


2017

Role of Middle Managers in Mitigating Employee Cyberloafing in the Workplace

Anizizo Aku
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>

 Part of the [Business Administration, Management, and Operations Commons](#), and the [Management Sciences and Quantitative Methods Commons](#)

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Anizizo Aku

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. Patricia Fusch, Committee Chairperson, Management Faculty

Dr. David Banner, Committee Member, Management Faculty

Dr. David Cavazos, University Reviewer, Management Faculty

Chief Academic Officer

Eric Riedel, Ph.D.

Walden University

2017

Abstract

Role of Middle Managers in Mitigating Employee Cyberloafing in the Workplace

by

Anizizo Aku

MSLS, Kaplan University, 2012

MBA, University of Phoenix, 2010

BEng, Nigerian Defence Academy, 1994

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

August 2017

Abstract

Companies in the United States are concerned about the indeterminate effectiveness of corporate cyberloafing mitigation efforts leading to the persistence of employee cyberloafing behavior. Although middle managers are the driving force behind the transformational influences that guide employee productivity and could proffer practical solutions, a lack of clarity surrounds the middle manager's role in the overall cyberloafing mitigation efforts within organizations. The central research question for this transcendental phenomenological research study explored the lived experiences of middle managers regarding their roles in mitigating employee cyberloafing at higher education institutions in Florida. This study used a social constructivist-interpretive framework that draws from the multiple realities constructed through social interactions and lived experiences. Participants included 7 middle managers with experience mitigating cyberloafing at higher education institutions in Florida. Four major themes emerged from an inductive analysis of the data, including managing employee performance, proximity matters, cyberloafing interventions, and understanding employee online technology use. The results and recommendations of this study provide implications for social change. Business organizations may modify cyberloafing mitigation strategies and policies from a better understanding of manager/employee interactions, transformational managerial influences used to mitigate employee cyberloafing, and managerial knowledge of employee appropriation of online technology.

Role of Middle Managers in Mitigating Employee Cyberloafing in the Workplace
by

Anizizo Aku

MSLS, Kaplan University, 2012

MBA, University of Phoenix, 2010

BEng, Nigerian Defence Academy, 1994

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

August 2017

Dedication

I dedicate this dissertation to my family, to my wife Kamella, I appreciate your love, support, understanding, endurance, and sharing in my anxieties and celebrating my milestones on this doctoral journey. To my parents, Professor Shekarau Aku and Professor (Mrs.) Patricia Aku, from whom I drew the inspiration and motivation for this project. Thank you for motivating me through all my years of school and helping me with homework or projects I procrastinated on. You taught me that education is the key to success and to get where you want to in life, you need to work hard, and you need to keep your eyes on the prize. To my older brother, Yakubu, thank you for being another huge part of my foundation. To my younger sisters, Tintin and Lami, thank you for being a part of my life and for all your support.

Acknowledgments

I give thanks to the Almighty God for His grace for the successful completion of this project. I owe a depth of gratitude to Dr. Patricia Fusch, my dissertation chair, for not only championing my cause as a doctoral candidate but also driving and encouraging me throughout this long journey. I admire you for your humility, your diligence, and your unwavering purpose. You have shown me how to be a more effective human being, and for that, I cannot thank you enough. I am profoundly grateful to my dissertation committee member, Dr. David Banner, who agreed to join my committee halfway into my project and provided invaluable support all the way. Finally, I would like to appreciate the University Research Reviewer, Dr. David Cavazos, for his valuable contributions that helped me achieve success.

Table of Contents

List of Tables	vi
List of Figures	vii
Chapter 1: Introduction to the Study.....	1
Background of the Study	1
Problem Statement.....	7
Purpose of the Study.....	7
Central Research Question.....	8
Conceptual Framework.....	8
Nature of the Study.....	11
Definitions.....	14
Assumptions.....	15
Scope and Delimitations	16
Limitations	17
Significance of the Study	18
Significance to Practice.....	19
Significance to Theory.....	20
Significance to Social Change	20
Summary and Transition.....	21
Chapter 2: Literature Review	23
Literature Search Strategy.....	24
Conceptual Framework.....	24

Symbolic Interaction Theory	27
Adaptive Structuration Theory	29
What Is Employee Cyberloafing?.....	31
Meaning Ascribed to the Employee Cyberloafing Phenomenon.....	33
The Digital Workplace.....	37
Antecedents of Cyberloafing	39
Typologies of Cyberloafing	41
Nomadic Computing and Cyberloafing.....	42
Online Social Networking Sites and Cyberloafing.....	45
The Cost of Cyberloafing.....	49
Management of Employee Cyberloafing	51
Technical Deterrence Mechanisms.....	57
Non-technical Deterrence Mechanisms	61
Middle Managers and the Management of Employee Cyberloafing	69
Summary and Conclusions	71
Chapter 3: Research Method.....	73
Research Design and Rationale	74
Qualitative Approach	75
Phenomenological Method	76
Role of the Researcher	78
Methodology	80
Participant Selection Logic.....	80

Instrumentation	80
Procedures for Recruitment, Participation, and Data Collection	83
Data Analysis Plan	85
Issues of Trustworthiness.....	86
Credibility	86
Transferability.....	87
Dependability	88
Confirmability.....	89
Ethical Procedures	90
Agreements to Gain Access to Participants	90
Treatment of Participants	91
Treatment of Data	92
Summary	92
Chapter 4: Results	94
Research Setting.....	94
Participant Demographics.....	95
Participant Recruitment	97
Data Collection	99
Data Organization and Management	101
Data Analysis	101
Hand Coding	102
Coding Using NVivo 11 Pro.....	103

Evidence of Trustworthiness.....	107
Credibility	109
Transferability.....	111
Dependability.....	111
Confirmability.....	112
Results: Emergent Themes	112
Emergent Theme 1: Managing Employee Performance.....	115
Emergent Theme 2: Proximity Matters.....	122
Emergent Theme 3: Cyberloafing Interventions.....	126
Emergent Theme 4: Understanding Employee Online Technology Usage	132
Emergent Subtheme 1: Mitigation Barriers	136
Emergent Subtheme 2: Observing and Persuading.....	139
Emergent Subtheme 3: Setting Clear Expectations	142
Emergent Subtheme 4: Understanding Duties and Obligations	145
Emergent Subtheme 5: Using Managerial Discretion	148
Emergent Subtheme 6: Working with Unclear Mitigation Policies	151
Emergent Subtheme 7: Staying Current With Technology Advancements.....	153
Discrepant Cases.....	155
The Essence of Participants Experience	156
Summary.....	159
Chapter 5: Discussion, Conclusions, and Recommendations.....	160
Overview.....	160

Interpretation of the Findings.....	161
Limitations of the Study.....	169
Recommendations for Further Research.....	170
Implications.....	173
Significance to Practice.....	173
Significance to Theory.....	173
Significance to Social Change.....	174
Conclusion.....	175
References.....	180
Appendix A: Participant Invite to Participate in Research Study.....	214
Appendix B: Follow Up Participant Invite to Participate in Research Study.....	215
Appendix C: Response Email to Prospective Participants With Eligibility	
Questions.....	216
Appendix D: Interview Questions.....	217

List of Tables

Table 1. Participant Demographics.....	96
Table 2. Emergent Themes, Nodes, Sources, and References.....	113

List of Figures

Figure 1. Initial word frequency query for participant interview transcripts.....	104
Figure 2. Mitigation text search query results.	105

Chapter 1: Introduction to the Study

The launch of the Internet in the early 1980s and the more recent advent of nomadic computing continue to change information sharing capabilities globally (Ciolfi & De Carvalho, 2014). Rapid advancements in online technologies have enabled easier access to the Internet by employees creating a significant concern for organizations and their managers. Approximately 64% of employees in the United States currently use work computers to conduct personal business during work hours, leading to approximately a 30% - 40% drop in organizational productivity (Jandaghi, Alvani, Matin, & Kozekanan, 2015; Nazareth, & Choi, 2014). Many business organizations have employed software programs designed to monitor, track, and block the inappropriate use of the Internet by their employees (Nicholas, 2014).

In this study, I promote positive social change by highlighting the important role that middle managers play in combating employee cyberloafing at work. In Chapter 1, I outline the background of the study, provide a summary of the pertinent literature, and present a problem and purpose statement. I also include the research question, a conceptual framework for the study, the nature of the study, and details of possible contributions of the study to positive social change. I conclude Chapter 1 with a summary and transition into the next chapter.

Background of the Study

The term *cyberloafing*, first coined by Kamins in 1995, gained prominence in 2002 at a presentation at the National University of Singapore (Jandaghi et al., 2015).

One of the first definitions of *cyberloafing* described the activity as the voluntary employee use of organization provided Internet access for *non-work-related* activity during work hours constituting unproductive work time and detracting the employee from work tasks (Lim, 2002). Today, the rapid expansion of Internet access using smart mobile technologies continues to evolve requiring expanded organizational strategies designed to mitigate the adverse effect on employee performance. Smith (2015) assessed ownership of smartphones among adults in the United States and found the percentage of adults with a smartphone rose from 35% in 2011 to 64%.

With ever-expanding Internet connectivity, available to employees outside organization resources, the definition of cyberloafing in contemporary research changed to reflect the current state of employee deviance. The broadened definition describes *cyberloafing* as an activity involving the use of computers and smart mobile devices at work for non-work-related activity by employees not working remotely (Jamaluddin, Ahmad, Alias, & Simun, 2015; Jandaghi et al., 2015). As the Internet continues undoubtedly to transform the workplace with troubling potential in areas such as deviant and addictive employee behavior, finding effective strategies for mitigating adverse consequences remains a significant concern for organizations (Anandarajan, Teo, & Simmers, 2014). The prevalence of employee cyberloafing within organizations has contributed to some of the losses in productivity recorded by organizations struggling in today's highly competitive marketplace.

Some studies have suggested that most business organizations share the common belief that non-work-related Internet use by employees is unproductive making the adoption of countermeasures an imperative (Coker, 2013; Francois, Hebbani, & Rintel, 2013). A widely-held perception among employers is that the implementation and enforcement of cyberloafing mitigation by information technology and human resources departments combined with technical deterrence methods are collectively the most efficient way to mitigate employee cyberloafing (Patrick, 2008; Sheriff, 2012). The organizational role of the middle manager in mitigation efforts aimed at curbing employee cyberloafing activity has not been elucidated. Approximately 64% of workers currently use work computers to conduct personal business during work hours with some adverse consequences on the security of online technology platforms (Nazareth & Choi, 2014).

In some cases, employees using an organization's Internet resources for personal use have created vulnerabilities for the security of organizational online technology platforms, necessitating the deployment of additional resources to prevent cyber-attacks, reduce vulnerability, and establish threat deterrence (Nazareth, & Choi, 2014). For instance, research indicates that employee cyberloafing could cost organizations about \$183 billion in productivity losses, issues relating to broadband, legal problems, and other associated costs (Jandaghi et al., 2015). Also, Grover (2014) noted that the misuse of computer networks by employees creates vulnerabilities and security threats costing tens of millions of dollars for each occurrence.

Most organizations use cyberloafing mitigation policies to regulate employee use of electronic communication and deployed technical mechanisms to monitor and control employee use of information and communication technologies (Glassman, Prosch, & Shao, 2015). Despite the adoption and deployment of the policies and techniques, employee cyberloafing continues to persist (Glassman et al., 2015). The adoption of cyberloafing mitigation policies within organizations aims at managing the risks associated with employee use of online technology (Ruhnka & Loopesko, 2013). Regulatory constraints make having a one-size-fits-all policy across various domains demanding to require organizations to develop individual plans that draw from the laws governing corporate liability for employee electronic communications.

Leftheriotis and Giannakos (2014) investigated employee motivations for using social media and found a positive relationship between social media use and performance because of the collaborative and information sharing opportunities. Leftheriotis and Giannakos offered alternative viewpoints on the management of cyberloafing advocating for non-technical mitigation strategies for potential misuse rather than monitoring or blocking access to social media sites. With the record sales growth within the software filtering market, the role of balancing information integrity, employee turnover, performance, and liability with employee Internet usage needs has become increasingly important. Jandaghi et al. (2015) pointed to the implausibility of eliminating employee cyberloafing activities. The contention is that cyberloafing mitigation policies need to be more explicit with a proactive rather than reactive structure.

Jandaghi et al. (2015) suggested that cyberloafing management requires sensitivity to issues regarding job design and work volume as ways of minimizing individual cyberloafing behavior. These are areas where managerial supervision could lend a hand in moderating some of the moderating factors that contribute to cyberloafing behavior. Rana and Punia (2014) discussed managerial strategies in place to mitigate the deviant environmentally related workplace practices with some potential for organizations seeking managerial nontechnical approaches. As cyberloafing studies continue to remain a major area of interest within contemporary organization research, appearing mainly in academic and scholarly journals, the focus has centered mostly on causation, typology, countermeasures, and supervision (Piotrowski, 2013; Piotrowski, 2012).

Many organizations rely on deterrence mechanisms without cognizing the importance of middle manager's physical proximity to employees and role in the mitigation process (Wang, Tian, & Shen, 2013). Studies on the management of cyberloafing have focused mainly on the use of technical solutions, the role of human resources managers, online technology managers, and the effectiveness of cyberloafing mitigation policies within organizations (Al-Shuaibi et al., 2014; Glassman et al., 2015; Gunia, Corgnet, & Hernan-Gonzalez, 2014; Shepherd, Mejias, & Klein, 2014). Middle managers are the driving force behind the transformational influences that guide employee performance (Parera, & Fernández-Vallejo, 2013). What is missing in

contemporary research on cyberloafing is an examination of the non-technical strategies used by middle managers to mitigate employee cyberloafing.

There is great concern that the indeterminate effectiveness of corporate cyberloafing mitigation efforts has contributed to the persistence of cyberloafing behavior among employees with the unplanned implication of reducing performance (Ugrin & Pearson, 2013). With the current challenges within the global economic challenges facing most organizations, organizations are transferring human resource management responsibilities from human resource personnel to middle managers (Cascón-Pereira & Valverde, 2014; Parera, & Fernández-Vallejo, 2013). Middle managers are the first-line supervisors of most organizations that regularly interact with lower level employees and are responsible for revealing management priorities and driving performance (Bhattacharya & Tang, 2013).

Parera and Fernández-Vallejo (2013) have maintained that middle managers are bridging the gaps between upper and lower level organization players creating opportunities to help drive organizational change. The role of middle managers in the implementation of organizational strategies designed to manage employee cyberloafing within the digital workplace is a new frontier that needs further exploration on the management of employee cyberloafing. This study is specifically designed to investigate the organizational role of middle managers in the mitigation of employee cyberloafing and implementing cyberloafing mitigation policies.

With the persistence of cyberloafing activities among employees at the workplace despite electronic monitoring and technical deterrence systems in place within organizations, there is a need to understand better middle manager roles in the overall organizational efforts aimed at combating employee cyberloafing.

Problem Statement

There is great perturbation from businesses about their inability to find ways to mitigate employee cyberloafing despite the adoption of technical deterrence mechanisms (Saraç & Çiftçioğlu, 2014). Between 60% and 80% of employees engage in cyberloafing activity during work hours resulting in losses in productivity (Nazareth & Choi, 2014). With the pervasiveness of employee cyberloafing, understanding the role middle managers play in the overall organizational mitigation efforts fills a gap in contemporary research on cyberloafing mitigation. The general business problem was the overreliance on technical deterrence without cognizing the role of middle managers as actors and agents in cyberloafing mitigation efforts. The specific business problem was the lack of information on the lived experiences of middle managers about their role in the mitigation of employee cyberloafing at work.

Purpose of the Study

The purpose of this phenomenological study was to explore the lived experiences of middle managers about their role in the mitigation of employee cyberloafing at higher education institutions in Florida. With the persistence of cyberloafing activities among employees at the workplace despite electronic monitoring and technical deterrence

systems in place within organizations, a need exists for a better understanding of how middle manager perceive their role in cyberloafing mitigation within their organization.

The study focused on the digital workplace where employees use only computer hardware, software, interfaces, and connectivity solutions to perform work tasks, collaborate, and provide services to clients. For this reason, I purposefully selected about 7 participants with experience managing employee cyberloafing from higher education institutions in Florida for interviews using a semistructured format.

Central Research Question

The objective of this study was to uncover the perspectives of middle managers on their role in mitigating employee cyberloafing in a digital workplace. I presented several questions aimed at capturing the perspectives, experiences, and knowledge of participants involved with the study on the scope of the issue. Nevertheless, the central research question for this phenomenological research study was: What are the lived experiences of middle managers about their role in the mitigation of employee cyberloafing at higher education institutions in Florida?

Conceptual Framework

Symbolic interaction and adaptive structuration theories formed the bedrock of this study. For businesses to drive employee performance, middle managers need to contain subordinate employee behavior through direct control and manipulation (Harding, Lee, & Ford, 2014). The management of employee cyberloafing within organizations has focused mainly on the technical deterrence mechanisms with limited

attention concentrated on the effectiveness of managerial control of cyberloafing behavior among employees. The conceptual framework guided and informed this study on the managerial perspectives on social premises surrounding employee technology use and the interactive relationships governing the control of cyberloafing behavior. In chapter 2, I will explain further how the explored theories in this section upheld the philosophies supporting the managerial controls used in employee cyberloafing mitigation.

Symbolic interaction theory as a conceptual framework is a well-established approach in qualitative research and compatible with interpretive description and workplace related studies (Michalski, 2013; Teague, Green, & Leith, 2013). Symbolic interaction theory offered an explanation why humans act based on the meaning developed from individual analysis and interpretation of social behavior and interactions within society (Blumer, 1969; Mead, 1934). The primacy of symbolic interaction theory assumes that subjective human interpretations of social interaction mainly shape human behavior rather than what is true and objective (Hallberg, 2006; Mead, 1934; Sedo, 2005). Social interactions at the workplace between employee and supervisor allow supervisors to develop situational awareness of what individual employees are doing, not doing, and can do (Bhattacharya & Tang, 2013).

For this study, the issue explored centered on the prevalence of cyberloafing mitigation policies and adoption of electronic deterrence systems within organizations and the persistence of employee cyberloafing activity despite the mitigation efforts

(Polzer-Debruyne et al., 2014). Symbolic interaction theory affords a means for developing a rich perspective that considers the dynamics of changing situations and circumstances extending from the thought processes of participants to their interactions within an organization. Also, using a symbolic interactionist lens unraveled the transformational influences middle managers used to elicit acceptable employee use of information and communication technologies.

Gallant (2014) used symbolic interactionism as the interpretive lens to examine the inadequacy of women representation in senior leadership positions within the higher education industry. Gallant noted that symbolic interactionism enhanced the uncovering of the subjective meaning ascribed to the lived experiences and behaviors of individuals. Coleman-Fountain and McLaughlin (2013) supported this view in his examination of the interrelationships between human physical impairments and the interconnecting social experience of having a disability.

Adaptive structuration theory focuses on information and communication technologies implementation and uses within groups and organizations (DeSanctis & Poole, 1994; Poole, 2013). DeSanctis and Poole (1994) claimed that the duality of human action and social structure perspectives enable a better understanding of the social aspects of technology use. Employee adaptations to the advancements in mobile phone technology that allow the use of devices for non-work-related activities are an area of concern for organizations (Jamaluddin et al., 2015). As an example, McBride, LeVasseur, and Li (2015) in an investigation of personal and frequent mobile device usage among

registered nurses working at a hospital, the researchers found the exchange of emails and text messages with friends and family as the most occurring cyber activity.

A broader perspective was adopted in support of using adaptive structuration theory to explicate technology appropriation from a socio-cultural dimension (Bar, Weber & Pisani, 2016). Bar et al. (2016) found interconnections between individual use and integration during appropriation of devices or applications developing unique and creative social practices. Adaptive structuration theory facilitated the exploration of the social premises surrounding the development and use of managerial control mechanisms for controlling employee abuse of information and communication technologies within organizations (Simons, 2013). The central research question for this study aimed to capture experiences of employee cyberloafing mitigation efforts of middle managers and their interpretations of those experiences.

Considering middle manager control of cyberloafing through an adaptive structuration worldview facilitated an understanding of the influences, choices, and identities related to control techniques for online technology usage. Also, the researcher gained a clearer perspective of the evolutionary character of the manager as an individual and employees as a group within an organization with the possibility of uncovering how managers exercise more influence than they realize (DeSanctis & Poole, 1994).

Nature of the Study

I used a qualitative research approach to gain a deep understanding of the middle manager's role in curbing employee cyberloafing through the implementation of

cyberloafing mitigation policies. Qualitative research methods provide researchers with a holistic framework that allow for a broad exploration of complex issues related to human behavior, human perception, and lived experience (Khan, 2014). Husserl's transcendental phenomenology represents an original form of phenomenology bound by intentionality and seeking to uncover knowledge of human experience in its absolute sense (Moustakas, 1994). Transcendental phenomenology, because of its self-given and interpretive form, was the best-suited approach for this study. In this study, I unraveled the real meaning ascribed to human experience from the lived experiences of participants.

The study relied on the modified Moustakas model of transcendental phenomenology that requires core processes aimed at facilitating the unraveling of knowledge. The four core processes included epoché, transcendental phenomenological reduction, imaginative variation, and synthesis (Moustakas, 1994). The core processes collectively involved steps taken to suspend judgments about the world around us, efficiently collate true essences about the phenomenon based on participant descriptions, and different thematic variations about the phenomenon. Through a qualitative phenomenological approach, middle managers working in digital work environments provided real and individual essences ascribed to the mitigation processes.

More specifically, I adopted the transcendental phenomenological model to unravel the true meaning attributed to participants' human experiences (Moustakas, 1994). The model represents the originally developed form of phenomenology that seeks to discover only the described lived experiences of the participant. For the study, I

conducted interviews to understand better the essences ascribed to the issue by middle managers at their organization. I used face-to-face interviews, one telephone interview, a semistructured interview format with open-ended questions, and a digital audio recording device.

Face-to-face interviewing served to capture the voices of participants about the phenomenon in person together with any elements nonverbal communication. I used telephone interviews as an alternative option to cater to participant's unable to meet in person. The data analysis for the planned study followed the modified Van Kaam method outlined in Moustakas (1994). For the data analysis process, I combined both hand-coding and coding using the NVivo 11 Pro software program for data analysis and data management and storage. Like Maxwell (2013) noted, reading, and understanding the raw data before analysis are an essential element of the qualitative data analysis process.

The first phase of the data analysis strategy involved deconstruction of the data using a manual hand-coding process and the NVivo 11 Pro software program to break down the transcribed interview responses into different codes or categories. A deconstruction process was a next step in the analysis process involving a sense-making technique aimed at identifying similarities or relationships, extracting themes, highlighting differences, and creating generalizations. The last phase included a reconstruction of related codes and themes identified during interpretation while considering the conceptual framework and existing knowledge on the issue.

Definitions

Cyberloafing: *Cyberloafing* is a generic term used interchangeably to mean cyberslacking or cyber deviance and involves the use of computers and smart mobile devices at work for non-work-related activity by employees not working remotely.

Cyberloafing mitigation policies: Organizational policies governing employee use of information and communication technologies and electronic communication within an organization that includes acceptable Internet use and information security policies.

Digital immigrants: *Digital immigrants* refers to adults born before the inception of the digital age that readily embraced information and communication technologies and considered average users (Prensky, 2001).

Digital natives: *Digital natives* refers to younger adults born during or after the inception of the digital age, accustomed to the fast pace of Web-based information sharing with a strong preference for parallel processing and multitasking (Prensky, 2001).

Digital workplace: The digital workplace includes all work environments where employees use mainly computer hardware, software, interfaces, and connectivity solutions to perform work tasks, collaborate, and provide services to clients (Deloitte, 2014).

Middle manager: Employees occupying central positions within an organization's hierarchy responsible for the establishment of productive work environments and ensuring compliance with organizational requirements, strategies, and policies.

Non-technical cyberloafing strategies: Non-technical strategies other than technical procedures used to monitor and control employee use of electronic devices for personal use that includes employee training, education, and use of sanctions or rewards.

Online technology: *Online technology* refers to computer communications (including emails, data and text communication, and online information exchanges), communication devices or applications including smartphones, tablets, computer networks, and computer hardware and software.

Technical cyberloafing strategies: *Technical cyberloafing strategies* refer to an organization's use of electronic monitoring and blocking software programs used to tackle employee cyberloafing behavior during work hours.

Assumptions

The objective of the study was to explore the lived experience of middle managers about their role in the mitigation of employee cyberloafing at higher education institutions in Florida. The initial assumption for the study related to the participants and held that a middle manager who embraces the expanding use of electronic communication by employees at the workplace was more efficient at using nontechnical strategies for combating misuse. In situations involving managerial unfavorable disposition to the expanding use of online technology by subordinate employees, managerial mitigation efforts rely more on technical mechanisms and would be less efficient at using non-technical strategies.

The second assumption related to the work environment of the participants and held that middle manager participant engaged in the study, work at organizations with existing cyberloafing mitigation policies. The third assumption related to the inherent and unidentifiable biases of participants during the research process. Finally, the fourth assumption was that the conduct of investigation within an organization with a digital work environment could adversely affect the potential for replication.

Scope and Delimitations

Simon and Goes (2013) noted that delimitations emerge from scope limitations and choices made during research design. This study did not intend to examine the management of employee cyberloafing from a non-technical strategy perspective. Rather, the aim of the study was to explore the experiences of middle managers on their organizational role mitigating employee cyberloafing.

The first step in the delimitation process involved the identification of a specific problem despite the host of challenges associated with the management of employee cyberloafing. During the research design phase, the deliberate restriction of the population of the study allows the researcher to enhance transferability (Rudestam & Newton, 2014). For this study, the research centered on middle managers working in organizations associated with digital work environments. Ultimately, the interest in exploring middle managers emanated from their responsibility as first-line supervisors for driving performance among subordinate employees.

Limitations

As a novice, qualitative researcher, the research study provided a unique opportunity to improve data collection and data analysis skills. The general data collection, analysis, and interpretation processes required additional expertise to ensure rigor of study outcomes. Because of the inexperience with doctoral-level research and to address any potential weaknesses, I sought guidance from peers and involved the dissertation committee comprising experienced faculty members during all phases of the research study to provide adequate guidance. Another limitation of the study involved the use of one primary data source for data analysis. The study relied on data obtained from semistructured interviews and interview journaling as the primary source of data collection.

Using a combination of data sources, methods, investigators, and theories enhance the credibility of a study's results. As an example, Patton (2014) maintained that triangulation serves to strengthen the actuality of the various elements of the empirical processes. Mitigating inherent weaknesses during the design development required my reliance on the expertise of the dissertation committee members during the data collection process. The last limitation anticipated involved the level of my engagement with participants involved with the study. I work within the higher education industry and recognized that my familiarity with the work environment could potentially create problems surrounding familiarity with participants and objectivity of responses.

To facilitate researcher engagement, I employed steps to engage with participants to build rapport and trust before commencing data. The credibility of qualitative research required adequate researcher engagement and open auditing processes. Guarding against this potential limitation required the development of a transparent audit trail that provided evidence of steps taken to ensure the quality of data collection through control checks like member checking and peer review action.

Significance of the Study

Establishing winning strategies for curbing employee cyberloafing behavior within businesses could emerge from paying close attention to the role of managerial control mechanisms. Business leaders could view the success of middle managers controlling cyberloafing as primary to the goal of establishing more practical strategies for the management of the employee cyberloafing phenomenon with the increasing levels of nomadic computing. The pervasive effects of employee cyberloafing on performance require the augmenting of existing cyberloafing strategies to enhance overall organizational performance (Kataria, Rastogi, & Garg, 2013). Most organizations encourage strong middle manager support of subordinate employees which in turn leads to high expectations for employee performance (Kauppila & Tempelaar, 2016).

In this study, I focused on the important role middle managers play in combating employee cyberloafing within a digital workplace for a variety of reasons. First, it provided information to a wider audience of scholars and practitioners that highlighted individual middle manager experiences and thoughts about their role in organizational

efforts aimed at curbing employee cyberloafing in digital work environments. Second, it built on existing research by further recognizing and acknowledging the meaning ascribed to the role of the middle manager in the employee cyberloafing mitigation efforts. Finally, this study contributed to positive social change by recognizing and acknowledging the significance of the middle manager's role in the implementation processes surrounding employee cyberloafing mitigation enabling organizations to clearly define the middle manager's role in the overall organization mitigation effort.

Significance to Practice

A few studies have explored managerial control strategies aimed at mitigating employee cyberloafing (Holguin, 2016). Daneshgari and Moore (2016) maintained that changing business operating situations involve paradigm changes that require organizational adaptation otherwise, the failure to adapt could lead to negative consequences. As the employee cyberloafing phenomenon continues to remain pervasive despite the adoption of technical control mechanisms and the implementation of mitigation policies, the explosive growth of nomadic computing necessitates a change in the methodologies used to mitigate employee cyberloafing.

Contemporary cyberloafing research has focused on the managerial control techniques providing businesses with benchmarking and learning opportunities to tap from the available best practices. This study enhanced the development of precisely defined roles and responsibilities for middle managers through the study's evaluation of participants' perceptions about the implementation of cyberloafing mitigation policies.

To this end, the significance of this study to practice was in illuminating the middle manager's role in cyberloafing mitigation efforts enhancing a better understanding of the role and responsibility.

Significance to Theory

Despite the prevalence of cyberloafing mitigation policies and the adoption of electronic deterrence systems within organizations, cyberloafing activities among employees continue to persist (Glassman et al., 2015). This study is the first to explore the cyberloafing phenomenon using the symbolic interaction and adaptive structuration theories. Symbolic interactionism allowed the study highlight the subsurface employee/supervisor interactive relationship and the social premises surrounding the use of information and communication technologies within organizations. Also, the study outcomes provided a window through which other researchers could understand influences, choices, and identities related to organizational online technology users. This study was significant to theory because it offered new knowledge that could help businesses reshape cyberloafing control mechanisms and policy implementation.

Significance to Social Change

Holguin (2016) noted that often, middle managers had experienced difficulties curbing employee cyberloafing activity because of a dearth of practical strategies. Achieving social change could be attained through business recognition and acknowledgment of the role middle managers play in curbing employee cyberloafing leading to the establishment of clearly defined roles and responsibilities for middle

managers in the overall organizational cyberloafing efforts. Understanding the transformational influences middle managers use to mitigate employee cyberloafing behavior offers businesses with potentially new mitigation strategies developed from a better understanding of the social interactions between employees and their supervisors.

Also, research outcomes elucidate how middle manager perception of their role in cyberloafing mitigation efforts influences the development of effective non-technical cyberloafing reduction strategies. Uncovering how meaning influences managerial behavior could help organizations that rely only on information technology and human resources departments improve employee performance by expanding their cyberloafing mitigation policies.

Summary and Transition

The study was designed to explore the lived experiences of middle managers on their organizational role mitigating employee cyberloafing and implementing cyberloafing mitigation policies. With the persistence of cyberloafing activities among employees at the workplace despite electronic monitoring and technical deterrence systems in place within organizations, understanding the role non-technical cyberloafing mitigation strategies used by the middle manager fills a gap in contemporary research on cyberloafing mitigation.

The findings from the study helped define the precise role of middle management, identified needs and deficiencies, and made recommendations for further development of cyberloafing mitigation policy implementation and strategies for combatting employee

cyberloafing. In the second chapter, I will present a review of the literature and highlight the relevance of the constructionist worldview together with a justification for the use of the adaptive structuration theory and the symbolic interaction theory before offering details on the role of middle managers in combating employee cyberloafing.

The second chapter will demonstrate the level of importance organizations place on the role middle managers play in driving efficiency and performance by discussing the relevance of studies that identified the ineffectiveness of the reliance on technical mechanisms aimed at monitoring and managing electronic employee communication at the workplace. Also, I will review the lack of empirical research available on the use of non-technical methods from a middle manager perspective. The chapter will conclude with a summary of the middle manager role in managing cyberloafing through the adoption of non-technical strategies.

Chapter 2: Literature Review

Despite the prevalence of cyberloafing mitigation policies and the adoption of electronic deterrence systems within organizations, cyberloafing activities among employees continue to persist (Polzer-Debruyne, Stratton, & Stark, 2014). The general business problem was the overreliance on technical deterrence without cognizing the role of middle managers as actors and agents in cyberloafing mitigation efforts. The specific business problem was the lack of information on the lived experiences of middle managers about their role in the mitigation of employee cyberloafing at work.

To effectively counter the prevalence of employee cyberloafing within organizations, organizations need to understand better middle manager roles in the prevention, enforcement, and rehabilitation of employee cyberloafing activities. The purpose of this qualitative study was to provide an explicit rendering of the ascribed meaning of middle managers about their role in mitigating employee cyberloafing at higher education institutions in Florida.

