures that reduce cyberloafing activity.

Managers encourage compliance with cyberloafing policy as part of change management. Ensuring employees understand why a practice contributes to the success of the organization helps with compliance (Curry et al., 2017). Forms of communication, such as mobile phones and email, increase productivity when used within the guidelines of the organization (Ha et al., 2017). Codes of conduct in conjunction with written policy aid in understanding while reducing computer misuse (Jafarkarimi et al., 2016). By systematically incorporating governance structures based on common values, beliefs, and desires, small businesses can develop compliance procedures that may reduce cyberloafing (Curry et al., 2017). After creating and defining these governance structures, managers will then write policies and procedures based on these structures.

Policies and Procedures

Technology policy provides a framework for users that work with the system. Well-written policies will foster beneficial uses while curbing actions such as cyberloafing (Kim, 2018). Policies improve the flow of information and increase productivity (Galli, 2015). Users can understand and work within the expectations found in the policies. Additionally, policies increase teamwork while promoting a shared understanding when different parties work to develop and modify the policies (Galli, 2015; Kim, 2018). However, there are negative effects of poorly written or poorly managed policy.

A poorly written policy can be detrimental when trying to curb cyberloafing. Policies that are too rigid can stifle creativity and teamwork (Galli, 2015). Some employees will be more likely to engage in cyberloafing despite policy (Arciniega et al., 2017). Poorly written policies cause a lack of clarity, which appears to permit cyberloafing (Hartijasti, & Fathonah, 2015). Finding loopholes seems to be human nature. For example, employees may move cyberloafing activities to cell phones or personal computers to bypass policy that applies only to the company resources (Hartijasti, & Fathonah, 2015). Since poorly written policies are an issue, small businesses must be able to develop good policy.

There are several features common to successful technology use policies. Management must support policy. Support means active participation and involvement in the development of and compliance with policy (Mohammad et al., 2019). Support also means explaining the necessity of the policy to employees (Jiang et al., 2020). Cooperation between employees and management in the development of policy produces a sense of trust, which leads to better compliance (Kim, 2018). A good policy is structurally sound, weighing potential side effects (Jiang, et al., 2020). Yet there needs to be some flexibility in the creation of policy and in recognizing the need to edit as new situations arise (Sampat & Basu, 2017). Although Galli (2015) argues that rigidity can encourage cyberloafing, Kim (2018) notes that policy should be specific enough that employees cannot find loopholes. This balance will increase compliance. Also, increasing compliance is training. Training on policy empowers employees as they learn to recognize internet abuse and its costly effects on the business (Hadlington, & Parsons, 2017). Some employees still will not follow the cyberloafing policy. Dealing with employees that a work around policy is extremely important to the functioning of the organization, which is in the Deterrence and Discipline section.

Deterrence and Discipline. Deterrence is the procedure put into place to curb cyberloafing. Deterrence is backed by discipline, which can be a punishment or other sanctions to reduce the behavior as posited by GDT. Deterrence is essential to managing cyberloafing and should not be ignored (Cheng et al., 2014). However, a strong deterrence policy based solely on punishment may encourage distrust, especially in the millennial age group (Kim, 2018). When developing a deterrence policy, management must carefully consider discipline.

In previous studies, researchers discussed several strategies for deterrence. Monitoring is a primary tool used to deter internet usage (Jiang, et al., 2020) discuss more fully in the Monitoring section. Along with monitoring, the arrangement of the workplace can discourage cyberloafing. The arrangement of workstations and cubicles so that foot traffic flows behind the employee increases transparency, which in turn reduces cyberloafing (Askew & Buckner, 2017). Retaining trust is essential during rearrangement. In a successful rearrangement, employees perceive the process as fair and done tactfully (Askew & Buckner, 2017).

Another option for deterrence is to allow some cyberloafing activity. Limited personal use of computers may improve performance through the reduction of stress and job burnout (Koay & Soh, 2018). Kim (2018) posited that a 10-minute break from work through cyberloafing made for a significantly more productive group of employees as opposed to a control group not allowed the cyberloafing break. Although counterintuitive, it appears that some cyberloafing is helpful.

One final approach is to overlook the behavior of highly valued employees. In this approach, management will forgive and forget even in egregious cases of noncompliance issues of any sort (Galli, 2015). There are two ramifications. First, the unfairness will cause trust issues that may lead to more cyberloafing (Kim, 2018). Second, cyberloafing behavior exposes the company to risks (Galli, 2015). This approach to deterrence is unacceptable because there are no consequences to the employee.

There should be consequences in the form of discipline for breaking cyberloafing policy (Cheng et al., 2014). The level of discipline varies by organization. Some organizations apply very stringent penalties (Hadlington & Parsons, 2017). Other companies will ignore the problem or use training to counteract cyberloafing activities.

Routinely terminating every noncompliant employee is an example of a very stringent policy (Galli, 2015). The number of employees fired for internet abuse is growing (Kim, 2018). However, the severity of the punishment has little or no effect on cyberloafing behavior (Cheng et al., 2014). Cyberloafing behavior may increase (Kim, 2018). Increased cyberloafing can be the company at risk.

A more practical approach to deterrence is training (Zoghbi-Manrique-de-Lara & Viera-Armas, 2017). By creating awareness of cyberloafing policy, the company may avoid unilateral deterrence that inhibits employee productivity (Kim, 2018). Discipline needs to be more guidance and less punishment.

Defining a Small Business

There are several factors used to define a small business. Usually, small businesses are privately owned with a small number of employees (Turner & Endres, 2017). The upper limit of employees for a small business is 249 (Virkkala et al., 2020). Hagqvist et al. (2020) defined small enterprises in Norway and Sweden as having fewer than 20 employees. In addition to number of employees, there are also characteristics of leadership, risk, and impact on the economy.

Small businesses tend to have an informal management structure that can lead to innovation (Curry et al., 2017). Small businesses are often entrepreneurial in nature

(Sharma & Sharma, 2020). Small businesses also are efficient mechanisms to create jobs and fuel the economy worldwide (Forth & Bryson, 2019). Up to 48% of employees in the U.S. are employed by small businesses (Orzechowski, 2020). Small businesses are also major sources of technological and competitive advantages in the marketplace (Qosasi et al., 2019). Small businesses, therefore, have a significant impact on the economy.

Impact on the local economy in which the business operates is one of the features considered when looking for a business to participate in this study. The number of employees is the primary factor. For this study, a small business is one with fewer than 100 employees.

Relationship of This Study to Previous Research

Teo and Lim studied cyberloafing tendencies as early as 2000. Lim (2002) defined the term cyberloafing two years later. Cyberloafing studies have continued regularly since that time. Table 1 shows the common topics of recent and seminal cyberloafing research. The primary topic of cyberloafing research is why it happens or the antecedents of the behavior. Twenty-nine studies addressed antecedents. Benefits and dangers inherent in cyberloafing, listed as outcomes in Table 1, were the primary topic of three studies. Monitoring and deterrence, listed simply as deterrence, were the primary topics of three studies. Topics did overlap as subtopics in some studies, although not shown in the table.

Table 1

Topics in Cyberloafing Research by Authors with Research Methodologies (When Identified)

Topic	Authors	Methodology
Antecedents	Agarwal (2019)	Quantitative
	Agarwal and Avey (2020)	Quantitative
	Akar and Karabulut Coskun (2020)	Quantitative
	Akbulut et al. (2017)	Quantitative
	Aladwan et al. (2021)	Quantitative
	Cheng et al. (2020)	Quantitative
	Fakoor Saghih and Nosrati (2021)	Quantitative
	Ghani et al. (2018)	Quantitative
	Gökçearslan et al. (2018)	Quantitative
	Güğerçin (2019)	Quantitative
	Huma et al. (2017)	Quantitative
	Jeong et al. (2020)	Quantitative
	Khansa et al. (2017)	Quantitative
	Kim (2018)	Secondary
	Koay (2018)	Quantitative
	Koay and Soh (2018)	Secondary
	Koay et al. (2017)	Quantitative
	Lim (2002)	Quantitative
	Mercado et al. (2017)	Secondary
	Oosthuizen et al. (2018)	Quantitative
	Pindek et al. (2018)	Quantitative
	Rahayuningsih and Putra (2018)	Secondary
	Rahman and Muldoon (2020)	Quantitative
	Sampat and Basu (2017)	Secondary
	Saygin and Güvenç (2019)	Quantitative
	Soh et al. (2017)	Secondary
	Soh et al. (2018)	Quantitative
	Teo and Lim (2000)	Quantitative
	Toker and Baturay (2021)	Quantitative
	Tosuntaş (2020)	Quantitative
	Ugrin et al. (2018)	Quantitative
	Usman et al. (2021)	Quantitative
	Varol and Yildirim (2018)	Qualitative
	Varghese and Barber (2017).	Quantitative
	Venkatraman et al. (2018)	Qualitative
	Yılmaz, and Yurdugül (2018)	Quantitative
	Zoghbi-Manrique-de-Lara and Viera-Armas (2017)	Quantitative
	Zhang et al. (2020)	Quantitative
Outcomes	Andel et al. (2019)	Quantitative
	Kim and Christensen (2017)	Secondary
	Hadlington and Parsons (2017)	Quantitative
	Mohammad et al. (2019)	Quantitative
Deterrence	Askew and Buckner (2017)	Quantitative
	Gorman (1998)	Secondary
	Hensel and Kacprzak (2020)	Quantitative
	Jiang et al. (2020)	Quantitative

Table 1 also shows the methodologies used in the studies cited in this literature review. Twenty-five studies stated using a quantitative methodology, four studies were qualitative, and eight were the analysis of secondary research. Providing a qualitative study will add to the understanding of the phenomenon (Xia, 2017) and fill the gap created with the imbalance of methodologies. No studies were specifically identified as a case study. The other qualitative studies described procedures found in case studies. Using a case study in this research will fill a gap in the research.

Computer monitoring research began with Gorman (1998). However, not much research has happened since. One recent exception is J. Lee et al. (2017) who studied monitoring of BYOD devices. Searches on monitoring in electronic databases, even with added keywords referring to a variety of computer terms, primarily result in articles on monitoring medical conditions. Some of the added terms included “computer,” “information technology,” and “workplace.” This study will fill a gap in the literature on monitoring employee computer usage. Filling this gap will be beneficial as the effectiveness of monitoring is debatable, may be ineffective, based upon the limited research currently available.

Lastly, most studies on cyberloafing focus on why people choose to engage in that behavior. Except for the studies referenced in the Deterrence and Discipline section, previous studies did not include deterrence. Few researchers identified the business setting and none of the researchers used small businesses as the basis for studying cyberloafing. Jeong et al. (2020) studied university students found on social media, Hensel and Kacprzak used 230 employees in the organization they studied, and

Oosthuizen et al. (2018) used a manufacturing facility for the location of the study. Educational facilities were the sites of several others (Gökçearslan et al., 2018; Soh et al., 2018; Varol & Yildirim, 2018; Wu et al., 2018). This study will fill the gap to understand how small businesses may monitor and deter cyberloafing.

Transition and Summary

In Section 1, I introduced the problem and explained its significance. I provided information on the purpose of the research. I explained how I would study the topic of cyberloafing. I provided research and interview questions and an overview of the conceptual framework. The literature review at the end of Section 1 provides an in-depth review of the academic literature supporting the topic of cyberloafing. The literature review includes an explanation of AST and how it will be used as the groundwork for the study. Section 2 includes the purpose statement then describes the role of the researcher. Following the role of the researcher are descriptions of the research method, research design, data collection, data organization, and reliability and validity of the study. Section 3 reiterates the purpose of the study and the research questions. I presented the findings of the study and their application.

Section 2: The Project

Section 2 includes the purpose statement and then addresses my role as the researcher. Following the role of the researcher are descriptions of the research method, research design, data collection, and data organization. I finish with reliability and validity of the study and a transition to Section 3.

Purpose Statement

The purpose of this qualitative, multiple case study research was to explore the strategies used by IT managers to monitor and deter cyberloafing in small businesses. The classification of a small business varies by industry, with 100 to 200 employees usually being the defined maximum (Small Business Administration, 2017). The population for this study was IT managers of small businesses who reported strategies to monitor and deter cyberloafing and were in the United States. In addition to interviews, I conducted review of policy documents and kept a journal of the research process, as I served as the main data collection tool. This study has implications for positive social change, in that application of the findings may lead to greater economic stability in the community as small businesses increase productivity and reduce risk through strategies to control cyberloafing behavior while increasing employee satisfaction in the workplace.

Role of the Researcher

I served as the primary data collection instrument in this research as this was a qualitative study (Unkovic et al., 2016). Data collection occurred using open questions with adapted follow-up questions (Henderson, 2018). My role as the researcher included designing questions along with conducting interviews. I also transcribed and analyzed the data collected. Data saturation occurs when a researcher gains no new themes or codes from data collection (Wall, 2015). A researcher can choose from three styles for data collection and analysis: (a) tidy, which focuses on content; (b) broad, which indicates that the structure of the answers is as important as the content; and (c) poetic, which involves seeking to recreate the voice of the participants (Henderson, 2018). A broad approach to the transcript was what I felt comfortable with, as it allowed the recording of pauses and hesitations.

I adhered to all the ethical principles of the Belmont Report throughout the study. Following the principles of the Belmont Report helped to ensure justice, beneficence, and respect to the participants (National Institutes of Health, 1979). Direct contact with the participants was required during the interview process; however, I had no relationship with the participants before the study began, despite living in the geographical area of the study. I obtained informed consent from the participants per the Belmont Report, and all potential risks and benefits were identified and disclosed (National Institutes of Health, 1979). I chose participants in a just manner to gain information on the topic of cyberloafing. I treated all participants respectfully, equally, and fairly following the study protocol. I minimized exposure to harm by presenting a consent form with details of risks and benefits, including the option to not participate in the study at any time. I protected all answers to research questions by storing the information on a password-protected USB drive stored in a locked filing cabinet.

I was familiar with the topic of cyberloafing as an IT instructor at a community college who had observed cyberloafing behavior in students. I also knew someone who had lost his job due to practicing cyberloafing behaviors, which was a bias that I needed to overcome. Bias can impede the scientific process if not dealt with in a professional manner (Tincani & Travers, 2018). Identifying potential bias was an important step. Bracketing is the primary tool for managing bias during interpretation. Bracketing increases the trustworthiness of the interpretation as the researcher suspends his or her own beliefs during the interpretation process (Johnston et al., 2017). I used bracketing in this study to mitigate bias. All data gathered were appropriate to the study, which is one of the requirements of the Belmont Report (National Institutes of Health, 1979). I protected data to ensure the anonymity of participants.

Participants

This study was an exploratory, multisite qualitative study. When exploratory in nature, a multisite study with several participants is proper (Holten et al., n.d.). The participants for this study were IT managers in businesses with fewer than 100 employees, as defined by the Small Business Administration (2017). Smaller businesses may not have the resources to combat cyberloafing (Curry et al., 2017); however, for this study, the participants needed to be from organizations that had strategies in place to manage and deter cyberloafing activities.

To gather participants, I enlisted the director of a small business center at a community college in North Carolina. The director forwarded emails inviting participation from small businesses that had enlisted the services of the center. I also utilized the Walden University Participant Pool. The invitation to participate was posted on the Participant Pool website for potential members. I estimated that data saturation would occur with participants from eight to 10 small businesses. Data saturation occurs when the researcher is unable to identify new themes or codes from data collection (Wall, 2015).

It is important to build a working relationship with participants in case study research (Olsen, et al., 2016). To establish a relationship of trust, it is necessary to be transparent and display candor (Øye et al., 2016). Therefore, I did not use colleagues as participants in this study. Personal opinions were not part of the interview process, as their addition introduces bias to a study (Unkovic et al., 2016). Bias reduces both transparency and candor.

Research Method

I considered three research methods for the topic of cyberloafing: qualitative, quantitative, and mixed methods. I chose the qualitative method because qualitative research is useful in gaining an in-depth understanding of a phenomenon (Xia, 2017). Researchers conduct qualitative studies in natural settings, with the researcher as a key instrument, using complex reasoning to interpret data (Cruz, 2015). Qualitative research allows participants to express their perceptions in their own words, which then can be used for follow-up questions (Henderson, 2018), which is why it aligns with an exploration of employee cyberloafing. Data collection in a qualitative study can be in the form of interviews, record and document reviews, and observation (Yin, 1981). In this study on cyberloafing, semistructured interview questions and document reviews were used, which was consistent with a qualitative methodology. Qualitative research provides a holistic perspective on uncovering phenomenon (Wall, 2015). The ability of the participants to provide holistic perceptions in their own words to garner on an-depth understanding of cyberloafing was the reason that I chose qualitative methodology for this study.

