CEC Theses and Dissertations   College of Engineering and Computing

2016

An Empirical Assessment of Employee Cyberslacking in the Public Sector

Wilnelia Hernández
Nova Southeastern University, wilnelia@nova.edu

An Empirical Assessment of Employee Cyberslacking in the Public Sector

by

Wilnelia Hernández-Castro

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

College of Engineering and Computing
Nova Southeastern University

2016

We hereby certify that this dissertation, submitted by Wilnelia Hernandez, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.
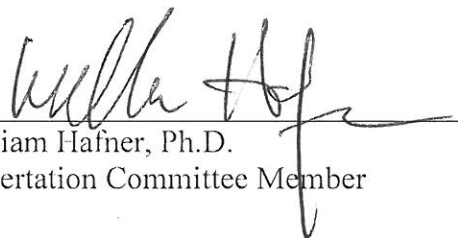
_____   _3/16/2016_
Yair Levy, Ph.D.   Date
Chairperson of Dissertation Committee

P.P. _____   _March 16, 2016_
Marlyn Littman, Ph.D.   Date
Dissertation Committee Member
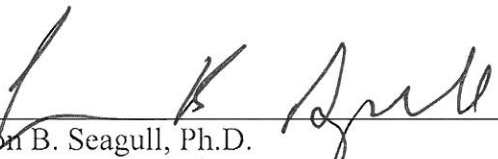
_____   _3/16/2016_
William Hafner, Ph.D.   Date
Dissertation Committee Member

Approved:

_____   _March 16, 2016_
Amon B. Seagull, Ph.D.   Date
Interim Dean, College of Engineering and Computing

College of Engineering and Computing
Nova Southeastern University

2016

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

Empirical Assessment of Employee Cyberslacking in the Public Sector

by
Wilnelia Hernández-Castro
March, 2016

With the increasing use of the Internet, new challenges are presented to employees in the
workplace. Employees spend time during work hours on non-work related activities
including visiting e-commerce Websites, managing personal email accounts, and
engaging in e-banking. These types of actions in the workplace are known as
cyberslacking. Cyberslacking affects the employees' productivity, presents legal
concerns, and undermines the security of the organization's network. This research study
addressed the problem of cyberslacking in the public sector, by assessing the ethical
severity of cyberslacking activities, as well as how employees perceived that the
frequency of such activities occurred by their co-workers. Participants from public sector
agencies were asked to report about their amount of time spent and frequency of
cyberslacking, what they report about their co-workers' amount of time spent and
frequency of cyberslacking, as well as their perceived ethical severity of cyberslacking in
the workplace. First, an expert panel, of 10 cybersecurity subject matter experts, was used
to initially validate the instrument, followed by quantitative data collection. This study
assessed the measures via a Web-based anonymous survey. Following pre-analysis data
screening, this study used a combination of descriptive statistics, analysis of covariance
(ANCOVA), as well as Ordinal Logistics Regression (OLR) and Multiple Linear
Regression (MLR) analyses to address the research questions (RQs). Comparisons of the
measures were also conducted. Results from 183 participants indicate that employees
report their co-workers to engage in cyberslacking significantly higher than what they
reported about themselves, and ethical severity of cyberslacking was not reported to be
high.

The problem of personal misuse of the Internet in the workplace was the focal point of
this research study. The Internet facilitates productive communication in the workplace.
However, it also poses a significant challenge to employees given its availability to
enable non-work related activities. As such, it was necessary to examine both the
perceptions about the ethical severity of IS misuse in the workplace and the actual self
reported amount of cyberslacking by employees, compared to what they claim their co-
workers are engaged in, especially in the public sector. Finally, this research study
attempted to contribute to the Information Systems body of knowledge by empirically
identifying the aforementioned relationships. Discussions and implications for future
research are provided.

Acknowledgments

My Lord, my life, my all, my Savior, the beginning and the end, there are no words that can express my thanks to you, not only during this step of my life, even more during all my life and the coming future that is in your purpose.

My beloved, handsome, wise, intelligent, loving, cheerful, patient, kind, and with great faith, incredible blessed husband. Thank you for being my husband. We started this adventure holding the hand of God and the hands of each other and today we can said: "Thanks God we did it!"

Thank you so much to my dissertation advisor, Dr. Yair Levy for your amazing intelligent and wise advise; it was spectacular how much I learned and I will keep learning with you; giant. Thank you so much to each of my committee members, Dr. Marlyn Littman, Dr. William Hafner, and Dr. Among B. Seagull for all your guidance and valuable advice. Thank you so much to the expert panel for your valuable recommendations.

Thank you so much to my blessed and beautiful family: the best parents in the Universe are Mamita & Papito, and the best sisters ever Damaris, Glendy, and Leisha, for your prayers and support. Thank you so much to the rest of my family, brothers, sisters, and friends that pray for me.

Thank you to the Office of Government Ethics for your support. Thank you to all the agencies that participated in the study. Thank you to the Universidad del Turabo for believes in this.

God bless you all!