This literature review includes an explanation of the phenomenon of employee cyberloafing; attitudes and perceptions about cyberloafing; the impact of the widespread adoption of deterrence mechanisms within organizations; a discussion of the contemporary cyberloafing mitigation strategies and their effectiveness; and a description of the importance of middle managers in driving performance and employee engagement.

Literature Search Strategy

The literature search strategy for this study involved using current peer-reviewed research about employee cyberloafing and its mitigation. I used Google Scholar for the identification of related articles and subsequently the Walden University Library for retrieving the articles. The key scholarly databases searched include Business Source Complete, ProQuest Central, Academic Search Complete, Sage Knowledge, and Dissertation and Thesis at Walden University. After selection and storage of relevant articles in the Google Scholar library, I reviewed the same articles for relevance starting with abstracts to identify research methods, validity, reliability, data collection methods, and findings before making a decision to keep or discard each article.

The primary keyword strings used during the article search include *acceptable Internet usage policy enforcement*, *Internet risk management*, *Internet filtering and monitoring*, *cyberloafing*, *cyber deviance*, and *cyberslacking*. Other keywords used include *cyberloafing behavior*, *cyberloafing mitigation policies*, *cyberloafing sanctions*, *cyberloafing detection*, *personal Internet use at work*, *neutralization techniques*, *social constructivism*, *adaptive structuration theory*, and *symbolic interaction theory*. In general, this literature review includes research studies conducted on the emerged issue of cyberloafing and its mitigation using technical strategies and organizational policies.

Conceptual Framework

Cyberloafing involves employee use of computers at work for personal activities other than their job-related work tasks. The cyberloafing phenomenon remains an

important area of interest for scholars, practitioners, and organizations because of its expansion despite the widespread adoption of technical mitigation strategies at the workplace. The notion that middle managers are the controlling force behind the transformational influences that guide employee performance continues to evolve (Harding et al., 2014). The middle manager's knowledge construction about any given phenomena is dependent on personal, cultural, and social learning factors and social constructivists believe that true learning cannot take place without social context and collaborative interaction (Deulen, 2013; Vygotsky, 1978; Watson, 2001). I used a social constructivist-interpretive framework that relies on the multiple realities constructed through social interactions and lived experiences of middle manager participants.

Pedagogy on social constructivism emphasizes the viewpoint that the intentional actions, thoughts, discourse, and practices of individuals or groups help create parts of our social world (Bassani, 2014). The views of social constructivism rely primarily on assumptions of reality, knowledge, and learning and draw from Vygotsky's claim that knowledge is developed from thought processes developed from social experiences (Doubleday et al., 2015). For instance, two major themes in Vygotsky's social development theory, first published in the US in 1962, asserted social interaction is critical to the cognitive development and require a more knowledgeable other (persons with a higher ability level than the learner).

Middle managers play a central role within organizations ensuring subordinate employees fulfill their roles through the application of control mechanisms and

manipulation of social interactions aimed at driving performance (Harding et al., 2014). The social constructivist-interpretive framework allowed the researcher to explain better the fundamental aspects of middle manager social experience, interpretation, and intentional actions aimed at managing employee cyberloafing.

Small group studies have used social constructivist perspectives to show that learners construct knowledge by socially negotiating meaning while developing an understanding of concepts or behaviors and not solely from transmission through training (Liu, Yang, & Chan, 2013; Schreiber & Valle, 2013). Through this perspective, middle managers do not intervene in cyberloafing situations by relying solely on their authority, control, and responsibility; rather, they construct meaning about cyberloafing activity before taking intentional actions aimed at mitigating or minimizing consequences.

Theoretical innovations in previous research on cyberloafing mitigation have centered mainly on theories of neutralization (Lim, 2002; Lim & Teo, 2005; Rahimnia & Mazidi, 2015), control (Kura, Shamsudin, & Chauhan, 2013), agency (Glassman et al., 2015; Shepherd et al., 2014), and deterrence (Hassan et al., 2015; Ugrin & Pearson, 2013). Also, qualitative methodological frameworks used to explore the management of employee cyberloafing within organizations have collected and analyzed data from a variety of populations as evidenced by scores of journal articles.

Symbolic interaction and adaptive structuration theories formed the bedrock of this study. Although extensive research has been carried out on the managerial cyberloafing mitigation strategies, no single study draws from theories of social

interactionism and adaptive structuration. Collectively, the two theories allowed the researcher to understand; first, the symbolic meaning middle managers develop about their roles in cyberloafing mitigation acquired during workplace interactions with subordinate employees; and second, the meaning they ascribe to the individual and group employee structuring of online technology use at the work and how that understanding affects their roles in mitigating such behavior.

Symbolic Interaction Theory

Piotrowski (2012) in a bibliometric research study on cyberloafing research literature noted that some of the overlooked areas included socialization, the proliferation of nomadic computing, and organizational development. Most organizations require that employees use technology to perform work tasks, and with the advent of nomadic computing, allowing for easier individual Internet connections, organizations continue to struggle to balance the private Internet use needs of employees with organizational performance requirements. A few studies noted that research is nudging organizations to focus on changing employee attitudes toward acceptable and unacceptable cyberloafing as well as a focus on training managers to identify and respond to Internet misuse while responding proactively to Internet abuse (Ugrin & Pearson, 2013, Young, 2010).

The notion that middle managers are the driving force behind the transformational influences that guide employee performance continues to evolve with the rapidly changing operating environments (Parera & Fernández-Vallejo, 2013). Social interactions at the workplace between employee and manager allow managers to develop situational

awareness of what individual employees are doing, not doing, and capable of doing (Bhattacharya & Tang, 2013). Middle managers in extant cyberloafing research have received little attention, yet they might play a fundamental role in the mitigation of employee cyberloafing behaviors and activities.

According to the symbolic interaction theory, people's intentional actions are driven by the meaning derived from experience with a situation or phenomenon, interaction with others, and interpretive processes (Sandstrom & Kleinman, 2005). Using a symbolic interaction lens to understand the peculiar and distinctive character of the manager/employee relationship with a focus on the management of cyberloafing is important because it allows for an unraveling of the joint actions through which the lives of employees and middle managers are organized and work environments are structured. Gallant (2014) posited that using a symbolic interaction framework enhanced a clearer uncovering of the subjective meaning individuals ascribed to their lived experiences and behaviors.

Middle managers use both manipulation and direct/indirect control mechanisms to ensure subordinate employees meet work task requirements, with informal, conversational, and social interactions influencing how middle managers work. Creary, Caza, and Roberts (2015) suggested that manager's use of inclusionary and exclusionary strategies based on perceptions on individual employee identities enhance opportunities to improve employee performance of work tasks and activities. Campbell, Stylianou, and Shropshire (2016) noted that middle managers have a fiduciary responsibility to protect

organizational interests when interacting with subordinate employees and should encourage whistleblowing Internet abuse among subordinate employees.

Adaptive Structuration Theory

As noted in Kahai (2013), the proliferation of advanced information technologies is creating new situations involving the acquisition, storage, and dissemination of information. DeSanctis and Poole (1994) claimed that the duality of human action and social structure perspectives enable a better understanding of the social aspects of technology use. Employees use both personal and work-provided information and communication devices for communication, manipulation, and storage of information and the decision to use the device depend on a variety of personal factors (Rice & Leonardi, 2013).

In most cases, employees working in digital work environments have free access to digital media technologies necessitating the prohibition of access to digital media by way of computer controls (Davison & Ou, 2016). With the proliferation of advanced information and communications technology today, the proximity between middle managers and individual employees provides opportunities for managers to comprehend the not only the effects of misuse but also the structures associated with the appropriation of the technologies. Per adaptive structuration theory, the effects of online technology within organizations is dependent on user adaptation about work tasks and structures integrated within the devices (DeSanctis & Poole, 1994; Poole, 2013).

Understanding how individual and group members structure their appropriation of personal or organization information and communication technologies for both work and non-work related activity could enhance the effectiveness of non-technical control measures. Wang, Xiang, and Fesenmaier (2016) argued that adaptive structuration theory offered a rich framework for examining the everyday use of smartphone technology in a travel context and showed that the appropriation of smartphone technology led to the development of new structures (habits and social obligations). This theory affords researchers with an opportunity to understand how managers interpret employee appropriation and the structuration of information and communication technologies at the workplace in the cyberloafing context.

A recent study by Golden (2013) involved an examination of information and communication technologies' mediation of individual management of work/life interconnections. Drawing from Giddens's (1984) work on structuration theory, Golden has been able to show how the recurrent structuring of online technology use by individuals affects the policies and organizational resources. Likewise, Wang et al. (2016) hold the view that the adaptive structuration theory offers researchers the opportunity to understand better the subjective nature of the individual's adoption, usage, and impact of technology.

Wang et al. (2016) used the adaptive structuration theoretical framework to investigate the ramifications of smartphone technology usage on the experiences of American tourists. The study found several linkages between individual adaptation to

smartphone technology and tourist experience. According to Liao, Luo, Gurung, and Li (2009), middle managers are responsible for controlling team members, therefore, an understanding of team member appropriation of online technology is vital when looking to mitigate misuse.

Difficulties arise, however, when attempting to implement cyberloafing mitigation policies because of the role ambiguity in the information technology and human resources manager positions. Holguin (2016) assumed that functional managers responsible for mitigating cyberloafing include supervisors managing departments within an organization including corporate staff. Al-Shuaibi, Shamsudin, and Subramaniam (2013) argued that human resources manager's activities positively influenced organizational employee cyberloafing mitigation efforts.

Hartijasti and Fathonah (2015) argued that the responsibility for controlling employee cyberloafing should reside within the human resources and information technology departments from a training, enforcement, and policy development perspective. What these studies fail to recognize is the direct responsibility middle managers have for driving performance making it imperative for them to monitor and control unacceptable behavior.

What Is Employee Cyberloafing?

Computer technology was initially developed to serve work-related needs within organizations. The introduction of the Internet facilitated the ubiquitous nature of computing fostering social connections and personal engagement with hobbies

(Glassman et al., 2015). Today, the easy access to computers and Internet connectivity play a significant role in shaping both the personal and professional lives of employees with some concern for organizations and their managers.

Another source of perturbation for organizations and their managers is the consumerization of personal information and communication devices like smartphones, tablets, portable gaming devices, and portable laptops substituting organization-owned devices (Pirani & Meister, 2014; Porter & Heppelmann, 2015). Cyberloafing, first identified by Kamins in 1995, was considered the misuse of information and communication technologies by employees at the workplace for non-work-related activity (Jandaghi et al., 2015). More recently, cyberloafing is best defined as the use of computers and smart mobile devices at work for non-work-related activity by employees not working remotely (Jamaluddin et al., 2015).

Notwithstanding the indistinct nature of the definition, cyberloafing is one of the most common elements of deviant workplace behavior and accounts for organizational losses in productivity and revenue (Corgnet, Hernán-González, & McCarter, 2015; Mahatanankoon, 2006). Prior research on cyberloafing focused on causation, typologies, technical mitigation, human resources department mitigation efforts, and information technology department mitigation efforts, and cyberloafing mitigation policies within organizations (Field & Chelliah, 2013; Glassman et al., 2015; Shepherd et al., 2014; Al-Shuaibi et al., 2014; Piotrowski, 2012).

Other researchers, however, looked at employee cyberloafing differently (see Quoquab, Salam, & Halimah, 2015; Bernier, 2014) and have focused on the beneficial attributes of employee cyberloafing and argued in support of the notion that cyberloafing could enhance performance. As an example, Quoquab et al. (2015) found no change in effect regarding cyberloafing performance losses in an investigation of organizations that support a self-governing work environment with liberal Internet policies. Similarly, Bernier reported that cyberloafing activity enhances employee concentration because cyber activity recharges individual attention.

Schalow, Winkler, Repschlaeger, and Zarnekow (2013) argued that some organizations escalate the employee cyberloafing problem by contributing to the creation of blurred boundaries between work related and non-work related online technology usage within their organizations. Schalow et al found that mobile communications and online social networking played a catalytic role in shaping employee attitudes toward the ambiguity of personal life and work life boundaries. For this study, cyberloafing behavior is of interest because of the widespread prevalence across industries with some variations depending on the organization's level of tolerance.

Meaning Ascribed to the Employee Cyberloafing Phenomenon

Betts, Setterstrom, Pearson, and Totty (2014) described two primary types of cyberloafing that include; minor cyberloafing involving the use of personal email and browsing the Internet for personal reasons, and severe cyberloafing that includes gambling and viewing of pornography. The employee cyberloafing phenomenon

produces shared mental impressions for organizations as a group and the employee as an individual that cyberloafing could yield both positive and negative outcomes. From an organizational worldview, most organizations recognize that the ubiquitous nature of nomadic computing and electronic connectivity necessitates some degree of corporate controls to restrict Internet and technology usage freedoms.

Jandaghi et al. (2015) highlight the negative attributes associated with cyberloafing that center on employee performance reduction, security vulnerabilities, bandwidth issues, legal issues, and costs related to specific incidences. From this line of thinking, cyberloafing activity is discouraged by most organizations and is validated by the widespread use of deterrence mechanisms and policies to mitigate misuse (Li, Sarathy, Zhang, & Luo, 2014; Coker, 2013). The fact that an increasing requirement for employee use of online technology applications in various business operations indicates a perceived organizational benefit in terms knowledge sharing and process improvement (Wet & Koekemoer, 2016; Peng, Quan, Zhang & Dubinsky, 2015).

Businesses increasingly use online platforms to encourage learning, social networking, and talent development. Carlson, Zivnuska, Harris, Harris, and Carlson (2016) noted the duality of workplace social media usage that could simultaneously encourage task-oriented and relationship-building as well as deviance activity. In a study of examining factors responsible for attitudinal differences in personal use of online social networking sites at the workplace, Andreassen et al. (2014) found that middle managers predominantly had a dim view about employee's personal use of social

network sites during work. Contrary to the notion held by some organizations that cyberloafing negates performance, it can be argued that cyberloafing activity could boost productivity.

As an example, Coker (2013) explored the positive attributes of cyberloafing and found an association between cyberloafing and performance regarding task vigilance while (Ugrin & Pearson, 2013) pointed to cyberloafing as an activity that allows employees to reduce stress while adding variety to their daily routines. From an employee perspective, cyberloafing is considered by some as a form of empty labor in situations when there is little work left to do and the time is spent slacking on the Internet. Some employees view cyberloafing as a means of getting away from or masking the internal or external stressors with gender-based differences about time spent engaging in such activity.

In Aghaz and Sheikh (2016) and Stoddart (2016), the authors suggested that employees view cyberloafing activity as a coping mechanism when seeking emotional and mental relief at work. Ferreira and Esteves (2016) showed how gender-based differences in employee perceptions about the amount of time spent on non-work-related activity was lower than the actual time spent performing such activities. In some instances, employees perceive cyberloafing as a strategy to compensate for perceived unjust actions within an organization. Öğüt, Şahin, and Demirsel (2013) reported that employees believe that in organizational situations where a sense of organizational justice

is lacking, engaging in intentional cyberloafing behaviors acts as a means of compensation.

In Hernandez-Castro's (2016) examination of employee perceptions about the ethical seriousness of cyberloafing activity at work, the author found that employees considered the moral gravity of cyberloafing activity as little which could contribute to the continued persistence of the issue at the workplace. Also, a group of employees, mainly digital natives, and the millennial generation, hold the impression that organizations must create flexible workplaces that allow for the unhindered use of technology for both personal and work-related communication and social networking. Zeff and Higby (2015) maintained that millennial employees live in a world characterized by technology-driven interruptions and willingly contravene control mechanisms aimed at prohibiting smartphone usage at the workplace because of an appendage to smartphones.

The author suggested that a need for new strategies to control the new generation of employees exacerbating the cyberloafing issue and constitute a fast-growing population in the US workforce. Cardon and Marshall (2015) examined the prevalence of organizational adoption of social networking platforms as a tool for the enhancement of team communication and collaboration. The authors surveyed business professionals within the United States and findings indicated that members of generations X and Y showed an inclination to consider social networking as a primary means of communication in future.

The Digital Workplace

In recent years, the modern work environment is transforming dramatically with a rapidly changing technological landscape enabling employee use of applications and solutions to improve processes and drive performance in both personal and professional situations. Per Deloitte (2014), the digital workplace includes all work environments where employees use mainly computer hardware, software, interfaces, and connectivity solutions to perform work tasks, collaborate, and provide services to clients. Colbert, Yee, and George (2016) noted that the digital workforce comprises digital natives and digital migrants that attained digital fluency leveraging interaction with technology at the workplace.

According to Prensky (2001), Digital Natives include young adults just starting to enter the workforce and heavy users of information and communication technologies while digital immigrants represent the category of adults that have readily embraced information and communication technologies since its inception. Wang, Myers, and Sundaram (2013a) take issue with the contention that the digital migrants and digital native are mutually exclusive groups based on a binary focus on age and Internet accessibility. Rather, the authors maintained that the concept of digital fluency best describes the differences between the two groups. Currently, in the US, the workplace is witnessing a surge of innovative solutions aimed at supporting mobile device usage, unifying communication capabilities, improving the flow of work, and business processes.

For instance, Dery, Tansley, and Hafermalz (2014) described how changing organizational recruiting and selection processes are influenced by the explosive growth of nomadic computing and social media usage. One problem for most employers' hinges on the over-exposure of employees to the distracting overflow of information made available by the easy access to Internet. According to (Ladner, 2015), "The primary unmet need for mobile productivity is managing the torrential onslaught of constant communication." A recent report by commissioned by Nokia, a multinational information, and communications technology company, as cited in (Spencer, 2013) indicated that smartphone users in the United States check their phones on average about 150 times daily.

According to Newswise (2013), between 60% and 80% of employee Internet work time is spent on non-work-related activity averaging about 90 minutes a day. Also, with over 64% of adults in the United States having ownership of smartphones with unrestrained access to the Internet, email, social networks, and entertainment, organizations and their managers must change their strategies aimed at managing misuse (Smith, 2015). Another problem facing organizations with predominantly digital work environments relates to finding the right balance between the legitimate employer rights to protections against liability issues resulting from employee misuse of technology at work and the privacy concerns of employees. In an analysis of current legislation on technology-related privacy rights, Park (2014) noted that the current law fails to delineate

clearly the boundaries about acceptable and unacceptable employee technology usage at the workplace.

The prevalence of cyberloafing behavior and activity involving internal and external communication within organizations contribute to mounting losses in productivity recorded by organizations struggling in highly competitive conditions. Consequently, most organizations developed strategies and policies aimed at regulating employee use of electronic communication and deployed technical mechanisms to monitor and control employee use of communication technologies. Despite the adoption and deployment of the policies and techniques, employee cyberloafing continues to persist at the workplace. In line with Bhattacharya and Tang's (2013) viewpoint that suggested precarious work conditions weaken workplace relationships, however, the promotion of employee participation is dependent upon effective supervisory practices, this study considered the creativity and resourcefulness of the middle manager in cyberloafing mitigation.

Antecedents of Cyberloafing

A study by Sheikh, Atashgah, and Adibzadegan (2015) aimed at verifying the contemporary explication of cyberloafing antecedents listed three antecedents: behavioral control, subjective norms, and the ability to conceal intention. Sheik et al. (2015) used the theory of planned behavior model developed in prior research to determine whether it explained cyberloafing in a different environment. Interestingly, Sheik et al found that with the enthrallment and captivation associated with online social networking, managers could seize the opportunity to engage employees in productive online activity centered on

the sharing of knowledge, the building of organizational culture, and improving employee socialization.

Relatedly, Askew et al. (2014) examined the degree of distinctness in the meaning of cyberloafing and its various conceptual elements and concluded that cyberloafing is a withdrawal behavior with behavioral control, subjective norms, and the ability to conceal intention as predictors. In contrast, Jandaghi et al. (2015) presented personality, work demands, role conflict, organizational justice, and policies as the antecedents of cyberloafing. Jandaghi et al argued that studies on the antecedents of cyberloafing behavior emanate from the following three distinct factors; personal, work-related, and organizational. Jandaghi et al noted that individual elements revolved around issues related to personality, extraversion, prosocial behavior, goal-directedness, neuroticism while work-related factors centered on low work demands and conflicting work duties and organizational policies.

The organizational factors consider issues with office politics, lacking transparency in cyberloafing mitigation policies, and perceptions about unfair treatment by the organization (organization justice). The study concluded by suggesting that organizations cannot mitigate cyberloafing by relying solely on control systems. In studies that examined personality traits with cyberloafing (O'Neill, Hambley, & Bercovich, 2014; Jia, Jia, & Karau, 2013), the researchers found a positive association between extroversion and cyberloafing and a negative association with conscientiousness, emotional stability, and openness. More specifically, O'Neill et al. (2014) focused on

employees working remotely and found the same relationship between cyberloafing and personality traits.

Many scholars hold the view that personality plays a role influencing individual workplace deviant behavior. Knowledge about the antecedents of cyberloafing behavior is necessary for managers to enable a better understanding of the positive and negative behavioral outcomes, the consequences of mitigation efforts, as well as the effects of organizational policies targeting cyberloafing.

Typologies of Cyberloafing

Lim (2002) made one of the first attempts at differentiating the types of cyberloafing behavior where she distinguished cyberloafing activity into browsing and emailing. Browsing activities included visiting websites for entertainment, financial services, news, social networking, shopping, sports, and pornography to name a few. Emailing activities involved the reviewing, receipt, and exchange of personal emails. After an investigation of actual cyberloafing behavior, Blau, Yang, and Ward-Cook (2006) expanded the types of cyberloafing activities by introducing another category that involved interactive Internet activity.

Interactive Internet activities included playing live online games, chatting online, making live posts on social networking sites, and downloading information. Blanchard and Henle (2008) argued for a further differentiation of cyberloafing forms and presented serious cyberloafing and minor cyberloafing as a better categorization grounded in research on deviant behavior. The authors noted that minor cyberloafing involved

emailing and commonly tolerated Internet usage at work while serious cyberloafing consisted of viewing pornography, downloading music and videos, online gambling, and online gaming.

Sheikh et al. (2015) took the differentiation of cyberloafing a step further when they asserted that three verified levels of cyberloafing included email and browsing activity, interactive online activity, and online social networking activity. Yasar's classification of cyberloafing activities (as cited in Keser, Kavuk, & Numanoglu, 2016) into four distinct types that included; individual, social, search, and news is a more recent attempt at expanding the existing types of cyberloafing activity.

Nomadic Computing and Cyberloafing

The advancements in smartphone technology allow for anytime and anywhere Internet connectivity increasing the capacity for individuals to sustain and continue engaging in cyberloafing behaviors during work hours. According to (Smith, 2015), since 2011, smartphone ownership in the US increased from 35% to 64% of the population surveyed by the Pew Research Center. In a study examining the association between narcissism, personality, and smartphone addiction, Pearson and Hussain (2015) found that the increasing number of smartphone owners could lead to the risk of rising addiction to social networking sites and narcissistic behavior among social network website users.

Dery et al. (2012) argued that smartphone usage creates ambiguity concerning the boundaries of work-related and non-work-related Internet use. Also, problematic smartphone usage is becoming a pervasive problem causing interruptions to employee

daily work routines. Jamaluddin et al. (2015) argued that the advent of smartphone technology has heightened the issue of employee's non-work related Internet usage leading to adverse outcomes. Jamaluddin et al noted that losing control of individual smartphone usage as well as a preoccupation with the Internet further contributes to productivity losses at the workplace.

Deloitte (2015) reported that the average person in the US checks his or her phone 46 times each day up from 33 checks in 2014 with a variation dependent on age group. The survey also indicated that younger smartphone user in the age group between 25 and 38 averaged 50 smartphone checks daily. Dery et al. (2014) posited that the evolving nature of mobile communication technology makes the regulation of connectivity increasing difficult for employers. Gökçearsan, Mumcu, Haşlaman, and Çevik (2016) advanced the position that smartphone addiction, particularly in young people, has negative consequences.

For MacCormick, Dery, & Kolb (2012), employee smartphone use facilitates engagement allowing for the achievement of work/life balance through temporal and spatial organizational flexibility. Some human resources managers agree that relaxing restrictions on Internet usage will result in positive outcomes in areas such as performance, job motivation, and increased internal communication. (Saraç & Çiftçioğlu, 2014). An investigation of the role of deficient self-regulation in excessive mobile phone use that mobile phones increase individual ability to stay connected even working remotely, but could reduce performance through increased distractions from current tasks

(Soror, Steelman, & Limayem, (2012). Soror et al suggested alternative strategies for handling excessive use of mobile phones by enhancing self-regulatory resources and identifying mechanisms to break bad habits.

In addition, findings in MacCormick, Dery, Kolb (2012) showed that smartphones enabled employee time management, client responsiveness, facilitated engagement and the achievement work/life balance through temporal and spatial flexibility. Many organizations provide mobile devices or allow employees to connect to personal devices to corporate networks creating vulnerabilities requiring the use of mobile device management software to secure mobile platform accessing the systems (Harris & Patten, 2014). In an investigation into the adoption of organizational policies that prohibited the use of mobile devices during performance related crisis management, Stephens and Ford (2014) found that digital inequities developing in different ways within organizations with knowledge and powerless workers.

Knowledge workers had access to computers at work while powerless workers did not and in both cases, organizations permitted the managerial use of personal mobile devices while enforcing the ban on employee use of mobile devices. The results showed that employee sentiments about organizational justice issues increased during crisis interventions leading to the prohibition of mobile devices. More recently, Stephens and Ford (2016) found four unintended ramifications of banning mobile device usage to mitigate employee misuses that include a further decline in employee performance,

inordinate monitoring problem for managers, reduced ability for the employee to improve capabilities, and an increase in employee levels of disengagement.

Online Social Networking Sites and Cyberloafing

Contemporary cyberloafing research emphasized the importance of the relationship between social media activity and employee cyberloafing behavior. Globally, the introduction of online social networking within organizations through a variety of applications and platforms creates opportunities for collaboration (Franchi, Poggi, & Tomaiuolo, 2013). Cardon and Marshall (2015) suggested that corporate social networking platforms could turn into the main platform used for business communication shortly. This study provides useful information pertaining to the use of social networking as a platform for internal communications which would affect the acceptable Internet usage policies for some organizations. Some researchers like Mutula (2013) argued that despite the global acceptance of social networking, gaps in policies governing user rights and technological weaknesses in social network platforms abound.

Others like Keyes (2013b) reported that the biggest challenge facing the online social networking adoption within organizations centers on problems with interoperability between the different social networking platforms. Keyes noted that lack of interoperability creates problems for employees looking to share and transfer information across social network platforms. Carlson et al. (2016) examined the positive and negative effects of employee social media usage at the workplace and found that

intense employee social media usage contributed very strongly to negative and deviant behavior and mildly to task and relationship building behavior.

Different theories exist in the literature linking the individual use of social networking sites with the various dimensions of human personality. Thus far, some studies have explored the relationships between employee use of social networking sites and the management of human resources within organizations. Some researchers suggested that high levels of social network messaging, gaming, dating, and random search activities result in damage to the organization regarding employee performance, brand image, and liability (Kluemper, Mitra, & Wang, 2016). Others have highlighted the relevance of individual addiction to social networking sites requiring more practical mitigation solutions.

Andreassen (2015) draws our attention to two distinctive dimensions of online social networking that include excessive and compulsive behavior. In her comprehensive review of the literature on online social networking addictive behavior, Andreassen (2015) suggested that interventions aimed at mitigating employee social networking addiction should focus on controlling rather than prohibiting usage. The study concluded by recommending a variety of intervention strategies organizations could offer to employees that include self-help, behavior therapy, and pharmacology. Unlike Andreassen, some studies like (Dijkmans, Kerkhof, & Beukeboom, 2015; Treem & Leonardi, 2013) indicated interest in the growth of work-related adoption of online social

networking with a broad range of corporate affordances in areas of consumer interaction, employee communication, community association, and organizational learning.

Relatedly, El Ouiridi, El Ouiridi, Segers and Henderickx (2015) claimed that online social networking sites have emerged as popular, cost effective, and flexible employee training, organizational learning and development tools used within organizations. Together, both studies (El Ouiridi et al., 2015; Treem & Leonardi, 2013) point to the positive benefits of the work-related use of online social networking sites but fail to address the negative dimensions of non-work related online social networking. Interestingly, Walden (2016) who presented a different account of the integration of online social media for a work-related use found some employee resistance because of work-task distraction and privacy.

Another interesting part of the literature on the relationship between online social media usage and cyberloafing relates to issues concerning addiction and mental disorders. As Schou Andreassen et al. (2016) reported, associations exist between the increasing levels of addiction to social networking and mental disorders. Schou Andreassen et al found associations between manifesting employee risk factors surrounding mental illness like attention deficit, obsessive compulsive, anxiety, and depression with a proclivity toward an addiction to social networking. More recent attention has focused on the frictions developing within employment relations as noted in McDonald and Thompson (2016) who listed three reasons why conflict exists within a significant number of work relationships.

These are excessive employee use of social network sites during work, pervasive employer profiling activity, and employee posts about work-related issues. McDonald and Thompson (2016) acknowledged the blurring of lines surrounding boundaries surrounding the work-related or personal use of social networking sites creating more complexities for organizations looking to monitor and control employee use of social networking sites using technical methods. Of interest is the excessive employee usage of social networking sites as noted in Andreassen et al. (2014) who reported the growing productivity concern within organizations about employee use of social networking sites for personal activity during work. Andreassen et al. (2014) suggested that finding solutions within organizations to improve job task relevance and the social climate could help counteract cyberloafing activity within an organization.

Field and Chelliah (2013) examined the various types of organizational risks associated with employee social media usage and made suggestions on the best approaches for mitigating such risks. The authors pointed to a need for organizations to not only understand the risks and consequences but also to understand how to mitigate such risk using effective and well documented human resources and general management strategies. The results of the study showed that for organizations looking to cover all bases in terms of their exposure to employee social media usage risks, two key policies would be required to cater for both business use and personal use of social media within the organization.

The Cost of Cyberloafing

One of the greatest developments of the 21st century is the emergence of the Internet and the growing use of data-driven technology in almost every facet of life (Castillo & Thierer, 2015; Jandaghi et al., 2015; Omole & Ayeni, 2013). In her compelling analysis of problematic employee use of the Internet, Mahatanankoon's (2006) developed a conceptual model from the perspective of employee cyberloafing policy violations within organizations that threaten its well-being through four major types of deviance related to property, production, political, and personal aggression. Property deviance involves the intentional and unauthorized acquisition of intellectual property causing damage or destruction while production deviance refers to the excessive non-work-related Internet use such as chatting, online gaming, social networking, and viewing entertainment in violation of organization prescribed norms and procedures.

The political deviance includes employee activity affecting co-workers like gossip, rumors, cyberbullying, and accusations, transmission of confidential information, corporate secrets, and intellectual property to unauthorized sources outside the organization while personal-aggression involves the transmission of malicious, abusive, or harassing messages electronically to other employees. The growing trend related employee misuse of the uninhibited access to the Internet and information and communications technologies is adversely affecting employers.

Prior research indicates that the costs of employee cyberloafing activities include lost productivity, theft of confidential information, liability, and monitoring and filtering

technology (Corgnet et al., 2015; Jandaghi et al., 2015; Glassman et al., 2015; Jia, Jia, & Karau, 2013). Indirect costs associated with cyberloafing include bandwidth reduction, reducing network speed, the introduction of computer viruses, loss of brand image, loss of customer loyalty, loss of potential sales, and destruction of general trust of the organization to name a few (Jia, Jia, & Karau, 2013).

Almost every paper written on cyberloafing includes a section relating to estimated costs associated with losses in productivity and the costs of technical deterrence mechanisms. In an analysis of the annual cyberloafing related productivity losses to businesses in the United States, Jia et al. (2013) reported that costs run between \$54 billion and \$84 billion. In a follow-up study, Jandaghi et al. (2015) suggested that the cyberloafing phenomenon in the United States costs about \$183 billion each year. Son and Park (2016) presented a conservative estimation that placed business losses in the United States at about \$85 billion each year.

The other substantial cost of cyberloafing to companies centers on the annual expenditure on monitoring and filtering software used to mitigate cyberloafing. Sanders, Ross, and Pattison (2013) described the increasing use of electronic monitoring by employers to block certain websites, monitor Internet use and emails, monitor retrieval of data and information, and recording and surveil phone conversations. According to Glassman et al. (2015), the Internet monitoring and filtering software industry witnessed tremendous growth with estimated revenue of \$1.18 billion in 2012.

Management of Employee Cyberloafing

In the past decade, we have seen the emergence of research on the management of employee cyberloafing with innovative theories and methodological procedures used in the context of social constructivist-interpretive conceptual frameworks. The conscious acts of intellection behind researcher interests in the management of employee cyberloafing centers on the need to improve employee performance and reduce revenue losses resulting from cyberloafing activity (Holguin, 2016). The precursors of employee cyberloafing behavior are attributable to personality, social norms, job demands, organizational policies, and organizational justice issues (Jandaghi et al., 2015; Sheikh et al., 2015; Askew et al., 2014).