The quantitative design gives detail and statistical support in research; however, it does not provide the in-depth information found in qualitative design, which involves asking “how” and “why” questions (Xia, 2017). Statistical significance is a requirement of quantitative research (Teater et al., 2017) but not necessary in the observation of a phenomenon to understand why or how it happens. The statistical relationship among variables is a feature of the quantitative method (Tominc et al., 2018). Quantitative research begins with hypothesis formation, followed by gathering data for analysis to support or reject the hypothesis (Travers et al., 2017). Researchers often seek cause and effect as part of the quantitative method (Baškarada & Koronios, 2018). There was no hypothesis to evaluate in this study on cyberloafing. There was also no need for statistical analysis. The lack of a hypothesis or statistical data, along with the desire to seek in-depth understanding, led to the rejection of the quantitative method.

The mixed methodology uses a combination of both qualitative and quantitative data collection and analysis (Baškarada & Koronios, 2018). Qualitative data collected supplement quantitative data to obtain a deeper analysis (Simard & Karsenti, 2016). Once a researcher analyzes quantitative data, the researcher seeks the rationale behind participants’ decisions from the data (Dursun et al., 2018). Because there was no quantitative data collected for this study, mixed methodology was not appropriate. I included the characteristics of in-depth understanding, natural setting, and the researcher as a key instrument in this study, which led to the choice of qualitative design.

Research Design

The research questions guided my choice of a multisite case study. Researchers use case study design in real-life settings that are bounded to explore and understand complex issues (Yin, 1981). When used to gain insight into issues, case study is instrumental (Stake, 1995). Researchers explore contemporary issues in the context of study sites (Holten et al., n.d.). Case study research answers “how” and “why” questions (Yin, 1981). Research that is exploratory benefits from the case study method (Park et al., 2016). A multisite case study design provides a greater depth of understanding than a single-site study (Yin, 1981). Multisite case studies enhance generalizability with their replication logic and greater data gathering (Park et al., 2016). I studied cyberloafing monitoring and deterrence within the bounds of small business organizations in the southeastern United States. The sites were real-life settings. I sought to answer a complex set of “how” and “why” questions in this study. The characteristics of a bounded system, the use of multiple sites along with a complex set of “how” and “why” questions, and the exploratory nature of the study led to the choice of a multisite case study method.

In addition to the case study, I considered ethnography, action research, and phenomenology as potential designs. Ethnographic research focuses on describing the culture of a group (Friberg, 2016). In ethnography, researchers describe the culture based on document analysis, interviews, and observations (Wall, 2015). Ethnographic researchers engage with groups over a prolonged time frame in a community setting to form a picture of the groups (Hartmann et al., 2018). Organizational culture was not the focus of this study on cyberloafing; the individual viewpoints of the participants were the basis for data analysis. I did not choose an ethnographic design because organizational culture was not being studied, and I was not engaging with groups for a prolonged period.

Action research involves collaboration between researchers and practitioners to either change practice or develop theory (Schwarz et al., 2019). Those who conduct action research try to solve logical problems with which they are actively involved (Sendall et al., 2018). A defining characteristic of action research is the application of the scientific method to the problem-solving process (Durcikova et al., 2018). Action research is also an iterative process that consists of planning, acting, observing, and reflecting (Schwarz et al., 2019). Durcikova et al. (2018) proposed that adding a statistical element to action research makes it more rigorous. For this study, there was no collaboration to solve a problem. Data collection and analysis explained cyberloafing deterrence and monitoring techniques; therefore, action research was not the best suited method for this study.

A researcher conducting phenomenological research explores and describes individual perspectives in everyday life to gain an understanding of a phenomenon (Kelly & Kelly, 2019). In phenomenology, researchers focus on the individual’s lived experiences, often concerning a specific event (Danielsson & Rosberg, 2015). Researchers using the phenomenological approach strive for in-depth understanding rather than simple theme development (Madeley et al., 2019). Researchers develop themes by extracting the participants’ meaning of phenomena based upon transcripts of participants’ descriptions (Kelly & Kelly, 2019). Phenomenology is a viable methodology for a study of the phenomenon of cyberloafing. However, a case study was chosen because the perspective of the participants was not the only source of data to be analyzed.

A researcher achieves data saturation when data yield no new information related to research questions (Lowe et al., 2018). Data saturation indicates that there are no new concepts or theme categories in the data (Park et al., 2016). Data saturation is not based on sample size (Lowe et al., 2018), but adding participants can ensure saturation (Kelly & Kelly, 2019). To ensure data saturation, I conducted interviews with participants using semistructured questions. I analyzed the data from those interviews for themes. After the initial analysis, I conducted member checking and coded any additional themes. I repeated the analysis process until no new themes appeared.

Population and Sampling

Purposeful sampling methods allow the researcher to narrow the target population to participants who are knowledgeable about the phenomenon studied (Hillson et al., 2015). Organizations selected through purposeful sampling should have similar characteristics and yield similar results during the study (Lehrer et al., 2018). Additionally, the choice of organizations is based on the ability of the organizations to fulfill the investigation potential of the study (Park et al., 2016). By choosing businesses with existing cyberloafing policies and procedures that were followed and enforced, I sought to ensure that the participants would be able to provide information to facilitate exploration of the research questions.

Therefore, eligible participants met the following criteria for inclusion in the study. For this study, the organizations were small businesses in the southeast with 100 or fewer employees. The organizations had cyberloafing monitoring and deterrence procedures in place. The participants from the organizations were IT managers or the owners of businesses that were too small to have their own IT staff. The participants enforced any policies and procedures related to cyberloafing behaviors in the organization. Potential participants who did not meet all these parameters were not eligible to take part in the study. I used a signed consent form to ensure that all participants met the criteria.

The number of participants in a case study can vary widely. Boddy (2016) suggested that 15-30 interviews are necessary for a case study. Raymond et al. (n.d.) conducted a case study with only five participants. For multiple-site case studies, Yin (1981) stated that three to four sites are sufficient. Lehrer et al. (2018) and Park et al. (2016) both fell within these guidelines in their studies by using four sites each. Errington et al. (2012) used 12 sites in their study. For this study, I estimated that I needed eight to 10 small business sites to reach data saturation. Eight to 10 sites were well above the suggested three to four sites but fewer than the 12 used by Errington et al. (2012). Once no new themes or codes emerged from data collection, I knew that I had reached saturation as suggested by Wall (2015). The primary source of data from these participants was semistructured interviews.

Interviews allow interpersonal contact and the ability for follow-up questions (Yates & Leggett, 2016). Anderson et al. (2014) recommended a naturalistic setting for conducting interviews to gain open responses. As such, I conducted the interviews in a comfortable, nonthreatening environment. I conducted interviews onsite for the convenience of the participants (Errington et al., 2012; Wall, 2015). I also held the interviews via Zoom and by telephone to accommodate participants. The length of interviews that is suggested in literature is 45-90 minutes (Lehrer et al., 2018). Based on the interview questions developed for this study, I scheduled interviews for 60 minutes.

Ethical Research

Academic research is based on regulated ethical principles (Øye et al., 2016). Study participants are entrusting themselves to the researcher (Olsen et al., 2016). Ethical principles for academic research on human subjects include respect for persons, beneficence, nonmaleficence, and justice (Gallagher et al., 2016). This research was, therefore, under the direction of the Walden University Institutional Review Board (IRB). The approval number was 03-06-20-0599577.

I used a gatekeeper to gather participants for the study. When using a gatekeeper to gather participants, Øye et al. (2016) recommended that the researcher take steps to ensure that the gatekeeper does not affect participant choice. To safeguard against the gatekeeper unintentionally affecting participant choice, I invited all small businesses that had completed training at the Small Business Center of a NC Community College. Invitation letters included details of the study and informed consent forms (Nichols, 2015). Participants needed to sign the informed consent to be eligible for the study. The letter and consent form outlined the purpose of the study, supplied sample interview questions, and explained practices to protect the rights of participants through the study.

Participation in the study was voluntary (Restubog et al.., 2011). Participants had the opportunity to ask questions before signing the consent form. Participants could withdraw from the study via email or verbal notification. No participants chose to withdraw, but if a participant had withdrawn, I would protect the information provided by that participant along with the information received from the participants completing the study. Participants were offered a $25 gift card for taking part in this study. I protected anonymity with coding. I used the codes Site 1, Site 2, etc. for the organizations. I used Participant 1, Participant 2, etc. for the individuals.

To further protect participants, I stored data on an external hard drive that is password protected. I store the drive in a locked cabinet. After five years, I will destroy all the data.

Data Collection

Instruments

A case study needs an explicit design to identify topics, data collection, and unit of analysis (Yin, 1981). Data collection follows specific guidelines, as well. The development of the data collection protocol is part of the planning of a case study (Plummer, 2001). The data collection protocol specifies the smallest amount of data collection, plans for interviews, documents analyzed, and the data collection instruments (Yin, 1981). The data collection instruments for this study were the researcher, interviews, and document analysis.

Researchers are the primary data collection instrument in qualitative studies (Anderson et al., 2014). A researcher collects data from interviews, focus groups, or observation in a qualitative study (Yates & Leggett, 2016). Additional data sources for case studies include agency records, documents, memoranda, newsletters, and other publications within an organization (Yin, 1981). For this multiple case study research, I was the primary data collection instrument. I collected data via semistructured interviews and document review for this study.

The interview process gathers rich data to understand the phenomenon studied (Johnston et al., 2017). Semistructured interviews provide in-depth examinations of participants' perceptions and viewpoints (Anderson et al., 2014; Lehrer et al., 2018). Researchers develop questions for a semistructured interview in advance to answer the research questions and help guide the interview process (Yates & Leggett, 2016). The interview questions for this study are found in Appendix B. I recorded the answers to the interview questions for later transcription and analysis with written notes and digital audio recording. I augmented the data gathered in the interview process with data gathered via document review.

Reviewing documents is a common data collection method in qualitative studies (Yates & Leggett, 2016). Dubé and Paré (2003) found that 64% of qualitative studies incorporate documentation review. Document analysis can include photographs, drawings, textbooks, or materials published in an organization (Yin, 2016). Yin (1981) recommended that researchers identify the documents to analyze in the study in advance as part of the study protocol. For this study written policies and procedures were analyzed to determine how cyberloafing is monitored and deterred within the organization as part of the case study protocol.

The choices made in the data collection protocol enhance reliability and validity (Dubé, & Paré, 2003). Validity is the extent to which findings accurately depict the phenomenon (Yates & Leggett, 2016). The credibility or trustworthiness represents internal validity and transferability, or generalizability represents external validity (Palinkas et al., 2013). Researchers increase validity by allowing participants to review data and its analysis (Yates & Leggett, 2016) in a process known as member-checking. In addition to improving validity by allowing participants to check the credibility of interpretations of the data (Abma, & Stake, n.d.), member-checking supplies a means to gather additional insights (Errington et al., 2012). I used member-checking to increase validity.

Reliability refers to the extent that a study is replicable, is consistent, and is auditable (Anderson et al., 2014). The researcher achieves both reliability and validity through triangulation. Triangulation uses multiple sources of evidence (Lehrer et al., 2018), such as interviews and secondary data (Park et al., 2016). Document review of cyberloafing policy and procedure was the secondary data analyzed in the study. To increase reliability and validity, I used the documentation review along with the semistructured interviews to triangulate findings.

Data Collection Techniques

I used semistructured interviews as the primary source of data collection with document review supplementing the data for analysis. Semistructured interviews have questions crafted in advance to help explore the research question but only guide the conversation with the opportunity to follow-up based on participant responses (Anderson et al., 2014). After receiving permission from the Walden University IRB to complete the study, I supplied the letter requesting participants to the director of a small business incubator. She sent the letter to the potential participants. The letter explained the study and how to take part in the study. I confirmed that anyone interested was eligible and presented with the informed consent form. I followed-up with potential study participants to clarify questions on the informed consent. Once participants signed the consent form, I scheduled interviews. Raymond et al. (n.d.) suggested that participants are more helpful when comfortable and valued. At the beginning of the interview process, I strove to make the participants comfortable by helping them feel valued and respected. I then covered informed consent once more and reminded the participants they may exit the study at any time. Next, I posed the interview questions and ask any follow-up questions. I audio-recorded interviews with permission from the participant. I made notes of any nonverbal cues I observed during the conversation. Lastly, I thanked the participants and explained that I would contact them again to review the data I have collected after transcription.

The process of having participants review my understanding of their responses is known as member checking. Member checking increases the validity of a study (Yates & Leggett, 2016). Member checking after data collection will sometimes result in added insights to include in the analysis (Errington et al., 2012). I conducted member checking at the convenience of the participants.

After the interview, I strove to triangulate data through document review. Document analysis can include photographs, drawings, textbooks, or materials published in an organization (Yin, 2016). I used the written policies and procedures on cyberloafing within the organization for the analysis. The focus of my review was how the organization monitors and deters cyberloafing. I examined the documents for evidence of monitoring and deterrence policies.

The data collection techniques had several advantages as well as disadvantages. A primary advantage of interviewing is consistent data collection (Anderson et al., 2014) while developing understanding through a variety of perspectives (Abma & Stake, n.d.). The researcher can extract emotional experiences and gather rich data (Park et al., 2016; Yates, & Leggett, 2016). Semistructured interviews add the ability to include follow-up questions to enhance understanding (Lehrer et al., 2018). For document review, a primary advantage is a historical look at the data (Yates & Leggett, 2016). Another advantage of including document review is triangulation with secondary data analysis (Park et al., 2016). Along with the advantages, each technique has disadvantages associated with them.

One disadvantage of interviews is the geographic dispersion of the participants (Wall, 2015). Since the small business incubator provides services to a large geographic region, there was a possibility that I would have to travel to complete the interviews. Another disadvantage of interviews is the time needed to transcribe the notes. There is a temptation to hire a transcriber due to the time commitment (Castleberry & Nolen, 2018). However, the immersion needed to transcribe the data carefully facilitates the analysis process later (Fleet et al., n.d.). The major disadvantage of document review is the time involved in reading and taking notes on the documents (Wall, 2015). Again, this type of immersion into the data helps with the analysis of the data.

Data Organization Techniques

Data organization allows the researcher to develop themes through analysis (Yates, & Leggett, 2016). In this study, the data organization began with the audio recording of interviews (Schwarz et al., 2019). I then transcribed that data using Microsoft Word so that I could later imported into Atlas.ti for analysis (Yates & Leggett, 2016). Further, I used memos to reflect on the study, record questions, and ideas (Lehrer et al., 2018). The reflection process recorded via memo aids in understanding the concepts (Rich, 2015). I stored the organized data on a password-protected external drive.

In addition to a password, I protect the external drive using BitLocker to Go. BitLocker to Go is a feature of the Windows 10 operating system that encrypts data on external drives (Microsoft, 2018). The data can only be read from the machine from which is it was saved to the external drive or a machine that has the encryption key. As a further precaution, I store the drive in a locked cabinet with a known key distribution.

Data Analysis Technique

Based on the research design, I conducted a thematic analysis using triangulation in conjunction with the five steps of qualitative analysis. Data that are collected, integrated, and presented data from a variety of sources is valued in qualitative research (Yin, 2016). In case studies, a phenomenon intertwines with its context (Yin, 1981). Triangulation helps make sense of the context by allowing a variety of instruments for data collection (Korstjens & Moser, 2018). For a multiple case study, triangulation provides a depth of information that enhances transferability (Stavros, & Westberg, 2009). Triangulating helped me to find themes in the data. The variety of sources yields a variety of themes. I used a documentation review of cyberloafing policies in small businesses along with the semistructured interviews to triangulate findings.