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

The implementation of a new strategic work process and the integration of a new electronic environment in the workplace, represent new challenges for employees in the 21st century (Kidwell, 2010). The incorporation of Internet technologies, computer technologies, information systems (IS), and, the misuse of those technologies, are on the rise daily (D'Arcy & Hovav, 2008; D'Arcy, Hovav, & Galetta, 2009; Wheatherbee, 2010). Mills, Hu, Beldona, and Clay (2001) defined *misuse* as "Cyberslacking, cyberloafing, and cyberbludging" (p. 34). According to Whitty and Carr (2006), "Cyberslacking is the overuse of the Internet in the workplace for purposes other than work" (p. 238). This problem included spending work hours to shop online, visit pornographic Websites, access social networking sites (SNS) for personal use, and utilize the work computer to manage personal data (Henle & Blanchard, 2008; Johnson & Indvik, 2003; Kidwell, 2010; Lara, Tacoronte, & Ding, 2006; Lim & Teo, 2005). Evidently, cyberslacking diminishes productivity in the workplace in both the governmental and private spheres. Thus, its proliferation in the workplace, in public sector organizations, warrants investigation (Whitty & Carr, 2006).

A study revealed that Americans spend approximately 21 hours each month surfing the Internet at work for personal purposes (*Business Wire,* 2000). Johnson and Rawlins (2008) stated, "One major cost to organizations is lower productivity. When

employees use workplace PCs for personal reasons, their productivity decreases" (p. 44). Thus, this research study assessed the extent of government employees' reports on their own and their co-workers' cyberslacking activities, the frequency of engagement in cyberslacking activities, and their impact on perceived ethical severity of these activities. This research also investigated if there are significant differences among these behaviors based on gender, age, level of education, job level, and years of working for the government. It is imperative that organization should be able to identify the cyberslacking problem and the financial ramifications of these activities (Mills et al., 2001).

Fundamental literature was reviewed to argue for this significant problem as a well-documented organizational problem. Moreover, it outlines the goals of this research study and depicts the research questions. Specifically, a section on the issue's relevance and significance to support the problem statement, as well as a brief review of the literature that identifies the problem in this study. In order to support the problem statement, a section on the issues relevance and significance was included. Accordingly, a brief review of the literature that serves as initial foundation for the study is included. Moreover, the proposed study barriers and issues, approach, milestones, resources, and definition of terms were provided.

Problem Statement

The research problem that this study addressed was the cyberslacking in the workplace, especially in public sector organizations (Johnson & Chalmers, 2007; Mills et al., 2001; Whitty & Carr, 2006). Slacking in the workplace, due to the introduction of

new technologies, is not a recent phenomenon. As additional technology is incorporated into the workplace, new challenges arise. A classical example from the past is the arrival of the telephone in 1876, which brought new communication channels to the workplace to enable more productive exchanges, but it also raised new challenges such as misuse (Katz, 2004). Manross and Rice (1986) showed that the introduction of the telephone in the workplace also tempt to increase the use of telephone technology for personal use, which resulted in slacking and the consequential loss of productivity. Similarly, the introduction of the Internet brought the same productivity challenges as well. According to Whitty and Carr (2006), "Cyberslacking can be a problem for companies as this can lead to loss of productivity and could be considered a waste of companies' resources" (p. 238). Nagi (2006) and Jefferies (2000) explained that people spend time misusing their access to cyberspace, when they spend time visiting Websites that are not related to their job duties (Whitty & Carr, 2006). Cyberslacking is the newest version of misuse of technology that employers are confronting today (Block, 2001; D'Arcy & Hovav, 2008; Lara et al., 2006). This problem results in loss of productivity, raises some information security issues, and, thus, can also represent a liability to the organization (Block, 2001).

Mills et al. (2001) mentioned three problems that cyberslacking activities present in the workplace: "(1) the exhaustive use of company resources, (2) productivity and financial loss, and (3) legal liability" (p. 36). However, the extent of cyberslacking proliferation has not been fully studied. Johnson and Rawlins (2008) stated that, "Cyberloafers and cyberslackers are becoming such a big enough problem in the corporate world that many companies are beginning to crack down" (p. 46). Companies need to support studies of employees' surfing habits, because the misuse of this resource

causes significant loss of productivity, legal liability, and waste of bandwidth (Johnson & Indvik, 2003).

Nowadays, Internet services are essential components of the underlying infrastructure of organizations (Whitty & Carr, 2006). The increased use of these services in the workplace presents new challenges that governments and companies need to control with the creation of policy, monitoring, and other interventions (Johnson & Chalmers, 2007). According to Mills et al. (2001), "Companies have developed an Internet acceptable-use policy (IAUP)" (p. 47). With an IAUP, a company establishes the policy for correct use of Internet technologies in the workplace, which, in conjunction with the enforcement controls implemented, can result in control over employees' use of those resources. With the increased use of the Internet, new ethical issues are presented; companies and governments need to confront its misuse (Dorantes, Hewitt, & Goles, 2006). Block (2001) raised several critical questions, including, "is cyber (or any other kind of) slacking on the job immoral?" (p. 226). Block (2001) puts cyberslacking activity in the category of immoral behavior. According to Gbadamosi (2004) the term ethics, "boils down to morality and good or bad conduct" (p. 1145).