Teh, Ahmed, and D'Arcy (2015) examined organizational factors that foster the neutralization of employee information security policy violations with a focus on employee disgruntlement. The findings indicated a positive association between role conflict and neutralization of information security policy violations. The study provided useful information on employee neutralization of information security policies on the implementation of acceptable Internet usage policies and mitigation of employee cyberloafing. In managing employee cyberloafing behavior, organizations have developed strategies to not only safeguard the information, data, and intellectual property but also to enhance employee performance at work (Jandaghi et al., 2015).

Despite the widespread use of mitigation strategies, employee cyberloafing activities continue to endure within companies (Polzer-Debruyne et al., 2014). In

addition, Chiu and Peng (2008) posited that abusive managerial control techniques at the work closely relates with employee workplace deviance. To better understand the mechanisms of corporate strategies for employee cyberloafing management, Holguin (2016) explored functional manager's perceptions about effective strategies for mitigating employee cyberloafing at a northeastern business organization in the United States.

Interestingly, Holguin's findings indicated that by combining deterrence mechanisms with the furtherance of performance management, social standards, and good citizenship behavior, functional managers developed a practical technique for controlling employee cyberloafing. Holguin results showed that functional managers controlled unacceptable cyberloafing by communicating expectations, creating conducive work environments, and keeping employees engaged. The author offered no explanation for the distinction between the meaning functional managers ascribe to their organizational role in the mitigation of employee cyberloafing and the strategies they employed.

In the same vein, another study on managerial perceptions about supervision of digital natives in the workplace by Pinzaru & Mitan, (2016) found that managerial attitudes about digital natives peculiarities helped influence the development of practical strategies used for supervision. Pinzaru & Mitan, (2016) noted that manager recognizance of the different needs and traits of their various team members helped drive performance improvement. In agreement, Holguin (2016) posited that managerial sensitivity to

employee requirements in technology usage empowering self-control allowed for a collaborative implementation of cyberloafing mitigation. Different theories exist in the literature regarding the management of employee cyberloafing. Theoretical frameworks used in a significant number of studies draw from the concept of deterrence that depends on punishment as the means of deterring people from engaging in prohibited activities.

More recent attention has focused on the deterrence mechanisms used by business organizations to mitigate cyberloafing that include technical and non-technical deterrence mechanisms (Shepherd et al., 2014; Ugrin & Pearson, 2013). Shepherd et al. (2014) examined organizational attempts to minimize security vulnerabilities and improve employee performance and suggested that mitigation efforts using surveillance mechanisms constituted an effective method for reducing cyberloafing activity. Shepard et al described technical surveillance tools as processes involving access to business online technology platforms or networks, audit logging, and keystroke systems, video/voice monitoring and recording, passwords requirements, anti-virus protection, intrusion detection, and data encryption.

In contrast to Shepard et al., (Glassman et al., 2015; Polzer-Debruyne et al., 2014) suggested that the widespread use of technical deterrence mechanisms were not effective as standalone strategies for mitigating employee cyberloafing. Numerous studies have compared technical and non-technical deterrence techniques used to mitigate employee cyberloafing at the workplace and found that they are mostly different. Technical deterrence techniques are reactive whereas non-technical deterrence techniques are

proactive. Glassman et al. (2015) found the technical deterrence prevented evasive employee activity and promoted compliance but acknowledged the need to combine control modules with additional resources.

Whereas, non-technical deterrence techniques involving the use of managerial control include planning, enforcement of usage and security policies, as well as the adoption of education, training, and awareness programs (Rahimnia & Mazidi, 2015). Rahimnia and Mazidi (2015) found that proximity of managerial control and monitoring works well for employees with lower levels of cyberloafing self-control. Grover (2014) maintained that using monitoring proximity required critical understanding to adopt mitigation strategies that avoid the backlash of animus and enhance positive responses from employees. Technical deterrence techniques tend to increase employee mistrust of their organization while non-technical deterrence techniques do not. As an example, Holland, Cooper, and Hecker (2015) found an inverse relationship between technical deterrence techniques and employee's trust of their organization's management.

Also, Jandaghi et al. (2015) noted that despite the technical control mechanisms used by organizations, the cyberloafing phenomenon continues unabated. In contrast, Holguin (2016) showed that managerial controls involving the promotion of citizenship behavior and creating a work environment with norms that discourage cyberloafing activity helped encourage employee self-control of cyberloafing. Studies on non-technical mechanisms focused on the enforcement of cyberloafing policy, policy dissemination, employee training, and sanctioning of violations which suggest a

conservative approach rather than a proactive approach (Piotrowski, 2012). Rahimnia and Mazidi (2015) found that human resource managers perceived non-technical cyberloafing control mechanisms as more efficient at preventing cyberloafing behavior than tracking or monitoring.

The study by Jandaghi et al. (2015) discussed the impracticality of trying to eliminate cyberloafing and suggested that organizations and their managers must make mitigation policies explicit, adopt effective mitigation mechanisms, focus on employee motivation, and encourage the right culture of Internet use. Prior research reports indicate that despite the massive financial investments made by business organizations in deterrence mechanisms aimed at countering cyberloafing activity, the cyberloafing phenomenon continues to persist (Son & Park, 2016; Jia, Jia, & Karau, 2013).

Researchers have not considered the managerial informal, conversational, and social interactions that may contribute to the non-technical deterrence mechanisms that focus employees on work tasks.

Some researchers (e.g. Andreassen et al., 2014) have attempted to draw subtle distinctions between employee perceptions about positive or negative workplace environments and cyberloafing behavior. Andreassen et al. (2014) pointed out that employees with stimulated work assignments, de-fragmentized work tasks, having workloads commensurate with available resources and abilities, and positive work environments tend not to engage in excessive cyberloafing. Al-Shuaibi et al. (2014) supported this view and wrote that the negative workplace environments contribute to the

facilitation of employee deviance. Once organizations can adopt effective policies, mechanisms, and the right culture, the prevailing view of most researchers is that organizations will avert productivity losses and the high costs of employee cyberloafing.

Understanding the managerial role in curbing employee cyberloafing based on their social interactions and proximity with employee's could lead to new approaches, policy re-development, or the realignment of existing mitigation techniques. In another major study, Bianchi and Andrews (2015) examined managerial perceptions of the advantages and disadvantages of using social media marketing platforms at a marketing organization in Chile. The study focused on uncovering the role of social media use in improving brand image and driving customer engagement and found that the technological and cultural issues played a role in managerial decision making whether to introduce social media marketing and in general used social media as a temperature gauge for their market.

Managers are expected to drive employee performance and productivity while resolving individual employee problems as well as problems among groups of employees. The inspiration for this study's methodological approach draws from Bianchi and Andrews' study that comprised data collected using interviews from 12 marketing managers from different marketing firms. In comparison to other qualitative studies on middle management perceptions, the fore mentioned study offered a unique examination of manager knowledge on the role of social media in the enhancement and

implementation of marketing strategy which is like this study examining the role of middle managers in mitigating employee cyberloafing.

Technical Deterrence Mechanisms

Technical deterrence mechanisms involve the monitoring of employee online technology use and Internet activity using a variety of electronic-enabled tools and techniques. According to Mahatanankoon (2006), technical deterrence mechanisms enable organizations to minimize the adverse impact of employee inappropriate Internet use by deploying three technologies that: prevent, detect, and enforce. Preventive technologies function by blocking and filtering Internet traffic by using packet filtering, state inspection, and proxy servers (Mahatanankoon, 2006). The detection technologies function to monitor and track inappropriate Internet activity by using the Internet log mining, software agents, and spyware mechanisms (Mahatanankoon, 2006).

Enforcement technologies work together with the organization's Internet usage policy to restrict specific websites, capture and record online activity allowing managers access reports (Mahatanankoon, 2006). Studies like (Cheng et al., 2014) described the electronic surveillance of employee online technology usage as processes that combine packet sniffing, monitoring of desktops, logging of file systems, filtering emails, controlling browsing, and monitoring Internet activity. The Electronic Communications Privacy Act (ECPA) allows employers to monitor employees through electronic monitoring activities for protective reasons (Moussa, 2015).

Wang et al. (2013b) noted that approximately 65% of business organizations use electronic means to monitor and prevent the inappropriate Internet use by their employees. Despite the technical cyberloafing countermeasures that remind and block inappropriate websites access, the issue of cyberloafing continues to persist (Polzer-Debruyne et al., 2014; Glassman et al., 2015). Gritzalis, Stavrou, Kandias, and Stergiopoulos (2014b) contributed to research on technical deterrence mechanisms integrated within business processes by examining the pros and cons of the current technical mitigation systems. The authors reported that the detection of employee online malevolence involves one of or a combination of the following forensic mechanisms: the monitoring of system call activity, linguistic analytic software, tracking of business processes by logging anomalies.

Gritzalis et al. (2014b) suggested that online monitoring allows organizations to develop shared patterns of employee usage to help determine when a deviation from normal behavior should trigger and issue alerts. Other studies on cyberloafing mitigation argue that technical mechanisms for monitoring employee Internet use only help deter cyberloafing through active enforcement (Sanders et al., 2013; Ugrin & Pearson, 2013). These studies suggest that technical strategies used to monitor Internet browsing, emails, and social network use are effective methods for tracking cyberloafing but require non-technical methods to enforce sanctions.

Similarly, Gritzalis, Kandias, Stavrou, and Mitrou (2014a) noted that Open Source Intelligence Techniques (OSINT) allow for the profiling of individual consumers

for advertisement without consent and could enable the prediction of different malevolent online behavior potentially catastrophic for a business organization. Again, the authors described how technical solutions, by themselves, do not mitigate malevolent online activity and recommended combining technical solution with managerial control. In contrast, studies focused on employee privacy issues and balancing work and non-work obligations, argue that technical deterrence mechanisms are counter-productive, violate employee privacy, and foster employee mistrust and disengagement (König & de la Guardia, 2014; Rokka, Karlsson, & Tienari, 2014).

König and de la Guardia's (2014) study on the personal use of Internet during work found that predominantly, private, and personal demands drive cyberloafing activity, and most individuals can balance work and non-work-related obligations. Studies with a discrepant view about technical deterrence of cyberloafing suggest that the current trends in employee online technology use require more of non-technical solutions rather than technical solutions.

Accessing social networking sites and browsing during work using company resources or personal devices represents a contentious area in the ongoing debate on cyberloafing. The increasing acceptance of the use of social networking by corporations globally further complicates the establishment of clear-cut boundaries on online technology use requiring changes to existing Internet access policies and guidelines. Bekkers, Edwards and de Kool (2013) explored the effects of Internet monitoring and

social media monitoring using technical tools to track, monitor, and detect deviant online behavior.

The author described the use of keywords fed into software programs that could either surveil social network sites for location and specific communication on social media or steer the software to search social networks for keywords. Bekkers et al. (2013) argued that the notion held by the public organizations examined in the study, that monitoring of individual social networking sites that is publicly accessible, still raises questions about ethics and privacy. Klemchuk and Desai (2014) examined a federal court case involving an employer's monitoring of an employee's social networking use to ascertain the extent of employee use of social media coverage under the Electronic Communications Privacy Act. The takeaway from the court ruling indicated that any unauthorized access by an employer to private employee social network content is illegitimate.

Managing the components of monitoring software infrastructure requires constant upgrading and the limitations relating to the control of personal employee smartphone devices connected to corporate networks presents unique challenges for organizations and their managers (Ali, 2013). Most researchers on cyberloafing agree that not all cyberloafing detrimental and the need for proactive cyberloafing intervention strategies. Research on technical mitigation efforts acknowledge the rising concerns about privacy and legitimacy issues related to the technical surveillance of employees (Moussa, 2015).

Non-technical Deterrence Mechanisms

Klotz and Buckley (2013) posited that the increasing immersion of online technologies into job roles, as well as the consumerization of smartphones, necessitates the need for a shift in the managerial categorization of cyberloafing as deviant behavior. Other researchers insinuate that age, gender, marital status, and level of education significantly affect individual levels of cyberloafing (Andreassen et al., 2014; Niaei, Peidaei, & Nasiripour, 2014; Coker, 2013). Also, honesty and procrastination constitute major predictors of cyberloafing while engagement and employee emotional stability moderate cyberloafing behavior providing managers with appropriate queues for managing subordinates (O'Neill, Hambley, & Chatellier, 2014; Kim, del Carmen Triana, Chung, & Oh, 2015).

According to Ratnamalala and Marett (2014), non-technical tools serve as a means of governing the security of organizational information systems used by employees. It is noteworthy that employee awareness of technical monitoring increases the likelihood of compliance with non-technical mechanisms and validation for the use of non-technical methods for combating cyberloafing derives from use and implementation of technical tools (Shepherd et al., 2014). As part of the non-technical tools used by organizations, cyberloafing mitigation policies allow organizations to define acceptable use of information and communication technologies at the workplace and help steer employees toward productive use.

Shepherd et al. (2014) described non-technical deterrence mechanisms as processes involving the planning, compliance, and enforcement of online technology usage policies, as well as the use of employee education, training, and awareness programs. Some of the first depictions of cyberloafing mitigation policies by (Gaskin, 1998) suggested that the policies serve to protect organizations from malevolent online employee activity and enhance the alignment of employee Internet usage with business processes and organizational objectives. Similarly, information security policies aim to safeguard the information resources of an organization and define the strategic direction of the entire organization regarding the management of information, employee conduct, infrastructure security measures, processes, and responsibilities, as well as information on the handling of violations (Peltier, 2001).

Validation for the use of non-technical methods for combating cyberloafing derives from the narrow focus on the use of technical strategies and policies (Shepherd, et al., 2014). Goel, Hart, Junglas, and Ives (2016) suggested that by influencing individual recognition of acceptable Internet usage, organizations have an opportunity to improve the security of their systems. Information security policies provide detailed descriptions of employee responsibilities and outline specific roles of employees about the protection of an organization's information resources and assets.

Barlow, Warkentin, Ormond, and Dennis (2013) reported that the communication and training of employees on the sanctioning of cyberloafing is persuasive and reduces employee intention to violate mitigation policies. The study shows how middle managers

could play a significant role in the implementation of non-technical mechanisms that contribute to the mitigation of employee cyberloafing through training and direct communication. Hassan et al. (2015) reinforced the notion that the intention to commit cyberloafing diminishes with active detection mechanisms, sanctions, and history of past enforcement.

Hassan et al in an examination of cyberloafing mitigation policies implementation, enforcement, and punishment at an organization in Iran, the results indicated that the fear of severe sanctions mitigated employee intentions to cyberloaf provided technical mechanisms were in place to monitor employees and stories of past retribution were commonplace. Kura, Shamsudin, and Chauhan (2015) examined the effects of factors relating to punishment certainty and punishment severity on deviant workplace behavior and found a negative correlation between punishment certainty and punishment severity with deviant workplace behavior.

The study validates the proposition that situation where employees perceive the certainty or severity of punishment for workplace deviance, the likelihood of engaging in such activity diminishes. Rahimnia and Mazidi (2015) described the conditions when employees could conceal cyberloafing behavior and suggested that a manager's close propinquity, considered a form of monitoring presence, combined with technical control serves as a useful cyberloafing mitigation technique provided a fear of formal punishment exists. Managerial control of behavior involves the use of strategies designed to ensure employee behaviors are largely in consonance with the goals of the organization, and

some cases are responsible for enforcing sanctions and punishments. In a study of managers at a public service organization in Pakistan, Manzoor, Arif, and Hassan (2015) found that managerial capacity building interventions fostered improvements in employee emotional intelligence and the reduction of counterproductive behaviors at the workplace.

In contrast, Zoghbi Manrique de Lara, Verano Tacoronte, and Ting Ding (2006) indicated that managerial proximity increased employee of cyberloafing perceptions about control reducing cyberloafing and increasing fear of sanctioning which increased cyberloafing behavior. Understanding the middle manager's role in employee cyberloafing mitigation based on the social interactions and proximity between supervisor and employee provides organizations with useful information that could enhance employee performance. According to Kolkowska and Dhillon (2013), the lacking compliance with information security and usage policies stems from the failure of existing policies to capture the emergence of new technologies as well as user resistance to the policies.

The study examined power relations within a public organization to gain an understanding of the effects on information security policy compliance. Kolkowska and Dhillon found that new policies implementation required strategic change and organization structure change, caused value conflicts, and required management engagement and employee mobilization to enhance effectiveness. Cyberloafing mitigation policies must be adaptive to the rapidly changing information technology

environment. Also, the proximity of managers to employees requires awareness and sensitivity to recognize the emergence and frequent use of new technologies by employees that can circumvent blocking software. Again, Rahimnia and Mazidi (2015) validated the importance of the managerial role in the management of employee cyberloafing by noting that managerial proximity enhances opportunities for supervisory communication with employee behavioral control.

In an investigation of the effects of leadership opinions and support of information systems security policies, Ifinedo (2016) argued that the active engagement of leadership in implementing, promoting, and enforcing policies, rather than delegating to other departments, entrenches a climate of effective sanctioning and punishment. This study validates the importance of the managerial role in the instigation of compliance with organizational policies aimed at mitigating the efficient use of information and communication technologies at the workplace. Aurigemma (2013) argued that notwithstanding the widespread use of information security policies, violations remain commonplace costing organizations in the US billions of dollars each year.

The author described the employee, considered a human agent, as the weakest link in the information security system within organizations. Aurigemma suggested that the lack of user compliance, manager engagement in policy enforcement, and manager adaptation to the rapid technology advancements impedes the effectiveness of cyberloafing mitigation policies within organizations. A new trend and fast growing development within business organizations involve the inclusion of a bring-your-own-

device policy. Leclercq-Vandelannoitte (2015) suggested that to capitalize on the consumerization of smartphone technology and enhance employee performance, business organizations are incorporating user-driven changes to their information systems and usage policies.

The author used a case study methodology to examine four different situations involving employees' introduction of personal devices to perform work tasks to gain an understanding of the adoption process, usage conditions, and organizational changes required. The findings seemed to suggest that the risk factors such as the loss of data and increased security vulnerabilities associated with the bring-your-own-device policy outweighed the advantages related to enhancing employee performance. Other studies like (Rose, 2013) argued that hidden costs, complexities related to operating systems and carrier differences, and the concerns of data leaks, theft, and compliance constitute a significant disincentive for organizations to bring-your-own-device policies.

Le (2015) described how organizations had developed new security infrastructures that allow employees to use personal devices on organizational platforms with widespread usage across a broad range of industries. Also, the study suggested that the security breaches online were attributable to issues related to employee behavior rather than the security of the technology used, debunking the notion that the bring-your-own-device policies were risky. According to Keyes (2013a), approximately 70% of organizations in the United States have adopted bring-your-own-device policies with effective cost controls that allow for the secure use of employee personal devices. Keyes

(2013a) noted that through the assignment of security responsibilities by senior management to various elements responsible for the management of security programs, security vulnerabilities arise due to the failure of assurance and compliance units.

The underlying benefit for organizations centers on employee satisfaction which in turn translates into the improved productivity of the organization. From a non-technical deterrence perspective, the effectiveness of the adoption of the bring-your-own-device policy requires the active enforcement of device usage agreements, security related training, what constitutes violations and the associated sanctions. Interestingly, Jandaghi et al. (2015) noted the implausibility of eliminating employee cyberloafing activities. Most organization rely on human resources managers and information technology managers to control the implementation of the technical and non-technical deterrence mechanisms within the organization (Gunia et al., 2014; Polzer-Debruyne, 2014).

In a study on the Van Gramberg, Teicher, and O'Rourke (2014) argued that the management of electronic communications policy development rests on the shoulders of the human resources function because of its dual responsibility acting as a champion for employees and strategic partner for the employer. The study examined contemporary research on human resource management and court case relating to the management of electronic employee communication in Australia. Van Gramberg et al. (2014) study described difficulties experienced by human resources managers struggling to balance competing employer and employee interests. The authors noted undermining effects of

cyberloafing technical control mechanisms that negate employee trust in the organization and employee perceptions about the human resources efforts aimed at helping employees manage work and non-work-related electronic communication at work.

The study reported that the human resources function is responsible for the investigation of violations and the processes resulting in employee sanctioning and punishment. According to Soomro, Shah, and Ahmed (2016), the management of information security systems within the organization is the responsibility of top management and the technical activities fall into two categories: technical and managerial. Information technology managers are responsible for providing technical solutions that enhance the security and integrity of the organization's online technology infrastructure, its monitoring systems, business processes, and its information and data storage.

Over 80% of business organization implemented online technology usage policies, however, the widespread misuse of online technology by employees continues to persist questioning the effectiveness and enforcement of the policies (Li, Sarathy, Zhang, & Luo, 2014; Young, 2010). Doherty, Anastasakis, and Fulford (2011) argued that acceptable online technology usage policies focused mainly on proving protections for organizations rather than educating employees on acceptable usage.

Implementation issues relating to the challenges associated with finding the right balance between employee online technology usage rights and organizational needs for productivity and liability have affected the potency of acceptable usage policies (Cox,

Goette, & Young, 2005). Ernest Chang and Ho (2006) found that managerial competency, unpredictability at the workplace, the size of the organization, and the industry influenced the implementation of usage policies. This study was designed to explore the role middle managers play in the mitigation of employee cyberloafing and could shed some light on the implementation of online technology usage policies within organizations.

Middle Managers and the Management of Employee Cyberloafing

Online technologies continue to transform the lives of individuals requiring increasing levels of incorporation into the day to day functioning (Melrose et al., 2016). According to Campbell et al. (2016), middle managers have contractual and legal obligations to not only guard the interests of their employers but also to control employees under supervision. Also, middle managers contribute to ensuring subordinate employees perform their roles by using control mechanisms and manipulating social interactions to drive performance (Harding et al., 2014).

Grossenbacher-Fabsits's (2011) findings indicated that non-work related use by employees was considered acceptable to male managers in so far as the usage is limited to sites considered acceptable within reasonable time limits. Indeed, cyberloafing employee behaviors and organizational strategies to mitigate non-work-related Internet usage vary across industries and organization type. According to Kim and Byrne (2011), most organizations have replaced personal communication processes with Internet-based communication creating more opportunity for Internet abuse.

Theoretically, Grossenbacher-Fabsits (2011) uses a subjective approach to identify patterns and themes based on a dynamic view of human behavior from the lived experiences of the participants. For example, 20 middle managers at a manufacturing organization provided the researcher with multiple realities of the cyberloafing phenomenon being investigated. From the resulting information collected, themes were developed that centered mainly on time spent on the Internet, unacceptable and acceptable Internet use, Internet abuse, personal communication versus online communication, and Internet addiction.

Other studies like Holguin (2016) have attempted to highlight the distinctive behavior control techniques employed by middle managers in control of employee cyberloafing. Unlike Holguin, Pînzaru and Mitan, (2016) examined more specific managerial strategies used to supervise digital natives. Similarly, studies like Manzoor et al. (2015) explored managerial strategies for developing employee capacity to improve emotional intelligence and reduce cyberloafing.

Toegel, Kilduff, and Anand (2013) found that middle managers actively monitored and employee instinctive feelings making it easy to identify situations when employees needed help or an intervention. Extant cyberloafing research has not treated the significance of the manager role in managing employee cyberloafing in much detail. Rather, the research to date has tended to focus on strategies managers use instead of the meaning managers ascribe to their role and how it influences the development of effective strategies in support of the overall organizations mitigation efforts.

Middle managers play a pivotal role driving team performance (Liao et al., 2009), therefore, understanding middle manager thoughts and beliefs about their roles in cyberloafing mitigation influences effective strategy development and implementation is invaluable. The gap between the managerial meaning ascribed to the role in the mitigation efforts and the effects such an understanding places on the development of tactical solutions could provide organizations with useful information to enhance the reduction of employee cyberloafing.

Summary and Conclusions

The gap between evidence of the effectiveness of detection mechanisms and the enforcement of cyberloafing mitigation policies may be due to poor supervision of online technology use. Middle managers play a significant role in enhancing the performance of teams under their supervision. Middle managers in extant cyberloafing research have received little attention, yet they might play a vital role in the management of employee cyberloafing behaviors and activities. Few studies have focused on the adequacy and effectiveness of the strategies used by middle managers aimed at mitigating the different typologies of employee cyberloafing.

This study specifically aimed at exploring middle manager roles during the implementation of cyberloafing mitigation policies and combating subordinate cyberloafing. Chapter 2 presented the significant findings related to the relevant literature reviewed. Also, I provided a direct linkage between the problem statement and the theoretical framework. The prior research literature on cyberloafing has not examined the

role of middle-level management in the implementation of cyberloafing mitigation policies and combating employee cyberloafing despite their close connections with employee's that engage in such behavior.

This chapter offered a summary of significant literature associated with the organizational management of employee cyberloafing. The literature review provided ample information on the following topics; organizational management of employee cyberloafing, neutralization techniques for mitigating employee cyberloafing, and the technical and non-technical strategies for combating cyberloafing. The chapter made a connection between the research problem, the theoretical foundation, and conceptual framework used in the study. The chapter offered the reasoning for using a social constructivist-interpretive conceptual framework that draws from adaptive structuration theory and symbolic interaction theory. In the third chapter, I will discuss the research design of the overall study and provide the reasoning behind the selected design approach, the role of the researcher, the participant selection process, the data collection, instrumentation, and management processes, and the data analysis plan.

Chapter 3: Research Method

In this study, I conducted exploratory research on the role of middle managers in the mitigation of employee cyberloafing within a digital workplace to gain an understanding of the meaning participants ascribed to their role and provided a clear outcome based on the researcher's inductive analysis, as suggested by Merriam (2002). The purpose of this study was to explore the perceptions and lived experiences of middle managers and their role in the mitigation of employee cyberloafing. Middle managers have direct responsibility for driving employee performance and are near subordinate employees and, therefore, can offer a perspicuous elucidation of their organizational role in the mitigation of cyberloafing behavior. Gaining a different worldview on the perceptions and experiences of middle managers in the reduction of employee cyberloafing is important.

The brainchild for this research stemmed from the inability to find research literature on employee cyberloafing mitigation from a middle manager's perspective as noted in Chapter 2. To address the goals of this study, I developed a qualitative research strategy that buttressed the descriptive essence of the research. Also, I adopted a phenomenological approach to allow for the description of one aspect of human experience not bounded by time or location using first person sources. In Chapter 3, I discuss the research design of the overall study. I also describe the rationale for the study design; my role as the researcher; the participant selection process; the data collection, instrumentation, and management processes; and the data analysis plan.

Research Design and Rationale

Social interactions between employees and supervisors, as well as the employee structuring of online technology use, informed the chosen research design. The central research question for this phenomenological research study was: What are the lived experiences of middle managers who have mitigated employee cyberloafing in a digital workplace? The central research question for this study was conceived to capture the perspectives, experiences, and knowledge of participants involved with the study on the scope of the issue.

Additional sub-questions aimed to establish the following: first, whether the social interactions and proximity between supervisors and employees within organizations influenced the middle manager's capacity to control employee cyberloafing activity; and second, whether an understanding of the way employees structure their appropriation of information and communication technologies affects the managerial control of employee cyberloafing. Cyberloafing activity involves the use of computers and smart mobile devices at work for non-work-related activity by employees not working remotely with a prevalence contributing to organizational losses in productivity in today's highly competitive marketplace.

The central concepts underlying this study focused on the interactive relationship between supervisors and employees and the social premises surrounding employee use of information and communication technologies that shape managerial control mechanisms and policy implementation. Symbolic interaction theory offered an explanation why

humans act based on the meaning developed from individual analysis and interpretation of social behavior and interactions within society. Adaptive structuration theory offered a viable alternative for understanding the adverse use of information and communication technologies within organizations. I selected a qualitative research approach for this study to explore the central issue surrounding the middle manager's role in the mitigation of employee cyberloafing.

Qualitative Approach

For this study, the qualitative approach served as the primary method of the inquiry since it offered an efficient way of uncovering the mental impression humans have about an issue. The use of qualitative research is a well-established practice in investigations about how groups ruminate and understand their role in a broad range of workplace-related issues. According to Khan (2014), qualitative research methods offer a holistic framework that allows for an in-depth exploration of complex issues related to human behavior, human perception, and lived experience. Quantitative measures do not usefully enable the researcher to acquire a realistic view of participants lived experiences and provide a comprehensive description of the issue under investigation.

The biggest problem with using a quantitative research method for this inquiry centered on its focus on determining the association between variables in a population, uncovering the disposition of the variables, and making justifications about knowledge. Another disadvantage of using a quantitative method was that it relied on the use of structured instrumentation for data collection with a dependence on objective processes

rather than subjective methods that allow for a better comprehension of the world around us. The focus of this study centered on exploring the perceptions and lived experience of participants with expertise mitigating employee cyberloafing and required the use of flexible and non-manipulative data collection processes. Bendassolli (2013) posited that the techniques used to validate knowledge in qualitative research involve either using logic to make sense of the ideas presented or by learning from experience about factual occurrences.

Phenomenological Method

Qualitative research studies employ a variety of data collection methods that include: in-depth interviews, surveys, focus groups, social media postings, direct observation, and document analysis (Patton, 2014). Before selecting the phenomenological method as the best-suited approach for this study, I was mindful to consider other research approaches outside the traditional qualitative research methods. Percy, Kostere, and Kostere (2015) showed that generic qualitative research methods could serve as viable options in situations where the research topic does not adapt well to the conventional qualitative research methods.

In considering the phenomenological approaches suitability for topics investigating attitudes, beliefs to name a few, Percy et al. (2015), argued that the researcher's concern must focus on the internal rather than external dimensions of cognitive processes surrounding the experience under investigation; otherwise, a generic qualitative method would suit the topic better. A serious weakness of this argument was

the rigid focus on the internal dimensions of cognitive processes mitigates openness and evocation because of the dichotomy between consciousness and cognition.

Zeroing only on the internal cognitive processes during a phenomenological study could create issues related to subjective mental content where individuals make subjective meaning based on external attributions or subjective experiences. As noted in Küpers (2014), phenomenological inquiry requires openness and evocation as it scrutinizes the preeminence of intuitive understanding. D'Angelo, Milliken, Jiménez, and Lupiáñez (2013) listed two categorizations for human attention: the slower controlled processing and the fast and spontaneous, automatic processing.

D'Angelo et al. (2013) highlighted the importance of recognizing the occurrence of situational processes while humans acquire sequential knowledge about a phenomenon. For this study, it is noteworthy that the situational context within which potential participants gained knowledge about their experiences could fall into either category. This study was not seeking to uncover shared different experiences derived from the human interaction of participants, a mainstay of descriptive qualitative research, rather, the study aimed to disclose human experience derived from consciousness (Willis, Sullivan-Bolyai, Knafl, & Zichi-Cohen, 2016).

The appearance of a subject in the consciousness of a human being underpins the phenomenological approach to qualitative inquiry. According to Eddles-Hirsch (2015), preconditions of human experience include noema (knowledge that is objective) and noesis (knowledge that is subjective). Determining the best-suited approach for this study

involved an iterative process that considered the conventional qualitative research methods (e.g., case study, ethnography, and grounded theory). The phenomenological approach was selected to enable the description of one aspect of human experience not bounded by time or location using first person sources. Phenomenological qualitative research consists of two methods of inquiry, hermeneutical and transcendental.

Hermeneutical phenomenology requires reflective interpretation of participant's subjective experiences to unravel the objective nature of the issue under investigation (Van Manen, 1990). For this study, the transcendental phenomenological method, an initially developed form of phenomenology that seeks to discover only the described and lived experiences of the participant, was adopted to unravel the true meaning ascribed by participants to their human experience (Moustakas, 1994). Through this qualitative phenomenological method, middle managers with expertise controlling employee cyberloafing provided genuine and individual essences ascribed to their participation in the cyberloafing mitigation effort.

Role of the Researcher

The researcher was the primary instrument used to collect and analyze data with a focus on understanding the participant's perceptions on the issue under investigation. Also, the role of the researcher entailed identifying own assumptions and biases before the data collection process began. I had some familiarity with the employee cyberloafing phenomenon at the workplace having observed first-hand employee personal Internet-related activity during work hours, and on one occasion, I collaborated with management

in mitigation efforts. To place the research approach for this study within a cluster of personal, competency and social values, I described my professional background.

I work in higher education and have prior leadership and management experience. I served in Nigerian Air Force as an Air Traffic Control instructor responsible for training military air traffic control officers, developmental military air traffic control assistants, and licensed military air traffic controllers. I believe that my experiences enhanced objectivity and sensitivity to issues under investigation enabling me to set aside own bias while remaining open to constructive criticism of others and differing opinions. I selected the face-to-face interviewing technique as the preferred data collection method because of the advantage of synchronous communication and social cues (verbal or non-verbal indicators).