The five steps of qualitative analysis are compiling, disassembling, reassembling, interpreting, and concluding (Yin, 2016). Compiling data includes the collection and recording of the data (Castleberry & Nolen, 2018). An example of compiling is the transcription of interviews. The immersion required to transcribe the data facilitates the analysis process (Fleet et al., n.d.). The transcription process and organization of textual data allows the researcher to become intimately familiar with the data (Castleberry & Nolen, 2018). Compiling data is more than simply recording the data; it is becoming conversant with the data for analysis. I compiled data from the written notes and digital recording of the interviews. I organized the textual data found in the document review of cyberloafing policies.

Once I completed the compilation, I disassembled the data. Data disassembly is taking apart the data to create meaningful groupings through coding (Castleberry & Nolen, 2018). Coding is a tool that aids in the replication of the study and helps the researcher avoid bias (Dubé, & Paré, 2003). Codes are labels or tags for unique pieces of information found within the data (van Rijnsoever, 2017). I began the coding process by searching for themes from the interview answers. I recorded added codes discovered during the analysis that answered the research questions. I compared the themes discovered in the interviews with those found in the literature.

After disassembly, the process of reassembling took place. During reassembly, the researcher maps coding into themes (Castleberry & Nolen, 2018). Emerging themes explain concepts and behaviors (Yin, 2016). Themes show the picture of the evidence portrayed by the data (Castleberry & Nolen, 2018). The reassembly process occurs until no new themes develop (Yates & Leggett, 2016). I organized codes in relation to each other to develop themes within the data to begin interpretation.

Interpretation is the making of analytical conclusions from the codes and themes discovered in the data (Castleberry & Nolen, 2018). Researchers draw all conclusions from the evidence portrayed by the themes (Yin, 2016). Interpretation is the making of meaning from the patterns and themes (Yates & Leggett, 2016). Researchers compare explanations from each case in a multisite study (Yin, 1981). I used the themes discovered from the disassembly and reassembly of the interview transcripts and document reviews to interpret how cyberloafing is monitored and deterred by small businesses.

Interpretation of the data leads to conclusions. Conclusions are responses to the research question (Castleberry & Nolen, 2018). Conclusions represent the views are perspectives are the participants (Yin, 2016). Conclusions from case studies are more convincing when triangulation occurs (Dubé, & Paré, 2003). Conclusions drawn from the data convincingly answer research questions. I used the interpretations to draw conclusions and record the process to form conclusions and complete the data analysis process.

To aid with the data analysis, I used two tools. I used Microsoft Word, to transcribe the interviews and make notes on the document reviews. Once the transcription and note-taking were completed, I uploaded data into Atlas.ti. Atlas.ti is a software for organizing, finding relationships, and finding insights with data. However, data analysis software, such as Atlas.ti should not replace the researcher for the final analysis (Castleberry & Nolen, 2018). I used these tools to discover patterns, codes, and themes to make a sound conclusion based upon the data.

Reliability and Validity

Any study must have reliability and validity. Reliability is the consistency of results if the study is repeated (Anderson et al., 2014). Gelo et al. (2008) note that validity is the level of accountability and legitimacy that is strived for through data analysis. In qualitative research, the concepts of reliability and validity are intertwined and shown through dependability, creditability, transferability, and confirmability (Moon et al., 2016). Reliability and validity increase the acceptability of the study within the field and the literature. To increase validity and reliability in this study, I used triangulation, the recorded answers to interview questions, and personal thoughts in a journal, the audit trail, member checking, and thick description.

Dependability

Dependability means that a reader can have faith in the conduction of the research and the findings analyzed (Ellis, 2019). Dependability is the reliability and consistency of research findings (Moon et al., 2016). Dependable data is stable over time, accurate, and consistent (Ellis, 2019), as are the findings based on the data (Korstjens & Moser, 2018). Dependability allows an outside reader to follow, audit, and critique the research (Moon et al., 2016). When dependability is present, data collection ensures a consistent manner, and the findings are based on the data. Bush and Amechi (2019) recommended the audit trail, triangulation, and reflexive journaling as tools to assure dependability. I suppled the audit trail in Sections 2 and 3 of the study. I triangulated the data with semistructured interviews and document review. I journaled the study.

Credibility

Credibility is when the researcher correctly interprets the meanings of the participants (Moon et al., 2016). Credibility is confidence that there is truth in the findings drawn from the participants' data (Korstjens & Moser, 2018). The credibility is the trustworthiness, which represents internal validity (Palinkas et al., 2013). The research design creates credibility (Moon et al., 2016). To have credibility, the research design allows for data analysis that results in findings that reflect the participants' meanings. Bush and Amechi (2019) recommended the audit trail, triangulation, member checking, and reflexive journaling to assure dependability. I increased dependability by using each of the recommended tools.

Transferability

Transferability is a type of external validity (Moon et al., 2016). Transferability refers to how well the results of the research can be applied to other contexts (Korstjens & Moser, 2018). The transferability can apply to theory, practice, or future research (Moon et al., 2016). For results to be transferable, the researcher uses a thick description (Korstjens & Moser, 2018). Transferability contends that results must be able to be applied to other contexts. Bush and Amechi (2019) recommended thick description to assure transferability. Moon et al. (2016) recommended purposeful sampling and member checking to assure transferability. I used purposeful sampling, member checking, and thick description are in this study.

Confirmability

Confirmability means that the researcher makes conclusions based on the data and not any biases held by the researcher (Castleberry & Nolen, 2018). Studies with confirmability are replicable with processes that other researchers can duplicate (Moon et al., 2016). Confirmability is internal validity (Korstjens & Moser, 2018). When confirmability is present, readers can assess whether they can come to the same conclusions with the same data (Ellis, 2019). Confirmability shows that interpretations are derived from the data (Korstjens & Moser, 2018). Confirmability is how the researcher overcomes biases to interpret data correctly. Castleberry and Nolen (2018) suggested member checking and triangulation assure confirmability. Another tool to assure confirmability is reflexive journaling (Ellis, 2019). I used member checking, triangulation, and reflexive journaling used in this study to support confirmability. I discuss the description and usage of each tool to increase validity and reliability for this study in the following sections.

Audit Trail

The audit trail enhances dependability and confirmability in my study. An audit trail is the documentation of design and implementation (Moon et al., 2016). An audit trail is a transparent description of the steps taken to conduct the research (Korstjens & Moser, 2018), including how data were collected and interpretations made (Ellis, 2019). The audit trail enables an outside reader to judge the research process and procedures

(Bush & Amechi, 2019). I created the audit trail in Sections 2 and 3 of this doctoral study.

Triangulation

Triangulation supports dependability, credibility, and confirmability in a study. Triangulation is using a variety of instruments or researchers to collect data (Korstjens & Moser, 2018). Triangulation uses multiple sources of evidence (Anderson et al., 2014). Triangulation can be achieved by gathering data at different times, multiple spaces, and different types of individuals (Korstjens & Moser, 2018). Simply comparing responses from one interviewee to another is not triangulation (Braganza et al., 2017). Data sources can include interviews and secondary data (Park et al., 2016). Document review of cyberloafing policy and procedure was the secondary data analyzed in this study to increase reliability and validity. I used documentation review of cyberloafing policies along with the semistructured interviews to triangulate findings.

Member Checking

Credibility, dependability, and confirmability are all enhanced by member checking, which is the process of having participants review the interview. During member checking, the researcher has participants verify the interpretation of the data (Korstjens & Moser, 2018). Member checking increases the validity of a study (Yates & Leggett, 2016). Having interpretations evaluated and supported by the participants strengthen a study (Korstjens & Moser, 2018). Member checking is at the convenience of the participant and used to gain feedback on interpretation. Member checking after data collection will sometimes result in additional insights to include in the analysis (Errington et al., 2012). Member checking again after analysis helps ensure the findings are accurate (Korstjens & Moser, 2018). I completed member checking by reviewing the responses after data collection and by reviewing the conclusions formed after data analysis.

Reflexive Journaling

Journaling allows a researcher to make sense of responses and data while increasing creditability, dependability, transferability, and confirmability. Through reflexive journaling, the researcher reduces bias and increases transparency in the research project via self-assessment (Moon et al., 2016). For the journaling process to be reflexive, the researcher names biases, preferences, and preconceptions (Korstjens & Moser, 2018). The impact of these biases and preconceptions are identified as part of the reflexive process (Ellis, 2019). The reflexive journaling of biases does not remove the bias but explains how the researcher interprets finding (Moon et al., 2016). I identified bias and its impact on the interpretation of data. I maintained a reflexive journal throughout the data collection and data analysis phases of the study.

Thick Description

Thick description offers completeness so that readers can follow how the researcher collected and interpreted data (Ellis, 2019). Researchers describe responses to interview questions along with describing contexts such as sample size, inclusion criteria, and interview procedures (Korstjens & Moser, 2018). Researchers must richly describe themes found in the data analysis (Anderson et al., 2014). I used thick description to enhance the transferability of the research study.

Data Saturation

In addition to ensuring validity and reliability, I looked for data saturation. Data saturation occurs when no new concepts or themes to develop in the data analysis (Park et al., 2016). Data saturation is the lack of new information related to the research questions that indicate data saturation (Lowe et al., 2018). Once data saturation was reached, I was not able to identify new concepts or theme categories. To ensure data saturation, I conducted interviews with participants using semistructured questions. I analyzed the data from those interviews for themes. After the initial analysis, I conducted member checking and coded additional themes. This process was repeated until no new themes emerge.

Transition and Summary

The purpose of this qualitative, multiple case study research is to explore the strategies used by IT managers to monitor and deter cyberloafing in small businesses. I used semistructured, digitally recorded interviews to collect data from small business owners and IT managers. I triangulated the data with a review of company cyberloafing policies and procedures.

In Section 2, I described the role of the researcher after reminding the reader of the purpose statement for this study. Within Section 2, I described the participants, the population, and how I used sampling to obtain the participants. I gave a rationale for the research methods and design of the study. I described ethical research. I also showed the data collection and data analysis techniques that I used in the study. Finally, I explained the reliability and validity of this study.

In Section 3, I presented the findings, applications to professional practice, and implications for social change. I added recommendations for action and future studies. I closed Section 3 with a reflective summary and the study conclusion.

Section 3: Application to Professional Practice and Implications for Change

In Section 1, I introduced the problem and explained its significance. I provided information on the purpose of the research. I explained how I would study the topic of cyberloafing. I provided research and interview questions. The literature review at the end of Section 1 provides an in-depth review of the academic literature supporting the topic of cyberloafing and an explanation of AST, the conceptual framework for the study. In Section 2, I described my role as the researcher after reminding the reader of the purpose statement for this study. I described the participants, the population, and how I used sampling to obtain the participants. I gave a rationale for the research methods and design of the study and described ethical research. I also showed the data collection and data analysis techniques that I used in the study. Additionally, I explained the reliability and validity of this study. In Section 3, I present my findings while describing applications to professional practice and implications for social change. The section ends with recommendations for further research, reflections, and conclusions.

Overview of Study

The purpose of this qualitative, multiple case study research was to explore the strategies used by IT managers to monitor and deter cyberloafing in small businesses. Data collection included semistructured interviews with IT managers and owners of small businesses and review of policies, procedures, and handbooks. I focused on small businesses in this study because smaller businesses must often be creative in developing strategies on a much more limited budget than large organizations (Curry et al., 2017). Three emergent themes from the data on monitoring cyberloafing were (a) tools to actively monitor cyberloafing, (b) tools to passively monitor cyberloafing, and (c) policy and procedure as a strategy to monitor cyberloafing. Three emergent themes from the data on deterrence of cyberloafing were (a) tools to deter cyberloafing, (b) trust as a strategy to deter cyberloafing, and (c) policy and procedure as a strategy to deter cyberloafing. The findings indicated that small business IT managers used hardware and software tools along with observation and measuring productivity for monitoring cyberloafing. IT managers limited access to organizational resources and used training and trust as strategies to deter cyberloafing. Policy and procedure are strategies used by IT managers for both monitoring and deterring cyberloafing.

Presentation of the Findings

There were two central research questions for this study: What strategies do IT managers use to successfully monitor cyberloafing in small businesses to discover inappropriate usage? What strategies do IT managers use to successfully deter cyberloafing in small businesses so that inappropriate usage is minimized? Nine organizations contributed to this multiple case study. One IT manager or small business owner from each site participated for a total of nine interviews. Seven participants reviewed my understanding of responses during member checking. Four organizations gave me access to their written policies, which helped with triangulation.

Research Question 1

Research Question 1 concerned the strategies that IT managers use to successfully monitor cyberloafing in small businesses to discover inappropriate usage. The analysis of data revealed three major themes for the first question: (a) tools to actively monitor cyberloafing, (b) tools to passively monitor cyberloafing, and (c) policy and procedure as a strategy to monitor cyberloafing.

Theme 1: Tools to Actively Monitor Cyberloafing

All of the participants in the study monitored cyberloafing, either actively or passively. Six of the organizations in this multisite case study used tools to monitor cyberloafing actively. Active monitoring for these organizations meant that tools were in place to track cyberloafing activities. The tools might be software or hardware, which represented the subthemes for Theme 1. Table 2 identifies the nodes related to Theme 1.

Table 2

Nodes Related to Question 1, Theme 1—Tools for Actively Monitoring Cyberloafing

Theme 1 nodes	Sources	References
Software tools	5	22
Hardware tools	3	7
Total references to Theme 1		29

Subtheme: Software Tools for Monitoring Cyberloafing. Most participants who actively monitored cyberloafing used software tools. Five study participants stated that their organizations used software tools specifically for monitoring employees. Software tools can be standalone tools that specifically monitor some aspects of cyberloafing, such as bandwidth monitors. Software tools such as firewalls have monitoring tools embedded within the software. By actively monitoring through software, organizations can then take steps to curb cyberloafing activities. Small businesses in this study actively used blacklisting, bandwidth monitoring, and firewall software.

Blacklisting was the most common software tool used by the small businesses in this study. Blacklisting software can block access to specific sites and be either standalone or embedded in a firewall. Blacklisting is an easy mechanism for small businesses to monitor cyberloafing activities so that business functions proceed as usual. IT managers use blacklists to monitor by reviewing reports when users attempt to visit inappropriate sites, and then the organization can take appropriate action. Participant 7 noted that blacklisting is an integral part of monitoring in the organization. Participant 5 stated, “traffic is throttled, and priority is given to business applications as well as certain traffic being completely blocked.” Participant 4 noted using software to block certain domains, stating, “actually, we've got a red list instead of a blacklist. In that case, if it pops up, the red list automatically generates an incident response ticket that says we need to follow up on this.” Participant 4 also mentioned that there had been times that follow-ups showed that employees needed a banned site. In such cases, the appropriate action was adjusting the blacklist, rather than a disciplinary measure.

Bandwidth monitoring was another tool used by organizations in this study. Bandwidth monitoring showing increased usage pinpoints activities such as movie streaming and gaming that are not job related. By identifying high bandwidth usage, small businesses can research logs of sites visited to determine cyberloafing activity. In addition to lost employee time due to cyberloafing activities, extensive bandwidth activities slow resources for needed processes. Participant 4 noted that employee streaming could be expensive because it kills other activities. Participant 9 stated that Site 9 monitored internet usage with bandwidth monitoring software called NetFlow

Analyzer. With NetFlow Analyzer, the organization had found mainly YouTube usage during working hours that was not related to work and had to deal with employees misusing the internet. Participant 8 noted that SolarWinds Real-Time Bandwidth Monitor was the specific software used in their organization.

Software firewalls provide a history of internet usage, keystroke logging, and websites’ logs visited by employees. Using software firewalls as monitoring tools is an economical solution for small businesses because they do not have to invest in a separate software to monitor employees. Firewalls alert management to misuse of resources. Participants 1 and 3 stated that they used Sonic Firewall in their organizations. Participant 4 noted that the organization found that 40% of the employees were cyberloafing with these firewall reports. The organization then took action to reduce cyberloafing with a campaign to remind employees of proper internet usage on the job.

Subtheme: Hardware Tools for Monitoring Cyberloafing. There were fewer hardware tools for actively monitoring for cyberloafing than software tools, as indicated in this study. The two tools mentioned by participants were hardware firewalls and closed-circuit television (CCTV). Three of the participants used hardware tools for active monitoring.

Hardware firewalls, like their software counterparts, alert management to cyberloafing activities. Separate software specifically for monitoring is not necessary with the hardware firewall because of these alerts. Participant 6 indicated that the site printed internet activity reports from the hardware firewall when the firewall sent an alert. The reports showed which websites employees reached. The reports also indicated when employees went to websites, which was important because the organization did allow employees to access the internet during breaks for personal use. The time stamps on reports meant that Participant 6 did not need to use disciplinary action if the sites were timestamped during breaks. Additionally, IT managers may use the reports generated by firewalls to actively scan for cyberloafing activity daily.

Two organizations used CCTV to monitor the computer usage of employees. CCTV records employee usage for cyberloafing activities. It is an inexpensive tool to monitor cyberloafing that is easy to use but time intensive. CCTV recordings are permanent evidence of cyberloafing activity. Participant 8 maintained that CCTV was a cheaper alternative to other monitoring mechanisms. Management did not need IT personnel to monitor the activity when using CCTV, according to Participant 8. Participant 9 added to this idea by stating that CCTV is useful in the early stages of a business due to cost and ease, especially when there are fewer employees.

Relationship to the Literature**.** According to Gorman (1998), monitoring is a primary mechanism for controlling cyberloafing behaviors within an organization. The tools identified by participants to actively monitor cyberloafing were either software or hardware, confirming one study by J. Lee et al. (2017). The participants in this study mentioned bandwidth monitoring, blacklisting, hardware and software firewalls, and CCTV as tools to monitor cyberloafing.

The literature explicitly mentions bandwidth monitoring and blacklisting. Reasons to monitor employees include abuse of company resources (Akar & Karabulut Coskun, 2020; Batabyal & Bhal, 2020) and bandwidth degradation and network congestion (Koay et al., 2017). J. Lee et al. (2017) noted that software is used to restrict downloading of blacklisted apps and block websites. Gorenc et al. (2016) described software that records history, keystrokes, and websites visited to monitor cyberloafing; although they did not explicitly mention software firewalls, they described their functionality. Participants did not mention the use of keystroke loggers or email monitoring software, although the literature identifies these items as monitoring tools (Gorenc et al., 2016; Venkatraman et al., 2018). As for hardware firewalls and CCTV monitoring identified by participants, there is no mention of them in cyberloafing literature.

Relationship to the Conceptual Framework. This theme ties into the conceptual framework, AST, because the need for tools to monitor cyberloafing indicates misuse of the system’s structure. Stoffregen and Pawlowski (2018) suggested that users adapt technology from its everyday usage. Employees using the internet for personal usage is an adaptation. Straying from the intended use of technology is known as unfaithfulness (Chin et al., 1997). This unfaithfulness has led to the need for cyberloafing monitoring tools.

One participant adapted the monitoring methods over time, switching from CCTV to bandwidth monitoring software. This ties directly to the feedback loop added AST for this study. The management and IT followed Bondarouk et al. (2017) by making judgments about tools and then adapting or changing technology to better monitor cyberloafing. Participant 9 began with CCTV as the organization’s cyberloafing tool but found it too time consuming to review all the footage; therefore, Participant 9 changed tools to bandwidth monitoring software while only spot-checking CCTV footage.

Participant 6 had not yet modified monitoring tools but was considering moving from blacklisting to specific monitoring software.

Theme 2: Tools to Passively Monitor Cyberloafing

Three of the sites in this study relied on passive tools to monitor cyberloafing. Additionally, three sites that depended on active monitoring used passive techniques. Passive techniques are observation of employees at work and quotas for measuring productivity to determine if cyberloafing may occur. In most cases, the study participants then took steps to prove that cyberloafing had occurred for disciplinary action. Table 3 identifies the nodes related to Theme 2.

Table 3

Nodes Related to Question 1, Theme 2—Tools for Passively Monitoring Cyberloafing

Theme 2 nodes	Sources	References
Observation	5	17
Measuring productivity	4	14
Total references to Theme 2		31

Subtheme: Using Observation to Monitor Cyberloafing. When their organization has no technical mechanisms to monitor cyberloafing, many small businesses' IT managers use observation to identify employee cyberloafing incidents. Using observation is a cost-saving measure; the organization does not need to purchase extra hardware or software to determine cyberloafing. The observation may be part of a routine to check in with employees or may involve simply coming upon employees using the internet for nonwork activities. For example, Participant 1 stated that it was a matter of "just walking up and seeing it," while Participant 2 noticed employees online in open areas. Participant 3 had "observed people in our organization using the internet for personal use time to time." Participant 5 stated that "you would see them just kind of staring blankly at a screen and not working." Participant 8 randomly went to employees to observe what was happening on their computers.

After observing cyberloafing activities, Participants 1 and 8 would then look through browser histories to determine the problem's extent. Participant 1 also stated that a review of firewall records might determine the user's amount of cyberloafing activity. Participant 3 would also retrieve firewall reports once management or IT observed an employee cyberloafing. The firewall usage differed from the active monitoring discussed earlier because reports were run as needed to substantiate cyberloafing instead of automatically being produced daily to monitor for cyberloafing activities.

Subtheme: Measuring Productivity to Monitor Cyberloafing. An employee not completing tasks could be a sign of cyberloafing. Several sites used lack of work as an indicator that cyberloafing might be taking place. Determining the amount or quality of work that an employee should accomplish is a routine part of the job description. Because the organization was looking for productivity from employees anyway, there was no additional cost to the company to use the process to determine possible cyberloafing. For example, Participant 1 stated that "if you are not doing your job, then it is addressed." Participant 5 was more direct in indicating that the site only hired by the job. If an employee did not finish a job on time due to cyberloafing, new contracts would not be issued. Participant 7 indicated that if employees meet objectives, cyberloafing is under control. Participant 9's viewpoint was that when the company meets its goals, cyberloafing is at a minimum. Participants 1, 7, and 9 noted that when lack of work suggested cyberloafing, they took steps to determine the extent of possible cyberloafing, such as viewing browser history or downloading firewall reports. Participant 3 added that lack of productivity was the measure used in determining cyberloafing activity.

Relationship to the Literature. Indirect monitoring is supported by literature as a formal control. Khansa et al. (2017) noted formal controls as a mechanism to reduce cyberloafing intention. Walking up to someone and accidentally observing cyberloafing is not a formal procedure. However, observation is a formal control when planned. An example of planning formal control is the workplace arrangement so that foot traffic increases transparency to reduce cyberloafing (Askew & Buckner, 2017). Educators also use the tactic of arranging workstations to enhance monitoring (Karabıyık et al., 2021). Only one participant in this study mentioned intentionally observing employees, so formal controls in the form of observation were lacking.

In this study, participants mostly used productivity as a passive measure to discover cyberloafing. Productivity as a monitoring technique is the opposite of J. Lee et al.’s (2017) observation that electronic monitoring is replacing task-performance to monitor. However, small businesses watch work performance to determine pay. Hartijasti and Fathonah (2015) advocated pay-for-performance systems with younger employees to offset cyberloafing. Assessing performance led to discovering cyberloafing activities with some of the student participants. Employers that use performance to monitor may cause privacy concerns for some employees (J. Lee et al., 2017). Jiang et al. (2020) recommended further research on performance or work productivity as a mechanism to monitor cyberloafing.

Relationship to the Conceptual Framework. This theme ties to the conceptual framework because, according to Sun et al. (2020), AST can be used to assess user performance in various systems. Participants in this study used observation and quotas to monitor for cyberloafing. They used the feedback from observation and lack of performance to further explore the extent of cyberloafing. Using feedback directly relates to Bondarouk et al. (2017), who suggested that judgments about adaptations led to changes in the structure.

Theme 3: Policy and Procedure as Strategy to Monitor Cyberloafing

Three of the participants in this study expressly referred to policy as a measure for monitoring cyberloafing. Six participants identified formal procedures regarding monitoring cyberloafing, which happened to be the same six sites that use active tools to monitor cyberloafing. Table 4 identifies the nodes related to Theme 3.

Table 4

Nodes Related to Question 1, Theme 1—Monitoring Policies and Procedures

Theme 1 nodes	Sources	References
Monitoring policies	3	10
Monitoring procedures	6	19
Total references to Theme 1		29

Subtheme: Cyberloafing Monitoring Policies. Although eight participants referred to the policy against cyberloafing at their sites, only three had specific language in the policies that discussed monitoring. Having language in the policy manual that warns of monitoring lets employees know what to expect. Participant 4 stated that the site's policies warn of monitoring, and the company sends periodic reminders of this policy. Participants 8 and 9 both cautioned that monitoring policies should be clear and shared with potential employees during the interview process. Once hired, management needs to reiterate the policy to the new employees. Participant 8 has employees sign off that they know monitoring takes place. Participant 1 adds that monitoring policies should be clearly defined at the beginning of a new business venture. Participant 1 also stated that failure to do so was an oversight at Site 1 when they began providing internet access. The oversight of not outlining policies at the beginning is one reason that Site 1 does not actively monitor cyberloafing but depends on passive techniques.

Subtheme: Cyberloafing Monitoring Procedures. Having a standardized procedure to monitor cyberloafing is helpful to employees because the process is fair and applied equally every time the organization uses that procedure. Small business IT managers should document the procedures to ensure consistent application. Participant 4 is the only site with written procedures for monitoring cyberloafing.

Participant 4 stated that the site formally documents procedures and reviews the procedures once per year but will be reviewed midyear if a situation warrants it. Other participants described procedures but do not have them in writing. For example, Participant 6 stated that the procedure to monitor is tracking websites with the firewall. Participant 8 described bandwidth monitoring as the site’s cyberloafing monitoring procedure. Participant 9 described changing the procedure from viewing CCTV footage to using NetFlow Analyzer to monitor cyberloafing.

Relationship to the Literature. This theme ties into the literature as monitoring policy as a formal control is addressed explicitly in several studies. Formal controls, such as monitoring, can help reduce cyberloafing intention (Khansa et al., 2017). Cyberloafing policy should provide control while balancing employee interests, such as privacy (Jiang et al., 2020). Well-written policies will foster beneficial uses while curbing actions such as cyberloafing (Kim, 2018). However, only three of the sites had written policies describing cyberloafing monitoring. It is challenging to confirm unwritten policies, a recommendation of Glassman et al. (2015) to reduce cyberloafing. Confirmation of policy via the monitoring software is one mechanism that reduces cyberloafing (Glassman et al., 2015). It is also harder to ensure employees understand why a practice contributes to the organization's success, as Curry et al. (2017) recommended. Poorly written policies cause a lack of clarity, which appears to permit cyberloafing (Hartijasti, & Fathonah, 2015). Unwritten policies and procedures also create a lack of clarity. However, observed unwritten policy and procedure as practiced by this study participants are better than none.

Relationship to the Conceptual Framework. According to AST, a system has structure built into it(Bresciani & Comi, 2017). Policy and procedure provide structure to the internet usage of an organization. A good policy is structurally sound (Malcolm, 2015). By systematically incorporating governance structures based on shared values, beliefs, and desires, small businesses can develop compliance procedures that may reduce cyberloafing (Curry et al., 2017).

By incorporating policy and procedure the organizations in this study provided structure to the system. Bondarouk et al. (2017) recommended making judgments about a system based on data then adapting or changing as needed. Participant 4 showed the loopback of reevaluating policy and procedure when employees were unfaithful to the system and participating in cyberloafing activities.

Research Question 2

Question 2: What strategies do IT managers use to successfully deter cyberloafing in small businesses so that inappropriate usage is minimized? The analysis of data revealed three major themes for the second question: (a) tools to deter cyberloafing, (b) trust as a strategy to deter cyberloafing, and (c) policy and procedure as a strategy to deter cyberloafing.

Theme 1: Tools to Deter Cyberloafing

All the participants in the study deterred cyberloafing. Monitoring tools help deter cyberloafing; however, this theme expands to tools explicitly used for deterrence. Eight of the organizations in this multisite case study used limiting access to resources as cyberloafing deterrence. Four sites in this study used training as a deterrence tool. Table 5 identifies the nodes related to Theme 1.

Table 5

Nodes Related to Question 2, Theme 1—Tools to Deter Cyberloafing

Theme 1 nodes	Sources	References
Limiting access	8	28
Training	4	8
Total references to Theme 1		36

Subtheme: **Limiting Access to Resources.** An often-used strategy to deter cyberloafing activities is to limit access to resources. By limiting access, small businesses reduce the potential to misuse computer resources in general and the internet specifically. There are two mechanisms for limiting access. One is not to allow employees internet capabilities. The second is to limit how users access resources and what a user can do on the internet.

When prohibiting users from connecting to the internet, an organization may simply lock down the Wi-Fi access. Participant 2 accomplished this by providing phones to employees who could not access the internet and have password-protected Wi-Fi that employees could not connect their own phones. Alternatively, the organization may structure the job duties so that employees do not need to use a computer. Participant 3 stated that "half of my workforce do not use a computer at all for their job." Site 5 noted in the policy manual it does not provide an employee a computer unless needed to do the job. Participant 2 only provides computers to the management team.

Small businesses limit access to resources with login credentials for authentication. The importance of authentication is that IT can grant access to the items needed for the job. The small business can also use the monitoring software discussed earlier to help deter by tracing misuse to specific employees. Logins can also help detect when an unauthorized person is attempting to access resources. Participant 1 noted that they use computer logins and acceptable use policies on their back-office system, which deals with financial information and special processes. Participant 4 noted using the login information to send reminder emails of usage policies to employees. Participant 5 uses login information to prioritize resource usage so that employees accomplishing tasks deemed more critical. The users at site 5 with specific login credentials, such as managers, have greater access to resources.

Subtheme: Training. Several small businesses reported using training as a tool for deterring cyberloafing. Training gives employees an understanding of the policies and the organization's expectations and can help deter misuse. In some organizations, employees gain an understanding of how cyberloafing activities affect the job. In other organizations, management focuses on how the job requirements impact the paycheck if an employee does not complete the job within specified time frames.

Participant 5 trains on the job itself and shows employees what to do on the job along with what is not allowed. Participant 5 tells the employees of the time frame the job must be completed in and will not offer new contracts to employees that cannot consistently do the work in the specified time frame. Cyberloafing is deterred because the training reinforces the specific tasks within a specified time frame. The necessary tasks cannot be accomplished if cyberloafing activities occur. Productivity has improved due to the training methodology, according to Participant 5.

Participant 7 also trains on the aspect of the job itself with production metrics. However, Participant 7 also trains employees at hiring on how to use the company internet and company usage policies. Participant 8 also trains on proper computer usage policy when a new employee starts at the organization. Participant 2 uses training as well and stated, "we have had very little if any issues once we explain our expectations and come to a mutual understanding on the use of their devices."

Relationship to the Literature. Previous studies tend to focus on why people cyberloaf and not how to stop it. Using authentication methods as identified by the participants is lacking in the literature. However, training as a mechanism to deter cyberloafing exists in the literature. Training will help guide ethical decision-making in differing situations. Jafarkarimi et al. (2016) posited that training reduces computer misuse. Zoghbi-Manrique-de-Lara and Viera-Armas (2017) consider training a practical approach to deterrence. Formal training on proper usage of phones, the internet, and other communication helps deter cyberloafing activities (Gorenc et al., 2016). By creating awareness of cyberloafing policy, the company may avoid unilateral deterrence that inhibits employee productivity (Kim, 2018), which several participants indicated in the interviews.

Relationship to the Conceptual Framework. This theme ties to the conceptual framework because policy and procedure provide structure. AST posits that structure is designed into a system, and users will alter the structure (DeSanctis & Poole, 1994). Both resources and policy are structural, according to AST (Khan et al., 2020). The use of authentication logins and policy is part of these participants' systems' structure to deter cyberloafing. Authentication limits employees' ability to be unfaithful to the structure by misusing the system for cyberloafing activities. The sites used training to inform employees of the structure present through the policies.

Theme 2: Trust as Strategy to Deter Cyberloafing

Eight of the nine participants mentioned trusting their employees to use the internet appropriately at work. This trust can increase employee satisfaction and productivity. Participants noted that employees would spend time on the internet doing personal activities regardless of policy and procedures. By allowing employees some flexibility, employees feel appreciated, and these employees accomplish assigned tasks.

As a bonus, the organizations appreciate their employees more. As Participant 8 stated about the site's employees, "they are good people."