According to Opendakker (2006), the distinctive nature of synchronous communication in time and place enables the advantage of social cues like body language, facial expression, voice pitch, and tone, etc. The signals participants send through social cues allowed me to extract additional information from non-verbal communication about participant's real perceptions about the issue in situations where verbal communication proved inadequate. I documented all details collected from non-verbal communication in a log during the face-to-face interviews. For the planned meetings, I conducted semistructured interviews using an audiotape recorder and an open-ended question type format. A backup audio tape recorder was available in case of a device failure involving the first audio tape recorder.

Lastly, as a beginner in qualitative research, I understood the potential shortcomings and barriers associated with my role as a researcher and incorporated steps during the design of the research methodology to improve the quality of data collection and analysis.

Methodology

Participant Selection Logic

The population of interest for this study included all middle managers with experience managing employee cyberloafing and employed at higher education institutions in Florida. During the design stages of this research study, I developed a sampling strategy that included a possible sampling frame. The sampling frame developed draws from the criterion-based sampling technique. The compelling reasoning for the choice of a criterion-based sampling method is because it allows for the selection of cases based on relevant and predetermined criteria. The goal of this study was to examine the role of middle managers with experience mitigating employee cyberloafing which is a predetermined criterion for the selection of participants. Patton (2014) suggested that criterion sampling allows for the identification of cases with experience on the issue using standardized questionnaires initially and following up with in-depth interviewing.

Instrumentation

The purpose of phenomenological data collection technique was to evoke participant's description of lived experience of the phenomenon and presenting the data

without adding or making inferences and generalizations. In conformity with the principles of phenomenological inquiry, and to ensure the accuracy of data, I discounted any preconceptions or suppositions about the phenomenon. Epoché, an essential element of the phenomenological inquiry technique, requires the adoption of a researcher attitude that sets aside all preconceptions about the phenomenon (Berdychevsky & Gibson, 2015; Moustakas, 1994).

The epoché process involved placing all suppositions about the phenomenon in a state of dormancy to create a new, receptive, and open consciousness of mind aligned with the essences of participant experiences (Berdychevsky & Gibson, 2015; Moustakas, 1994). Interviewing represents an essential element of data collection methods used in qualitative inquiry and more generally in the social sciences (Patton, 2014). Also, the focal point of phenomenological interviewing centers on participant's experiences and the meaning ascribed to the experiences (Seidman, 2013). For this study, I employed mainly face-to-face interviews with a semistructured interview format, a digital audio recording device, and open-ended questions.

Face-to-face interviewing served to capture the voice of the participant about the phenomenon in person together with any elements nonverbal communication like tone, facial expression, and gestures. Onwuegbuzie and Byers (2014) highlighted the importance of using nonverbal communication data to strengthen the description and interpretation research process. I offered participants unable to meet face-to-face the option for a telephone interview.

The semistructured interview format provided a flexible questioning format and enhanced interviewee freedom of expression about perceptions and experiences with the phenomenon (Patton, 2014). During the interview process and after obtaining the consent of each interviewee, I used a digital audio recording device to capture all conversations. The audio recording captured nonverbal communication and provided verbatim summaries of the interview conversation useful during data analysis (Given, 2008; Gubrium, Holstein, & Marvasti, 2012).

Also, I incorporated interview journaling to support the interview method and help improve the quality of research analysis. Reflective journaling helped add clarity and accountability while reducing the complexity associated with the examination of recorded responses about a participant's experiences (Janesick, 2011). Participants for this study included middle managers chosen from higher education institutions in Florida with experience managing employee cyberloafing behavior. The data collection technique adopted involved face-to-face interviews conducted using a semistructured interview format to understand the ascribed meaning middle managers have about their role in mitigating employee cyberloafing in a digital workplace.

Preset open-ended questions guided the semistructured interviews with latitude to probe deeper eliciting clarity of responses about the phenomenon (Doody & Noonan, 2013; Moustakas, 1994).

Procedures for Recruitment, Participation, and Data Collection

The recruitment strategy developed for this study involved an initial participant screening process for Florida-based participants using listings from management groups on LinkedIn.com. The identification of qualified candidates involved pre-screening processes from LinkedIn.com. After pre-screening potential candidates, I sent a LinkedIn InMail invitation soliciting participation in the study and a willingness candidly to share lived experiences of the phenomenon (see Appendix A).

Lunnay, Borlagdan, McNaughton, and Ward (2014) noted that social media is increasingly facilitating the mutuality of information sharing, rapport building, participant engagement, and scheduling interviews for qualitative researchers. To make each interviewee feel as comfortable as possible, the interviewer explained the objective of the study and emphasized the steps taken to ensure confidentiality. Participant eligibility criteria specified that potential participants hold a middle management position responsible for supervising, developing, and coaching subordinate employees (see Appendix C).

Also, I required that potential candidates have experience mitigating employee cyberloafing and hold current employment with a higher education institution in Florida. After receiving responses from potential participants indicating a willingness to participate, a brief questionnaire was emailed together with the informed consent form. All participants submitted an informed consent form before the data collection process began. I offered adequate recourse for participants to opt out of the study at any time to

ensure that participants felt comfortable with the data collection process. During my pre-screening process of potential participants, I considered the degree of homogeneity of possible candidates before making my selection. After completing the pre-screening process,

I conducted a final follow-up telephone conversation with potential participants to finalize the selection process for each participant. Sample sizing for this study relied on the data saturation concept to help identify the point during data collection when no new information emerged. Patton (2014) discussed the challenges and strategies for practical and purposeful sampling and suggested specifying a minimum sample size during the design phase allowing for the flexibility due to the emergent nature of the data generation. Polkinghorne (1989) noted that determining commonality from among qualitative research participants requires the collection of data based on the experiences of between 5 and 25 participants.

Cleary, Horsfall, and Hayter (2014) stated that the most typical sample size for qualitative research is 20, but the actual relevant data usually originates from about one-half of the sample. Notwithstanding the option to interview a maximum of 25 participants, I chose to use a minimum sample of 15 participants. Patton (2014) suggested documenting evidence of data saturation during research situations with sample size predicated on reaching saturation point.

Data Analysis Plan

The aim of the data analysis plan for this study was to develop analytical outputs about the factors influencing how middle managers feel about their role mitigating employee cyberloafing and what helps them achieve positive outcomes. Data analysis procedures for this study drew from the modified Van Kaam method outlined in Moustakas (1994) with the researcher employing hand coding for analysis and the NVivo 11 Pro software for software coding, data management, and data storage. The modified Van Kaam method was particularly useful for qualitative phenomenological data analysis because the approach emphasized a revisitation of an individual's encounter with the phenomenon before securing descriptions used in portraying the essence of the experience (Moustakas, 1994).

Previous studies based their criteria for using the modified Van Kaam method because it involved grouping, reducing, thematizing, and identifying logical units of information. The modified Van Kaam's method required three core processes to facilitate the unraveling of knowledge that includes: epoché, transcendental phenomenological reduction, and imaginative variation (Moustakas, 1994). Collectively, the core processes involved deliberate actions suspending judgments about the world to collate true essences about the phenomenon based on participant descriptions, and different thematic variations about the phenomenon.

The key aspects of the analysis process involved: (1) listing and grouping all relevant participant responses; (2) determining unchanging elements of each participant's

responses; (3) grouping and labeling immutable elements of participant responses; (4) validating unchanging elements and theme development; (5) developing individual/textural descriptions using transcendental phenomenological reduction; (6) developing textural/structural descriptions of meaning participants ascribed to their experiences using imaginative variation; and (7) developing composite description of meaning participants as a whole group attribute to their experiences.

Hilal and Alabri (2013) reported that making sense of text-rich qualitative research data involves laborious processes during the manual ordering and structuring of the data. For this study, I conducted an original coding scheme that connects different terms and data units purposefully sorted out of the large text-based qualitative data. Coding processes associated with qualitative research included combining both a manual hand-coding and NVivo 11 Pro software coding techniques. This study employed the manual hand-coding method during data reduction to comb through all units of the information gathered and avoid omitting important information and used the software coding as an auditing process. Maxwell (2013) highlighted the importance of reading and understanding the different groups of data collected during qualitative data analysis.

Issues of Trustworthiness

Credibility

In qualitative research, establishing credibility requires believable results in the judgment of research participants. Elo, Kääriäinen, Kanste, Pölkki, Utriainen, and Kyngäs (2014) maintained that flawed data collection methods, conceptual frameworks,

and description of results adversely affect a study's trustworthiness. For this study, I focused on enhancing credibility by ensuring data triangulation through the following processes: data collection from participants in a digital workplace; using different data types that include interview transcripts, interview journaling, and the documented details of the modified Van Kaam method used for data analysis. Patton (2014) asserted that credibility in qualitative research hinges on researcher competency, attention to detail, and corroboration of evidence from different sources with appropriate levels of engagement, observation, and open auditing.

Participants for the study included middle managers with experience managing employee cyberloafing in a digital workplace setting allowing me to draw multiple views of the issue. The different types of data collected contributed to the accuracy of the data collected by eliminating the possibility of misrepresentation. By providing detailed documentation of the three core processes that facilitate the unraveling of knowledge using the modified Van Kaam method for data analysis indicates transparency and enhances credibility.

Transferability

Contemporary research on employee cyberloafing mitigation has not investigated the middle manager role in the prevention, enforcement, and rehabilitation of employee cyberloafing activities. The primary focus of this study centered on the role of middle managers mitigating employee cyberloafing which is a predetermined criterion for the selection of participants. The population of interest for this study included all middle

managers managing employee cyberloafing and working at organizations with digital work environments. I recruited participants by soliciting individuals identified on LinkedIn.com.

To enhance transferability, I provided a thorough description of the context of and setting for the research study. In an examination of the transferability of the investigation, Burchett, Mayhew, Lavis, and Dobrow (2013) found that researchers considered results, methodology, and design as insignificant while setting, researcher experience, the simplicity of application, and adaptation of methods were significant considerations for transferability. Researchers seeking to transfer this study's results would need to make a personal judgment decision about the applicability of the results to the needs of his/her research.

Dependability

Establishing dependability in qualitative research requires the researcher to ensure the application of consistent and stable processes throughout the entire study. I selected the criterion-based sampling method to increase the reliability of measures and provide the appropriate selection of respondents. Face-to-face interviews conducted using a semistructured interview format, a digital audio recording device, and open-ended questions enhanced the capturing of real and lived presuppositions through synchronous communication. I provided an audit trail with member checking procedures and described methodological coherence for the study. Audit trailing provided detailed records of the entire study from the research development stages up to the presentation of investigation

results. Member checking procedures offered details of the steps taken during data collection to allow participants clarify responses to avoid misrepresentation.

Methodological coherence involves ensuring congruity between the research questions and the different elements of the data gathering and analysis process. Aust, Diedenhofen, Ullrich, and Musch (2013) reported that scrutinizing the seriousness of participant responses allows the researcher to check for consistent and plausible answers during data collection. The appropriateness of sample sizing used in this study fostered the sufficiency and completeness of data collected on the phenomenon. Finally, I incorporated theoretical balancing to reflect on helpful ways to conceptualize the research problem thereby enhancing dependability.

Confirmability

Confirmability in qualitative research requires adequate provision for ensuring that the results are confirmable and can be corroborated by others. Baskerville (2014) described confirmability as a verification process requiring the appropriate documentation of the different steps of the inquiry from the knowledge development phase up to the research completion stage. For this study, I followed diligently the steps outlined in the research design and documented all decision-making processes during the study. Concurrent data collection and analysis during the study fostered iterative processes connecting the technical steps used to investigate the issue with the underlying conceptualizations. To establish congruence of procedures used for data collection and

analysis, the initial interviews and a reflective journal allowed me to check and recheck emerging themes and ideas with participants.

Ethical Procedures

For this study, safeguards guided the data collection process to prevent the hampering of participant rights, values, and needs. I paid close attention to my responsibility as a researcher to ensure the adequacy of ethical consideration during research processes involving the soliciting of participation, establishing protections to prevent harming participants, and treating data with confidentiality and anonymity. To ensure that no legal or ethical issues surround the data collection processes, the first step of the ethical procedures established for the study involved gaining permission from the Walden University Institutional Review Board (IRB approval number 02-27-17-0435968) to ensure compliance with institutional and federal regulations.

Agreements to Gain Access to Participants

Jones (2014) noted some important considerations about handling gatekeeping controls when attempting to access participants. The authors specifically highlighted the barriers and challenges during the processes aimed at gaining participant access and obtaining participant consent. In line with Jones suggestions, participant selection for this study employed a well-structured selection strategy via social networks. Potential participants for this study received impersonal email invitations soliciting participation and a readiness to share their experiences truthfully reducing the cyberloafing activity within their organization.

The first step used to gain access to participants involved the development of an email aimed at soliciting participation in the study (see Appendix A). To prompt potential participants after sending the first email with no response, I developed a second follow up email soliciting participation (see Appendix B). This study took steps to document participant access and discussions about consent during the different stages of the inquiry. A dedicated email address (managencyberloafingstudy@gmail.com) was created for all email communications between researcher and respondents.

Treatment of Participants

Qualitative research entails a greater role for the participant-researcher relationship and the use of more intrusive and personal approaches during the inquiry. The treatment of participants during research creates specific responsibilities for the researcher. The responsibilities center on ensuring voluntary participation, obtaining informed consent, and guaranteeing participant confidentiality and anonymity. I conducted myself in a professional manner emphasizing the option for participants experiencing any difficulty to stop the inquiry and opt out at any time. Fairness during participant selection and other aspects of the study was a significant characteristic of the study. The telephone interviewing option served as an alternative method to the preferred face-to-face interviewing method in anticipation of any participants unable to meet in person.

Treatment of Data

My professional training as a manager, employee and trainer allowed me to set boundaries during interactions with participants while gaining an understanding of their personal experiences related to the issue under investigation. Jones (2014) suggested that role researcher must be grounded in self-regulation concerning establishing standards of ethical behavior. For this study, I was unfamiliar with participants and did not need to disclosed familiarity with the subject or explain the need to set aside any presuppositions during the data collection process. I used a combination of manual and electronic data management systems like notepads and audio recording devices. More specifically, the NVivo 11 Pro software program served as the primary repository for the analyzed data. An email address was created and dedicated for all email communication with participants.

Summary

This study was designed to uncover managerial role experiences about the mitigation of cyberloafing. The direct responsibility for driving employee performance rests on the shoulders of middle managers and, therefore, can offer a clear description of their role in cyberloafing mitigation. Gaining a different worldview on the perceptions of middle managers is important. To validate the choice of qualitative research strategy used for this study, Chapter 3 discussed the research design of the overall study with the rationale for the design, the role of the researcher, the participant selection process, the data collection, the instrumentation, the data management processes, and the data analysis

plan. In Chapter 4, I discussed the research setting, participant demographics, participant recruitment, data collection, data analysis process, strategies for ensuring trustworthiness and ended with a summary of the findings.

Chapter 4: Results

The purpose of this study was to explore the perceptions and lived experiences of middle managers and their role in the mitigation of employee cyberloafing at work. With the pervasiveness of employee cyberloafing, understanding the role middle managers play in the overall organizational mitigation efforts fills a gap in contemporary research on cyberloafing mitigation. I adopted a qualitative research approach as the primary method of the inquiry to uncover the mental impressions of participants about the issue.

The central research question for this phenomenological research study was: What are the lived experiences of middle managers about their role in the mitigation of employee cyberloafing at higher education institutions in Florida? Chapter 4 offers a description of the research setting, participant demographics, participant recruitment, data collection, data analysis process, and the strategies for ensuring trustworthiness. The chapter ends with a summary of the results and main findings, as well as an introduction to Chapter 5.

Research Setting

Face-to-face interviews and one telephone interview formed the data collection methods that I used during the data collection process. Venues for the interviews for this study included only public places to ensure comfortability of interviewees. After establishing initial contact each participant over the phone, I scheduled face-to-face interviews with all six participants who indicated a preference to be interviewed at their workplace for convenience. One participant mentioned that his role required a lot of

travel and could not commit to a face-to-face interview but disclosed a willingness to participate in a telephone interview. I conducted interviews at the workplaces for each of the interviewees to allow for convenience and comfortability. I interviewed participants in various locations that include, conference rooms, a private office, and over the telephone. The individual settings allowed for privacy eliminating any distractions or interruptions. Follow up sessions involved telephone calls, email exchanges, and in person meetings enabling participant transcript reviews and member checking of data interpretation.

Participant Demographics

Middle-level managers employed at higher education institutions in the state of Florida constituted the population of interest for this study. Seven middle manager participants met the criteria established that allowed for a representation of any age group, race, gender, experience mitigating employee cyberloafing, employment in a digital workplace within higher education, and residency established in any geographic location in the state of Florida. Participants cut across different departments spanning financial aid, admissions, and test preparation at three different higher education institutions in the Central Florida Area. Also, participants included a Director of Admissions, two Associate Directors of Admissions, an Associate Director of Health Sales, a Customer Services Manager, a Financial Aid Manager, and a Campus Director.

The years of managerial experience held by participants ranged from 2 years to 9 years. All participants worked in digital work environments where employees used

mainly computers to interface and connect while performing work tasks and had experience mitigating cyberloafing. It is noteworthy that I did not know any of the participants; however, three participants interviewed held positions within my workplace. The three participants interviewed at my workplace held management positions (ranked above me in terms of seniority or employment hierarchy) and worked in different divisions within my organization. The average interview time was 23 minutes and the participant demographics are in Table 1 below.

Table 1

Participant Demographics

Participants	Occupation	Years in role	Employed in digital workplace	Experience mitigating cyberloafing	Gender
P1	Associate director	2	Yes	Yes	Male
P2	Director of admissions	4	Yes	Yes	Male
P3	Customer services manager	2	Yes	Yes	Male
P4	Financial aid manager	8	Yes	Yes	Male
P5	Associate director of admissions	9	Yes	Yes	Female
P6	Campus manager	3	Yes	Yes	Male
P7	Associate director of admissions	8	Yes	Yes	Female

Participant Recruitment

I received approval from the Walden University institutional review board (IRB) before commencing the active recruitment of participants (IRB approval number 02-27-17-0435968). As detailed in the study design, the participant recruitment process was intended to recruit participants using LinkedIn.com and the Walden University research participant system. An initial participant screening process for Florida-based participants using listings from online higher education management groups in LinkedIn.com resulted in the identification of approximately 40 potential participants.

The Walden University Center for Research Quality posted information on the study and sent out an email to users of the Walden University Participant Pool website, letting them know that a new study was available. No responses came from the Walden University online research participation system. I reached out to all potential participants using the LinkedIn.com InMail messaging system by sending the invitation to participate (see Appendix A). There was no pressure on individuals to participate. The outreach to potential participants was restricted to only 2 emails to avoid creating ill feelings from a barrage of emails soliciting participation.

A few problems arose during the initial participant selection process. The first issue of significance was the unanticipated LinkedIn.com restriction preventing basic members from sending InMail messages to other unconnected LinkedIn members. To overcome this challenge, I upgraded my basic account to a premium account and was required to purchase each InMail sent which added an unforeseen cost. As a result, I sent

more than 50 InMail messages soliciting participation. A second problem involved the initially slow and sporadic LinkedIn.com responses from potential participants with the first response coming forty-eight hours after sending out the first set of emails.

Forty-eight hours after sending the initial invitation InMail, one follow-up InMail request was sent to avoid pestering the individuals. A total of ten volunteers responded to the invitation InMail sent via LinkedIn.com. Subsequently, a preparticipation email was sent to all volunteers to confirm eligibility to participate in the study (see Appendix C). I determined participant eligibility to participate in the study based on the following criteria: current employment in a middle management position responsible for supervising employees; work in a digital workplace where employees use mainly computer technology to perform work tasks; experience mitigating subordinate cyberloafing activity; and a willingness to share their experiences and understanding about their role in the mitigation of employee cyberloafing at work.

The third problem during participant selection was the distance or closeness between some participants and the researcher. Of the ten volunteers, 4 volunteers that indicated a willingness to participate in the study held positions within my own workplace. It is noteworthy that 1 volunteer was eliminated because the potential participant was familiar with and worked in the same department with me. The 9 volunteers who responded to the eligibility email questions all met the eligibility requirements to participate in the study. Participants displayed enthusiasm and a sense of curiosity with the about the topic during the phone conversations prior to the interviews.

Data Collection

The data collection phase of this study took place within a four-week period between March and April 2017. The approved research methods I implemented included face-to-face interviewing (Englander, 2012) as the main data collection method and reflective journaling (Chan, Fung, & Chien, 2013; DeFelice & Janesick, 2015) as a bracketing strategy during interviews, a means of reflecting on nonverbal cues observed during interviews, and to document the research processes from the research design phase to the research conclusion phase. My first step before proceeding with the data collection process involved practicing bracketing (epoché) as prescribed in Moustakas (1994) to recall and suspend any personal views about the issue and increase my sensitivity to participant feelings about the issue.

In clearing my thoughts, I focused on recollecting any meaningful personal experiences I encountered during my 12-year management career. Only one recent personal experience came to the fore involving a co-worker that was involved in excessive cyberloafing activity that affected my teams' performance necessitating my intervention as a team leader and escalation to management. I deliberately uncoupled my mental conversations and thoughts relating to the previously mentioned personal experience, to focus my sight and hearing directly on participant responses.

All participants indicated consent before the commencement of interviews. Data collection was achieved in accordance with the instrumentation procedures and ethical guidelines as prescribed in Chapter 3. I conducted six face-to-face interviews and one

telephone interview using a semistructured interview format with open-ended questions and prompts designed to encourage in-depth responses from participants. During all interviews, I used a voice recording application on my iPhone to record all interviews saving each recording in MP4 file format.

Semistructured interview questions including seven core questions with associated probing questions related to the central research question and designed to systematically elicit participant's perceptions about the issue (Jamshed, 2014; DiCicco Bloom & Crabtree, 2006). I used a reflective journal to document methodological modifications during data collection. Through the researcher's documentation of steps taken during the data collection and analysis, transparency in the research process is enhanced (Lincoln & Guba, 1985; Ortlipp, 2008; Peredaryenko & Krauss, 2013).

Immediately following interviews, I offered participant's an opportunity to correct inaccuracies captured in the interview transcripts. Also, after completing the data analysis, I provided each participant an opportunity to challenge any perceived misinterpretation of meaning ascribed to their role mitigating cyberloafing. All participants responded to initial member checks (review of interview transcripts) without corrections. After the completion of data analysis, I met with each participant to verify and confirm the accuracy of the meaning each participant ascribed to the issue under investigation. In phenomenological research, obtaining informant feedback about the authenticity and completeness of summaries reflecting participant experiences is an

essential to help improve the trustworthiness of the research results (Birt, Scott, Cavers, Campbell, & Walter, 2016; Lincoln & Guba, 1985; Sandelowski, 1993).

Data Organization and Management

I remain solely responsible for participant's recruitment, determining eligibility, obtaining their informed consent, and confirming the accuracy of interview transcripts. Data collected for the study was secured using strong passwords on computers and devices used to file all digital and text data and in one file the NVivo 11 Pro software program as detailed in Chapter 3. All computers and devices used to access digital, and text data will have regularly updated anti-virus protection with access restricted to the researcher. Data will be kept for at least five years, as required by Walden University.

Data Analysis

The central focus of the analysis of textual data collected for this study was to develop analytical outputs about the lived experiences of participants surrounding their role mitigating employee cyberloafing at work and what helps them achieve positive outcomes. Data analysis procedures relied on the modified Van Kaam modified data analysis method outlined in Moustakas (1994) using transcribed participant responses and a combination of hand coding and coding using NVivo 11 Pro software to increase validity. The NVivo 11 Pro software program also serves as the central repository for data management and storage. The data analysis processes consisted of two data coding cycles, the first and second data coding cycles while triangulating with the modified Van Kaam data analysis method.

Hand Coding

One of the advantages of using hand coding during data analysis is the ability to gain familiarity with data and to develop an overall picture presented by participants (Basit, 2003; Stuckey, 2015). I adopted the hand coding process as a starting point for the data analysis to illuminate intricate details contained in the interview transcripts. I began the slow and tedious process that involved reading and re-reading transcripts several times to gain familiarity with the participant's individual responses about their experience with the role mitigating employee cyberloafing at work. Hand coding enables the researcher to get physically involved with the data and allows the researcher to drive the analysis process (Klenke, 2016).

To enhance the unraveling of ideas contained in the raw data during data content analysis, I used the open coding method to develop codes (DeCuir-Gunby, Marshall, & McCulloch, 2011). My hand coding scheme involved horizontalization using the participant interview transcripts to list and group all relevant participant responses. I adopted a cut-and-paste approach (Basit, 2003) for the horizontalization process and developed a list of significant participant responses in a table to facilitate abstracting and labeling. The identification of unchanging elements in participant responses about experience requires the listing and grouping of relevant statements, as well as the reduction and elimination of irrelevant statements (Moustakas, 1994, p. 120 - 121).

Two hundred and eleven verbatim significant participant responses were identified representing unchanging elements of the participant experience. The next step

in the hand coding process involved a careful examination of significant participant responses to facilitate the clustering of the unchanging elements of participant experience into themes. The clustering of unchanging elements in participant responses involved a painstaking process used to find and organize ideas and concepts within participant responses. As prescribed in Moustakas' (1994) modified Van Kaam method, I identified specific words and phrases to understand the participant's attitudes, feelings, and perceptions about their role in the mitigation of employee cyberloafing.

The final step in the data coding process involved validating all unchanging elements and themes before generating individual textural descriptions for each participant. I further developed the individual textural descriptions using imaginative variation and generated textural/structural descriptions for each participant integrating the unchanging elements and themes. I generated composite descriptions of meaning for participants as a group based on their experiences and saved the descriptions for comparison with results from coding using the software.

Coding Using NVivo 11 Pro

The first step in the data analysis process using NVivo 11 Pro software program involved several steps used to clean and reorganize the data in readiness for the upload into the software program. The data cleaning process involved eliminating all irrelevant information in the interview transcripts and creating pseudonyms for each of the participants. As prescribed in Adu (2016), cleaning the transcript data is necessary when using NVivo 11 for data analysis to allow the researcher remove irrelevant information,

I used a text search query look out for and analyze occurrences of the word *mitigation* (see Figure 2).

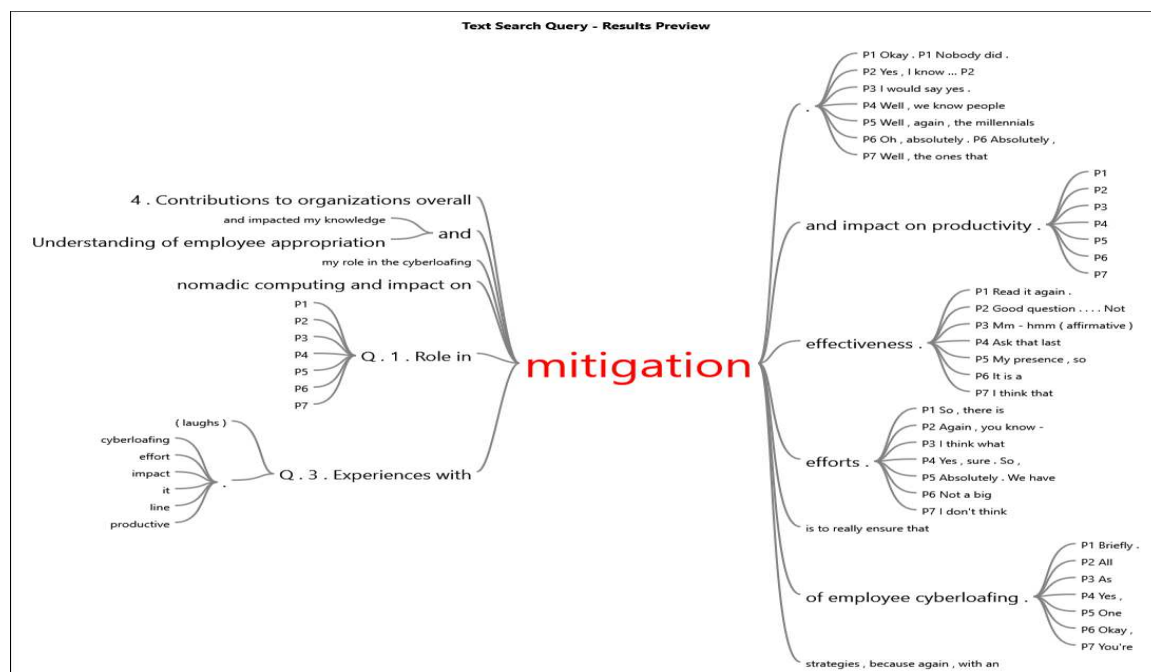


Figure 2. Mitigation text search query results.

I started the initial coding process using the Values coding method and applying codes to statements reflecting the values, attitudes, and beliefs of participants as recorded in the transcripts. Values coding involves the use of codes to depict the important attributes, thoughts or feelings, and perceptions about individual experiences (Miles, Huberman, & Saldana, 2013). After the first cycle of coding, I clustered and thematized unchanging elements from participant responses to develop the core themes of participant experiences.

Transitioning to the second data coding cycle using NVivo 11 Pro software program involved steps used to examine the codes developed in the first cycle coding

process. I began the second data coding process using the Pattern coding method to further reduce the data into smaller and more meaningful data units, identifying patterns and relationships, before labeling the emergent themes (Miles et al., 2013). Pattern coding involves coding processes aimed at developing major themes, searching for causes or explanations, examining relationships, and formulating theoretical constructs (Miles et al., 2013, p. 87).

After identifying emergent patterns and labeling the new emergent themes, I developed a narrative describing each of the emergent themes. The next step in the data analysis phase involved a reexamination of the data to ensure adherence to the modified Van Kaam method of phenomenological data analysis outlined in Moustakas (1994). The first cycle coding process enabled the horizontalization, reduction, and elimination of changing elements from the full participant responses about their experiences. The second cycle coding process allowed for the clustering and thematization of unchanging elements of participant responses about their experiences.

I developed emergent themes after sorting and synthesizing the data by categorizing codes based on relationship, frequency, and meaning. A validation process was used to further eliminate any irrelevancies to participant experiences based on an absence of explicit expression or compatibility. As part of the analysis process, I compared descriptions generated using hand coding with the descriptions developed using coding software before developing the final composite descriptions of participant experiences.

Evidence of Trustworthiness

Providing evidence of trustworthiness in qualitative research is intended to illuminate the internal consistencies used to establish rigor in research processes as well as in the dissemination of the results (Lincoln & Guba, 1985). For this study, I developed and used a documentation strategy to illuminate the participant selection process (a form of triangulation), peer debriefing (working with dissertation committee), using established research methods and a thick description of the issue under investigation. Prior to the commencement of data collection, I consulted with experienced faculty research committee members to strengthen the quality of my research instrument.

Following Fusch and Ness's (2015) data saturation guidelines for novice researchers, I used the same interview questions for all interviews with probing questions designed to encourage in-depth responses from participants. In addition, I suspended all personal views about the issue and increased my sensitivity to participant feelings about the issue. Applying Brod, Tesler, and Christensen's (2009) data saturation grid allowed me to establish data saturation after the first five participant interviews by identifying and recognizing the replication of information insufficient enough to develop new categorizations. To confirm the emergence of no new information during interviews, I conducted two additional interviews after the first five that returned no new information.

Bergman and Coxon (2005) highlighted the importance of interviewer sensitivity to internal inconsistencies during research interviews necessitating the use of probing questions to clarify any inconsistencies in interviewee responses. To guard against any

inconsistency resulting from possible misinterpretation of interview questions, I used follow-up or probing questions during interviews to clarify any inconsistencies detected in participant responses relating to the research (see Appendix D). As noted in Edwards and Holland (2013), using follow-up and probing questions during qualitative interviews allows the researcher to clarify initial responses or provide additional details.

I recorded all face-to-face interviews using an audio recording device before transcribing each of the participant's responses. Although the initial interviews generated long and detailed responses from most participants, I found some inconsistent responses during data analysis necessitating follow-up sessions to clarify meaning. I conducted follow-up sessions with participants immediately following the completion of data analysis to ensure the accuracy of findings. During each follow-up session, I challenged any inconsistent interpretations arising from the initial interviews asking more probing questions to elicit further explanations and to clarify contradictory statements.

I am an employed by a university and work in a digital work environment and to guard against any researcher bias, I disclosed my work background in higher education. The first step in the data collection process involved my engagement in a bracketing process (*epoché*) as prescribed in Moustakas (1994) to recall and suspend any personal suppositions about the issue and increase my sensitivity to participant feelings about the issue. I diligently recollected any meaningful personal experiences before deliberately uncoupling any mental conversations relating to personal experiences to facilitate a focus directly on participant responses.