As an example of trusting employees, Participant 1 said, "you can literally sit here and do whatever you want as long as you get your job done." Participant 5 echoed the sentiment stating, "if you want to stop and look at a YouTube channel for five minutes, I don't care. cause I'm paying you by the job". Participant 2 allowed employees to use personal devices when on break and in emergencies. Additionally, Participant 2 felt that presenting employees with company policy in terms of behaving as adults with responsibilities with a need to respect company policies then giving the employees the trust to behave accordingly deters cyberloafing activities. Participant 3 indicated that the organization trusts employees to take small internet breaks as long as they complete their work. Participant 4 revealed that the site encourages employees to use company time for social networking related to company activities such as LinkedIn. Sales increased after implementing social media. Participants 7 and 8 also allowed free time to access the internet.

The primary reason for the trust is that participants feel a break is good for productivity. Participant 2 shared that spending about 5 minutes at a time cyberloafing for a couple of breaks a day relieves a bit of stress. Participant 4 noted that cyberloafing a bit allows the brain to relax. As Participant 4 explained:

> It's kind of like every couple of semesters in university. You want to go take basket weaving, or lunar archaeology, or something. We are finding a few minutes on the internet is helping people deal with the stress of working. They are

> in the office every day. And a big part of that experience is the ability to socially interact with those around them. So, we're finding digital virtual ways of doing that while they're working on it. We actually allow access to the Netflix and Amazon Primes of the world.

Relationship to the Literature. The literature supports using trust as a mechanism to deter cyberloafing. Usman et al. (2021) recommended that managers actively build trust with employees to increase productivity. Gorman (1998) suggests that exhibiting trust in employees to behave as adults may be enough to increase productivity. Kim (2018) indicated trust leads to compliance with company policy. The increase in compliance may be due to an increased sense of organizational justice. The increase in organizational justice increases trust, which increases productivity (Oosthuizen et al., 2018). Managers should apply strategies to deter cyberloafing that avoid distrust from strict regulations and monitoring (Nivedhitha & Sheik Manzoor, 2020). A firm deterrence policy based solely on punishment may encourage distrust (Kim, 2018). Monitoring policies may also elicit distrust if not fully disclosed (Urbaczewski & Jessup, 2002) or when implemented for the first time (Jiang et al., (2020). None of the organizations in this study noted balancing trust with policy or procedures.

Several participants noted that cyberloafing fulfills a need to have a break. Literature backs this claim. Kim (2018) found a 10-minute break from work through cyberloafing made for a significantly more productive group. Limited personal use of computers may improve performance by reducing stress and job burnout (Koay & Soh, 2018). Derin and Gökçe (2016) argue that employees that cyberloaf are more innovative and perform at a higher level from them being more refreshed by taking a break from the work routine. Aladwan et al. (2021) found that cyberloafing breaks positively impact productivity and employee morale.

Relationship to the Conceptual Framework. This theme relates to the conceptual framework because employees try to deviate from the structure by cyberloafing. Through the structuration process, users or user groups shape norms, values, and resources (Stoffregen, & Pawlowski, 2018). Whitaker and New (2016) noted emergent structures deviate from the base structure envisioned by the organization. Users will modify a system according to AST. In cyberloafing situations, that modification is using the internet, not as intended by the organization. Using trust as a deterrent for cyberloafing, the organization shapes values in the employees. There is a sense of worth to the organization, and productivity increases. By incorporating trust in cyberloafing policy, the organization encourages the emergent structure instead of simply allowing employees to create it by their cyberloafing activities. The new structure in the system is indicated in the feedback loop of the framework for this study.

Theme 3: Policy and Procedure as Strategy to Deter Cyberloafing

Policy and procedure to deter cyberloafing is the most used strategy used by participants in this study. Eight of the participants in this study referred to policy for deterring cyberloafing. All nine participants identified formal procedures regarding cyberloafing deterrence. Table 6 identifies the nodes related to Theme 3.

Table 6

Nodes Related to Question 2, Theme 3—Policy and Procedure to Deter Cyberloafing

Theme 3 nodes	Sources	References
Deterrence policy	8	28
Deterrence procedure	9	23
Total references to Theme 3		51

Subtheme: Cyberloafing Deterrence Policy. Deterrence policy provides a structure for the use of the organization's computer assets. Policies inform employees of management expectations when using the system. Policies also outline the ramifications if not followed. Deterrence policy also gives IT managers the structure they need to enact cyberloafing deterrence procedures. As Participant 4 stated, "We depend on our HR group to help us promulgate policy, and we the device to implement the policy." When discussing policy, this study's participants mentioned three things: specific deterrence policy, changing policy, and policy importance.

Specific deterrence policy varied widely between the participants. Participant 1 mentioned that the site does not have a strict cyberloafing policy but uses the employee handbook's general guidance. The handbook notes that the internet is to be used for business purposes, and the privilege can be removed if misused. Participant 3 uses professional conduct policies to formulate cyberloafing deterrence procedures. The policy for Site 3 stated, "employees are expected to use the internet responsibly and professionally." Participant 6 referred to a section in the employee handbook outlining acceptable usage of company-owned computers and systems. Participants 8 and 9 both indicated strict predefined internet usage policies. Participant 4 had a complete policy, which defined cyberloafing, outlined acceptable use, and outlined discipline. Participants

1, 2, 7, 8, and 9 indicated that policy defined general discipline procedures such as verbal warnings, written warnings, suspension, termination, and criminal prosecution and applied to cyberloafing cases.

Five of the participants mentioned the ability to change policy. Only Participant 4 had formal policy update procedures. Every November, human resources (HR) and the IT manager review policy and make changes if necessary. However, Participant 4 also said that the organization would make changes between the formal reviews and reduce restrictions to access specific sites during COVID. Participant 3 indicated that the organization updates the handbook if a situation arises not coved in the handbook. Participant 6 stated that the site updates policy on an as-needed basis. Participant 7 also updated policies as needed. Participant 8 noted that the site had to update policy when the store grew to have more customers. Cyberloafing activities resulted in poor customer service, and the organization rewrote policies to be stricter.

There is a need for formal policy in organizations. The participants indicated the need for policy in terms of best practices or advice to new IT managers. Participant 1 recommended having formal policies and procedures established at the start of a business, so there is no gray area. Participant 8 noted that strict measures should be in place early and did Participant 9. Participant 4 also lamented not having policies in place early and noted an extensive change management exercise when a policy is added or updated. Participant 4 recommended having a formal definition of cyberloafing, specifically the percentage of time an employee may use the computer for nonwork activities. Participant 4 also recommended using consistent language in policies.

Subtheme: Cyberloafing Deterrence Procedure. Cyberloafing deterrence procedures are the steps taken to enforce the policy. These steps can be the specific implementation of deterrence practices. The procedure may also be the application of discipline if an employee abuses policy. Without the procedures to enforce policy, the policy would have no power. Procedures also create a work environment that reduces stress. Participant 2 provided an example,

> We find it interesting when our employees visit a job site. They come back and tell us they wished the site had the same technology policies we had in place because it would have taken less time for their visit if the other person would have put down their devices and let us do our job.

All nine participants mentioned procedures to enforce cyberloafing deterrence. Procedures to implement deterrence policy are the tools used for deterrence discussed earlier. IT could limit access to Wi-Fi, such as Site 3 does. Training can be a deterrence procedure. Participant 5 stated, "I literally still have to teach them very specifically what to do." Trusting employees to use resources appropriately was a procedure used by eight participants. Participant 2 stated the trust procedure best, "Employees are presented company policy in terms of behaving as adults with responsibilities with a need to respect company policies then are given the trust to behave accordingly."

Six participants specified procedures to discipline employees that deviate from policy. Participant 1 stated that management asks for data on possible cyberloafing. Using the firewall software, Participant 1 provides the data then HR disciplines the employee. Participant 2 indicated management counseled employees found deviating from the policy on acceptable usage. Participant 3 issues verbal warnings followed by written warnings then termination in repeat offenses, as does Participants 7, 8, and 9. Participant 4 stated the first procedure is to offer a discreet message on the computer when an employee is cyberloafing. Both Participants 4 and 9 mentioned criminal action if the situation warrants it.

Like policy, small business IT managers updated procedures when necessary. Participants 4 and 7 mentioned updating blacklists after cyberloafing incidents. Participant 4 stated that when an employee attempts to reach the same blocked site multiple times, the verbal warning process includes asking the employee how it is related to the job. When an employee shows the value of the site, the blacklist is updated. Participant 7 also stated that IT had removed websites from the blocked list.

Relationship to the Literature. The literature supports using employee policy as a deterrence strategy. The literature suggests that policy is a fundamental deterrence approach. Kim (2018) posited employees knowing the cyberloafing policies may result in increased employee productivity. Jeong et al. (2020) extoll the necessity of concrete policy. Cheng et al. (2020) posited that IT managers should make policy to control cyberloafing based on perceived overqualification by employees. Regardless, the policy should contain consequences for breaking the cyberloafing policy (Cheng et al., 2014).

IT managers back deterrence policy with discipline, which can be a punishment or other sanctions. Small business IT managers must consider discipline carefully because deterrence policy based solely on punishment may encourage distrust (Kim, 2018). Some organizations apply very stringent penalties (Hadlington & Parsons, 2017). Participants in this study used a variety of penalties, usually on a sliding scale. First offenses resulted in verbal warnings, and penalties moved to written warnings, then termination. Other companies will ignore the problem or use training to counteract cyberloafing activities. Whatever the discipline procedures, IT needs to administer them fairly. Perceived unfairness may cause trust issues leading to more cyberloafing (Kim, 2018).

Relationship to the Conceptual Framework. This theme ties into the conceptual framework, AST, because policy provides a structure for using internet resources in the organization. According to AST, designers build structure into a system (Bresciani & Comi, 2017). Procedure enforces policy within the structure. Compliance procedures may reduce cyberloafing (Curry et al., 2017). Stoffregen and Pawlowski (2018) indicated that users adapt technology from its everyday usage. By updating policy and procedure, IT managers utilize the feedback loop added to AST for this study. Participants updating policy and procedure directly supports Bondarouk et al. (2017), who advised making judgments on feedback then adapting. Five of the participants noted the ability to change policy as needed.

Applications to Professional Practice

In this study, I researched strategies that small business IT managers used to successfully monitor and deter cyberloafing activities. These strategies may discourage cyberloafing and improve productivity. With careful management, these strategies should also help retain employee satisfaction.

The findings in this study reveal that cyberloafing exists in all nine organizations to a degree. The participants were able to apply strategies that monitor and deter cyberloafing activities affordable to a small business. Tools built into other functions, such as restricting website access with firewalls, produce no additional expense to the organization. Blacklisting software built into the operating system is another example of a tool that causes no additional cost to a small business. Other tools, such as CCTV cameras and some bandwidth monitoring software, are available at a low cost to small business IT departments. Using production metrics and observation to determine cyberloafing cost nothing but time to the organization.

Embedding training on cyberloafing with job expectation training is a low-cost strategy to deter cyberloafing. IT managers that utilize training may have a more productive workforce. The employees understand the organization's expectations of them in terms of production. Training highlights cyberloafing policies and ramifications.

IT managers should utilize policy and procedure in the cyberloafing monitoring and deterrence practices. Policies should be clear. The policy should contain a formal definition of cyberloafing. The organization should outline procedures as part of policies. Participants reviewed policy and procedure annually, but a best practice is to revise policies as needed due to detected cyberloafing activities or business processes changes.

Trust as a strategy to deter cyberloafing allows employees to have some power over their daily activities. As such, employees tended to be more productive and invested in the organization. The empowerment inherent in a trust relationship aids in employee growth and employee satisfaction. IT managers benefit from greater productivity as well. Eight of the nine participants of this study used trust as a strategy to some degree and found it successful in deterring excessive cyberloafing activities.

Implications for Social Change

The implication for positive social change is contributing to greater economic stability in the community while promoting a healthy working environment. Increasing productivity and reducing risk by controlling cyberloafing creates economic stability. Small businesses also are efficient mechanisms to create jobs and fuel the economy worldwide (Francis & Willard, 2016). Economic stability can lower the stress level of employees. Reducing stress reduces burnout (Kim & Christensen, 2017). The strategies to deter and monitor cyberloafing used by this study participants increased productivity in the organizations. Increased productivity means gainful employment, which helps the economic stability of the community. The participants also reduced risk to their organizations by restricting harmful internet practices such as visiting websites containing viruses or inappropriate materials that customers could see.

The strategies used by the participants can provide positive social change for their employees by providing a healthy work-life balance. Employees need work-life balance (Soh et al., 2017). Employees who check work email from home can also check personal email at work. By exhibiting trust in employees to control cyberloafing, participants helped employees with personal growth while increasing productivity. Allowing breaks for employees may increase morale.

Recommendations for Action

Small business IT managers and owners seeking to monitor or deter cyberloafing may consider the strategies identified in this study. Cyberloafing increases business risk by threatening the information technology (IT) system (Glassman et al., 2015). IT managers may use the strategies identified in this study to reduce risk with small businesses' limited resources cost-effectively.

The first recommendation is to incorporate cost-effective tools for monitoring cyberloafing. Monitoring discourages internet usage that is not work-related (Gorenc et al., 2016). Monitoring software tracks company computer usage for activities that are not work-related (Arciniega et al., 2017). Small business IT managers may purchase inexpensive monitoring software. However, participants in this study emphasized options that were already on hand or free to use. IT managers need to look at firewalls to see what mechanisms for monitoring are built-in to the software. IT managers should also incorporate techniques such as observation as a cost-effective tool for monitoring.

The second recommendation is to incorporate trust as a strategy to deter cyberloafing. Gorman (1998) suggests that exhibiting trust in employees to behave as adults may be enough to increase productivity. By allowing employees to take small breaks by cyberloafing, productivity improves, as does employee satisfaction. Derin and Gökçe (2016) argue that employees that cyberloaf are more innovative and perform at a higher level from them being more refreshed by taking a break from the work routine. The participants of this study allowed small breaks and were happy with the overall productivity of their employees.

The third recommendation is to develop written policies and procedures on cyberloafing monitoring and deterrence. Well-written policies will foster beneficial uses while curbing actions such as cyberloafing (Kim, 2018). Participants in this study recommended having policies in place when opening a business. One site recommended defining cyberloafing based on a percentage of time allowed for nonwork activities to clear expectations. Additionally, IT managers should also develop written procedures to monitor and deter cyberloafing. Lastly, a formal routine to review all policies and procedures will keep them up-to-date and reliable for the organization.

I will disseminate the findings of this study by sharing the results with the study participants. I also plan to share findings at conferences and through scholarly journals.

Recommendations for Further Study

The research design was an exploratory multisite case study. A limitation of this design is the small sample size of nine sites. There were only nine participants. Eight of the cases were small retail businesses. Future research in small businesses, that are not retail, could result in similar or contrasting results.

A second limitation of the study was a small geographical area. The participants were from five states with the United States; four of those states were in the American South. One case was a bank representing a small business in the service industry. Future researchers could replicate this study in more sites or in a larger geographic area to search for similar or contrasting results.

The participants described cyberloafing monitoring and deterrence strategies on the organization's equipment while employees were using organization resources. These findings do not address working from home. More employees at home due to COVID and planning to remain as teleworkers in the future. A recommendation for future research would be monitoring and deterring cyberloafing strategies for small businesses with teleworkers.

Similarly, this study did not address workers on their own devices. Participants mentioned workers searching online on their own devices. Only one participant mentioned blocking Wi-Fi access to users to not access the internet through company resources on their own phones. Strategies for cyberloafing deterrence on BYOD policies could be a future possibility.

In this study, four participants measured performance to monitor cyberloafing. Jiang et al. (2020) recommend further research on performance or work productivity as a mechanism to monitor cyberloafing. The exploratory nature of this case study also indicates possible future research on productivity to monitor cyberloafing.

Several sites actively monitored cyberloafing while stating they trusted their employees to behave like grownups. This ‘monitor but trust’ relationship feels like a mixed message. Future researchers could explore how this balance between monitoring and trust works.

Reflections

I have worked in higher education for 20 years. During that time, I have observed students cyberloafing instead of focusing on schoolwork. Also, I have a friend that was terminated for cyberloafing on the job. As such, I had to work to control my bias on strategies to monitor and deter cyberloafing. I limited my bias with member checking, triangulation, and reflection on participant responses. The member checking allowed participants to determine if my reflections were correct, limiting bias.

I used a reflective journal to document the process. This was difficult for me as I do not like to journal. However, through the journaling, I found that preconceived ideas were not confirmed. Notes that I took after each interview helped me understand the participants' views and reflect on what each participant said. This helped with bias along with the member checking. The Doctor of Business Administration (DBA) doctoral study process expanded my understanding of research methodology and allowed me to practice scholarly research.

The doctoral study process has shaped my ability to practice scholarly research. This process has helped me develop patience as I struggled to find participants due to COVID shutting down small businesses. The study has taught me perseverance as I navigated several personal setbacks during the process. The study has also taught me to appreciate the voices of others better.

Summary and Study Conclusions

This study's findings indicated that small business IT managers apply strategies that moderate cyberloafing activities rather than eliminate cyberloafing. The monitoring and deterrence strategies resulted in higher productivity while maintaining employee satisfaction. Employees felt the organizations treated them as adults. The organizations' leadership felt that strategies implemented by the IT managers resulted in good employees. Although many spent some time cyberloafing, issues requiring discipline were few.

Nine organizations contributed to this multisite case study. At each site, one IT manager took part for a total of nine participants for interviews. Seven participants contributed to my understanding via member checking. Three major themes emerged for monitoring cyberloafing: (a) tools to actively monitor cyberloafing, (b) tools to monitor cyberloafing passively, and (c) policy and procedure as a strategy to monitor cyberloafing. Three significant themes emerged for deterrence of cyberloafing: (a) tools to deter cyberloafing, (b) trust as a strategy to deter cyberloafing, and (c) policy and procedure as a strategy to deter cyberloafing.

In conclusion, small business IT managers can find cost-effective solutions to monitor and deter cyberloafing by using existing tools. Well-written policies and procedures aid in monitoring deterring cyberloafing, and the participants of this study used these tools extensively. However, the best approach may simply be giving employees short breaks to use the internet for personal items to increase productivity and employee satisfaction.

References

Abma, T. A., & Stake, R. E. (n.d.). Science of the particular: An advocacy of naturalistic case study in health research. *Qualitative Health Research*, *24*(8), 1150–1161. https://doi.org/10.1177/1049732314543196

Agarwal, U. (2019). Impact of supervisors' perceived communication style on subordinate's psychological capital and cyberloafing. *Australasian Journal of Information Systems*, *23,* 1–27. https://doi.org/10.3127/ajis.v23i0.1759

Agarwal, U. A., & Avey, J. B. (2020). Abusive supervisors and employees who cyberloaf: Examining the roles of psychological capital and contract breach. *Internet Research*, *30*(3), 789–809. https://doi.org/10.1108/INTR-05-2019-0208

Akar, I., & Karabulut Coskun, B. (2020). Exploring the relationship between creativity and cyberloafing of prospective teachers. *Thinking Skills and Creativity*, *38.* https://doi.org/10.1016/j.tsc.2020.100724

Akbulut, Y., Dönmez, O., & Dursun, Ö. Ö. (2017). Cyberloafing and social desirability bias among students and employees. *Computers in Human Behavior*, *72,* 87-95. https://doi.org/10.1016/j.chb.2017.02.043

Aladwan, M. A., Muala, I. A., & Salleh, H. S. (2021). Cyberloafing as a mediating variable in the relationship between workload and organizational commitment. *Management Science Letters*, 1013–1022. https://doi.org/10.5267/j.msl.2020.9.041

Andel, S. A., Kessler, S. R., Pindek, S., Kleinman, G., & Spector, P. E. (2019). Is cyberloafing more complex than we originally thought? Cyberloafing as a coping response to workplace aggression exposure. *Computers in Human Behavior*, *101*, 124–130. https://doi.org/10.1016/j.chb.2019.07.013

Anderson, C. A., Leahy, M. J., DelValle, R., Sherman, S., & Tansey, T. N. (2014). Methodological application of multiple case study design using modified consensual qualitative research (CQR) analysis to identify best practices and organizational factors in the public rehabilitation program. *Journal of Vocational Rehabilitation*, *41*(2), 87–98. https://doi.org/10.3233/JVR-140709

Anni, C. T. (2018). School counselors' intention to use technology: The technology acceptance model. *Turkish Online Journal of Educational Technology*, *17*(2), 120–124. https://eric.ed.gov/?id=EJ1176168

Arciniega, L. M., Stanley, L. J., Puga-Méndez, D., Obregón-Schael, D., & Politi-Salame, I. (2017). The relationship between individual work values and unethical decision-making and behavior at work. *Journal of Business Ethics*, 1-16. https://doi.org/10.1007/s10551-017-3764-3

Askew, K. L., & Buckner, J. E. (2017). The role of the workstation: Visibility of one's computer screen to coworkers influences cyberloafing through self-efficacy to hide cyberloafing. *The Psychologist-Manager Journal*, *20*(4), 267–287. https://doi.org/10.1037/mgr0000061

Atitumpong, A., & Badir, Y. F. (2018). Leader-member exchange, learning orientation and innovative work behavior. *Journal of Workplace Learning*, *30*(1), 32–47. https://doi.org/10.1108/JWL-01-2017-0005

Banerjee, S., & Thakur, S. (2016). A critical study of factors promoting cyberloafing in organizations. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies* (pp. 139-144). Association for Computing Machinery. https://doi.org/10.1145/2905055.2905355

Barrett, A. K. (2018). Technological appropriations as workarounds: Integrating electronic health records and adaptive structuration theory research. *Information Technology & People*, *31*(2), 368-387. https://doi.org/10.1108/ITP-01-2016-0023

Baškarada, S., & Koronios, A. (2018). A philosophical discussion of qualitative, quantitative, and mixed methods research in social science. *Qualitative Research Journal*, *18*(1), 2–21. https://doi.org/10.1108/QRJ-D-17-00042

Batabyal, S. K., & Bhal, K. T. (2020). Traditional cyberloafing, mobile cyberloafing and personal mobile-internet loafing in business organizations: Exploring cognitive ethical logics. *Journal of Information, Communication & Ethics in Society*, *18*(4), 631-647. https://doi.org/10.1108/jices-07-2019-0081

Bhattacherjee, A., & Shrivastava, U. (2018). The effects of ICT use and ICT laws on corruption: A general deterrence theory perspective. *Government Information Quarterly*, *35*(4), 703–712. https://doi.org/10.1016/j.giq.2018.07.006

Bicket, M. C., Brat, G. A., Hutfless, S., Wu, C. L., Nesbit, S. A., & Alexander, G. C. (2019). Optimizing opioid prescribing and pain treatment for surgery: Review and conceptual framework. *American Journal of Health-System Pharmacy*, *76*(18), 1403–1412. https://doi.org/10.1093/ajhp/zxz146

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal*, (4), 426-432. https://doi.org/10.1108/QMR-06-2016-0053

Bondarouk, T., Harms, R., & Lepak, D. (2017). Does e-HRM lead to better HRM service? *The International Journal of Human Resource Management*, *28*(9), 1332-1362. https://doi.org/10.1080/09585192.2015.1118139

Braganza, M., Akesson, B., & Rothwell, D. (2017). An empirical appraisal of Canadian doctoral dissertations using grounded theory: Implications for social work research and teaching. *Journal of Teaching in Social Work*, *37*(5), 528-548. https://doi.org/10.1080/08841233.2017.1386259

Bresciani, S., & Comi, A. (2017). Facilitating culturally diverse groups with visual templates in collaborative systems. *Cross Cultural & Strategic Management, 24*(1), 78-98. https://doi.org/10.1108/CCSM-12-2015-0200

Bush, A. A., & Amechi, M. H. (2019). Conducting and presenting qualitative research in pharmacy education. *Currents in Pharmacy Teaching and Learning*, *11*(6), 638–650. https://doi.org/10.1016/j.cptl.2019.02.030

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning*, *10*(6), 807–815. https://doi.org/10.1016/j.cptl.2018.03.019

Cheng, B., Zhou, X., Guo, G., & Yang, K. (2020). Perceived overqualification and cyberloafing: A moderated-mediation model based on equity theory. *Journal of Business Ethics*, *164*(3), 565–577. https://doi.org/10.1007/s10551-018-4026-8

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. https://doi.org/10.1016/j.chb.2014.05.043

Che Pa, N., Anthony Jnr, B., Jusoh, Y., Nor, H., Nor, R., Aris, M., & Noranis, T. (2017). A risk mitigation decision framework for information technology organizations. *Journal of Theoretical & Applied Information Technology, 95*(10), 2102-2113. Retrieved from www.jatit.org

Chin, W. W., Gopal, A., & Salisbury, W. D. (1997). Advancing the theory of adaptive structuration: The development of a scale to measure faithfulness of appropriation. *Information systems research, 8*(4), 342-367. https://doi.org/10.1287/isre.8.4.342

Ching-Chiu, H., Jeong-Yang, P., & Lew, Y. K. (2019). Resilience and risks of cross-border mergers and acquisitions. *Multinational Business Review, 27*(4), 427-450. https://doi.org/10.1108/MBR-05-2019-0035

Cruz, L. (2015). Self-reflexivity as an ethical instrument to give full play to our explicit and implicit subjectivity as qualitative researchers. *The Qualitative Report*, *20*(10), 1723-1737. Retrieved from http://nsuworks.nova.edu/tqr/vol20/iss10/13/

Curry, M., Marshall, B., & Kawalek, P. (2017). A normative model for assessing SME IT effectiveness. *Communications of the IIMA, 15*(1), 35-60. Retrieved from http://scholarworks.lib.csusb.edu/ciima/vol15/iss1/3/

Danielsson, L., & Rosberg, S. (2015). Opening toward life: Experiences of basic body awareness therapy in persons with major depression. *International Journal of Qualitative Studies on Health and Well-Being, 10*(1), 24-44. https://doi.org/10.3402/qhw.v10.27069

Derin, N., & Gökçe, S. G. (2016). Are cyberloafers also innovators? A study on the relationship between cyberloafing and innovative work behavior. *Procedia-Social and Behavioral Sciences*, *235*, 694-700. https://doi:10.1016/j.sbspro.2016.11.070

DeSanctis, G., & Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. *Organization Science*, *5*(2), 121-147. https://doi.org/10.1287/orsc.5.2.121

Deslonde, V., & Becerra, M. (2018). The technology acceptance model (TAM): Exploring school counselors' acceptance and use of Naviance. *The Professional Counselor, 8*(4), 369-382. https://doi.org/10.15241/vd.8.4.369

Dubé, L., & Paré, G. (2003). Rigor in information systems positivist case research: Current practices, trends, and recommendations. *MIS Quarterly*, *27*(4), 597–635. https://doi.org/10.4135/9781473915480.n65

Durcikova, A., Lee, A. S., & Brown, S. A. (2018). Making rigorous research relevant: Innovating statistical action research. *MIS Quarterly*, *42*(1), 241-A13. https://doi.org/10.25300/MISQ/2018/14146

Dursun, O. O., Donmez, O., & Akbulut, Y. (2018). Predictors of cyberloafing among preservice information technology teachers. *Contemporary Educational Technology*, *9*(1), 22–41. https://doi.org/10.30935/cedtech/6209

Ellis, P. (2019). The language of research (part 20): understanding the quality of a qualitative paper (2). *Wounds UK*, *15*(1), 110–111. Retrieved from https://www.wounds-uk.com

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, *6*, 323-337. https://doi.org/10.28945/3325

Errington, G., Watson, M. C., Hamilton, T., Mulvaney, C., & Binley, S. (2012). Implementing a national programme at local level: findings from a multiple-site case study. *International Journal of Health Promotion & Education*, *50*(6), 318–327. https://doi.org/10.1080/14635240.2012.735386

Fakoor Saghih, A. M., & Nosrati, S. (2021). The antecedents of job embeddedness and their effects on cyberloafing among employees of public universities in eastern Iran. *International Journal of Islamic & Middle Eastern Finance & Management*, *14*(1), 77–93. https://doi.org/10.1108/IMEFM-11-2019-0489

Fedorko, I., Bacik, R., & Gavurova, B. (2018). Technology acceptance model in e-commerce segment. *Management & Marketing*, *13*(4), 1242-1256. https://doi.org/10.2478/mmcks-2018-003

Fleet, D., Burton, A., Reeves, A., & DasGupta, M. P. (n.d.). A case for taking the dual role of counsellor-researcher in qualitative research. *Qualitative Research in Psychology*, *13*(4), 328–346. https://doi.org/10.1080/14780887.2016.1205694

Forst, B. (1983). Capital punishment and deterrence: Conflicting evidence. *Journal of Criminal Law & Criminology*, *74*, 927-942. https://doi.org/10.2307/1143139

Forth, J., & Bryson, A. (2019). Management practices and SME performance. *Scottish Journal of Political Economy*, *66*(4), 527–558. https://doi.org/10.1111/sjpe.12209

Francis, M. M., & Willard, M. (2016). Unlocking the potential of information and communication technology for business sustainability by small, micro and medium enterprises in Vhembe District, South Africa. *ICT, Society, and Human Beings 2016*, 41-49. Retrieved from http://irep.iium.edu.my

Frémeaux, S., Michelson, G., & Noël-Lemaitre, C. (2018). Learning from Greek Philosophers: The Foundations and Structural Conditions of Ethical Training in Business Schools: JBE. *Journal of Business Ethics, 153*(1), 231-243. https://doi.org/10.1007/s10551-016-3398-x

Friberg, T. (2016). Generating ethnographic research questions: an anthropological contribution to the study of higher education. *Ethnography & Education*, *11*(3), 345–358. https://doi.org/1080/17457823.2015.1101386

Gallagher, B., Berman, A. H., Bieganski, J., Jones, A. D., Foca, L., Raikes, B., Schiratzki, J., Urban, M., & Ullman, S. (2016). National human research ethics: a preliminary comparative case study of Germany, Great Britain, Romania, and Sweden. *Ethics & behavior*, *26*(7), 586-606. https://doi.org/10.1080/10508422.2015.1096207

Galli, C. D. (2015). A compliance crisis is a terrible thing to waste: Counsel's role to enhance corporate culture. *Natural Resources & Environment*, *30*, 8-12. Retrieved from www.americanbar.org

Gelo, O., Braakmann, D., & Benetka, G. (2008). Quantitative and qualitative research: Beyond the debate. *Integrative Psychological & Behavioral Science, 42*(3), 266-290. https://doi.org/10.1007/s12124-008-9078-3

Ghani, F. A., Muslim, N. A., Rasli, M. A. M., Bhaskaran, K. N. A., Rashid, R. E., & Kadir, S. A. S. A. (2018). Problematic usage of digital technologies at workplace: A study on job stress and cyberloafing behaviour among government servants in Malaysia. *Global Business & Management Research, 10*(8), 754–760. Retrieved from https://www.questia.com

Glassman, J., Prosch, M., & Shao, B. B. (2015). To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure. *Information & Management*, *52*(2), 170-182. https://doi.org/10.1016/j.im.2015.11.001

Gökçearslan, Ş., Uluyol, Ç., & Şahin, S. (2018). Smartphone addiction, cyberloafing, stress and social support among university students: A path analysis. *Children and Youth Services Review, 91*, 47–54. https://doi.org/10.1016/j.childyouth.2018.05.036

Gorenc, M., Blažič, B. J., & Urnaut, A. G. (2016). Abuse of Internet services in the workplace and the emergence of addiction. *IIASS: Innovative Issues and Approaches in Social Sciences, 9*(2), 116-136. https://doi.org/10.12959/issn.1855-0541.IIASS-2016-no2-art7

Gorman, J. (1998). Monitoring employee Internet usage. *Business Ethics: A European Review, 7*(1), 21-24. https://doi.org/10.1111/1467-8608.00081

Güğerçin, U. (2019). Does technostress justify cyberslacking? An empirical study based on the neutralisation theory. *Behaviour & Information Technology*, 1–13. https://doi.org/10.1080/0144929x.2019.1617350

Ha, S. T., Nguyen, T. N., & Braa, J. (2017). Transformation of daily work practices because of information technology introduction: The case of medical licensing system. *Journal of Health Informatics in Developing Countries*, *11*(1), 1-16. Retrieved from www.jhidc.org