Credibility

Ensuring credibility in qualitative research requires researcher transparency about the research procedures and specific steps are taken that provide assurances about the quality of the results. Steps taken to enhance a qualitative research study's credibility must include using well-established research methods, familiarity with the participating research environments, random sampling of participants, triangulation, ensuring internal consistency of participant responses, discrepant case analysis, and peer debriefing (Lincoln & Guba, 1985; Miles et al., 2013; Shenton, 2004).

I provided details of the core processes that facilitated the unraveling of knowledge using the modified Van Kaam method for data analysis demonstrating openness and transparency. Also, the data analysis process involved using a combination of two theoretical schemes to interpret and support the data. Additional steps are taken to ensure credibility involved using eligibility criteria designed to confirm participant willingness to share honest experiences and prompts during interviews to clarify inconsistent participant responses. Peer debriefing with the dissertation committee, experienced faculty members, and peers during data collection and analysis.

By collaborating with seasoned researchers and peers, I enhanced my decision-making ability and widened my research vision learning from shared experiences and perceptions about courses of action, development of ideas, and interpretation. Greene (2014) suggested using peer debriefing as a means of enhancing researcher critical thinking skills and research credibility during qualitative research. Discrepant cases

involving responses unexplainable by interpretation and member checking were identified during data analysis through deliberate steps taken to familiarize the researcher with the data. I conducted follow-up sessions (member checking) to help eliminate any inconsistencies in participant responses during the data collection process.

A culmination of the validation process used in qualitative research involves member-checking to establish the correctness of interpretation (Colaizzi, 1978; Lincoln & Guba, 1985). Each participant agreed to follow-up member checking sessions and I provided each participant a copy of the interview transcripts to confirm accuracy and subsequently discussed the interpretations developed during data analysis to confirm the accuracy of meaning. My employment status working in an environment where computer hardware, software, interfaces, and connectivity solutions are used to perform work tasks, collaborate, and provide services to clients helped establish familiarity with the research setting. Random selection of participants was established by reaching out to pre-screened potential participants using the LinkedIn.com InMail messaging system to send invitations to participate.

Four potential participants that indicated a willingness to participate in the study held positions within my own workplace. To guard against any potential bias and to avoid the creation of possible conflicts of interest, during the final selection of participants, I selected three volunteer's unknowns to me that worked within my organization in a different division. Also, participants volunteered to participate and indicated an intention to help foster the development of new knowledge. The participants

interviewed within my own organization occupied managerial positions placing them above me in terms of seniority or employment hierarchy.

Transferability

Demonstrating the applicability of the findings and results of qualitative research to wider populations presents significant challenges for the researcher because of the small number of participants and research environments. Shenton (2004) suggested avoiding a preoccupation with transferability and instead, focusing on providing contextual information about peculiarities associated with the research environment and population. For this study, I provided details about the number of participants, organizations with their locations, the period of data collection, and the demographics of participants interviewed. This information would enable readers to identify boundaries of the study to determine transference of results.

Dependability

The dependability of qualitative research studies is determined by using consistent and stable research processes that show the possibility of replicability if the study were replicated in a comparable setting. Elo et al. (2014) noted that stating participant selection criteria and demographics enhances dependability of qualitative research leading to stable data over time even in diverse conditions. For this study, I used a criterion-based sampling method, face-to-face interviews, a semistructured interview format with open-ended questions, and described methodological coherence for the study. I provided detailed explanations about all elements of the research design, data collection, and

analysis procedures, as well as data management and storage procedures to provide future researchers with sufficient information to allow for replication.

Confirmability

Ensuring confirmability in qualitative research requires adequate steps taken to facilitate confirmable results that can be corroborated by others. Miles et al. (2013) maintained that a vital element for achieving confirmability in qualitative research requires the provision of a detailed record of methods and procedures that allow for scrutiny by others as well as the retention of data available on request for re-analysis. For this study, I established congruence of procedures during data collection and analysis with a documentation process using a reflective journal with analytic memos and the NVivo 11 Pro software program to capture and record procedural steps, decision rules, and analysis operations. An audit trail documenting all research processes especially changes that emerged during the iterative research and the reasoning behind such changes is available.

Results: Emergent Themes

The lack of information available on the role of middle managers in the mitigation of employee cyberloafing at work is the main motivation for this phenomenological study focused on exploring the lived experiences of participants at higher education institutions in Florida. The results presented in Chapter 4 tally with the central research question; what are the lived experiences of middle managers about their role in the mitigation of employee cyberloafing at higher education institutions in Florida? After a detailed

analysis of participant interview transcripts, development and categorization of nodes, and the development of the main themes encapsulating the meaning of participant experience, four major themes and seven subthemes on participant experiences about their role mitigating employee cyberloafing at work emerged (see Table 2).

Table 2

Emergent Themes, Nodes, Sources, and References

Emergent themes	Nodes	Sources	References
Managing employee performance	Managing employee performance	7	19
	Mitigation barriers	7	17
	Observing and persuading	6	23
	Setting clear expectations	4	7
	Understanding duties and obligations	5	18
	Using managerial discretion	6	14
	Working with unclear mitigation policies	5	9
Cyberloafing interventions	Experience during cyberloafing interventions	6	13
Proximity matters	Proximity matters	6	14
Understanding employee Online technology usage	Employee technology usage	6	17
	Staying current with technology advancements	3	8

The four major themes include: managing employee performance, proximity matters, cyberloafing interventions, and understanding employee online technology usage. Seven subthemes emerged under the managing employee performance and understanding employee online technology usage themes. Collectively, the seven

subthemes include mitigation barriers, observing and persuading, setting clear expectations, understanding duties and obligations, using managerial discretion, working with unclear mitigation policies, and staying current with technology advancements.

My conceptual framework combined symbolic interaction and adaptive structuration theories to help provide answers to the central research questions by uncovering managerial perspectives related to the social premises surrounding employee online technology use and the interactive relationships governing managerial control of cyberloafing behavior. As the data analysis evolved, two additional constructs, the extrinsic motivation and situational leadership theories to further illuminate meaning contained in the data. The construct of extrinsic motivation pertains to actions taken with the primary intention of achieving a specific and distinct outcome (Ryan & Deci, 2000). The middle manager motivation for mitigating cyberloafing activity is extrinsic in nature because the objective is to enhance employee performance which is one of the functions of management.

Similarly, the situational leadership construct maintains that the effectiveness of leadership rests on style adaption to the situational happenings identifying suitable tasks, understanding group dynamics, and relevant factors that would positively affect the success of the endeavor at hand (Hersey, Blanchard, & Ntemeyer, 1979). One important aspect of situational leadership pertains to the maturity level of the followership. Task oriented maturity levels of employees under middle management supervision influence

the choice of leadership style during cyberloafing mitigation interventions (Hersy et al., 2000).

Emergent Theme 1: Managing Employee Performance

Theme 1 *managing employee performance* emerged as the most important role activity for participants based on their experiences with the mitigation of employee cyberloafing activity at work. Employee performance is an important indicator used to measure an employee's financial contributions to an organization's bottom-line (Anitha, 2014). When employee performance ties in with organizational success, leadership must align the relationship between the organization and its workers to facilitate organizational success (Sorenson, 2013). Cyberloafing activity distracts employees from task performance and like Ugrin and Pearson (2013) indicated, the unrestrained cyberloafing activity at work results in a reduction in employee productivity and revenue losses for organizations.

When asked to describe their role mitigating employee cyberloafing, all participants believed that managing employee cyberloafing through situational awareness about employee performance was an important role activity because of their responsibility for driving employee performance. It is noteworthy that all seven participants provided responses with 19 references as shown in Table 1. One participant described his feelings about his role in the following way during our interview, "My role in the cyberloafing mitigation is to really ensure that my staff are consistently on task for the most part." Another participant described his role mitigating cyberloafing stating that,

In my role, it does require that I assist my team and my advisors to manage their time properly so that they are still successful in their role and meeting their daily expectations here in the organization and not misusing their time and placing themselves in danger by doing so.

A third participant stated, “My job is to not only monitor their production but monitor what they’re doing whether they’re using the company computers illicitly for non-work-related functions.” In a more vivid rendition of his experience, a fourth participant related his role mitigating cyberloafing to his responsibility driving performance when he stated,

My role with mitigating against cyberloafing is extremely important because again, at the end of the day, if my team’s not hitting their number, it’s a third of the business. It’s very important to me that my team is successful and we’re hitting our targets and I mitigate against it because it can be a distraction... I don’t care if it’s a company computer, your watch, your cell phone, your iPad; it’s still company time. And at the end of the day, if you’re not meeting business results and you’re not meeting your daily objectives, it’s an unacceptable practice to be doing that.

As participants recounted their experiences mitigating employee cyberloafing, they unanimously indicated that their role required deliberate actions aimed at monitoring employee performance to understand and assess events and activities associated with cyberloafing activity. The data supports Ryan and Deci’s (2000) form of extrinsic

motivation that includes an external controlling force with individuals acting to satisfy the demands of an external source. In the case of participants, the organizational demands for performance serve as the external motivation driving managerial control of cyberloafing.

Participants asserted that their mitigation role activities required active interaction and engagement with employees to drive performance. A fifth participant described his strategy for managing performance by actively engaging with employee in the following way,

For myself, type of manager I am, especially in this business, I just basically ... I manage by action. What I mean by that is ... I'm constantly on the floor and finding out what's going on and checking in on them so, that's basically how I police it.

Each participant understood their responsibility for controlling employee behaviors and activities within the workplace. This understanding aligned with Campbell et al.'s (2016) notion that middle managers have contractual and legal obligations to not only guard the interests of their employers but also to control employees under supervision. In a digital workplace, the problem for most employers' hinges on the over-exposure of employees to the distracting overflow of information made available by the easy access to Internet (Ladner, 2015; Sheikh et al., 2015). Participants acknowledged that work environments where employees use mainly online technology to perform work

tasks, collaborate, and provide services to clients required proactive managerial control of online technology usage. A sixth participant stated,

I generally manage their productivity... I view it from their productivity and the tasks and the things I need them to do... in a call center as you probably know, we have metrics on everything. I know when you take a break, I know when you're in between a call, I know everything. So, that's how I would manage cyberloafing. If you have too much of what we refer to as 'after call' work, it's probably a direct correlation to you're on some other website or you're doing something.

Participants felt that managing cyberloafing through productivity allowed them to easily identify individuals engaged in the unproductive activity. This aligns with Pînzaru and Mitan's (2016) claim that managerial cognizance of the different needs and traits of their various team members helped drive performance improvements during cyberloafing mitigation. Another participant stated,

A lot of the management just do observation and production. I look at if your production's low, I see what you're doing every day. I observe for a while, are you spending too much time on the Internet and not focusing on your students in queue, and usually if that is the case then I would have one-on-one conversations with those advisers. But, if you're producing, and overproducing, and on top of your students, I don't pay much attention to what's your personal use of the Internet, because it is allowed on the floor.

During interviews, I used probing questions further to elicit thicker descriptions to help provide clear and concise answers to the central research question of lived experience about the managerial role in cyberloafing mitigation (see Appendix D). During a situation where I asked, ‘how do you control employee cyberloafing activity at work?’ to elicit a deeper response, the participant responded,

I approach the management from the productivity standpoint. So, if you’re a digital native and you can ... if you can do the job with a cell phone in your left hand and still get it done and it sounds good, have at it. But if you can’t then you need to put the cell phone down.

Participants expressed a certain level of conviction that their active role managing cyberloafing affected employee performance; however, one participant reported taking specific actions aimed at redirecting employees away from unproductive activities like cyberloafing. The participant stated,

I am able to impact productivity, because I just again redirect attention away from the activities we shouldn’t be doing towards the activities that we should be doing... if I walk right up to them and they have a screen on that they’re not supposed to be on, maybe they’re shopping for something, I’ll see them kind of strategically click their mouse and it’s on a different screen. I can kind of catch on to all those small things... I find that, again, redirecting attention to what is important for productivity works.

Participants discussed how they maintained situational awareness about employee cyberloafing while managing employee performance. This supports Rahimnia and Mazidi's (2015) findings that monitoring employee activity works well for employees with lower levels of cyberloafing self-control. One participant stated,

We spend more time there watching, monitoring what they're doing while on their computer... we try to be out on the floor with them, face-to-face so I can see exactly what they're doing... if somebody's constantly on their cell phone and not doing their job, that's when I intervene and now it's getting excessive cause you've been on the phone for the last 15 minutes as opposed to doing your job.

When asked about daily interactions with employees during mitigation, some participants indicated some concerns about minor cyberloafing activity being permitted at work. As an example, one participant mentioned that,

If you're producing and overproducing, and on top of your students, I don't pay much attention to what's your personal use of the Internet, because it is allowed on the floor... I think I more take an interest in what are you doing with your time if I see a reduction in production if I see you're not meeting your numbers if I see you're missing appointments. It usually is the behaviors that will lead me to start looking at what are you doing.

Jandaghi et al. (2015) noted the impracticality of eliminating cyberloafing suggesting that managers adopt effective mitigation mechanisms while encouraging productive online technology use. The results of this study support these assertions, as all

participants agreed about the essentiality of proactively watching employee performance levels as a precursor for cyberloafing mitigation. During member checking, participants recapitulated their feelings about the important role activity managing employee cyberloafing through situational awareness about employee performance with no new information.

Viewing the data from a symbolic interaction theoretical perspective, a part of the conceptual framework for this study, managerial understanding of their roles in mitigating employee cyberloafing is shaped by daily interaction with employees involving the employment of daily tactics to curb the effects of cyberloafing on performance and learned experiences during cyberloafing interventions (Bhattacharya & Tang, 2013). Social interactions at the workplace between employee and manager allow managers to develop situational awareness of what individual employees are doing, not doing, and capable of doing (Bhattacharya & Tang, 2013). Maintaining a situational awareness about employee performance to manage employee cyberloafing shows that this role activity is essential to the effective managerial control of employee cyberloafing.

Drawing from the extrinsic motivation theoretical perspective, the middle manager's keenness to mitigate employee cyberloafing behavior at work stems from a required function within the organization to establish an innovative and creative work environment (Deci & Ryan, 2000; Gagné & Deci, 2005). Mollick (2012) found that middle managers played a more significant role in driving organizational performance

because of their indispensable role managing multiple projects, allocating organizational resources, and supervising the completion of projects.

From this human motivation theoretical perspective, the ramifications of managing employee cyberloafing, if conducted using employee performance metrics to detect distractions, could offer practitioners a useful method in combination with technical mechanisms for identifying individual cases of cyberloafing in digital workplaces. Another interesting revelation from the data connotes participant display of situational leadership as evidenced by their preparedness to intervene when employees engage in unproductive cyberloafing affecting their performance. Participants exhibited elements of the Hersey-Blanchard situational leadership model with four distinct styles delegating, participation, selling, and telling (Hersey et al., 1979).

Emergent Theme 2: Proximity Matters

Theme 2 proximity matters revealed that participants believed that proximity to employees provides a mechanism for ameliorating the problem of cyberloafing enhancing the effectiveness of their mitigation efforts. Employee perceptions of exposure to the watchful eyes of the supervisor because of physical proximity and workplace layout acts as a cyberloafing deterrence mechanism (Rahimnia & Mazidi, 2015). In addition, Rahimnia and Mazidi (2015) noted that managerial proximity enhances opportunities for supervisory use of verbal persuasion and manipulation to control employee behavior.

When asked how their monitoring presence influenced their roles in controlling employee cyberloafing at work, participant's descriptions centered on how their physical

proximity to employees enhanced their ability to mitigate cyberloafing positively affecting performance. As participants recounted their experiences, they indicated that proximity facilitated physical closeness with problematic employees enabling the use of prompts or verbal instruction to redirect attention or behavior. One participant asserted,

My team knows that I can hear just about everything that's going on. Whether it's being able to see their screen all day, which again, they know I'm not looking over their shoulder like looking for that kind of stuff... I think that there is a difference between having an onsite manager and having an offsite manager.

Another participant stated,

I have twenty-two employees that work in the building. For the most part, they're seated in a close range to me... I do believe that me physically being there affects their attention to their work or their productivity... in my experience, there's still some human element to them seeing me sitting right there. They're probably a little more attentive to their work. Whereas if I was off-site all day, their numbers may be slightly less productive.

A third participant expressed concern that he did not have available technical monitoring software to monitor technology usage but being physically close to employees facilitated active monitoring of cyberloafing activity. The participant stated,

I'd say being close positively affects cyberloafing mitigation because I can physically see what they are doing. Without being close, it could be difficult.

Because, I don't have a technology role, so, I couldn't use technology to track that

information unless I'm going to request it... So, just being there and being able to see what they're doing. Because otherwise if I have an employee struggling, I can only guess that, "Hey, you're probably on the Internet". But if I can walk by and see that the employee is struggling because part of a distraction is because he or she is on the Internet, then I am better able to address the situation.

Rahimnia and Mazidi (2015) posited that having an open office layout at the workplace enhanced managerial control of cyberloafing by exposing employee online technology usage to physical monitoring by their supervisors. The results of this study support this assertion, as participants agreed that a monitoring presence positively affected the effective managerial control of employee cyberloafing at work. Another participant acknowledged the benefits of having an office layout that enhanced supervisory monitoring presence. The participant stated,

My monitoring presence has helped in reducing cyberloafing activity. My desk is within proximity of my team. I can see the majority, about 50% of my staff, from where I sit and work out of... It does enhance it because we are talking about either business matters or just simply continuing our rapport-building process.

Similarly, another participant an open office layout enhanced the opportunity to monitor employee activities and behavior and stated,

I think I more take an interest in what are you doing with your time if I see a reduction in production if I see you're not meeting your numbers if I see you're missing appointments. It usually is the behaviors that will lead me to start looking

at what are you doing... I think it helps to be able to because from where I sit I can see most of my teams' computer screens, so it does help.

One participant acknowledged the benefits of having an onsite manager however, he felt that his proximity to employees was ineffectual to his managerial role mitigating cyberloafing at work. The participant described a preference for empowering the employee to take ownership of their work rather than relying on proximity to drive compliance. The participant emphatically stated,

As to whether I'm here, they still take pride in being successful in their job. I really, really, really, work towards getting my agents and my team to a place where they have that ownership so that it's like an intrinsic motivation for them to be successful. Not a, oh my boss is here so I better make sure that I'm chipping away. I want to make sure that I set them up for success in that regard and empower them to have that intrinsic motivation. So again, there's always going to be a difference when your manager or your supervisor is onsite but it's minimal. I travel sometimes quite a bit for work and when I'm gone for three days at a time, two, three days at a time, I'm not worried about what they're doing here. In regards, I don't think it's anything different that they're doing than when I am onsite.

During a follow-up session, the participant reiterated how his monitoring presence minimally affected employee cyberloafing behavior or activities because his employees felt empowered to self-regulate online technology use having a clear understanding of his

expectations and the organization's policies. An explanation for this participant's response relates to his employee's high level of maturity using online technology which resulted in his adoption of a delegating leadership style with minimal cyberloafing interventions (Hersey et al., 1979).

Except for the one participant, with a differing view on the effects of managerial proximity, member checking produced no new information as the remaining participants agreed that their monitoring presence affected the role performance during cyberloafing mitigation. Looking at the data from a symbolic interaction conceptual lens, a part of the conceptual framework for this study, the meaning participants derived about the effects of their monitoring presence on their roles in mitigating employee cyberloafing is shaped by the activities and interactions with employees at the workplace. This aligns with one of the premises put forward by Blumer (1969) which holds that meaning people have about an issue is acquired from social interaction.

Emergent Theme 3: Cyberloafing Interventions

Theme 3 cyberloafing interventions emerged as an offshoot of mental conversations where participants recounted their experiences while acting to redirect employee behavior during cyberloafing mitigation. The middle manager's role within business organizations entails the containment of employee behavior through direct control and manipulation (Harding, Lee, & Ford, 2014). Participants believed that personal efforts during cyberloafing interventions taking charge and directing subordinates contributed positively to the overall organization's mitigation effort.

Excessive cyberloafing activity affects employee performance requiring varying levels of managerial interventions. According to Hersey and Blanchard (1979), the leadership style managers choose to use during interventions must be guided by the situational context and the task-maturity level of the employees under supervision. The data shows that participants shared their unique set of experiences about the social interactions during cyberloafing interventions and the effects of the interventions on employee performance. One participant shared an experience involving an employee request for special attention after recognizing a challenge with self-controlling cyberloafing activity. The participant stated,

I had somebody on my team at the time that their sales performance was suffering and I'd see them on Facebook or whatever the social media stuff was all through the day. And I'm like 'what are you doing?' And they're 'ah no, no, no, I'm going to get back to my leads now, I'm going to get back to my leads now.' And after a week, a week, and a half of having a pretty sharp conversation with 'you need to have your business activities done before you're doing that.' This person came to me and said 'hey, sit me right in front of you and I need you to watch me like a hawk. I need it. Like please, I need you to do it because I need that. That's the type of support that I need.' And I was totally taken aback and dumbfounded by the fact that somebody wanted that. And the fact that that person was honest with them self and honest with me to say for me to be successful, I need this from you, and I did. And it was much easier to have the difficult conversation at that point

because the employee that I had at that point opened them self up to it so for me to be able to walk over to them, I wouldn't even have to say anything. I'd walk over and I would just look at them and they'd be like, you were right, and go right back to work. So, that was something for me that was a very eye-opening experience as to how to manage people.

The perception of the participant points to the adoption of the supportive situation leadership style that incorporated shared decisions to drive behavior change (Hersey and Blanchard, 1979). Another participant shared details of the conversations between supervisor/employee during cyberloafing interventions. The participant stated,

In almost every case, during an intervention like that, I'm going to reference what the team average is in comparison to what you're doing, which eliminates the concept of that it's my thought of them. It's everybody else is doing this thing, and you're not there. So, it's clearly a reflection of you being outside the norm... And then I think most people will attempt to then increase. And they do show some increase in productivity... there's obviously some people who maybe do a minor spike and go right back to their old ways or don't increase at all. And then that leads into tougher conversations which maybe probably ends in a person losing their job.

The initial response provided by this participant required a follow-up session to clarify meaning. The participant reaffirmed that his cyberloafing interventions usually involved presenting production metrics to the employee indicating showing a reduction in

performance and emphasizing the need to refocus on productive behavior rather than cyberloafing. This response aligned with Harding et al.'s (2014) assertion that managerial contributions to driving employee's performance involve using control mechanisms and manipulation. Similarly, a different participant described the use of employee focused coaching sessions in situations involving cyberloafing activity leading to poor employee performance. This perception aligns with the coaching leadership style as described in Ryan and Deci (2000) where the leader uses verbal persuasion to influence a change in employee behavior. The participant stated,

What I'll do if I have someone on my team who is struggling to meet production goals is more attention to the person. Because I'm trying to figure out why is an employee struggling to meet these goals...? I've passed your desk five times a day and from the five times I've passed your desk, you were either surfing the Internet shopping, or you were watching something on YouTube, or you were instant messaging somebody that's not work related. And, from there, we have a sit-down, we have a coaching session. Recap the coaching session so they know it's a documented coaching.

Again, another participant refers to 'production goals' which points to the extrinsic motivation for using managerial control to ensure employee performance as described in (Ryan & Deci, 2000). Participants agreed that interventions provided an opportunity to develop mitigation plans to help encourage productive employee behavior.

One participant shared an experience involving an employee's inundation with unproductive online technology usage leading to an intervention. The participant stated,

The experiences that I have had over the last five or six years or so has been simply watching how a person can become so engulfed in their cyberloafing activity that they lose sight of why we come in each day. I have watched employees come in, and before they are looking at business matters, they are turning on the last episode of their favorite show and playing it at their desk on the screen without even worrying that someone might watch them, or catch them in a sense... With some individuals, they can become so accustomed to the cyberloafing that it becomes second nature to their daily work habits... For one employee, I can recall was watching a show at his desk. I just kind of stood behind him while he was watching his movie, and not to create an awkward circumstance, I sat down next to him and was just kind of, you know, had my hands underneath my chin, kind of just waiting for him to notice that I was there. Without really having to say much, he realized that what he was doing was wrong. Again, addressing it directly for some can be helpful, but I feel in my experience just kind of taking a lighter approach and somewhat redirecting attention and continuing to redirect attention has helped my team.

This participant's description buttresses Hersey and Blanchard's (1979) supporting leadership style that shares the decision-making process aimed at redirecting the employee to productive activity. One participant shared a different perspective

highlighting the importance of factoring the cyberloafing activity into the hiring and employee selection process. Also, the participant felt that mitigating cyberloafing in a work environment with strong technical mitigation and strict acceptable usage policies enhanced role performance. The participant stated,

If we get the right person, if we interview somebody the right way, correctly, then essentially we're going to end up with a positive result, we'll have somebody that actually understands that hey, we can monitor everything, we can see it, at the end of the day... the Company has complete ownership over the workstation and they know that ahead of time, so whether you're doing something personal, either checking your bank account or something like that, they know ahead of time, we know we can see it. Anything that you do with a computer is technically the property of the Company. When you let, them know ahead of time, they're a little leery of what they do on the computer, because we can always come back and, hey, this is what you did. Why did you do that for this allotted period or what, did you not read the internet policy? That type of thing.

This participant represents to directed leadership style as characterized by the preference for communicating employee role with an expectation of compliance (Deci & Ryan, 2000). In sharing practical knowledge about personal experience with employee cyberloafing interventions, a participant acknowledged that some top performing employees engaged in cyberloafing but managed their production. The participant stated,

I have top performers that are on the Internet most of the day, but they're able to exceed their numbers every single cycle, and others that never are on the Internet who are barely making their numbers. So, it really depends on the person. Yes, I have those few that overuse it. They should be focusing more on getting better at their jobs and it's just a constant cycle back and forth.

Follow up sessions aimed at clarifying interpretation did not yield any new information. Participants believed that cyberloafing interventions allowed them to take charge and direct subordinates contributing positively to the overall organization's mitigation effort. In line with Blumer's (1969) symbolic interaction theory, participants showed that meaning acquired during cyberloafing interventions helped them develop functional strategies aimed at driving performance.

Emergent Theme 4: Understanding Employee Online Technology Usage

The theme *understanding employee online technology usage* revealed that participants understanding of employee technology use facilitated the development of coercive strategies used to demand and obtain employee compliance with acceptable online technology behavior. According to de Wet, Koekemoer, and Nel (2016), employee online technology usage creates opportunities for individuals to get distracted and losing track of time. As online technologies continue to transform our daily lives creating increasing levels of dependency, participants recognized the need to remain vigilant and redirect the attention of distracted employees (Melrose et. al., 2016).

Participants believed that an understanding of employee appropriation of

technology use enhanced their cyberloafing mitigation role. As participants recounted their experiences, they indicated that the prevalence of online technology affecting everyday life required an understanding of employee use to mitigate misuse. One participant mentioned that,

Things have changed and now that it's a requirement that you must be on a computer every single day, and for some people, every minute of your shift; I absolutely think that it has changed the potential for cyberloafing to exist. It invented cyberloafing in a certain regard.

Similarly, another participant described how an understanding of online technology use required managerial vigilance because of the distractive influences of online technology. The participant stated,

I think that there is an element to be more vigilant towards productivity... there's an element of, you bring in these distractions with you and they're right next to you and around you. So, I must spend more of my effort and time in keeping you focused on your work and with the remainder of my time, then try to teach you how to be better at the work.

Relatedly, some participants recognized addictive nature of online technology and disparities in online technology usage between younger and older employees at work.

As an example, one participant stated,

Most young people are going to be on their phones more than an older individual. Especially with all these different social media that young people join... I can easily identify if an employee is overusing their phone or not.

Participant knowledge about employee online technology use was based on experience monitoring usage. One participant recalled that,

Being able to monitor their use of cell phones or any technology and what they're doing with that technology has helped me to understand what their needs are to a certain extent... I would have to say that with the different generations that I do have on my team, I have noticed that because we use technology every single day, everyone is cyberloafing to an extent. Where it might be just one website that someone who isn't, a millennial might use because Facebook is it, you like to look at Facebook all day, whereas someone who's a millennial might be hopping from one website to the other, so they might be focused on several activities at the same time, whereas someone who isn't quite as tech-savvy might just be on one or two websites.

One participant acknowledged the dependence on online technology by digital native employees requiring vigilance. The response aligned with Pînzaru & Mitan's (2016) findings that showed how managerial attitudes about digital native's peculiarities influenced the use of practical strategies for supervision. The participant stated,

The majority of the employees that I have are Millennials, so the ones that grew up with the technology so, I have had issues because of their dependence on it, the majority of the people are constantly on some type of social media.

Pearson and Hussain (2015) posited that the increasing number of smartphone owners was likely to increase addiction to social networking sites and narcissistic behavior. Smartphone usage is one of the common online technology devices employees use to connect to the Internet (Jamaluddin et al., 2015). One participant acknowledged that reasonable use of smartphones was permitted at work and employees tended to be more familiar with their own devices compared to work-related online technology. The participant stated,

Usually when people text they use two hands, like I do, but, or their one finger, then it's harder to decide what are they actually doing. Are they playing a game on their phone? Which, is also allowed... I feel like everybody on my team has no issues with using all devices... They have issues with their own systems, but they are very familiar with how you use Facebook, YouTube, text, and Pandora, or whatever they're doing, but come on our system, they don't take the time to learn those as well as they use...

No new information emerged during follow-up sessions aimed at validating either interview transcripts or themes development after data analysis. Participants expressed the view that understanding employee online technology usage facilitated the adoption of more effective coercive strategies to demand and obtain employee compliance with

acceptable behavior. This line up with DeSanctis and Poole's (1994) theory which put forward the notion of the effect of online technology usage within organizations depended on employee adaptations to work and structures integrated within the devices themselves.

Emergent Subtheme 1: Mitigation Barriers

The subtheme *mitigation barriers* emerged from the participant's descriptions about their role performance during employee cyberloafing mitigation. Mitigation barriers reported range from issues relating to balancing cyberloafing expectations for an employee working remote and non-remote employees, a distraction from other responsibilities, enabling workplace policies, blurred lines between work-related and personal online technology usage, employee cyberloafing evasive actions, and repetitive cyberloafing behavior. A common perception held by participants indicated that the mitigation barriers adversely affected their role performance mitigating cyberloafing.

When asked about the contributions participants made to the overall organizational efforts aimed at mitigating employee cyberloafing, and prompted to shed more light on successes and challenges during mitigation, the participant responded overwhelmingly with the following challenges they experienced. One participant noted the challenges created by having a large workforce working remotely and stated,

Over 80% of our workforce works from home. So, when you think about that, and then out of the 20% of the workforce that's onsite, almost all that is right here in this building. So, when you have 80% remote workforce, it's not necessarily the

best thing to say, ‘well you absolutely shouldn’t be doing this’ because what about the 80% of the company that is working from home right now. Is somebody sitting there looking over their shoulder?

Another participant acknowledged that other responsibilities make it difficult to constantly watch employees and stated, “It’s kind of difficult to do it all the time and even with the employees themselves, they are constantly on the phone with students per se and there are things going on, so sometimes it’s difficult to monitor everything...”

Interestingly, one other participant noted that mitigating cyberloafing often takes away from other managerial responsibilities. The participant stated,

There’s an element of, you bring in these distractions with you and they’re right next to you and around you. So, I have to spend more of my effort and time in keeping you focused on your work and with the remainder of my time, then try to teach you how to be better at the work... So, the challenge in that role is to keep you efficient and productive.

Two participants described the use of social media for work-related business creating complexities for organizations looking to curb personal social media use (a form of cyberloafing). As discussed in Chapter 2, Schalow et al. (2013) pointed to an escalation of the cyberloafing problem by organizations requiring employee use of online technology creating obscurities deciphering between non-work and personal usage. One participant stated,

How do we tell our employees that they cannot be on social media when we do a lot of promoting on social media? ...It has really placed that balancing act on the role of the immediate supervisor to say, 'Okay, let's redirect. It's not that you can't do it. Let's just make sure that we are managing our time properly.' That's really where the ball has been placed in our court because we really cannot define, hey, one hour of Facebook and you're cut off...

A few participants affirmed that their employees used social media for work-related tasks making it difficult to regulate personal use. According to Dery et al. (2012), employee online technology usage creates ambiguities related to the setting of boundaries between work-related and non-work-related activities. One participant stated,

We do utilize social media to market, so it's kind of a fine line, cause sometimes they may be on it for personal, sometimes they may be on it for actual business purposes, so sometimes it's a fine line that we have to see, well, what is it that you're doing, you're spending too much time on it...

In the words of another participant,

We are a company based on the use of technology, right? That's something that we promote. We also do a great deal of marketing through social media channels... How do we tell our employees that they cannot be on social media when we do a lot of promoting on social media? It has really placed that balancing act on the role of the immediate supervisor to say, 'Okay, let's redirect.

It's not that you can't do it. Let's just make sure that we are managing our time properly.'