Hadlington, L., & Parsons, K. (2017). Can cyberloafing and Internet addiction affect organizational information security? *Cyberpsychology, Behavior, and Social Networking*, *20*(9), 567-571. https://doi.org/10.1089/cyber.2017.0239

Hagqvist, E., Vinberg, S., Tritter, J. Q., Wall, E., & Landstad, B. J. (2020). The same, only different: Doing management in the intersection between work and private life for men and women in small-scale enterprises. *Work, Employment & Society*, *34*(2), 262–280. https://doi.org/10.1177/0950017019871244

Hartijasti, Y., & Fathonah, N. (2015). Motivation of cyberloafers in the workplace across generations in Indonesia. *International Journal of Cyber Society and Education*, *8*(1), 49-58. https://doi.org/10.7903/ijcse.1360

Hartmann, W. E., St. Arnault, D. M., & Gone, J. P. (2018). A return to “the clinic” for community psychology: Lessons from a clinical ethnography in urban American Indian behavioral health. *American Journal of Community Psychology*, *61*(1–2), 62–75. https://doi.org/10.1002/ajcp.12212

Henderson, H. (2018). Difficult questions of difficult questions: the role of the researcher and transcription styles. *International Journal of Qualitative Studies in Education, 31*(2), 143-157, https://doi.org/10.1080/09518398.2017.1379615

Hensel, P. G., & Kacprzak, A. (2020). Curbing cyberloafing: studying general and specific deterrence effects with field evidence. *European Journal of Information Systems*, 1–17. https://doi\.org/10.1080/0960085x.2020.1756701

Hillson, R., Alejandre, J. D., Jacobsen, K. H., Ansumana, R., Bockarie, A. S., Bangura, U., Lamin, J. M., & Stenger, D. A. (2015). Stratified sampling of neighborhood sections for population estimation: A case study of Bo City, Sierra Leone. *PLoS One*, *10*(3), 9-23. https://doi.org/10.1371/journal.pone.0132850

Holten, L., Hollander, M., & de Miranda, E. (n.d.). When the hospital is no longer an option: A multiple case study of defining moments for women choosing home birth in high-risk pregnancies in The Netherlands. *Qualitative Health Research*, *28*(12), 1883–1896. https://doi.org/10.1177/1049732318791535

Huma, Z., Hussain, S., Thurasamy, R., & Malik, M. I. (2017). Determinants of cyberloafing: a comparative study of a public and private sector organization. *Internet Research*, *27*(1), 97–117. https://doi.org/10.1108/intr-12-2014-0317

Hur, W. M., Moon, T. W., & Ko, S. H. (2018). How employees' perceptions of CSR increase employee creativity: Mediating mechanisms of compassion at work and intrinsic motivation. *Journal of Business Ethics, 153*(3), 629-644. https://doi.org/10.1007/s10551-016-3321-5

Iannacci, F., Seepma, A. P., de Blok, C., & Resca, A. (2019). Reappraising maturity models in e-Government research: The trajectory-turning point theory. *Journal of Strategic Information Systems*, *28*(3), 310–329. https://doi.org/10.1016/j.jsis.2019.02.001

Iyamu, T. (2017). Improvising information technology projects through the duality of structure. *South African Journal of Information Management*, *19*(1), 1-9. https://doi.org/10.4102/sajim.v19i1.797

Jafarkarimi, H., Saadatdoost, R., Sim, A. T. H., & Hee, J. M. (2016). Behavioral intention in social networking sites ethical dilemmas: An extended model based on theory of planned behavior. *Computers in Human Behavior*, *62*, 545-561. https://doi.org/10.1016/j.chb.2016.04.024

Janson, A., Söllner, M., & Leimeister, J. M. (2020). Ladders for learning: Is scaffolding the key to teaching problem-solving in technology-mediated learning contexts? *Academy of Management Learning & Education*, *19*(4), 439–468. https://doi.org/10.5465/amle.2018.0078

Jeong, Y., Jung, H., & Lee, J. (2020). Cyberslacking or smart work: Smartphone usage log-analysis focused on app-switching behavior in work and leisure conditions. *International Journal of Human-Computer Interaction*, *36*(1), 15–30. https://doi.org/10.1080/10447318.2019.1597574

Jiang, H., Tsohou, A., Siponen, M., & Li, Y. (2020). Examining the side effects of organizational Internet monitoring on employees. *Internet Research*, *30*(6), 1613–1630. https://doi.org/10.1108/INTR-08-2019-0360

Johnston, C. M., Wallis, M., Oprescu, F. I., & Gray, M. (2017). Methodological considerations related to nurse researchers using their own experience of a phenomenon within phenomenology. *Journal of Advanced Nursing*, *73*(3), 574-584. https://doi.org/10.1111/jan.13198

Joo, Y. J., Park, S., & Lim, E. (2018). Factors influencing preservice teachers' intention to use technology: TPACK, teacher self-efficacy, and technology acceptance model. *Journal of Educational Technology & Society*, *21*(3), 48-59. Retrieved from https://dspace.ewha.ac.kr/

Karabıyık, C., Baturay, M. H., & Özdemir, M. (2021). Intention as a mediator between attitudes, subjective norms, and cyberloafing among preservice teachers of English. *Participatory Educational Research*, *8*(2), 57–73. https://doi.org/10.17275/per.21.29.8.2

Kelly, T., & Kelly, M. H. (2019). Living with ureteric stents: a phenomenological study. *British Journal of Nursing*, *28*(9), S29–S37. https://doi.org/10.12968/bjon.2019.28.9.S29

Khan, A., Boroomand, F., Webster, J., & Minocher, X. (2020). From Elements to Structures: An Agenda for Organisational Gamification. *European Journal of Information Systems*, *29*(6), 621–640. https://doi.org/10.1080/0960085X.2020.1780963

Khansa, L., Kuem, J., Siponen, M., & Kim, S. S. (2017). To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls.

Journal of Management Information Systems, *34*(1), 141-176. https://doi.org/10.1080/07421222.2017.1297173

Kim, S. (2018). Managing millennials' personal use of technology at work. *Business Horizons*, *61*(2), 261-270. https://doi.org/10.1016/j.bushor.2017.11.007

Kim, S., & Christensen, A. L. (2017). The dark and bright sides of personal use of technology at work: A job demands–resources model. *Human Resource Development Review, 16*(4), 425–447. https://doi.org/10.1177/1534484317725438

Koay, K. Y. (2018). Workplace ostracism and cyberloafing: a moderated-mediation model. *Internet Research*, *28*(4), 1122–1141. https://doi.org/10.1108/IntR-07-2017-0268

Koay, K. Y., Soh, P. C.-H., & Chew, K. W. (2017). Do employees' private demands lead to cyberloafing? The mediating role of job stress. *Management Research Review*, *40*(9), 1025–1038. https://doi.org/10.1108/MRR-11-2016-0252

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *The European Journal of General Practice*, *24*(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092

Koul, S., & Eydgahi, A. (2018). Utilizing technology acceptance model (TAM) for driverless car technology adoption. *Journal of Technology Management & Innovation*, *13*(4), 37–46. https://doi.org/10.4067/S0718-27242018000400037

Lee, D., Choi, Y., Youn, S., & Chun, J. U. (2017). Ethical leadership and employee moral voice: The mediating role of moral efficacy and the moderating role of leaderfollower value congruence: JBE. *Journal of Business Ethics*, *141*(1), 47-57. https://doi.org/10.1007/s10551-015-2689-y

Lee, J., Jr., Warkentin, M., Crossler, R. E., & Otondo, R. F. (2017). Implications of monitoring mechanisms on bring your own device adoption. *Journal of Computer Information Systems*, *57*(4), 309–318. https://doi.org/10.1080/08874417.2016.1184032

Lehrer, C., Wieneke, A., vom Brocke, J., Jung, R., & Seidel, S. (2018). How big data analytics enables service innovation: materiality, affordance, and the individualization of service. *Journal of Management Information Systems*, *35*(2), 424–460. https://doi.org/10.1080/07421222.2018.1451953

Lim, K. G. (2002). The IT way of loafing on the job: cyberloafing, neutralizing, and organizational justice. *Journal of Organizational Behavior 23*(5), 675–694. https://doi.org/10.1002/job.161

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, *122*, 875-888. https://doi.org/10.1016/j.jbusres.2019.10.006

Lowe, A., Norris, A. C., Farris, A. J., & Babbage, D. R. (2018). Quantifying thematic saturation in qualitative data analysis. *Field Methods*, *30*(3), 191-207. https://doi.org/10.1177/1525822X17749386

Luna-Reyes, L. F., Zhang, J., Ramon Gil-Garcia, J., & Creswell, A. M. (2005). Information systems development as emergent socio-technical change: a practice approach. *European Journal of Information Systems*, *14*(1), 93-105. https://doi.org/10.1057/palgrave.ejis.3000524

Madeley, A.-M., Williams, V., & McNiven, A. (2019). An interpretative phenomenological study of midwives supporting home birth for women with complex needs. *British Journal of Midwifery*, *27*(10), 625–632. https://doi.org/10.12968/bjom.2019.27.10.625

Malcolm, J. (2015). Criteria of meaningful stakeholder inclusion in internet governance. *Internet Policy Review. 4*(4), 1-14. https://doi.org/10.14763/2015.4.391

Marakarkandy, B., Yajnik, N., & Dasgupta, C. (2017). Enabling internet banking adoption. *Journal of Enterprise Information Management*, *30*(2), 263-294. https://doi.org/10.1108/JEIM-10-2015-0094

Maymi, F., Bixler, R., Jones, R., & Lathrop, S. (2017). Towards a definition of cyberspace tactics, techniques and procedures. *2017 IEEE International Conference on Big Data (Big Data), Big Data (Big Data), 2017 IEEE International Conference On*, 4674–4679. https://doi.org/10.1109/BigData.2017.8258514

Mercado, B. K., Giordano, C., & Dilchert, S. (2017). A meta-analytic investigation of cyberloafing. *Career Development International*, *22*(5), 546-564. https://doi.org/10.1108/CDI-08-2017-0142

Michl, S., Katsarov, J., Krug, H., Rogge, A., & Eichinger, T. (2021). Ethics in times of physical distancing: virtual training of ethical competences. *GMS Journal for Medical Education*, *38*(1), 1-6. https://doi.org/10.3205/zma001424

Microsoft. (2018). Bitlocker. *Microsoft Docs*. Retrieved from https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

Miller, W. F., & Shawver, T. J. (2018). An exploration of the state of ethics in UK accounting education. *Journal of Business Ethics*, *153*(4), 1109–1120. https://doi.org/10.1007/s10551-016-3396-z

Mohammad, J., Quoquab, F., Halimah, S., & Thurasamy, R. (2019). Workplace internet leisure and employees' productivity. *Internet Research, 29*(4), 725-748. https://doi.org/10.1108/IntR-05-2017-0191

Moon, K., Brewer, T. D., Januchowski-Hartley, S. R., Adams, V. M., & Blackman, D. A. (2016). A guideline to improve qualitative social science publishing in ecology and conservation journals. *Ecology and Society*, *21*(3). https://doi.org/10.5751/ES-08663-210317

Mubako, G., Bagchi, K., Udo, G., & Marinovic, M. (2020). Personal values and ethical behavior in accounting students. *Journal of Business Ethics,* https://doi.org/10.1007/s10551-020-04606-1

National Institutes of Health. (1979). The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research. *Bethesda, Maryland*.

Nawaz, F., Shakeel, S., Nawaz, Z., & Hamza, M. A. (2017). Acceptance of social fellow groups for learning: extension of Technology Assessment Model (TAM). *Scientific Journal of Logistics*, *13*(2), 151-157. https://doi.org/10.17270/J.LOG.2017.2.3

Nichols, L. M. (2015). The use of mind-body practices in counseling: A grounded theory study. *Journal of Mental Health Counseling, 37*, 28-46. https://doi.org/10.17744/mehc.37.1.v4324462l1272p4r

Nivedhitha K. S., & Sheik Manzoor A. K. (2020). Get employees talking through enterprise social media! Reduce cyberslacking: a moderated mediation model. *Internet Research*, *30*(4), 1167–1202. https://doi.org/10.1108/INTR-04-2019-0138

Nixon, T. S., & Barnes, J. C. (2018). Calibrating student perceptions of punishment: A specific test of general deterrence. *American Journal of Criminal Justice*, *44*(3), 430-456. https://doi.org/10.1007/s12103-018-9466-2

Olsen, D. P., Lehto, R. H., & Chan, R. R. (2016). Ethical case study of the researcher–participant relationship in end-of-life research. *Western journal of nursing research*, *38*(9), 1205-1220. https://doi.org/10.1177/0193945916639590

Oosthuizen, A., Rabie, G. H., & De Beer, L. T. (2018). Investigating cyberloafing, organizational justice, work engagement, and organizational trust of South African retail and manufacturing employees. *SA Journal of Human Resource Management*, *16*, 1-11. https://doi.org/10.4102/sajhrm.v16i0.1001

Orzechowski, P. E. (2020). U.S. Small Business Administration loans and U.S. state-level employment. *Journal of Economics and Finance*, *44*(3), 486-505. https://doi.org/10.1007/s12197-019-09495-3

Øye, C., Sørensen, N. Ø., & Glasdam, S. (2016). Qualitative research ethics on the spot: Not only on the desktop. *Nursing Ethics*, *23*(4), 455-464. https://doi.org/10.1177/0969733014567023

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2013). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health, 42*, 133-144. https://doi.org/10.1007/s10488-013-0528-y

Park, E. H., Ramesh, B., & Cao, L. (2016). Emotion in IT investment decision making with a real options perspective: The intertwining of cognition and regret. *Journal of Management Information Systems*, *33*(3), 652–683. https://doi.org/10.1080/07421222.2016.1243893

Pindek, S., Krajcevska, A., & Spector, P. E. (2018). Cyberloafing as a coping mechanism: Dealing with workplace boredom. *Computers in Human Behavior, 86*, 147–152. https://doi.org/10.1016/j.chb.2018.04.040

Plummer, A. (2001). Information systems methodology for building theory in health informatics: the argument for a structured approach to case study research. *Proceedings of the 34th Annual Hawaii International Conference on System Sciences, System Sciences, 2001. Proceedings of the 34th Annual Hawaii International Conference on System Sciences.* https://doi.org/10.1109/HICSS.2001.926577

Poole, M. S., & DeSanctis, G. (1990). Understanding the use of group decision support systems: The theory of adaptive structuration. In J. Fulk & C. Steinfeld (Eds). Organizations and Communication Technology. Newbury Park, CA: Sage.

Qosasi, A., Maulina, E., Purnomo, M., Muftiadi, A., Permana, E., & Febrian, F. (2019). The impact of information and communication technology capability on the competitive advantage of small businesses. *International Journal of Technology*, *10*(1), 167–177. https://doi.org/10.14716/ijtech.v10i1.2332

Rahayuningsih, T., & Putra, A. A. (2018). Impact of adversity intelligence and work commitment on cyberloafing behavior. *COUNS-EDU: The International Journal of Counseling and Education*, *3*(2). https://doi.org/10.23916/0020180311620

Rahman, M. S., & Muldoon, J. (2020). Dark side of technology: Investigating the role of dark personality traits and technological factors in managing cyberloafing behavior. *Journal of Strategic Innovation and Sustainability*, *15*(3), 36-54. Retrieved from https://articlegateway.com/index.php/JSIS

Raymond, C., Profetto-McGrath, J., Myrick, F., & Strean, W. B. (n.d.). Process matters: successes and challenges of recruiting and retaining participants for nursing education research. *Nurse Educator*, *43*(2), 92–95. https://doi.org/10.1097/NNE.0000000000000423

Reimers, K., Johnston, R. B., & Klein, S. (2014). An empirical evaluation of existing IS change theories for the case of IOIS evolution. *European Journal of Information Systems*, *23*(4), 373-399. https://doi.org/10.1057/ejis.2013.7

Restubog, S. L. D., Garcia, P. R. J. M., Toledano, L. S., Amarnani, R. K., Tolentino, L. R., & Tang, R. L. (2011). Yielding to (cyber)-temptation: Exploring the buffering role of self-control in the relationship between organizational justice and cyberloafing behavior in the workplace. *Journal of Research in Personality*, *45*(2), 247-251. https://doi.org/10.1016/j.jrp.2011.01.006

Rich, M. (2015). Reflection-in-addition: Using reflective logs to build research into undergraduate projects. *Electronic Journal of Business Research Methods*, *13*(2), 85–93. Retrieved from http://openaccess.city.ac.uk/id/eprint/16859/1/ejbrm-volume13-issue2-article402.pdf

Rojas-Fallas, J., & Williams, J. F. (2020). Wage differences matter: An experiment of social comparison and effort provision when wages increase or decrease. *Games*, *11*(4), 59. https://doi.org/10.3390/g11040059

Romanow, D., Rai, A., & Keil, M. (2018). CPOE-enabled coordination: Appropriation for deep structure use and impacts on patient outcomes. *MIS Quarterly*, *42*(1), 189-A11. https://doi.org/10.25300/MISQ/2018/13275

Rönnby, S., Lundberg, O., Fagher, K., Jacobsson, J., Tillander, B., Gauffin, H., Hansson, P., Dahlström, Ö., & Timpka, T. (2018). mHealth self-report monitoring in competitive middle- and long-distance runners: Qualitative study of long-term use intentions using the technology acceptance model. *JMIR mHealth and uHealth, 6*(8), e10270. https://doi.org/10.2196/10270

Salmimaa, T., Hekkala, R., & Pekkola, S. (2018). Dynamic activities for managing an is-enabled organizational change. *Business & Information Systems Engineering*, *60*(2), 133–149. https://doi.org/10.1007/s12599-018-0524-6

Sampat, B., & Basu, P. A. (2017). Cyberloafing: The di (sguised) gital way of loafing on the job. *IUP Journal of Organizational Behavior, 16*(1), 19-37. Retrieved from https://www.iupindia.in

Saygin, M., & Güvenç, K. (2019). Cyberloafing tendencies of the workers: The case of Sýlýfke organized industrial zone. *International Journal of Eurasia Social Sciences / Uluslararasi Avrasya Sosyal Bilimler Dergisi*, *10*(37), 820–832. https://doi.org/10.35826/ijoess.2597

Schmitz, K., Teng, J., & Webb, K. (2016). Capturing the complexity of malleable IT use: adaptive structuration theory for individuals. *MIS Quarterly, 40*(3), 663-686. https://doi.org/10.25300/misq/2016/40.3.07

Schwarz, B., Wienert, J., & Bethge, M. (2019). Development and implementation of work-related medical rehabilitation in cancer patients using organizational ethnography and action research methodology. *International Journal of Occupational Medicine and Environmental Health, 32*(2), 217–228. https://doi.org/10.13075/ijomeh.1896.01250

Sendall, M., McCosker, L., Brodie, A., Hill, M., & Crane, P. (2018). Participatory action research, mixed methods, and research teams: learning from philosophically juxtaposed methodologies for optimal research outcomes. *BMC Medical Research Methodology*, (1), 1-6. https://doi.org/10.1186/s12874-018-0636-1

Shah, S. I., Afsar, B., & Shahjehan, A. (2020). Unique contextual conditions affecting coworker knowledge sharing and employee innovative work behaviors. *Journal of Work and Organizational Psychology*, *36*(2), 125–134. https://doi.org/10.5093/jwop2020a12

Sharma, M. K., & Sharma, P. (2020). Small businesses survival and success: An exploration of socioeconomic motivators and restraints. *IUP Journal of Business Strategy*, *17*(4), 7–24. Retrieved from https://iupindia.in/Business_Strategy.asp

Simard, S., & Karsenti, T. (2016). A quantitative and qualitative inquiry into future teachers' use of information and communications technology to develop students' information literacy skills. *Canadian Journal of Learning and Technology*, *42*(5), 1-23. https://doi.org/10.21432/T2DW5K

Small Business Administration. (2017). Summary of sizes by industry sector. Retrieved from www.sba.gov

Soh, P. C. H., Koay, K. Y., & Chew, K. W. (2017). Conceptual view of cyberloafing and nonwork domain. *SHS Web of Conferences*, *33*(00029), 1-6. https://doi.org/10.1051/shsconf/20173300029

Soh, P. C. H., Koay, K. Y., & Lim, V. K. G. (2018). Understanding cyberloafing by students through the lens of an extended theory of planned behavior. *First Monday*, *23*(6). https://doi.org/10.5210/fm.v23i6.7837

Spence, L. (2002). 'Like building a new motorway': Establishing the rules for ethical e-mail use at a UK higher education institution. *Business Ethics: A European Review*, *11*(1), 0-51. https://doi.org/10.1111/1467-8608.00257

Stake, R. (1995). *The art of case study research*. Thousand Oaks, CA: Sage.

Stavros, C., & Westberg, K. (2009). Using triangulation and multiple case studies to advance relationship marketing theory. *Qualitative Market Research: An International Journal*, *12*(3), 307–320. https://doi.org/10.1108/13522750910963827

Stoffers, J. M. M., & Van der Heijden, B. I. J. M. (2018). An innovative work behaviour-enhancing employability model moderated by age. *European Journal of Training and Development*, *42*(1), 143–163. https://doi.org/10.1108/EJTD-10-2016-0074

Stoffregen, J., & Pawlowski, J. M. (2018). Theorizing about barriers to open e-learning systems in public administrations. *Technological Forecasting and Social Change*, *132*, 81-91. https://doi.org/10.1016/j.techfore.2018.01.010

Sun, Y., Guo, Y., & Zhao, Y. (2020). Understanding the determinants of learner engagement in MOOCs: An adaptive structuration perspective. *Computers & Education*, *157*, 103693. https://doi.org/10.1016/j.compedu.2020.103963

Teater, B., Roy, J., Carpenter, J., Forrester, D., Devaney, J., & Scourfield, J. (2017). Making social work count: A curriculum innovation to teach quantitative research methods and statistical analysis to undergraduate social work students in the United Kingdom. *Journal of Teaching in Social Work*, *37*(5), 422–437. https://doi.org/.1080/08841233.2017.1381216

Teo, T. H., & Lim, V. G. (2000). Gender differences in Internet usage and task preferences. *Behaviour & Information Technology*, *19*(4), 283-295. https://doi.org/10.1080/01449290050086390

Thaker, M. A. M. T., Thaker, H. M. T., & Pitchay, A. A. (2018). Modeling crowdfunders' behavioral intention to adopt the crowdfunding-waqf model (CWM) in Malaysia: The theory of the technology acceptance model. *International Journal of Islamic and Middle Eastern Finance and Management, 11*(2), 231-249. https://doi.org/10.1108/IMEFM-06-2017-0157

Theurer, C. P., Tumasjan, A., & Welpe, I. M. (2018). Contextual work design and employee innovative work behavior: When does autonomy matter? *PLoS One*, *13*(10), e0204089. https://doi.org/10.1371/journal.pone.0204089

Tincani, M., & Travers, J. (2018). Publishing single-case research design studies that do not demonstrate experimental control. *Remedial and Special Education*, *39*(2), 118-128. https://doi.org/10.1177/0741932517697447

Toker, T., & Baturay, M. H. (2021). Factors affecting cyberloafing in computer laboratory teaching settings: Revista de Universidad y Sociedad del Conocimiento. *International Journal of Educational Technology in Higher Education*, *18*(1), 1-24. https://doi.org/10.1186/s41239-021-00250-5

Tominc, P., Krajnc, M., Vivod, K., Lynn, M. L., & Frešer, B. (2018). Students' behavioral intentions regarding the future use of quantitative research methods. *Our Economy (Nase Gospodarstvo)*, *64*(2), 25–33. https://doi.org/10.2478/ngoe-2018-0009

Tosuntaş, Ş. B. (2020). Diffusion of responsibility in group work: Social loafing. *Journal of Pedagogical Research*, *4*(3), 344-358. https://doi.org/10.33902/JPR.2020465073

Travers, J., Cook, B., & Cook, L. (2017). Null hypothesis significance testing and p values. *Learning Disabilities Research & Practice (Wiley-Blackwell)*, *32*(4), 208–215. https://doi.org//10.1111/ldrp.12147

Turner, J. R., Morris, M., Atamenwan, I., Baker, R., Yoon, H. J., & Kwon, K. (2019). A theoretical literature review on adaptive structuration theory as its relevance to human resource development. *Advances in Developing Human Resources*, *21*(3), 289–302. https://doi.org/10.1177/1523422319851275

Turner, S., & Endres, A. (2017). Strategies for enhancing small business owners' success rates. *International Journal of Applied Management and Technology*, *16*(1), 34-49. https://doi.org/10.5590/IJAMT.2017.16.1.03

Ugrin, J. C., Pearson, J. M., & Nickle, S. M. (2018). An examination of the relationship between culture and cyberloafing using the Hofstede Model. *Journal of Internet Commerce*, *17*(1), 46–63. https://doi.org/10.1080/15332861.2018.1424395

Unkovic, C., Sen, M., & Quinn, K. M. (2016). Does encouragement matter in improving gender imbalances in technical fields? Evidence from a randomized controlled trial. PLoS One, 11(4), 55-86. https://doi.org/10.1371/journal.pone.0151714

Urbaczewski, A., & Jessup, L. M. (2002, January 1). Does electronic monitoring of employee internet usage work? Using a controlled setting to study the effects of monitoring. *Communications of the ACM*, *45*(1), 80-83. https://doi.org/10.1145/502269.502303 Usman, M., Javed, U., Shoukat, A., & Bashir, N. A. (2021). Does meaningful work reduce cyberloafing? Important roles of affective commitment and leader-member exchange. *Behaviour & Information Technology*, *40*(2), 206–220. https://doi.org/10.1080/0144929X.2019.1683607

van Rijnsoever, F. J. (2017). (I can't get no) saturation: A simulation and guidelines for sample sizes in qualitative research. *PLOS ONE*, *12*(7), 1-17. https://doi.org/10.1371/journal.pone.0181689

Varghese, L., & Barber, L. K. (2017). A preliminary study exploring moderating effects of role stressors on the relationship between Big Five personality traits and workplace cyberloafing. *Cyberpsychology*, *11*(4), 1–15. https://doi.org/10.5817/CP2017-4-4

Varol, F., & Yildirim, E. (2018). An examination of cyberloafing behaviors in classrooms from students' perspectives. *Turkish Online Journal of Qualitative Inquiry*, 26–46. https://doi.org/10.17569/tojqi.349800

Venkatraman, S., Cheung, C., Lee, Z. W. Y., Davis, F. D., & Venkatesh, V. (2018). The "Darth" side of technology use: An inductively derived typology of cyberdeviance. *Journal of Management Information Systems*, *35*(4), 1060–1091. https://doi.org/10.1080/07421222.2018.1523531

Veridiana, R. P., Antonio Cesar, A. M., & Diógenes de, S. B. (2019). Resistance to change in BPM implementation. *Business Process Management Journal*, *25*(7), 1564-1586. https://doi.org/10.1108/BPMJ-07-2018-0184

Vijayakumar, K., & Arun, C. (2017). Analysis and selection of risk assessment frameworks for cloud-based enterprise applications. *Biomedical Research, Special Issue*, 129-136. Retrieved from www.biomedres.info

Virkkala, P., Saarela, M., Hanninen, K., Kujala, J., & Simunaniemi, A.-M. (2020). Business maturity models for small and medium-sized enterprises: A systematic literature review. *Management (18544223)*, *15*(2), 137–155. https://doi.org/10.26493/1854-4231.15.137-155

Wall, S. (2015). Focused ethnography: A methodological adaptation for social research in emerging contexts. Forum: Qualitative Social Research, 16(1), 44-66. Retrieved from http://www.qualitative-research.net/

Whitaker, J., & New, J. R. (2016). MOOCs and the online delivery of business education: What's new? What's not? What now? *Academy of Management Learning & Education 15*(2), 345-365. https://doi:10.5465/amle.2013.0021

Woods, S. A., Mustafa, M. J., Anderson, N., & Sayer, B. (2018). Innovative work behavior and personality traits: Examining the moderating effects of organizational tenure. *Journal of Managerial Psychology*, *33*(1), 29–42. https://doi.org/10.1108/JMP-01-2017-0016

Wu, J., Mei, W., & Ugrin, J. C. (2018). Student cyberloafing in and out of the classroom in China and the relationship with student performance. *Cyberpsychology, Behavior, and Social Networking*, *21*(3), 199–204. https://doi.org/10.1089/cyber.2017.0397

Xia, B. S. (2017). An in-depth analysis of learning goals in higher education: Evidence from the programming education. *Journal of Learning Design*, *10*(2), 25-34. https://doi.org/10.5204/jld.v10i2.287

Yang, S. O., Hsu, C., Sarker, S., & Lee, A. S. (2017). Enabling effective operational risk management in a financial institution: an action research study. *Journal of Management Information Systems*, *34*(3), 727-753. https://doi.org/10.1080/07421222.2017.1373006

Yang, T. H., Ku, C. Y., & Liu, M. N. (2016). An integrated system for information security management with the unified framework. *Journal of Risk Research*, *19*(1), 21-41. https://doi.org/10.1080/13669877.2014.940593

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. *Radiologic Technology*, *88*(2), 225-231. Retrieved from http://www.radiologictechnology.org/content/88/2/225.extract

Yılmaz, R., & Yurdugül, H. (2018). Cyberloafing in IT classrooms: Exploring the role of the psycho-social environment in the classroom, attitude to computers and computing courses, motivation and learning strategies. *Journal of Computing in Higher Education*, *30*(3), 530–552. https://doi.org/10.1007/s12528-018-9184-2

Yin, R. K. (1981). The case study as a serious research strategy. *Knowledge*, 3(1), 97-114. https://doi.org/10.1177/107554708100300106

Yin, R. K. (2016). *Qualitative research from start to finish* (2nd ed.). New York, NY: Guilford Press.

Zha, X., Cao, F., Yan, Y., Guo, J., & Wang, J. (2019). Exploring innovative information seeking: The perspectives of cognitive switching and affinity with digital libraries. *Journal of Academic Librarianship*, *45*(5), 1-9. https://doi.org/10.1016/j.acalib.2019.102045

Zhang, J., Akhtar, M. N., Zhang, Y., & Sun, S. (2020). Are overqualified employees bad apples? A dual-pathway model of cyberloafing. *Internet Research*, *30*(1), 289–313. https://doi.org/10.1108/INTR-10-2018-0469

Zoghbi-Manrique-de-Lara, P., & Viera-Armas, M. (2017). Corporate culture as a mediator in the relationship between ethical leadership and personal Internet use. *Journal of Leadership & Organizational Studies*, *24*(3), 357-371. https://doi.org/10.1177/1548051817696877

Appendix A: Organizational Permission

[redacted]

January 13, 2020

Dear Veronica Dooly,

Based on my review of your research proposal, I give permission for you to conduct the study entitled **Strategies to Monitor and Deter Cyberloafing in Small Businesses: A Case Study** within the [redacted]. As part of this study, I authorize you to invite participants via email, interview participants, review the transcription of interviews with the participants, and document results in the doctoral study. Individuals' participation will be voluntary and at their own discretion.

We understand that our organization's responsibilities include forwarding the invitation letter to potential participants and access to space to conduct interviews. We reserve the right to withdraw from the study at any time if our circumstances change.

I understand that the student will not be naming our organization in the doctoral project report that is published in Proquest.

I confirm that I am authorized to approve research in this setting and that this plan complies with the organization's policies.

I understand that the data collected will remain entirely confidential and may not be provided to anyone outside of the student's supervising faculty/staff without permission from the Walden University IRB.

Sincerely,

Authorization Official
Contact Information

Appendix B: Interview Questions

1. How have you observed users using the Internet or other resources for personal use?
2. What policies do you have that address the restriction of computer usage, particularly the Internet and email, to only business purposes?
3. How do you update policies if you discover a violation or deviation by the users?
4. What monitoring software do you use to observe user interaction with the computers?
5. How do you monitor computer usage in addition to monitoring software?
6. What deterrence mechanisms do you have in place to prohibit personal usage of computer resources and the Internet?
7. What happens if an employee misuses computer resources or the Internet?
8. What happens if the misuse is repeated?
9. How successful are your mechanisms to deter cyberloafing?
10. What, if anything, would you have done differently when implementing your cyberloafing monitoring and deterrence program?
11. Is there any other information you can share that would be useful in understanding cyberloafing in your organization?