When describing barriers, one participant noted that his organization permitted employees listening to music using smartphones at work making it difficult for managers to decipher between the employee's listening to music and cyberloafing. This aligns with Dery et al.'s (2012) position that smartphone usage creates ambiguities surrounding the establishment of boundaries between work-related and non-work-related use. The participant stated,

One of the difficulties sometimes is because we do allow them to listen to music so you might be passing and they might be changing a song. But, how often you pass and that same employee is changing a song is one way to determine whether you need to have a conversation with an employee.

Emergent Subtheme 2: Observing and Persuading

Subtheme two *observing and persuading* emerged as participants recounted their role behaviors during employee cyberloafing interventions using observation and verbal persuasion to mitigate employee cyberloafing at work. When asked the question about how participants controlled employee cyberloafing activity at work, participants responded sharing details about keeping a watchful eye on employee cyberloafing activity and using verbal persuasion to drive compliance. Responses presented captured mental conversations in the minds of participants about their actions as individuals and behavior as actors involved in controlling employee cyberloafing.

Participant's views on their role behaviors support Zoghbi Manrique de Lara et al.'s (2006) position that leadership physical proximity, a precursor to employee perceptions about organizational control, facilitate the reduction of employee cyberloafing. One participant stated, "I'm constantly on the floor and finding out what's going on and checking in on them so, that's basically how I police it. Just by watching and observing what they're doing daily." A second participant mentioned,

My role is to understand which employees get off task and which employees stay on task. To know which employees are going to be on the Internet or trying to be on Netflix or Hulu and things like that...when you're not making the right decisions as a professional, I'm going to have some type of conversation...

Another participant stated,

I also do observation when I walk past employee's screen... if I point out to you that you're on the Internet, and you know that I'm watching, if you're on the Internet, then you must spend more time doing the actual work.

One participant providing a thick description of observation and persuasion as a manipulative tool used to coerce acceptable online technology usage. The participant stated,

If I know that I have a team member that is not on pace to be productive that term and I see them doing something that is not work-related on their computer, I may redirect them by going through their pipeline with them... simply just talking about what we need to do next right now to be productive. I do a great deal of

walking around, just for the sake of communication, so I believe that that also helps in reducing the cyberloafing itself...

A fifth participant affirmed that,

It's just kind of being there on the floor with them, seeing what they're doing...

My approach is more like just having that open line of communication... if you explain it enough I feel like you can bring it home, it's not hard to understand that the policies are there, there in place for a reason. So, once you get to the same page as the employee so they can understand why the policy is there, I think they walk away with a good understanding, they think, all right, I understand... when we communicate with it, after they see why, and then that way they back off and then they start doing the correct thing.

An interesting response shared by one participant in response to a follow-up question about mitigation activity described how the participant used verbal persuasion to redirect employee behavior. He stated,

I would tell that employee, you know how it makes me feel when I ask you to do something and you don't do it and I come in here and you're not meeting business objectives and you're still on Facebook or whatever the case is; you don't respect your job. You don't respect me as an employer; you don't respect the organization and you're just coming in here and that's worrisome to me.

The participant noted that having these types of conversations was persuasive and

helped redirect employee behavior. Finally, the last response to the probing question relating to how participants controlled cyberloafing, the participant stated,

I take a look at if your production's low, I see what you're doing every day. I observe for a while, are you spending too much time on the Internet and not focusing on your students in the queue, and usually if that is the case then I would have one-on-one conversations with those advisers... After we've talked about it and if decided they need to spend less time on the Internet or they need to be doing other activities, and I still observe that they're not, I probably would pull them aside again and ask them why they're not doing what we discussed... It's getting them to understand, 'You are here to do your job. You're not here to download your music or movies or play your game. I understand you want something to do between calls.'

Participants during member checking confirmed the accuracy of transcripts and restated summarized versions of initial responses during the follow-up sessions. In summary, participant believed that using observation and verbal persuasion positively affected the effectiveness of their role performance mitigating employee cyberloafing.

Emergent Subtheme 3: Setting Clear Expectations

The subtheme *setting clear expectations* corroborates the notion that setting clear expectations and monitoring results is an important managerial cyberloafing control strategy (Holguin, 2016). Participants recognized the value of communicating instructions relating to the 'what, why and how' of online technology usage expectations

to facilitate the effective control of employee cyberloafing behavior. This strategy aligns with Hersey and Blanchard's (2000) directing situational leadership style that involves the provision of clearly defined followership tasks. This subtheme emerged because of participants repeated references to the channeling techniques used to mitigate cyberloafing in relation to their responsibilities as managers. Participants mentioned that setting clear expectations about acceptable and unacceptable cyberloafing behavior empowered employees to self-regulate their online technology usage.

One participant stated, "I set very clear expectations with the team and I believe that the style of me being able to empower them and giving them the tools that they need to have ownership of their job."

Non-technical mitigation of online technology usage requires managerial control mechanisms that include planning, enforcement of usage policies, as well as employee sensitization programs (Rahimnia & Mazidi, 2015). Participants agreed that sensitizing employees with acceptable and unacceptable behavior empower them to self-regulate to meet the standard. Another participant stated emphatically,

I'm going to set expectations what I expect you to do, and you need to meet those expectations... So, I think that a person, and most individuals, they're going to go out if I'm clear in setting expectations that you're not meeting the productivity standards. Most people will go out and try to increase their standards and improve that.

Managerial capacity building interventions help reduce counterproductive employee workplace behaviors (Manzoor et al., 2015). One participant described how he used employee capacity building strategy to drive compliance that included having expectations sessions with team members. He stated,

One of the things that we usually do, especially at the beginning of the year, I personally do an expectations meeting... One of my expectations is... to be on task. I usually stress the current expectations for my team... my team, for the most part, complies, especially now.

Rahimnia and Mazidi (2015) indicated the managerial role in the management of employee cyberloafing allows for supervisory communication with the employee to control cyberloafing behavior. One participant described how engaging in supervisory communication with employees facilitated employee compliance with acceptable online technology usage. He stated,

My approach is more like just having that open line of communication, setting the expectation up front so they know exactly what they have to do and explaining the consequences, I think that's key, too, so you let them know exactly, okay, you can do it, I'm not going to be able to watch you 24/7 but if you do get caught this is what could potentially happen.

Middle manager participant's responses showed that channelizing managerial cyberloafing mitigation activity enhances the nurturing of productive employee behavior.

Emergent Subtheme 4: Understanding Duties and Obligations

The emergence of this subtheme *understanding duties and obligations* developed from responses shared by participants about their role experience as occupants of leadership positions responsible for driving employee performance and mitigating employee cyberloafing behavior. The middle manager's role effectiveness managing employee cyberloafing was linked with the middle managers understanding of the responsibility to ensure compliance of team members with acceptable online technology usage. As one of the participants worded it, "We are responsible for making sure that our employees once again are managing their time properly."

Middle manager participants presented a shared commitment to driving performance and a clear understanding of their responsibility for controlling employee cyberloafing in digital work environments. They understood that cyberloafing activity had the potential to adversely affect employee performance requiring them to adopt measures to control it. One participant explained this during our interview,

My role with mitigating against cyberloafing is extremely important because again, at the end of the day, if my team's not hitting their number, it's a third of the business... It's very important to me that my team is successful and we're hitting our targets and I mitigate against it because it can be a distraction.

Campbell et al. (2016) asserted that middle managers have contractual and legal obligations to safeguard their employer's interests and control employees under supervision. Middle manager participants found it indispensable to understand and

perform their responsibilities in relation to controlling employee activities and behavior.

One participant described this vividly during our interview,

My role in that would again be to be observant of what people are doing... My role is to understand which employees get off task and which employees stay on task. To know which employees are going to be on the Internet or trying to be on Netflix or Hulu and things like that. That is my role as a manager which again to me, I process that as to know who's going to be productive and who's not. So, in doing that as a manager, I do know who my heavy Internet users are and who are not.

A common denominator for this subtheme was that middle managers understood the responsibility that their organizations permitted minor cyberloafing within reason, however, serious cyberloafing was unacceptable and requiring active enforcement. An interview with a participant described this as follows, "Culture and employee satisfaction from productive employees is very important to us. So, by that stance, we are okay with personal Internet usage to a level... pornography, indecent exposure, is unacceptable. Profanity, those are unacceptable things..."

Middle managers also understood that their role in the mitigation of employee cyberloafing required equitable enforcement within their teams. As one participant described it,

Everybody is managed to the same business result and with the same standard of what is acceptable and what's not but the delivery of those messages and the style

of the delivery of those messages is different based on how the receiving party and the varied employee would receive it.

Although all participants agreed that having a clear understanding of their responsibilities for mitigating cyberloafing activity facilitated effective enforcement and performance. Some expressed an aversion toward non-work related online technology usage. As one participant stated, “My role in the cyberloafing mitigation is to really ensure that my staff are consistently on task for the most part... it comes down to if you can get your employees engaged, and doing their work, that means they’ll become more productive overall... I’ve always identified being on the computer, on the Internet surfing, as one of the distractions that my employees should always try to avoid.”

There were participants who indicated an understanding of the managerial responsibility for helping employees manage their work time efficiently enhanced the role performance mitigating cyberloafing. One participant stated,

In my role, it does require that I assist my team and my advisors to manage their time properly so that they are still successful in their role and meeting their daily expectations here in the organization and not misusing their time and placing themselves in danger by doing so. It has really placed that balancing act on the role of the immediate supervisor to say, ‘Okay, let’s redirect. It’s not that you can’t do it. Let’s just make sure that we are managing our time properly.

Others noted that as middle managers, they were held accountable for employee

online technology misuse requiring them to have a clear understanding of their responsibilities. As one participant described it,

My job is to not only monitor their production but monitor what they're doing while they're using the computer for Company... my responsibility on it is, if it gets to that level, let's say IT or someone upper level, in operations, sees it, I'm looked at like, well, you missed it. Like, okay, there's something ... if it got to us, it means it went further than you, so that one aspect you missed that this employee was doing this and then I'm questioned, 'where were you, what did you do to prevent this, did you communicate to the employee?'

Campbell et al. (2016) posited that middle managers have contractual and legal obligations to guard the interests of their organization and to control employees under supervision. Middle manager participant's descriptions of their lived experiences showed that having a good grasp about managerial duties and obligations and a commitment to driving performance enhanced their role performance mitigating employee cyberloafing activity. Participants did not provide any additional information or disagree with the interviews transcripts or themes development during member-checking.

Emergent Subtheme 5: Using Managerial Discretion

This subtheme *using managerial discretion* emerged from responses participants offered indicating that middle managers with the latitude of actions available to exert control on their employee cyberloafing activity behavior were likely to be more effective in their role performance. Participants expressed feelings of satisfaction with having the

freedom to be flexible in their approach to controlling employee cyberloafing activity. Some participants indicated an aversion to micromanaging employee activity because they wanted to encourage employee self-regulation of daily activities with a focus on work-related activity. In agreement with Chiu and Peng (2008) micromanaging employees could lead to the perception of abusive supervision resulting in employee deviance.

Participants described how they used latitude of actions available to them to exert control to drive the desired cyberloafing mitigation outcomes. As an example, one participant stated,

I am the furthest thing from a micromanager... If somebody is successful and their job is done, I'm not sitting there saying 'hey, why are you on Facebook' things like that, but if there's somebody on the team who is suffering and their numbers aren't there and I see them on Facebook all day, I'm going to say 'hey, what are you doing? Is that the best use of your time?' It's kind of a give and take because again, we're all adults here, I'm not here to say 'hey, why are you on the Internet.'

In response to a follow-up question to clarify meaning, participants described how using discretion allowed the manager relax control during downtimes at work and as he described it,

There are days where some of my agents are on the phone every minute of every day and then there are days where they're waiting two hours between calls.

There's only so much outreach activity that we can do and it kind of depends.

Another participant described how he allowed minor cyberloafing activity as far as the employee meets performance requirements. As one of the participants worded it,

As long as those are getting done, they can cyberloaf if they want to. I don't have a problem with them doing other things if it's not interfering with the tasks and responsibilities they do at their jobs... I view you as a professional who understands what you need to do to get your job done. And I don't have to, maybe some would say micro-manage you, stand over you, and make sure you're doing that.

Other participants adopted a laid-back approach to cyberloafing management and as one participant described it, "My success comes from just my leadership style, to be honest with you. I'm not the type of leader that's always going to be...I don't micro-manage. Similarly, another participant stated, "I do not set a rule on the team that says, 'You may not be on the Internet for an hour per day,' I do not do that. Instead, I will redirect. I do not set a time limit or a rule on my team about that." One participant, however, indicated a willingness to closely control employee online technology usage when required. He stated, "If it comes to the point that I have to micro manage I will, it's not my preference, but, if it's necessary then it's done."

Likewise, one more participant described using managerial discretion to determine when or when not to adopt a micro-management strategy to deal with employee cyberloafing. The participant stated,

If you're producing and overproducing, and on top of your students, I don't pay much attention to what's your personal use of the Internet, because it is allowed on the floor. I like to have my hand in the business and I like to be voluntarily told what's going on without me having to go into your business. However, if I feel the need or I feel that you are not handling your business correctly, I will start to micromanage you.

Emergent Subtheme 6: Working with Unclear Mitigation Policies

Organizations continue to struggle with issues relating to balancing employee online technology usage rights and organizational needs for employee performance and protections against liability creating ambiguities in mitigation policies (Cox, Goette, & Young, 2005). In line with Cox, Goette, & Young (2005), the subtheme *working with unclear mitigation policies* emerged during participant's responses about the effectiveness of their implementation and enforcement of organizational acceptable online technology usage policies in a rapidly changing technological environment. Participants expressed feelings of frustration with having ambiguous cyberloafing mitigation policies within their organizations. As one participant stated,

There is, not a specific policy around it... regarding checking personal email and being able to go on YouTube and watch a video here and there, there's not an explicit that you absolutely under no circumstances should be doing this, versus like a..., as long as you're doing your job, your successful in your job, again the thinking is we are all adults.

Other participants reported that within their organizations, employee cyberloafing mitigation policies were unclear or unspoken. As one participant worded it, “It’s an unspoken policy.” Another participant acknowledged having a policy in place but noted a lack of explicitness when he stated,

Our policy would be more something, and I’m not quoting it word for word, but it would say something to the effect that any conduct that would be offensive to your neighbor, or something like that, is unacceptable. So, there’s no policy that would say, ‘You cannot look at pornography. Or you cannot watch TV shows where they use profanity.’ But it would say, ‘Conduct that is viewed as unprofessional in the workplace or offensive to your co-workers is unacceptable.’ That would be the extent to the policy we have.”

One participant described how her organization transitioned from tighter control policies to more flexible policies because of the nature of work empowering more managerial autonomy. The participant stated,

There is no policy, per se. I don’t think we have a real strategy. It’s more of it’s up to the associate director to manage their team. We’ve had in the past, had floor guidelines, and we try to stick with those, but it’s not something that’s brought up regularly. It’s just up to the associate directors to manage their teams and make sure production is still moving along... I feel that there should be some tighter rules in place for some of the floor guidelines, such as the Internet usage to make sure our advisors are being more productive, but because we’re in the

environment of waiting for calls most of the time it's hard to do that. When you're in the outbound environment it's a lot easier, because there are things that you could be doing every minute.

Another participant noted that because of the downtime at work, the organization permitted minor cyberloafing during work. A participant stated, "Here at work we have a lot of downtime between phone calls, so it is permitted that the advisors can use the Internet, personal use between calls, ensuring their work is done as well outside of the calls."

Emergent Subtheme 7: Staying Current With Technology Advancements

The subtheme staying current with technology advancements emerged as participant described how their knowledge about the proliferation of nomadic computing and the consumerization of mobile devices affected the effectiveness of their role performance mitigating employee cyberloafing. Some participants felt it was important to keep abreast with advancements in online technology to facilitate a better understanding of employee cyberloafing behavior. Rice and Leonardi (2013) noted that employee decisions to use both personal and work-provided online technology to communicate, manipulate, and storage of information for personal business depend on a variety of personal factors.

Participants felt that keeping current with technology advancements allowed them to be more proactive with their mitigation strategies. One participant stated,

My role in mitigating against it is to be staying current with how technology is changing and evolving so that I can plan how to mitigate against that... Staying up to date and in tune with these enhancements and developments as much as possible so that I can be proactive instead of reactive. So, that I can have a generalized idea of what's happening and how to mitigate against it versus having somebody show up and it's like, there's this whole new era of people doing crazy different things.

Another participant described how knowledge about online technology advancements facilitated effective non-technical mitigation strategies. The participant stated,

My knowledge about those additional technologies available does. It has helped and impacted my knowledge and mitigation strategies, because again, with an iWatch, right, you can send messages back and forth. You can do quite a few things with your wearable technologies and tablets and things like that. It just helps me to not just look at the computer screen, maybe pay attention to what's on the employee's desk as I walk around. Just for awareness, I don't plan to be a stickler for those things. I mean, if you're wearing an iWatch and you're checking a message, I'm not really opposed to that. I even have employees that will bring in their own laptop separate from the work device, and they'll play a basketball game on their desk from a separate device. I'm not opposed to that as long as they

aren't working, but yes, it does make me more aware and attuned to looking at not just the screen but everything that's going on.

Other participants acknowledged how technological advancements have created dependencies affecting individual daily activities. The participant stated,

I think it impacts it just because I think it's more the reliance, if you notice, just go back the last 10 years, there's more reliance on technology that there ever has been. People are dependent on it for just about everything, we're talking about from shopping to just traveling. People don't look at maps anymore. People use the GPS on their phones... They can do more on a phone or on that type of device than they can do on the computer there. When they're dependent on it, it's almost like an addiction now, so, if somebody's constantly on it, then yes, that's going to affect their work.

Discrepant Cases

All participants answered interview questions providing useful details about their experiences with their role managing employee cyberloafing behavior at work. None of the participants refused to answer any of the interview questions. During a review of the interview transcripts, I identified two discrepant cases where participant responses differed significantly from the responses of other participants. In the first instance, one participant felt that manager/employee proximity had minimal effects on his role mitigating cyberloafing at work. He explained that only 20% of his employees work

onsite and he empowered his employees to take ownership of their Internet activity and made sure to set the right expectations.

In the second instance, the responses to interview question by another participant that was the highest-ranking manager that participated in the study, were bereft of significant detail even when prompted to expand his answers. The participant controlled and oversaw an entire admissions department and as such, he demonstrated a lesser amount of knowledge about the role compared to all other participants. As an example, each of the participants shared specific examples of experiences encountered during employee cyberloafing interventions. Responses made by all the other six participants to the interview question on experiences with mitigation and the effects on performance described their experiences as either an astonishing, an illuminating, or a learning experience.

In contrast, the participant offered no specific experience even after probing further during the interview his senior position within his department provided for additional layers of supervision under him which appeared to shield him from having sufficient direct experience with mitigating the employee cyberloafing. This explained the inability to share specific instances relating to personal experience with cyberloafing mitigation interventions.

The Essence of Participants Experience

The essence of participant's experience is a composite depiction of the meanings participants ascribed based on first-hand accounts about their role as middle managers in

the mitigation of employee cyberloafing. This depiction provides an intuitive amalgam of the textural and structural participant descriptions about their experience. The middle managers interviewed shared stories about their role perceptions, role behaviors, and role performance; lived within the context of mitigating employee cyberloafing.

They shared their beliefs, feelings, and thoughts about their role in the mitigation of employee cyberloafing at work and suggested that the most important control activity required active monitoring of employee's cyber-behavior and performance. Cyberloafing activity is permitted to some extent within organizations and middle managers need a good grasp of their role in the mitigation of cyberloafing behavior to help set clear expectations, recognize unproductive activity, and intervene when necessary (Schalow et al., 2013). Also, participants displayed situational leadership as evidenced by their preparedness to intervene when employees engaged in unproductive cyberloafing affecting their performance. Participants exhibited elements of the Hersey-Blanchard situational leadership model with the four distinct styles delegating, participation, selling, and telling (Hersey et al., 1979).

Workplace responsibilities holding participants accountable for driving employee performance together with the adverse effects of cyberloafing activity made it an imperative for middle managers to mitigate cyberloafing to enhance performance. Middle managers interviewed believed that if the mitigation barriers they experienced were removed, their role mitigating cyberloafing behavior would be significantly enhanced and could yield increased levels of employee performance.

Each participant understood that cyberloafing activity, especially in digital work environments, required managerial vigilance to redirect employees from cyberloafing. Also, participants viewed the mitigation of employee cyberloafing from a performance perspective, channelizing mitigation efforts, and combining observation with verbal persuasion. Having a personal commitment to driving performance and an understanding of the responsibility for controlling employee cyberloafing is essential for managers in digital work environments.

When the workplace allows managerial discretion in the control of employee cyberloafing activity, employee performance can be assured as far as the manager channels his or her mitigation efforts proactively. Individuals involved in that role have the ability use their proximity with employees to monitor and intervene when cyberloafing activity begins to affect employee performance. Manager propinquity to employees under supervision is a useful tool that provides a mechanism for the effectiveness of managerial control of cyberloafing behavior.

Organizations with digital work environments benefit from having on-site managers that understand their responsibility managing cyberloafing with work facilities designed to enhance the effectiveness of managerial monitoring. Finally, participants viewed an understanding of employee appropriation of technology use and technological advancements as useful enhancers of mitigation performance and effectiveness.

Summary

In Chapter 4, I presented a description of the research setting, participant demographics, participant recruitment, data collection, data analysis process, and evidence of measures used to establish trustworthiness. I provided information about the results of the data analysis used to uncover the meaning participants ascribed to their role in the mitigation of employee cyberloafing at work. Also, in this chapter, I offered details on the thematic development process used to derive the essences of participant experiences and discussed discrepant cases identified during data analysis. In Chapter 5, I describe how the results contribute to the body of knowledge on cyberloafing management. The chapter includes information on the study's limitations and its influence on trustworthiness. Chapter 5 ends with recommendations for future research and implications of the study from a social change perspective.

Chapter 5: Discussion, Conclusions, and Recommendations

This chapter provides a recapitulation of the study's purpose, the methods used to facilitate discovery, as well as a summation of the results. In addition, I discuss the conceptual frameworks influence on the interpretation process from a post-data analysis perspective. The chapter includes information on the study's limitations and its influence on trustworthiness. Recommendations for future research and implications of the study from a social change perspective will conclude the chapter.

Overview

This phenomenological study was designed to explore the lived experiences of middle managers about their role mitigating employee cyberloafing at work. The pervasive nature of employee cyberloafing activities at the workplace despite electronic monitoring and technical deterrence systems within organizations informed the decision to conduct this study. The study specifically focused on the digital workplace where employees use only computer hardware, software, interfaces, and connectivity solutions to perform work tasks, collaborate, and provide services to clients.

This study used a qualitative research method and the transcendental phenomenological approach that involved core processes aimed at facilitating the unraveling of knowledge. Qualitative research methods offer a holistic framework that facilitates a broad exploration of complex issues related to a lived experience (Khan, 2014). The lived experience of middle managers concerning their role in the mitigation of employee cyberloafing at work was the central focus of this study. A quantitative method

did not usefully allow for the uncovering of a realistic view of participants lived experiences and provide a comprehensive description of the issue (Yilmaz, 2013).

This study is pioneering the first research effort aimed at exploring the role of middle-level management in the mitigation of employee cyberloafing at work using a conceptual framework that draws from the symbolic interaction and adaptive structuration theories. Contemporary research on cyberloafing management within organizations continues to hover around combining deterrence mechanisms with functional strategies individual manager develop to drive performance. This study extends the knowledge on cyberloafing management by providing insights as to the mental conversations middle managers controlling cyberloafing behavior in digital workplaces have about their role.

Interpretation of the Findings

Descriptive phenomenology aims to recount the all-important and meaningful essences of an issue relying primarily on the rich textual data from participant responses (Giorgi, 2012). Contemporary research studies focused predominantly on the variation of managerial strategies used to mitigate cyberloafing behavior in terms of successes recorded, significance, and working with digital natives, as discussed in Chapter 2. In terms of the central research question that looked at the role of middle managers in the mitigation of employee cyberloafing at work, the findings of this study helped extend knowledge on the managerial role in the organizational cyberloafing management efforts.

Blumer's (1969) symbolic interaction theory and DeSanctis and Poole's (1994) adaptive structuration theory served as tools of engagement governing the data collection plan and illuminating information during data analysis. The symbolic interactionist worldview helped elicit the multiple realities participants developed through social interaction and lived experience while the symbolic interactionist lens advanced the uncovering of influences that shaped middle managerial perceptions about their role in cyberloafing mitigation.

The middle manager's role experience mitigating cyberloafing involves a continuous process shaped by periodic monitoring of employee performance on one end, the use of functional interventions on the other, and a varied mix of ideas developed in between. The daily routine of the middle manager involves activities that facilitate the development of a working knowledge of employee appropriation of technology for both work and non-work-related activity which in turn fosters the development of effective cyberloafing control measures.

The results provided a window through which other researchers could understand meaning middle manager participants ascribed to the mitigation of cyberloafing based on their proximity with employees and their first-hand experiences with employee appropriation and use of online technology. Traditional understanding about the middle manager has been that of using managerial control to keep employees in line with their work performance requirements (Holguin, 2016; Manzoor et al., 2015; Pînzaru & Mitan,

2016). The participants shared their perceptions about their role perceptions, behaviors, and performance within the context of mitigating employee cyberloafing at work.

The key findings of this study helped recognize and illuminate the significance of the middle manager's role in the organizational efforts aimed at employee cyberloafing mitigation. Predominantly, I identified four key components of the middle manager's role in cyberloafing mitigation. The themes encapsulating the meaning of the middle manager's role in cyberloafing mitigation at work include managing employee performance, proximity matters, cyberloafing interventions, and understanding employee online technology usage.

Subthemes representing the different elements of the non-technical techniques embraced by participants during cyberloafing mitigation included mitigation barriers, observing and persuading, setting clear expectations, understanding duties and obligations, using managerial discretion, working with unclear mitigation strategies, and staying current with technology advancements. Also, the findings support the notion that middle managers, especially in digital workplaces play a key role using a combination of managerial control mechanisms to curtail employee cyberloafing. Evidently, the middle manager's role in the mitigation of employee cyberloafing at work required active monitoring of employee's cyber-behavior and activity.

The first theme, managing employee performance, was the most important because of middle managers understand that maintaining situational awareness about employee performance fosters the recognition of cyberloafing activity.

Unlike findings in Holguin (2016) and Grossenbacher-Fabsits (2011), the results of this study highlighted middle manager experiences and thoughts about their roles in organizational efforts aimed at curbing employee cyberloafing in digital work environments. Managerial role perceptions about cyberloafing mitigation are developed through workplace interaction allowing for increased sensitivity to situational elements related to employee online technology use, activities or behaviors affecting production and necessitating intervention. The results revealed that managers who maintained a situational awareness about performance while managing employee performance were more likely to control employee cyberloafing activity more effectively.

The second theme, proximity matters, proved to be an important element of the middle manager's role in the organizational efforts aimed at the mitigation of cyberloafing. The theme confirmed Rahimnia and Mazidi's (2015) findings that managerial proximity enhances opportunities for supervisory use of verbal persuasion and manipulation to control employee behavior. Also, data from this study supported Grover's (2014) assertion that monitoring proximity required managerial critical understanding to foster the adoption of cyberloafing mitigation strategies that avoid the backlash of animus and instead enhance positive outcomes from employees.

Monitoring proximity creates some complexities especially in workplaces that combined both remote and onsite workers. The challenge is dealing with online technology misuse when more than half of the workforce worked remotely. An open office layout facilitated physical closeness with problematic employees making it easier

to use prompts or verbal instruction. Managers taking advantage of proximity control are likely to be more effective in their organizational role controlling employee cyberloafing.

The theme cyberloafing interventions align with Harding et al.'s (2014) findings that the middle manager's role within business organizations entails the containment of employee behavior through direct control and manipulation. Managerial experience with employee cyberloafing interventions provides an opportunity to develop mitigation plans to help encourage productive employee behavior. Mitigating cyberloafing in a work environment with strong technical mitigation and strict acceptable usage policies enhances their role performance.

The theme understanding employee online technology usage confirmed the findings by Liao et al. (2009) that suggested middle manager's responsibility for controlling team members necessitated an understanding of appropriation of online technology when looking to mitigate misuse. The data from this study also supported results from Andreassen et al.'s (2014) study that indicated middle manager aversion to employee online technology misuse. Managers with a good understanding of employee technology usage would more likely adopt effective coercive strategies to demand and obtain employee compliance with acceptable behavior.

The subtheme mitigation barriers revealed that cyberloafing mitigation barriers adversely affected their role performance mitigating employee cyberloafing. The results support findings in Schalow et al. (2013) that found an escalation of the cyberloafing problem through the employee requirement to use of online technologies like social

media for work creating challenges setting boundaries between non-work and personal usage. Using observation and verbal persuasion positively affects the effectiveness of their role performance mitigating employee cyberloafing.

The subtheme observing and persuading depicts participant's beliefs about their role behavior during employee cyberloafing interventions using observation and verbal persuasion to mitigate employee cyberloafing at work. Travis, Sarah, Bharat, and Jitendra's (2017) conclusion that managerial use of verbal persuasion is vital especially in situations dealing with difficult employees seems to be generated by the prevalence of problematic employee behavior at work. Jamaluddin et al. (2015) found communicating the linkage between cyberloafing activity and reductions in performance enhanced the effectiveness of managerial control of cyberloafing which seems to parallel the results of this study indicating the use of situational awareness about employee performance as a precursor for managing cyberloafing.

Using observation and verbal persuasion are important mechanisms that positively affect the effectiveness of the middle manager's role performance driving acceptable employee online technology usage. The results support Soror et al.'s (2012) advocacy for alternative strategies for handling excessive online technology usage by facilitating self-regulation and identifying mechanisms to encourage acceptable usage.

The subthemes setting clear expectations confirmed findings in Holguin (2016) that indicated functional managers controlled unacceptable cyberloafing by communicating expectations about online technology usage. Communicating clear

expectations is an integral part of performance management at the workplace (Pulakos, Hanson, Arad, & Moye, 2015). Managers channelize their cyberloafing mitigation efforts to enhance productive employee behavior. Setting clear expectations and holding the employee accountable provided an opportunity to encourage self-regulation and autonomy.

Managerial understanding of duties and obligations, one of the subthemes that emerged during data analysis, is an important part of the middle manager's role during cyberloafing mitigation. This subtheme aligned with Campbell et al.'s (2016) assertion that middle managers have contractual and legal obligations to protect employer interests while controlling employees under their supervision. In addition, the subtheme resonates with viewpoint shared in Harding et al. (2016) that middle managers have the responsibility for using control mechanisms and manipulating social interactions to drive performance. Managerial commitment to driving productivity and an understanding of the responsibility to control employee cyberloafing are an essential part of the middle manager's role in the organization's mitigation efforts.

The subtheme using managerial discretion emerged after participant responses showed that they did not like to control every employee activity. Managerial discretion refers to managers at the workplace having the latitude to take decisions about how they manage employee cyberloafing behavior (Birdsall, 2017). Managers use latitude when making decisions about their approaches dealing with cyberloafing interventions.

This subtheme does not align with Henle, Kohut, Booth (2009) finding that pointed out the arbitrary nature of allowing managerial discretion in the mitigation of cyberloafing within organizations leading to employee perceptions of unfair treatment. Despite the aversion, using managerial discretion can be explained by the lack of clear mitigation policies within some business organizations. In theory, having the flexibility to control managerial approach to mitigating employee cyberloafing activity increased the effectiveness of their role performance.

Working with unclear mitigation policies was the next subtheme that emerged during data analysis. Cyberloafing activity is permitted to some extent within organizations requiring middle managers to have a good grasp of their role in the mitigation of cyberloafing behavior. Schalow et al. (2013) showed how cyberloafing continues to pervade organizations, especially as employee requirements to use of online technologies for work making it difficult for the employee to establish clear boundaries between non-work and personal online activity. Working with unclear cyberloafing mitigation policies adversely affects managerial mitigation role performance.

The last subtheme, staying current with technological advancements affects the middle manager's role performance mitigating employee cyberloafing. This supports Melrose et al.'s (2016) assertion that advancements in online and communication technologies continue to transform the lives of humans with increasing levels of incorporation into the day to day functioning. An understanding of new technological developments facilitates the proactive development of new strategies aimed at mitigating

employee misuse of the new technology. In general, staying current with technological advancement creates the opportunities for proactive approaches to mitigation of employee cyberloafing activity rather than reactive approaches.

Limitations of the Study

In this study, I have addressed only the role of the middle manager in mitigating employee cyberloafing at work specifically within the context of a digital work environment. The research setting for this study was restricted to work environments within the higher education industry in Florida; however, it would have been useful to have had a wider spread of contexts with a participant pool drawn from other industries with predominantly digital work environments.

Although the interview questions generated valuable information about the experience, I believe it would have been beneficial to have included participant observation in the research design. Data collection, analysis, and interpretation processes required additional expertise to ensure rigor due to my inexperience with qualitative research. Another limitation involved using of face-to-face interviews and one telephone interview as the primary data collection method. I addressed this limitation by triangulating data sources combining interview data, with data from interview notes, and reflective journals.

A potential for researcher bias developed during data collection because three participants included in the study occupied management position at the same organization where I hold employment. I ensured to fully disclose the nature of the relationship with

participants and it is noteworthy that the three participants in reference, work in a different division and occupied positions above me in terms of hierarchy, therefore eliminating any potential for undue pressure. I believe they provided true and honest responses because their transcripts did not indicate any more positive information in comparison with the other participants.

My engagement with all participants did not present any challenges surrounding undue familiarity influencing the objectivity of responses. One participant that indicated a willingness to participate that was well known to me was eliminated from participating during the pre-selection process.

Recommendations for Further Research

My focus for this study centered on gaining an understanding of middle manager feelings about their role managing employee cyberloafing within a digital work environment. I purposefully selected 7 participants with experience managing employee cyberloafing from higher education institutions in Florida for interviews using a semistructured format. From the themes that emerged after data analysis, the transcendental phenomenological approach, an initially developed form of phenomenology that seeks to discover only the described and lived experiences of the participant, facilitated the unraveling of true meaning participants ascribed to their human experience mitigating employee cyberloafing (Moustakas, 1994).

I used a combination of face-to-face interviews and telephone interviews to collect data on participant's feelings about their role mitigating employee cyberloafing in

a digital workplace. The study aimed to disclose human experience derived from human consciousness presenting the data without adding or making inferences and generalizations. As outlined in the data analysis plan, the data analysis for this study developed analytical outputs about the factors influencing how middle managers felt about their role mitigating employee cyberloafing at work. Data analysis procedures used in this study drew from the modified Van Kaam method outlined in Moustakas (1994) and I combined hand coding and NVivo 11 Pro software coding during data analysis with the NVivo 11 Pro software program used for data management and storage.

The research design development involved the identification of a specific problem despite the host of challenges associated with the management of employee cyberloafing. This study centered on middle managers working in organizations associated with digital work environments. The interest in exploring middle managers emanated from their responsibility as first line supervisors for driving performance among employees.

As outlined in Chapter 1, the limitations of this study provide opportunities for further research using an alternative research approach or research instrument to gain a different perspective of the issue. Future researchers could consider collecting data using a case study research design to gain a deeper understanding of the issue through interviewing and observation. Including observation to the researcher's data collection plan could foster the identification of observable elements not included in my study. Furthermore, my study pioneered the adoptions of the symbolic interaction and adaptive

structuration theories as a conceptual framework. Using a case study design would allow the researcher an opportunity to challenge the theoretical assumptions of this study.

Participants in this study indicated that managing employee cyberloafing, if conducted using employee performance metrics to detect distractions, offers managers a useful method in combination with technical mechanisms for identifying individual cases of cyberloafing in digital workplaces. Another opportunity for future research would involve the adoption of a quantitative design to explore further the relationships between maintaining situational awareness about employee performance and the management of employee cyberloafing activity. Quantitative research methods focus on determining the association between variables in a population, uncovering the disposition of the variables, and making justifications about knowledge.

The third opportunity for future research involves taking a closer look at the barriers hindering the effectiveness of the middle manager's role performance during cyberloafing mitigation to uncover possible ways to overcome them. An ethnographic research design would facilitate the immersion of the researcher within the target population's environment to gain a first-hand worldview of the issue. Relatedly, the results of this study revealed managerial adaptation to working with unclear cyberloafing mitigation policies. Another opportunity for future research would involve conducting research to understand the associated peculiarities.

Implications

My study provided answers to the research question offering the wider community of interest on cyberloafing management valuable information about managerial contributions to the overall organizational efforts aimed at mitigating employee cyberloafing. Seemingly, the results make several contributions to the research literature on the management of cyberloafing supporting the need for organizations to consider redefining their managerial functions. The results also suggested that the middle manager plays a consequential role in the mitigation of employee cyberloafing at work.

Significance to Practice

Until recently, the focus of cyberloafing research has centered on managerial control supplying business organizations with best practices and learning opportunities. In contrast, this study zeroed in on the managerial role of middle managers mitigating cyberloafing behavior by evaluating participant's perceptions about their experiences. Consequently, the results of this study are important to practice because they bring to light the masked middle managerial role enhancing a better understanding of their mitigation efforts. Recognizing and illuminating important managerial cyberloafing role activities could help facilitate the development of clearer definitions of the middle manager organizational role mitigating cyberloafing within organizations.

Significance to Theory

This examination of the managerial role in the management of employee cyberloafing at work using a conceptual framework drawing from the symbolic

interaction and adaptive structuration theories enhanced the originality of the research study. Collectively, the two theories facilitated a deeper understanding of the symbolic meaning middle managers developed about their role in cyberloafing mitigation acquired during workplace interactions with subordinate employees and the meaning they ascribed to employee appropriation of online technology use at the work and how that knowledge affects their role mitigating such behavior.

The target population of the study was all middle manager's responsible for supervising employees using online technology to perform work tasks, research into the managerial role in the management of employee cyberloafing is minimal compared to that on the strategies middle managers use to manage cyberloafing. Even though some research is available on managerial approaches to cyberloafing management (e.g. Grossenbacher-Fabsits, 2011; Holguin, 2016; Manzoor et al., 2015; Pînzaru & Mitan, 2016; Saraç & Çiftçioğlu, 2014), they have been conducted mainly a strategy perspective, rather than a role one as is the case in this study.

This study's outcomes provided a window through which other researchers could understand influences, choices, and identities related to organizational online technology users. The study was significant to theory because it offered new knowledge that could help businesses reshape cyberloafing control mechanisms and policy implementation.

Significance to Social Change

The participants involved in this study were mid-level managers actively engaged mitigating employee cyberloafing activity at work. Among the four role activities

identified, managing employee performance through situational awareness of employee cyberloafing activity was considered the most important managerial role activity, especially for managers working in predominantly digital work environments. An understanding of the transformational influence the middle manager uses to mitigate employee cyberloafing behavior offers businesses with an opportunity to develop new mitigation strategies developed from a better understanding of the manager/employee interactions as well as managerial knowledge of employee appropriation of online technology. Consequently, my results should broaden our knowledge on the role middle managers play in the organizational efforts aimed at mitigating employee cyberloafing at work.

Conclusion

In the July 1995 edition of the New York Daily News, Kamins published an article “Cyber-loafing: Does Employee Time Online Add Up to Net Losses?” At the time, few organizations and their employees concerned themselves with the relatively unknown term. Today, the cyberloafing phenomenon permeates globally creating productivity losses for organizations and consternation for managers responsible for driving employee performance. Indeed, the relentless advancements in online technology continue to transform people’s lifestyles, workplaces, businesses, in terms of the ease of accessing, disseminating and sharing information (Connell, Gough, McDonnell, & Burgess, 2014; Melrose et al., 2016). Per Deloitte (2014), the digital workplace includes all work environments where employees use mainly computer hardware, software,

interfaces, and connectivity solutions to perform work tasks, collaborate, and provide services to clients.

Yet, the consumerization of personal information and communication devices like smartphones, tablets, portable gaming devices, and portable laptops substituting organization-owned devices is causing great perturbation for organizations and their managers because of the associated distractions resulting in productivity losses (Pirani & Meister, 2014; Porter & Heppelmann, 2015). Today, between 60% and 80% of employees engage in cyberloafing activity during work hours resulting in losses in productivity (Nazareth & Choi, 2014). In an analysis of the annual cyberloafing related productivity losses to businesses in the United States, Jia et al. (2013) reported that costs run between \$54 billion and \$84 billion.

Despite the adoption and deployment of the policies and technical deterrence mechanisms, employee cyberloafing continues to persist (Glassman et al., 2015). The pervasive effects of employee cyberloafing on performance require the augmenting of existing cyberloafing strategies to enhance overall organizational performance (Kataria, Rastogi, & Garg, 2013). Lim (2002) made one of the first attempts at differentiating the types of cyberloafing behavior where she distinguished cyberloafing activity into browsing and emailing. Browsing activities included visiting websites for entertainment, financial services, news, social networking, shopping, sports, and pornography to name a few. Emailing activities involved the reviewing, receipt, and exchange of personal emails. After an investigation of actual cyberloafing behavior, Blau, Yang, and Ward-

Cook (2006) expanded the types of cyberloafing activities by introducing another category that involved interactive Internet activity. Interactive Internet activities included playing live online games, chatting online, making live posts on social networking sites, and downloading information.

In the past decade, we have seen the emergence of research on the management of employee cyberloafing with innovative theories and methodological procedures used in the context of social constructivist-interpretive conceptual frameworks. The conscious acts of intellection behind researcher interests in the management of employee cyberloafing centers on the need to improve employee performance and reduce revenue losses resulting from cyberloafing activity (Holguin, 2016).

The gap between evidence of the effectiveness of detection mechanisms and the enforcement of cyberloafing mitigation policies may be due to poor supervision of online technology use. Middle managers play a significant role in enhancing the performance of teams under their supervision. Middle managers in extant cyberloafing research have received little attention, yet they might play a vital role in the management of employee cyberloafing behaviors and activities. Few studies have focused on the adequacy and effectiveness of the strategies used by middle managers aimed at mitigating the different typologies of employee cyberloafing. This study explored middle manager roles perceptions about their experiences during the combating of employee cyberloafing.

Manager physical proximity to employees under supervision is a useful tool that provides a mechanism for the effectiveness of managerial control of cyberloafing

behavior. Organizations with digital work environments benefit from having on-site managers that understand their responsibility managing cyberloafing with work facilities designed to enhance the effectiveness of managerial monitoring. Participants shared their beliefs, feelings, and thoughts about their role in the mitigation of employee cyberloafing at work and suggested that the most important control activity required active monitoring of employee's cyber-behavior and performance.

Cyberloafing activity is permitted to some extent within organizations and middle managers need a good grasp of their role in the mitigation of cyberloafing behavior to help set clear expectations, recognize unproductive activity, and intervene when necessary (Schalow et al., 2013). Also, participant displayed situational leadership as evidenced by their preparedness to intervene when employees engaged in unproductive cyberloafing affecting their performance. Participants exhibited elements of the Hersey-Blanchard situational leadership model with the four distinct styles delegating, participation, selling, and telling (Hersey et al., 1979).

Workplace responsibilities held participants accountable for driving employee performance together with the adverse effects of cyberloafing activity made it an imperative for middle managers to mitigate cyberloafing to enhance performance. Middle managers interviewed believed that if the mitigation barriers they experienced were removed, their role mitigating cyberloafing behavior would be significantly enhanced and could yield increased levels of employee performance. Seemingly, the results of this study make several contributions to the research literature on the management of

cyberloafing supporting the need for organizations to consider redefining their managerial functions. The results also suggested that the middle manager plays a consequential role in the mitigation of employee cyberloafing at work.

References

- Adu, P. (2016, August 8). *Step-by-step process of conducting qualitative analysis using NVivo 11*. Retrieved from <https://www.slideshare.net/kontorphilip/stepbystep-process-of-conducting-qualitative-analysis-using-nvivo-11>
- Aghaz, A., & Sheikh, A. (2016). Cyberloafing and job burnout: An investigation in the knowledge-intensive sector. *Computers in Human Behavior, 62*, 51-60.
doi:10.1016/j.chb.2016.03.069
- Al-Shuaibi, A., Subramaniam, C., & Shamsudin, F. M. (2014). The mediating influence of job satisfaction on the relationship between HR practices and cyberdeviance. *Journal of Marketing and Management, 5*, 105-119. Retrieved from <http://www.gsmi-ijgb.com/>
- Al-Shuaibi, A. S. I., Shamsudin, F. M., & Subramaniam, C. (2013). Do human resource management practices matter in reducing cyberloafing at work: Evidence from Jordan. *Journal of WEI Business and Economics, 2*, 37-47. Retrieved from <http://westeastinstitute.com/journals/jweibe/>
- Ali, S. M. (2013). Challenges and security issues in future IT infrastructure components. *International Journal of Computers & Technology, 8*, 845-847. Retrieved from <https://cirworld.com/index.php/ijct>
- Anandarajan, M., Teo, T. S., & Simmers, C. A. (2014). *The Internet and workplace transformation* (2nd ed.). New York, NY: Routledge.
- Andreassen, C. S. (2015). Online social network site addiction: A comprehensive review.

- Current Addiction Reports*, 2, 175-184. doi:10.1007/s40429-015-0056-9
- Andreassen, C. S., Torsheim, T., & Pallesen, S. (2014). Predictors of use of social network sites at work: A specific type of cyberloafing. *Journal of Computer-Mediated Communication*, 19, 906-921. doi:10.1111/jcc4.12085
- Anitha, J. (2014). Determinants of employee engagement and their impact on employee performance. *International Journal of Productivity and Performance Management*, 63, 308-323. doi:10.1108/IJPPM-01-2013-0008
- Askew, K., Buckner, J. E., Taing, M. U., Ilie, A., Bauer, J. A., & Coovert, M. D. (2014). 2014. Explaining cyberloafing: The role of the theory of planned behavior, *Computers in Human Behavior*, 36, 510-519. doi:10.1016/j.chb.2014.04.006
- Aurigemma, S. (2013). A composite framework for behavioral compliance with information security policies. *Journal of Organizational and End User Computing (JOEUC)*, 25, 32-51. doi:10.4018/joeuc.2013070103
- Aust, F., Diedenhofen, B., Ullrich, S., & Musch, J. (2013). Seriousness checks are useful to improve data validity in online research. *Behavior Research Methods (Online)*, 45, 527-535. doi:10.3758/s13428-012-0265-2
- Bar, F., Weber, M. S., & Pisani, F. (2016). Mobile technology appropriation in a distant mirror: Baroquization, creolization, and cannibalism. *New Media & Society*, 18, 617-636. doi:10.1177/1461444816629474
- Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Dont make excuses: Discouraging neutralization to reduce IT policy violation. *Computers & Security*,

39, 145-159. doi:10.1016/j.cose.2013.05.006

Basit, T. (2003). Manual or electronic? The role of coding in qualitative data analysis.

Educational Research, 45, 143-154. doi:10.1080/0013188032000133548

Baskerville, R. (2014). Rigour. In D. Coghlan & M. Brydon-Miller (Eds.), *The Sage*

encyclopedia of action research (pp. 691-692). Thousand Oaks, CA: Sage

Publications Ltd. doi:10.4135/9781446294406.n305

Bassani, P. B. (2014). Virtual learning communities: Interaction in blended learning

using Web 2.0 tools. In I. R. Management (Ed.), *Cyber behavior: Concepts*

methodologies tools and applications (pp. 599-619). Hershey, PA: IGI Global.

Bekkers, V., Edwards, A., & de Kool, D. (2013). Social media monitoring: Responsive

governance in the shadow of surveillance? *Government Information Quarterly*,

30, 335-342. doi:10.1016/j.giq.2013.05.024

Bendassolli, P. F. (2013). Theory building in qualitative research: Reconsidering the

problem of induction. *Forum: Qualitative Social Research*, 14. Retrieved from

<http://www.qualitative-research.net/>

Berdychevsky, L., & Gibson, H. J. (2015). Phenomenology of young women's sexual

risk-taking in tourism. *Tourism Management*, 46, 299-310.

doi:10.1016/j.tourman.2014.07.008

Bergman, M. M., & Coxon, A. P. (2005, May). The quality in qualitative methods. *FSS*

Forum: Qualitative Social Research, 6. Retrieved from [http://www.qualitative-](http://www.qualitative-research.net/fqs-texte/2-05/05-2-34-e.htm)

[research.net/fqs-texte/2-05/05-2-34-e.htm](http://www.qualitative-research.net/fqs-texte/2-05/05-2-34-e.htm)

- Bernier, L. (2014, August 11). Cyberloafing not always a negative. *Canadian HR Reporter*. Retrieved from <http://www.hrreporter.com/>
- Betts, T. K., Setterstrom, A. J., Pearson, J. M., & Totty, S. (2014). Explaining cyberloafing through a theoretical integration of interpersonal behavior and theory of organizational justice. *Journal of Organizational and End User Computing*, 26, 23-42. doi:10.4018/joeuc.2014100102
- Bhattacharya, S., & Tang, L. (2013). Middle managers role in safeguarding OHS: The case of the shipping industry. *Safety Science*, 51, 63-68. doi:10.1016/j.ssci.2012.05.015
- Bianchi, C., & Andrews, L. (2015). Investigating marketing managers' perspectives on social media in Chile. *Journal of Business Research*, 68, 2552-2559. doi:10.1016/j.jbusres.2015.06.026
- Birdsall, C. (2017). The synthetic control method for comparative case studies: An application estimating the effect of managerial discretion under performance management. *International Public Management Journal*, 20, 49-77. doi:10.1080/10967494.2015.1121178
- Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking a tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, 26, 1802-1811. doi:10.1177/1049732316654870
- Blanchard, A. L., & Henle, C. A. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior*,

24, 1067-1084. doi:10.1016/j.chb.2007.03.008

Blau, G., Yang, Y., & Ward-Cook, K. (2006). Testing a measure of cyberloafing. *Journal of Allied Health, 35*, 9-17. Retrieved from

<http://www.asahp.org/publications/journal-of-allied-health/>

Blumer, H. (1969). *Symbolic interactionism: Perspective and method*. Englewood Cliffs, N.J: Prentice-Hall.

Brod, M., Tesler, L. E., & Christensen, T. L. (2009). Qualitative research and content validity: developing best practices based on science and experience. *Quality of Life Research, 18*, 1263-1278. doi:10.1007/s11136-009-9540-9

Burchett, H. D., Mayhew, S. H., Lavis, J. N., & Dobrow, M. J. (2013). When can research from one setting be useful in another? Understanding perceptions of the applicability and transferability of research. *Health Promotion International, 28*, 418-430. doi:10.1093/heapro/das026

Campbell, M., Stylianou, A. C., & Shropshire, J. (2016). The impact of attitudinal factors on intention to report workplace Internet abuse. *Journal of Information Privacy and Security, 12*, 68-83. doi:10.1080/15536548.2016.1160677

Cardon, P. W., & Marshall, B. (2015). The hype and reality of social media use for work collaboration and team communication. *International Journal of Business Communication, 52*, 273-293. doi:10.1177/2329488414525446

Carlson, J. R., Zivnuska, S., Harris, R. B., Harris, K. J., & Carlson, D. S. (2016). Social media use in the workplace: A study of dual effects. *Journal of Organizational*

and End User Computing, 28, 15-31. doi:10.4018/JOEUC.2016010102

Cascón-Pereira, R., & Valverde, M. (2014). HRM devolution to middle managers: Dimensions identification. *BRQ Business Research Quarterly*, 17, 149-160. doi:10.1016/j.brq.2013.05.001

Castillo, A., & Thierer, A. D. (2015). Projecting the growth and economic impact of the Internet of things. *Social Science Research Network*, 1-10. doi:10.2139/ssrn.2618794

Chan, Z. C., Fung, Y. L., & Chien, W. T. (2013). Bracketing in phenomenology: only undertaken in the data collection and analysis process? *The Qualitative Report*, 18, 1-9. Retrieved from <http://nsuworks.nova.edu/tqr/vol18/iss30/1>

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

Chiu, S. F., & Peng, J. C. (2008). The relationship between psychological contract breach and employee deviance: The moderating role of hostile attributional style. *Journal of Vocational Behavior*, 73, 426-433. doi:10.1016/j.jvb.2008.08.006

Ciolfi, L., & De Carvalho, A. F. P. (2014). Work practices, nomadicity and the mediational role of technology. *Computer Supported Cooperative Work (CSCW)*, 23, 119-136. doi:10.1007/s10606-014-9201-6

Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative

research: Does size matter? *Journal of Advanced Nursing*, 70, 473-475.

doi:10.1111/jan.12163

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

Colbert, A., Yee, N., & George, G. (2016). The digital workforce and the workplace of the future. *Academy of Management Journal*, 59, 731-739.

doi:10.5465/amj.2016.4003

Coleman-Fountain, E., & Mclaughlin, J. (2013). The interactions of disability and impairment. *Social Theory & Health*, 11, 133-150. doi:10.1057/sth.2012.21

Corgnet, B., Hernán-González, R., & McCarter, M. W. (2015). The role of the decision-making regime on cooperation in a workgroup social dilemma: An examination of cyberloafing. *Games*, 6, 588-603. doi:10.3390/g6040588

Cox, S., Goette, T., & Young, D. (2005). Workplace surveillance and employee privacy: Implementing an effective computer use policy. *Communications of the IIMA*, 5, 57-66. Retrieved from <http://scholarworks.lib.csusb.edu/ciima/>

Creary, S. J., Caza, B. B., & Roberts, L. M. (2015). Out of the box: How managing a subordinates multiple identities affect the quality of a manager-subordinate relationship. *Academy of Management Review*, 40, 538-562.

doi:10.5465/amr.2013.0101

Daneshgari, P., & Moore, H. (2016). Organizational transformation through improved employee engagement: How to use effective methodologies to improve business

productivity and expand market share. *Strategic HR Review*, 15, 57-64.

doi:10.1108/SHR-02-2016-0007

D'Angelo, M. C., Milliken, B., Jiménez, L., & Lupiáñez, J. (2013). Implementing flexibility in automaticity: Evidence from context-specific implicit sequence learning. *Consciousness and Cognition*, 22, 64-81.

doi:10.1016/j.concog.2012.11.002

Davison, R. M., & Ou, C. X. (2016). Digital work in a digitally challenged organization.

Information & Management, 54, 1-9. doi:10.1016/j.im.2016.05.005

Deci, E. L., & Ryan, R. M. (2000). The what and why of goal pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry*, 11, 227-268.

doi:10.1207/S15327965PLI1104_01

DeFelice, D., & Janesick, V. J. (2015). Understanding the marriage of technology and phenomenological research: From design to analysis. *The Qualitative Report*, 20, 1576-1593. Retrieved from <http://nsuworks.nova.edu/tqr/>

Deloitte. (2014). *The digital workplace: Think share do transform your employee experience*. Retrieved from

http://www.2deloitte.com/content/dam/Deloitte/mx/Documents/human-capital/The_digital_workplace.pdf

Deloitte. (2015). *2015 global consumer survey: US edition the rise of the always connected consumer*. Retrieved from

<http://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media->

capital/The_digital_workplace.pdf

- Dery, K., Kolb, D., & MacCormick, J. (2014). Working with connective flow: How smartphone use is evolving in practice. *European Journal of Information Systems*, 23, 558-570. doi:10.1057/ejis.2014.13
- Dery, K., Tansley, C., & Hafermalz, E. (2014). Hiring in the age of social media: New rules new game. *University of Auckland Business Review*, 17, 44-51. Retrieved from <http://www.uabr.auckland.ac.nz/>
- DeSanctis, G., & Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. *Organization Science*, 5, 121-147. doi:10.1287/orsc.5.2.121
- Deulen, A. A. (2013). Social constructivism and online learning environments: Toward a theological model for Christian educators. *Christian Education Journal*, 10, 90-98. Retrieved from <http://journals.biola.edu/ns/cej/>
- de Wet, W., Koekemoer, E., & Nel, J. A. (2016). Exploring the impact of information and communication technology on employees' work and personal lives. *SA Journal of Industrial Psychology*, 42(1), 1-11. doi:10.4102/sajip.v42i1.1330
- DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education*, 40(4), 314-321. doi:10.1111/j.1365-2929.2006.02418.x
- Dijkmans, C., Kerkhof, P., & Beukeboom, C. J. (2015). A stage to engage: Social media use and corporate reputation. *Tourism Management*, 47, 58-67. doi:10.1016/j.tourman.2014.09.005

- Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse Researcher*, *20*, 28-32. doi:10.7748/nr2013.05.20.5.28.e327
- Doubleday, A. F., Brown, B., Patston, P. A., Jurgens-Toepke, P., Strotman, M. D., Koerber, A., Haley, C., Briggs, C., & Knight, G. W. (2015). Social constructivism and case-writing for an integrated curriculum. *Interdisciplinary Journal of Problem-based Learning*, *9*, 44-57. doi:10.7771/1541-5015.1502
- Eddles-Hirsch, K. (2015). Phenomenology and educational research. *International Journal of Advanced Research*, *3*, 251-260. Retrieved from <http://www.journalijar.com/>
- Edwards, R., & Holland, J. (2013). *What is qualitative interviewing?* New York, NY: Bloomsbury Publishing.
- El Ouiridi, A., El Ouiridi, M., Segers, J., & Henderickx, E. (2015). Employees' use of social media technologies: A methodological and thematic review. *Behaviour & Information Technology*, *34*, 454-464. doi:10.1080/0144929X.2015.1004647
- Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis. *Sage Open*, *4*, 1-10. doi:10.1177/2158244014522633
- Englander, M. (2012). The interview: Data collection in descriptive phenomenological human scientific research. *Journal of Phenomenological Psychology*, *43*(1), 13-35. doi:10.1163/156916212X632943
- Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data*

Systems, 106(3), 345-361. doi:10.1108/02635570610653498

Field, J., & Chelliah, J. (2013). Employers need to get to grips with social-media risks.

Human Resource Management International Digest, 21(7), 25-26.

doi:10.1108/HRMID-10-2013-0088

Ferreira, A. I., & Esteves, J. D. (2016). Perceptions of time at work: Why the clock ticks

differently for men and women when they are not working at work. *Personnel*

Review, 45, 29-50. doi:10.1108/PR-02-2014-0033

Franchi, E., Poggi, A., & Tomaiuolo, M. (2013). Open social networking for online

collaboration. *International Journal of e-Collaboration (IJEC)*, 9, 50-68.

doi:10.4018/jec.2013070104

Francois, A., Hebbani, A., & Rintel, S. (2013). Facebook and the university workplace.

Media International Australia, 149(1), 15-27. doi:10.1177/1329878X1314900104

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative

research. *The Qualitative Report*, 20(9), 1408-1416. Retrieved from

<http://nsuworks.nova.edu/tqr/>

Gagné, M., & Deci, E. L. (2005). Self-determination theory and work motivation.

Journal of Organizational Behavior, 26(4), 331-362. doi:10.1002/job.322

Gallant, A. (2014). Symbolic interactions and the development of women leaders in

higher education. *Gender, Work & Organization*, 21, 203-216.

doi:10.1111/gwao.12030

Gaskin, J. E. (1998). Internet acceptable usage policies: Writing and implementation.

Information Systems Management, 15, 20-25.

doi:10.1201/1078/43184.15.2.19980301/31115.4

Giorgi, A. (2012). The descriptive phenomenological psychological method. *Journal of Phenomenological Psychology*, 43(1), 3-12. doi:10.1163/156916212X632934

Given, L. M. (2008). *The Sage encyclopedia of qualitative research methods*. Thousand Oaks, CA: Sage Publications Ltd. doi:10.4135/9781412963909

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

Goel, L., Hart, D., Junglas, I., & Ives, B. (2016). Acceptable IS use: Conceptualization and measurement. *Computers in Human Behavior*, 55, 322-328. doi:10.1016/j.chb.2015.09.029

Golden, A. G. (2013). The structuration of information and communication technologies and work–life interrelationships: Shared organizational and family rules and resources and implications for work in a high-technology organization. *Communication Monographs*, 80, 101-123. doi:10.1080/03637751.2012.739702

Greene, M. J. (2014). On the inside looking in: Methodological insights and challenges in conducting qualitative insider research. *The Qualitative Report*, 19, 1-13.

Retrieved from <http://nsuworks.nova.edu/tqr/>

Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L. (2014a). History of information: The case of privacy and security in social media. In *Proceedings of the History of*

Information Conference (pp. 283-310). Retrieved from

<https://www.infosec.aueb.gr/>

Gritzalis, D., Stavrou, V., Kandias, M., & Stergiopoulos, G. (2014b, March). Insider threat: Enhancing BPM through social media. In *2014 6th International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-6). IEEE. doi:10.1109/NTMS.2014.6814027

Grossenbacher-Fabsits, D. (2011). *Male middle managers' perceptions of non-work-related Internet use* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Full-Text database. (UMI No. 3452415).

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

Gubrium, J. F., Holstein, J. A. & Marvasti, A. B. (2012). The interpersonal dynamics of in-depth interviewing. In Gubrium, J. F., Holstein, J. A. & Marvasti, A. B. *The Sage handbook of interview research: The complexity of the craft* (pp. 99-114). Thousand Oaks, CA: Sage Publications Ltd. doi:10.4135/9781452218403.n7

Gunia, B. C., Corgnet, B., & Hernan-Gonzalez, R. (2014). Surf's up: Reducing Internet abuse without demotivating employees. In *Academy of Management Proceedings* (Vol. 2014, No. 1, p. 13761). Academy of Management. doi:10.5465/AMBPP.2014.40

Gökçearsan, Ş., Mumcu, F. K., Haşlamam, T., & Çevik, Y. D. (2016). Modeling smartphone addiction: The role of smartphone usage, self-regulation, general self-

- efficacy and cyberloafing in university students. *Computers in Human Behavior*, 63, 639-649. doi:10.1016/j.chb.2016.05.091
- Hallberg, L. R. (2006). The core category of grounded theory: Making constant comparisons. *International Journal of Qualitative Studies on Health and Well-being*, 1, 141-148. doi:10.1080/17482620600858399
- Harding, N., Lee, H., & Ford, J. (2014). Who is the middle manager? *Human Relations*, 67, 1213-1237. doi:10.1177/0018726713516654
- Hartijasti, Y., & Fathonah, N. (2015). The importance of Internet policies socialization on cyberloafing in Indonesian workplace. *Asian Journal of Information and Communications*, 7(2), 68-80. Retrieved from <http://www.tandfonline.com/toc/rajc20>
- Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security*, 22, 97-114. doi:10.1108/IMCS-03-2013-0019
- Hassan, H. M., Reza, D. M., & Farkhad, M. A. A. (2015). An experimental study of influential elements on cyberloafing from general deterrence theory perspective case study: Tehran subway organization. *International Business Research*, 8(3), 91-98. doi:10.5539/ibr.v8n3p91
- Hernandez-Castro, W. (2016). *An empirical assessment of employee cyberslacking in the public sector* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Full-Text database. (UMI No. 10096094).

- Hersey, P., Blanchard, K. H., & Natemeyer, W. E. (1979). Situational leadership, perception, and the impact of power. *Group & Organization Studies*, 4(4), 418-428. doi:10.1177/105960117900400404
- Hilal, A. H., & Alabri, S. S. (2013). Using NVivo for data analysis in qualitative research. *International Interdisciplinary Journal of Education*, 2, 181-186. Retrieved from <http://www.ijoe.org/>
- Holguin, E. S. (2016). *Strategies functional managers use to control cyberloafing behaviors* (Doctoral dissertation). Retrieved from <http://scholarworks.waldenu.edu/dissertations>. (UMI No. 10141379)
- Holland, P. J., Cooper, B., & Hecker, R. (2015). Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type. *Personnel Review*, 44, 161-175. doi:10.1108/PR-11-2013-0211
- Ifinedo, P. (2016). Critical times for organizations: What should be done to curb workers noncompliance with IS security policy guidelines? *Information Systems Management*, 33, 30-41. doi:10.1080/10580530.2015.1117868
- Jamaluddin, H., Ahmad, Z., Alias, M., & Simun, M. (2015). Personal Internet use: The use of personal mobile devices at the workplace. *Procedia-Social and Behavioral Sciences*, 172, 495-502. doi:10.1016/j.sbspro.2015.01.391
- Jandaghi, G., Alvani, S. M., Matin, H. Z., & Kozekanan, S. F. (2015). Cyberloafing management in organizations. *Iranian Journal of Management Studies*, 8, 335-349. Retrieved from <https://ijms.ut.ac.ir/>

- Janesick, V. J. (2011). *Stretching exercises for qualitative researchers* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.
- Jia, H., Jia, R., & Karau, S. (2013). Cyberloafing and personality: The impact of the big five traits and workplace situational factors. *Journal of Leadership & Organizational Studies*, 20, 358-365. doi:10.1177/1548051813488208
- Jones, M. (2014). Getting in: Seeking and negotiating access. In *Researching organizations: The practice of organizational fieldwork* (pp. 74-114). London, United Kingdom: Sage Publications Ltd. doi:10.4135/9781473919723.n5
- Kahai, S. S. (2013). Leading in a digital age: What's different, issues raised, and what we know. In M. C. Bligh & R. E. Riggio (Eds.), *Exploring distance in leader-follower relationships: When near is far and far is near* (pp. 63-108). New York, NY: Routledge.
- Kataria, A., Rastogi, R., & Garg, P. (2013). Organizational effectiveness as a function of employee engagement. *South Asian Journal of Management*, 20, 56-73. Retrieved from <http://www.sajm-amdisa.org/>
- Kauppila, O., P., & Tempelaar, M., P. (2016). The social-cognitive underpinnings of employees ambidextrous behaviour and the supportive role of group manager's leadership. *Journal of Management Studies*, 53, 1019-1044. doi:10.1111/joms.12192
- Keser, H., Kavuk, M., & Numanoglu, G. (2016). The relationship between cyberloafing and Internet addiction. *Cypriot Journal of Educational Sciences*, 11, 37-42.

doi:10.18844/cjes.v11i1.431

Keyes, J. (2013a). *Bring-your-own devices (BYOD) survival guide*. Boca Raton, FL: CRC Press.

Keyes, J. (2013b). *Enterprise 2.0: Social networking tools to transform your organization*. Boca Raton, FL: CRC Press.

Khan, S. N. (2014). Qualitative research method - phenomenology. *Asian Social Science*, 10, 298-310. Retrieved from <http://www.ccsenet.org/>

Kim, K., del Carmen Triana, M., Chung, K., & Oh, N. (2015). When do employees cyberloaf? An Interactionist perspective examining personality, justice, and empowerment. *Human Resource Management*. 55(6), 1041-1058.

doi:10.1002/hrm.21699

Klemchuk, D. M., & Desai, S. (2014). Can employer monitoring of employee social media violate the electronic communications privacy act? *Intellectual Property & Technology Law Journal*, 26, 9-13. Retrieved from <https://lrus.wolterskluwer.com/>

Klenke, K. (Ed.). (2016). *Qualitative research in the study of leadership* (2nd ed.).

Bingley, United Kingdom: Emerald Group Publishing Limited.

Klotz, A. C., & Buckley, M. R. (2013). A historical perspective of counterproductive work behavior targeting the organization. *Journal of Management History*, 19(1), 114-132. doi:10.1108/17511341311286222

Kluemper, D. H., Mitra, A., & Wang, S. (2016). Social Media use in HRM. In *Research*

in personnel and human resources management (pp. 153-207). Bingley, United Kingdom: Emerald Group Publishing Limited. doi:10.1108/S0742-730120160000034011

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, 33, 3-11. doi:10.1016/j.cose.2012.07.001

Küpers, W. (2014). *Phenomenology of the embodied organization: The contribution of Merleau-Ponty for organizational studies and practice*. New York, NY: Springer.

Kura, K. M., Shamsudin, F. M., & Chauhan, A. (2013). Influence of organizational formal control on workplace deviance: A pilot study. *Middle-East Journal of Scientific Research*. doi:10.5829/idosi.mejsr.2013.13.4.312

Kura, K. M., Shamsudin, F. M., & Chauhan, A. (2015). Does self-regulatory efficacy matter? Effects of punishment certainty and punishment severity on organizational deviance. *Sage Open*, 5, 1-14. doi:10.1177/2158244015591822

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

doi:10.1016/j.chb.2013.09.021

Ladner, S. (2015, November 3). Mobile productivity: It aint about doing more [Web log comment]. Retrieved from <http://www.samladner.com/page/2/>

Le, A. T. (2015). *Factors influencing the adoption of bring-your-own device (BYOD) by decision-making managers* (Doctoral dissertation). Retrieved from ProQuest

Dissertations & Theses Full-Text database. (UMI No. 3669431).

- Leclercq-Vandelannoitte, A. (2015). Managing BYOD: How do organizations incorporate user-driven IT innovations? *Information Technology & People*, 28, 2-33. doi:10.1108/ITP-11-2012-0129
- Leftheriotis, I., & Giannakos, M. N. (2014). Using social media for work: Losing your time or improving your work? *Computers in Human Behavior*, 31, 134-142. doi:10.1016/j.chb.2013.10.016
- Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics, and sanction on Internet use policy compliance. *Information Systems Journal*, 24, 479-502. doi:10.1111/isj.12037
- Liao, Q., Gurung, A., Luo, X., & Li, L. (2009). Workplace management and employee misuse: Does punishment matter? *Journal of Computer Information Systems*, 50(2), 49-59. Retrieved from <http://www.tandfonline.com/toc/ucis20/current>
- Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior*, 23, 675-694. doi:10.1002/job.161
- Lim, V. K., & Teo, T. S. (2005). Prevalence perceived seriousness justification and regulation of cyberloafing in Singapore: An exploratory study. *Information & Management*, 42, 1081-1093. doi:10.1016/j.im.2004.12.002
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Newbury Park, CA: Sage Publications Inc.

- Liu, N., Yang, X., & Chan, H. C. (2013). Exploring the antecedents to learning continuance in virtual worlds: A balanced thinking-feeling and social-constructivism perspective. *Journal of Global Information Management (JGIM)*, 21, 1-22. doi:10.4018/jgim.2013040101
- Lunnay, B., Borlagdan, J., McNaughton, D., & Ward, P. (2014). Ethical use of social media to facilitate qualitative research. *Qualitative Health Research*, 25, 99-109. doi:10.1177/1049732314549031
- MacCormick, J. S., Dery, K., & Kolb, D. G. (2012). Engaged or just connected? Smartphones and employee engagement. *Organizational Dynamics*, 41(3), 194-201. doi:10.1016/j.orgdyn.2012.03.007
- Mahatanankoon, P. (2006). Internet abuse in the workplace: Extension of workplace deviance model. In M. Anandarajan, T. S. Teo, & C. A. Simmers (Eds.), *The Internet and workplace transformation* (pp. 15-27). Armonk, NY: M.E. Sharpe.
- Manzoor, S. R., Arif, S., & Hassan, S. (2015). Role of capacity building and emotional intelligence on counterproductive work behavior. *The Pakistan Journal of Social Issues*, 5, 68-87. Retrieved from <http://uog.edu.pk/research/>
- Maxwell, J. A. (2013). *Qualitative research design: An interactive approach* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.
- McBride, D. L., LeVasseur, S. A., & Li, D. (2015). Non-work-related use of personal mobile phones by hospital registered nurses. *JMIR mHealth and uHealth*, 3, e3. doi:10.2196/mhealth.4001

- McDonald, P., & Thompson, P. (2016). Social media (tion) and the reshaping of public/private boundaries in employment relations. *International Journal of Management Reviews*, 18, 69-84. doi:10.1111/ijmr.12061
- Mead, G. H. (1934). *Mind self and society: From the standpoint of a social behaviorist*. Chicago, IL: University of Chicago Press.
- Merriam, S. B. (2002). *Qualitative research in practice: Examples for discussion and analysis*. San Francisco, CA: Jossey-Bass.
- Michalski, M. P. (2013). Symbolic meanings and e-learning in the workplace: The case of an intranet-based training tool. *Management Learning*, 45, 145-166. doi:10.1177/1350507612468419
- Miles, M. B., Huberman, A. M., & Saldana, J. (2013). *Qualitative data analysis: A methods source book* (3rd ed.). Thousand Oaks, CA: Sage Publications Inc.
- Mollick, E. (2012). People and process, suits and innovators: The role of individuals in firm performance. *Strategic Management Journal*, 33(9), 1001-1015. doi:10.1002/smj.1958
- Moussa, M. (2015). Monitoring employee behavior through the use of technology and issues of employee privacy in America. *Sage Open*, 1-13. doi:10.1177/2158244015580168
- Moustakas, C. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage Publications, Inc.
- Mutula, S. M. (2013). Policy gaps and technological deficiencies in social networking

environments: Implications for information sharing. *South African Journal of Information Management*, 15, 1-9. Retrieved from <http://www.sajim.co.za/index.php/SAJIM>

Nazareth, D.L., & Choi, J. (2014). A system dynamics model for information security management. *Information and Management*, 52, 123-134.
doi:10.1016/j.im.2014.10.009

Newswise (2013). *Policy, enforcement may stop employees from wasting time online at work*. Retrieved from: <http://www.newswise.com/articles/policy-enforcement-may-stop-employees-from-wasting-time-online-at-work-researcher-finds>

Niaei, M., Peidaei, M. M., & Nasiripour, A. A. (2014). The relation between staff cyberloafing and organizational commitment in the organization of environmental protection. *Kuwait Chapter of the Arabian Journal of Business and Management Review*, 3(7), 59-71. Retrieved from <http://arabianjbmr.com/>

Nicholas, A. J. (2014). Systematic ICT surveillance by employers: Are your personal activities private? *Salve Regina University Faculty and Staff Articles & Papers*, 54, 1-12. Retrieved from http://digitalcommons.salve.edu/fac_staff_pub/

Öğüt, E., Şahin, M., & Demirsel, M. T. (2013). The relationship between perceived organizational justice and cyberloafing: Evidence from a public hospital in Turkey. *Mediterranean Journal of Social Sciences*, 4, 226-233.
doi:10.5901/mjss.2013.v4n10p226

- Omole, C. O., & Ayeni, B. O. (2013). Internet use: Breakthrough or breakdown? *Ife Psychologia*, 21, 260-267. Retrieved from <http://www.ajol.info/index.php/ifep>
- O'Neill, T. A., Hambley, L. A., & Bercovich, A. (2014). Prediction of cyberslacking when employees are working away from the office. *Computers in Human Behavior*, 34, 291-298. doi:10.1016/j.chb.2014.02.015
- O'Neill, T. A., Hambley, L. A., & Chatellier, G. S. (2014). Cyberslacking, engagement, and personality in distributed work environments. *Computers in Human Behavior*, 40, 152-160. doi:10.1016/j.chb.2014.08.005
- Onwuegbuzie, A. J., & Byers, V. T. (2014). An exemplar for combining the collection, analysis, and interpretations of verbal and nonverbal data in qualitative research. *International Journal of Education*, 6, 183. doi:10.5296/ije.v6i1.4399
- Opendakker, R. (2006). Advantages and disadvantages of four interview techniques in qualitative research. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, 7. Retrieved from <http://www.qualitative-research.net/index.php/fqs>
- Ortlipp, M. (2008). Keeping and using reflective journals in the qualitative research process. *The Qualitative Report*, 13, 695-705. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Parera, L. B., & Fernández-Vallejo, A. M. (2013). Changes in the role of middle manager: A historical point of view. *International Journal of Information and Education Technology*, 3, 362-365. doi:10.7763/IJiet.2013.V3.298

- Park, S. (2014). Employee Internet privacy: A proposed act that balances legitimate employer rights and employee privacy. *American Business Law Journal*, 51, 779-841. doi:10.1111/ablj.12039
- Patrick, E., (2008). *Employee Internet management: Now an HR issue*. Society for Human Resource Management (SHRM). Retrieved from https://www.shrm.org/hr-today/news/hr-magazine/pages/cms_006514.aspx
- Patton, M. Q. (2014). *Qualitative research and evaluation methods: Integrating theory and practice* (4th ed.). Thousand Oaks, CA: Sage Publications, Inc.
- Pearson, C., & Hussain, Z. (2015). Smartphone use addiction narcissism and personality: A mixed methods investigation. *International Journal of Cyber Behavior, Psychology and Learning (IJCBL)*, 5, 17-32. doi:10.4018/ijcbpl.2015010102
- Peltier, T. R. (2001). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Boca Raton, FL: Auerbach Publications.
- Peng, J., Quan, J., Zhang, G., & Dubinsky, A. J. (2015). Knowledge sharing social relationships and contextual performance: The moderating influence of information technology competence. *Journal of Organizational and End User Computing*, 27, 58-73. doi:10.4018/joeuc.2015040103
- Percy, W. H., Kostere, K., & Kostere, S. (2015). Generic qualitative research in psychology. *The Qualitative Report*, 20, 76-85. Retrieved from <http://nsuworks.nova.edu/tqr/>

- Peredaryenko, M. S., & Krauss, S. E. (2013). Calibrating the human instrument: Understanding the interviewing experience of novice qualitative researchers. *The Qualitative Report, 18*, 1-17. Retrieved from <http://nsuworks.nova.edu/tqr/>
- Pînzaru, F., & Mitan, A. (2016). Managers versus digital native's employees. A study regarding the perceptions of the Romanian managers working with youngsters. *Management Dynamics in the Knowledge Economy, 4*, 153-166. Retrieved from <http://www.managementdynamics.ro/index.php/journal>
- Piotrowski, C. (2013). Counterproductive work behavior: Topical domain in emergent research. *Journal of Instructional Psychology, 40*(3), 78-80. Retrieved from http://www.projectinnovation.biz/journal_of_instructional_psychology
- Piotrowski, C. (2012). Cyberloafing: A content analysis of the emerging literature. *Journal of Instructional Psychology, 39*, 259-261. Retrieved from http://www.projectinnovation.biz/journal_of_instructional_psychology
- Pirani, N., & Meister, D. (2014, December). *IT consumerization: A model of private IT use in organizations*. Paper presented at the 2014 Diffusion Interest Group in Information Technology (DIGIT) Conference, Auckland, New Zealand. Retrieved from <http://aisel.aisnet.org/digit2014>
- Polkinghorne, D. E. (1989). Phenomenological research methods. In R. S. Valle & Halling S. (Eds.), *Existential-phenomenological perspectives in psychology* (pp. 41-60). Boston, MA: Springer.
- Polzer-Debruyne, A., Stratton, M. T., & Stark, G. (2014). Personal web use in the

workplace: Why does it persist in a context of strict security and monitoring?

International Journal of Business Administration, 5, 1-18.

doi:10.5430/ijba.v5n3p1

Poole, M. (2013). Adaptive structuration theory. In E. Kessler (Ed.), *Encyclopedia of management theory* (pp. 23-26). Thousand Oaks, CA: Sage Publications, Inc.

doi:10.4135/9781452276090.n7

Porter, M. E., & Heppelmann, J. E. (2015). How smart connected products are transforming companies. *Harvard Business Review*, 93, 96-114. Retrieved from <https://hbr.org/>

Prensky, M. (2001). Digital natives, digital immigrants part 1. *On the Horizon*, 9, 1-6.

doi:10.1108/10748120110424816

Pulakos, E. D., Hanson, R. M., Arad, S., & Moye, N. (2015). Performance management can be fixed: An on-the-job experiential learning approach for complex behavior change. *Industrial and Organizational Psychology*, 8(1), 51-76.

doi:10.1017/iop.2014.2

Quoquab, F., Salam, Z. A., & Halimah, S. (2015, August). Does cyberloafing boost employee productivity? *2015 International Symposium on Technology Management and Emerging Technologies* (pp. 119-122).

doi:10.1109/ISTMET.2015.7359013

Rahimnia, F., & Mazidi, A. R. K. (2015). Functions of control mechanisms in mitigating workplace loafing: Evidence from an Islamic society. *Computers in Human*

Behavior, 48, 671-681. doi:10.1016/j.chb.2015.02.035

Rana, H., & Punia, B. K. (2014). Management mechanisms and implications of workplace deviance for green organisational behaviour. *International Journal of Advance Research in Computer Science and Management Studies*, 2, 1-8.

Retrieved from <http://www.ijarcsms.com/>

Ratnamalala, N., & Marett, K. (2014). *The impact of computer monitoring on policy compliance: An agency and stewardship view*. Paper presented at the Twentieth Americas Conference on Information Systems, Savannah, GA. Retrieved from <http://aisel.aisnet.org/>

Rice, R. E. & Leonardi, P. M. (2013). Online technology use in organizations. In L.L. Putnam and D.K. Mumby (Eds.). In *The Sage handbook of organizational communication* (pp. 425-448). Thousand Oaks, CA: Sage Publications Inc.

Rokka, J., Karlsson, K., & Tienari, J. (2014). Balancing acts: Managing employees and reputation in social media. *Journal of Marketing Management*, 30, 802-827. doi:10.1080/0267257X.2013.813577

Rose, C. (2013). BYOD: An examination of bring-your-own device in business. *The Review of Business Information Systems (Online)*, 17, 65-70. doi:10.19030/rbis.v17i2.7846

Rudestam, K. E., & Newton, R. R. (2014). *Surviving your dissertation: A comprehensive guide to content and process* (4th ed.). Thousand Oaks, CA: Sage Publications, Inc.

- Ruhnka, J., & Loopesko, W. E. (2013). Risk management of email and Internet use in the workplace. *Journal of Digital Forensics, Security & Law*, 8, 7-19. Retrieved from <http://www.jdfsl.org/>
- Sandelowski, M. (1993). Rigor or rigor mortis: the problem of rigor in qualitative research revisited. *Advances in Nursing Science*, 16(2), 1-8. Retrieved from <http://journals.lww.com/advancesinnursingscience/>
- Sanders, D. E., Ross, J. K., & Pattison, P. (2013). Electronic snoop's spies and supervisory surveillance in the workplace. *Southern Law Journal*, 23, 1-27. Retrieved from <http://www.southernlawjournal.com/>
- Sandstrom, K. & Kleinman, S. (2005). Symbolic interaction. In G. Ritzer (Ed.). In *Encyclopedia of social theory* (pp. 822-827). Thousand Oaks, CA: Sage Publications Ltd. doi:10.4135/9781412952552.n304
- Saraç, M., & Çiftçiöğlü, B. A. (2014). What do human resources managers think about the employee's Internet usage? *Anadolu University Journal of Social Sciences*, 14, 1-12. Retrieved from <http://sbd.anadolu.edu.tr/home.html>
- Schalow, P. R., Winkler, T. J., Repschlaeger, J., & Zarnekow, R. (2013). *The blurring boundaries of work-related and personal media use: A grounded theory study on the employee's perspective*. Paper presented at the 21st European Conference on Information Systems. Utrecht, the Netherlands: AIS Electronic Library (AISeL) Retrieved from http://aisel.aisnet.org/ecis2013_cr
- Schreiber, L. M., & Valle, B. E. (2013). Social constructivist teaching strategies in the

small group classroom. *Small Group Research*, 44, 395–411.

doi:10.1177/1046496413488422

Sedo, D. (2005). Symbolic interactionism theory. In R. Heath (Ed.), *Encyclopedia of public relations* (pp. 835-838). Thousand Oaks, CA: Sage Publications, Inc.

doi:10.4135/9781412952545.n420

Seidman, I. (2013). *Interviewing as qualitative research: A guide for researchers in education and the social sciences*. New York, NY: Teachers College Press.

Sheikh, A., Atashgah, M. S., & Adibzadegan, M. (2015). The antecedents of cyberloafing: A case study in an Iranian copper industry. *Computers in Human Behavior*, 51, 172-179. doi:10.1016/j.chb.2015.04.042

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information*, 22(2), 63-75. doi:10.3233/EFI-2004-22201

Shepherd, M., Mejias, R., & Klein, G. (2014). *A longitudinal study to determine non-technical deterrence effects of severity and communication of Internet use policy for reducing employee Internet abuse*. Paper presented at the 47th International Conference on System Science (HICSS) in Hawaii, United States. Retrieved from <https://www.computer.org/csdl/proceedings/hicss/2014/2504/00/2504d159>

Sheriff, A. M. (2012). The techniques and rationale of e-surveillance practices in organizations. *Zenith International Journal of Multidisciplinary Research*, 2. Retrieved from <http://www.zenithresearch.org.in>

Simon, M. K., & Goes, J. (2013). *Dissertation and scholarly research: Recipes for*

success. Seattle, WA: Dissertation Success LLC

Simons, R. (2013). *Levers of control: How managers use innovative control systems to drive strategic renewal*. (2nd ed.). Boston, MA: Harvard Business School Press.

Smith, A. (2015). *The smartphone difference*. Retrieved from

<http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/>

Son, J. Y., & Park, J. (2016). Procedural justice to enhance compliance with non-work-related computing (NWRC) rules: Its determinants and interaction with privacy concerns. *International Journal of Information Management*, 36, 309-321.

doi:10.1016/j.ijinfomgt.2015.12.005

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36, 215-225. doi:10.1016/j.ijinfomgt.2015.11.009

Sorenson, S. (2013). How employee engagement drives growth. *Gallup Business Journal*, 1, 1-4. Retrieved from

http://www.gallup.com/topic/all_gbj_headlines.aspx

Soror, A., Steelman, Z. R., & Limayem, M. (2012, January). *Discipline yourself before life disciplines you: Deficient self-regulation and mobile phone unregulated use*.

Paper presented at the 45th International Conference on System Sciences, Maui, HI. doi:10.1109/HICSS.2012.219

Spencer, B. (2013, February 10). Mobile users cant leave their phone alone for six minutes and check it up to 150 times a day. *Daily Mail*. Retrieved from

<http://www.dailymail.co.uk/news/article-2276752/Mobile-usersleave-phone-minutes-check-150-times-day.html>.

Stephens, K. K., & Ford, J. L. (2014). *Banning mobile devices: Workplace policies that selectively exclude can shape crisis communication*. Paper presented at the 11th Annual Conference on Information Systems for Crisis Response and Management (ISCRAM), University Park, PA. Retrieved from <http://www.iscram.org/legacy/ISCRAM2014/papers/p127>

Stephens, K. K., & Ford, J. L. (2016). Unintended consequences of a strategically ambiguous organizational policy selectively restricting mobile device use at work. *Mobile Media & Communication, 4*, 186-204.
doi:10.1177/2050157915619211

Stoddart, S. (2016). *The impact of cyberloafing and mindfulness on employee burnout* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Full-Text database. (UMI No. 10105022).

Stuckey, H. L. (2015). The second step in data analysis: Coding qualitative research data. *Journal of Social Health and Diabetes, 3*, 7-10. doi:10.4103/2321-0656.140875

Teague, C., Green, L., & Leith, D. (2013). Symbolic interactionism in safety communication in the workplace. In Norman K. Denzin (Ed.) *40th anniversary of studies in symbolic interaction: Studies in symbolic interaction* (Vol. 40, pp.175 - 199) Bradford, United Kingdom: Emerald Group Publishing Limited.
doi:10.1108/S0163-2396(2013)0000040011

- Teh, P., Ahmed, P. K., & D'Arcy, J. (2015). What drives information security policy violations among banking employees? Insights from neutralization and social exchange theory. *Journal of Global Information Management (JGIM)*, 23(1), 44-64. doi:10.4018/jgim.2015010103
- Toegel, G., Kilduff, M., & Anand, N. (2013). Emotion helping by managers: An emergent understanding of discrepant role expectations and outcomes. *Academy of Management Journal*, 56(2), 334-357. doi:10.5465/amj.2010.0512
- Travis, T., Sarah, S., Bharat, M., & Jitendra, M. (2017). How to manage difficult employees. *Advances in Management*, 10, 1-6. Retrieved from <http://www.connectjournals.com/>
- Treem, J. W., & Leonardi, P. M. (2013). Social media use in organizations: Exploring the affordances of visibility, editability, persistence, and association. *Annals of the International Communication Association*, 36, 143-189. doi:10.1080/23808985.2013.11679130
- Ugrin, J. C., & Pearson, J. M. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior*, 29, 812-820. doi:10.1016/j.chb.2012.11.005
- Van Gramberg, B., Teicher, J., & ORourke, A. (2014). Managing electronic communications: a new challenge for human resource managers. *International Journal of Human Resource Management*, 25, 2234-2252. doi:10.1080/09585192.2013.872166

- Van Manen, M. (1990). *Researching lived experience: Human science for an action sensitive pedagogy*. Albany, NY: The State University of New York Press.
- Vygotsky, L. S. (1978). *Mind in society*. Cambridge, MA: Harvard University Press.
- Walden, J. A. (2016). Integrating social media into the workplace: A study of shifting technology use repertoires. *Journal of Broadcasting & Electronic Media*, 60, 347-363. doi:10.1080/08838151.2016.1164163
- Wang, Q., Myers, M. D., & Sundaram, D. (2013a). Digital natives and digital immigrants. *Business & Information Systems Engineering*, 5, 409-419. doi:10.1007/s12599-013-0296-y
- Wang, D., Xiang, Z., & Fesenmaier, D. R. (2016). Smartphone use in everyday life and travel. *Journal of Travel Research*, 55, 52-63. doi:10.1177/0047287514535847
- Wang, J., Tian, J., & Shen, Z. (2013b). The effects and moderators of cyber-loafing controls: An empirical study of Chinese public servants. *Information Technology and Management*, 14, 269-282. doi:10.1007/s10799-013-0164-y
- Watson, J. (2001). Social constructivism in the classroom. *Support for Learning*, 16(3), 140-147. doi:10.1111/1467-9604.00206
- Wet, W. D., & Koekemoer, E. (2016). The increased use of online technology (ICT) among employees: Implications for work-life interaction. *South African Journal of Economic and Management Sciences*, 19, 282-201. Retrieved from <http://www.sajems.org/index.php/sajems>
- Willis, D. G., Sullivan-Bolyai, S., Knafl, K., & Zichi-Cohen, M. (2016). Distinguishing

features and similarities between descriptive phenomenological and qualitative description research. *Western Journal of Nursing Research*. 38, 1185-1204.

doi:10.1177/0193945916645499

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions:

Epistemological, theoretical, and methodological differences. *European Journal of Education*, 48, 311-325. doi:10.1111/ejed.12014

Young, K. (2010). Policies and procedures to manage employee Internet abuse.

Computers in Human Behavior, 26, 1467-1471. doi:10.1016/j.chb.2010.04.025

Zeff, L. E., & Higby, M. A. (2015). To multitask or not that is the question. *The*

Quarterly Review of Business Disciplines (QRBD) 2, 221-234. Retrieved from

<http://iabdn.net/QRBD/>

Zoghbi Manrique de Lara, Pablo, Verano Tacoronte, D., & Ting Ding, J. (2006). Do

current anti-cyberloafing disciplinary practices have a replica in research findings:

A study of the effects of coercive strategies on workplace Internet misuse.

Internet Research, 16(4), 450-467. doi:10.1108/10662240610690052

Appendix A: Participant Invite to Participate in Research Study

Middle Manager Invitation to Participate in Research Study

Dear Sir/Ma'am,

My name is Anizizo Aku, and I am a doctoral student at Walden University. I am currently conducting a study on the middle manager's role in mitigating employee cyberloafing to fulfill requirements of the Walden University Ph.D. in Management program with a focus on leadership and organizational change.

I am conducting interviews as part of a research study designed to elicit feedback about your experiences and understanding about your middle management role in curbing employee cyberloafing in a digital work environment. The overall aim of the full-scale study is to compile meaningful insights from the lived experiences and perceptions of middle managers about possible barriers or best practices associated with the effectiveness of non-technical organizational strategies aimed at combating employee cyberloafing and implementing anti-cyberloafing policies.

This study is not looking to assess or evaluate your personal management style, experience, or technique. Alternatively, the focus is to learn more about the role middle managers play in the overall organization efforts aimed at mitigating the cyberloafing phenomenon.

No compensation will be made for participating in the study. Participation is completely voluntary and in the event, you feel uncomfortable during the interview, you can stop at any time. No harm is intended to you as a participant and anonymity of Participants responses will be kept confidential.

Should you choose to participate, your contribution would provide valuable insights and enhance a better understanding of the phenomenon. Pre-arranged face-to-face interviews will be conducted and will last for approximately 30-45 minutes. Audio recordings will be made during the interview with notes written as the interview progresses (transcripts of audio recording will be provided to all participants).

If you have any questions, please email me at managingcyberloafingstudy@gmail.com.

Thank you.

Anizizo Aku
Doctoral Student
Walden University

Appendix B: Follow Up Participant Invite to Participate in Research Study

Middle Manager Follow-Up Invitation to Participate in Research Study

Dear Sir/Ma'am,

I just wanted to check again to see whether you would be interested in participating in a research study designed to elicit feedback about your experiences and understanding about your middle management role in curbing employee cyberloafing in a digital work environment. The overall aim of the full-scale study is to compile meaningful insights from the lived experiences and perceptions of middle managers about possible barriers or best practices associated with the effectiveness of non-technical organizational strategies aimed at combating employee cyberloafing and implementing anti-cyberloafing policies.

This study is not looking to assess or evaluate your personal management style, experience, or technique. Alternatively, the focus is to learn more about the role middle managers play in the overall organization efforts aimed at mitigating the cyberloafing phenomenon.

No compensation will be made for participating in the study. Participation is completely voluntary and in the event, you feel uncomfortable during the interview, you can stop at any time. No harm is intended to you as a participant and anonymity of Participants responses will be kept confidential.

Should you choose to participate, your contribution would provide valuable insights and enhance a better understanding of the phenomenon. Pre-arranged face-to-face interviews will be conducted and will last for approximately 30-45 minutes. Audio recordings will be made during the interview with notes written as the interview progresses (transcripts of audio recording will be provided to all participants).

If you have any questions, please email me at managingcyberloafingstudy@gmail.com.

Thank you.

Anizizo Aku
Doctoral Student
Walden University

Appendix C: Response Email to Prospective Participants with Eligibility Questions

Response Email to Prospective Participants with Eligibility Questions

Dear Sir/Ma'am,

Thank you for your email response. To determine your eligibility to participate, please respond via email and answer the following 'yes' or 'no' questions:

1. Are you currently employed in a middle management position responsible for supervising, developing, and coaching subordinate employees?
2. Do you work in a digital workplace where employees use mainly computer technology to perform work tasks, collaborate, and provide services to clients?
3. Do you have experience mitigating subordinate cyberloafing activity?
4. Are you male or female?
5. Are you willing to candidly share your experiences and understanding about your role in the mitigation of employee cyberloafing?

I truly appreciate your inclination to participate and look forward to reading your response.

Sincerely,

Anizizo Aku
Doctoral Student
Walden University

Appendix D: Interview Questions

Interview Questions with prompts

Interviews are semistructured with questions and prompts designed to encourage in-depth responses from participants.

1. Describe your role in the mitigation of employee cyberloafing at work?
 - a. Prompt: What meaning do you ascribe to your role in the mitigation of employee cyberloafing at work?
 - b. Prompt: How do you control employee cyberloafing activity at work?
 - c. Prompt: What personal experiences with employee cyberloafing mitigation have allowed you to be more knowledgeable about your role in cyberloafing mitigation?
 - d. Prompt: What non-technical mitigation strategy(s) have you used at work to mitigate employee cyberloafing?
2. Describe how your monitoring presence (proximity) to employees impacted your role controlling employee cyberloafing at work?
 - a. Prompt: How does your monitoring presence facilitate effective supervision of employee cyberloafing activity?
 - b. Prompt: How does your daily interaction with employees enhance your situational awareness about employee cyberloafing activity?
 - c. Prompt: How does your monitoring presence enhance your understanding of employee appropriation of information and communication technologies?
3. Describe how your experiences and interaction with employees during employee cyberloafing mitigation interventions have influenced positive employee conduct and productivity.
 - a. Prompt: How does the knowledge constructed while mitigating employee cyberloafing allow you to improve employee productivity?
 - b. Prompt: How does authority and control contribute to the effectiveness of your role mitigating employee cyberloafing behavior or activity?
 - c. Prompt: How have you handled employee cyberloafing violations and the processes surrounding employee sanctioning and punishment?
4. Describe what contributions you have made to the overall organizational efforts aimed at mitigating employee cyberloafing?
 - a. Prompt: What strategies have you used to motivate and reward good behavior in your role mitigating employee cyberloafing?

- b. Prompt: Explain contributions you have made to your organization's cyberloafing mitigation efforts in terms of education, training, and awareness programs.
 - c. Prompt: What are some barriers you experienced executing non-technical mitigation strategies aimed at curbing employee cyberloafing?
 - d. Prompt: What are some successes you achieved executing non-technical mitigation strategies aimed at curbing employee cyberloafing?
5. Describe how your understanding of employee appropriation of information and communication technologies at work enhanced the effective conduct of your role in cyberloafing mitigation?
 - a. Prompt: Tell me about your experience identifying patterns of behavior and evasive actions employee's use to access the Internet for non-work-related activity?
 - b. Prompt: How has your knowledge of employee appropriation of information and communication technologies for non-work-related activity influenced your role in the cyberloafing mitigation effort?
 - c. Prompt: What importance did you believe that the proliferation of advanced information and communication technologies would play over your role in cyberloafing mitigation?
6. Describe how your knowledge about the proliferation of nomadic computing and the consumerization of mobile devices impacted your role in employee cyberloafing mitigation?
 - a. Prompt: How did the knowledge about individual employee sophistication with information and communication technologies impact your role in mitigating cyberloafing?
 - b. Prompt: How did the knowledge about individual employee possession and use of wearable technology, mobile communication devices with Internet access technologies impact your role in mitigating cyberloafing?
 - c. Prompt: How do you see the effectiveness of your organization's acceptable usage policies and your implementation and enforcement of the policies in a rapidly changing technological environment?
7. Is there any other important information you would like to share about your role mitigating employee cyberloafing at work?
 - a. Prompt: Insights on the important role middle managers play in the employee cyberloafing mitigation efforts.
 - b. Prompt: The shared role between Information Technology managers, Human Resources managers, and middle managers in the mitigation of employee cyberloafing.