The development of new technologies present new behavioral characteristics that is necessary to identify before and after the implementation of those technologies (Stahl, Rogerson, & Wakunuma, 2009). According to Smith (1997), "At the end of the millennium, the ethical design of computer networks and the development of adequate security safeguards and standards have yet to be required" (p. 242). This shortcoming represents a constant technological challenge to companies and government agencies, as well as other public sector organizations.

With the advent of new technologies, SNS is a new trend that companies are integrating in their business (Burrus, 2010). Facebook®, Twitter®, YouTube®, Digg™, Delicious®, and Visual Communications® are some examples of personal SNS (Burrus, 2010). Bennett, Owers, Pitt, and Tucker (2010) argued, "organizations that have implemented social networking have experienced a shift in culture from information gathering to information participation" (p. 139). Accordingly, SNS is a protagonist in the daily process and activities of the workplace. As Burrus (2010) stated, "unfortunately, many businesses feel that Web 2.0 and social networking are problematic when used by employees" (p. 50). The problem exists when employees spend work time updating their personal SNS accounts rather than, if their duties call for it, using SNS for job-related activities (Henle & Blanchard, 2008; Kidwell, 2010).

One approach to address this problem, it is for companies to adopt strategies to reinforce the powerful use of the SNS as a tool in the workplace, and not as a personal utility (Burrus, 2010). According to Mills et al. (2001), "the need to monitor employees' Internet use has helped to spawn a half-billion-dollar Internet management industry" (p. 44). There is very little research in the literature that recognizes cyberslacking as a problem in the business and public sectors. According to Burrus (2010), "corporate bureaucracies resist losing control of information flows and some leaders are reluctant to embark on a personalized communications program that may raise expectations of employees" (p. 50).

A study in 2000 revealed that 56% of employees used Internet technologies in the workplace for personal reasons (Greengard, 2002). Another study in 2003 showed that nearly 56% of employees used the Internet for activities that were not related to their

work (Griffiths, 2003). According to Malachowski (2005), "1,404 of the 2,700 people polled cited web surfing as their #1 distraction at work" (p. 1). All of these misuses of Internet technologies in the workplace are called cyberslacking, referring to a counterproductive unethical behavior that affects the workplace today (Weatherbee, 2010). The estimated time that the employees spend in cyberslacking is between 2.5 and 3 hours per week, yet no exact numbers recently appear to be provided in empirical investigations, while very little is known about such numbers in the public sector (Greenfield & Davis, 2002; Mills et al., 2001).

This type of problem is on the rise daily and is affecting productivity in the workplace (Lim & Teo, 2005; Malachowski, 2005; Scheuermann & Langford, 1997; Stewart, 2000). Lim and Teo (2005) stated that, "it seemed important to find what motivated employees to engage in such behavior so that effective organizational intervention programs and policies could be developed and implemented" (p. 1080). Prior studies revealed that many companies have policies to control the use of the Internet, but there are some employees that are not aware about that policy (Whitty, 2002, 2004).

According to Zhang, Oh, and Teo (2006), there is a relation between people that knows the moral of cyberslacking and the frequency of that. Furthermore, Oswalt, Florence, and Austin (2003) stated that, "Internet is a powerful distraction and there is a fine, ethical line between the use and abuse of the Internet on the job" (p. 649). Also, Oswalt et al. (2003) showed that "reduction of cyberslacking will help prevent lost employee productivity, reduce employer liability, improve company security, and minimize the drain on company resources" (p. 651). According to Ínce and Gül (2011),

there is a relation between work inefficiency and employees that are engage in cyberslacking activities.

People misuse the Internet during work hours in a variety of ways (D'Arcy & Hovav, 2008; D'Arcy et al., 2009). Misuses depend upon demographic indicators such as gender, age, and educational level (Weatherbee, 2010). According to Morris and Venkatesh (2000), older workers are more ethical in the workplace, while younger and more educated employees are less ethical when it comes to the use of Internet technologies (Zhang, 2005). Moreover, it was found that gender is a demographic indicator that influences the misuse of this type of technology (Akman & Mishra, 2009; Fiore & Nelson, 2003; Garrett & Danziger, 2008; Gruber, 1999). Studies revealed that cyberslacking activities occur more with men than with women, and more with younger men than with older (Henle & Blanchard, 2008). However, the study of Henle and Blanchard (2008) was based on data collected from 194 employed students, yet it appears that very little is known about the magnitude of such phenomena in the context of public sector organizations, especially in government agencies, and from employees who are not students or being surveyed in the context of an educational institution.

According to Kidwell (2010), "high-ranking employees of the U.S. Securities and Exchange Commission violated ethics rules by spending many hours using government computers to surf the web and access pornographic websites, rather than performing their jobs of overseeing the nation's troubled financial system" (p. 3). This illustrate that cyberslacking is indeed occurring in the public sector. Furthermore, other federal agencies are monitoring employees' e-mails to reduce IS misuse (Sweeper, Boos, Hakesley, & Thurston, 2000). According to that action, and, given the increased

government spending on Internet technologies, cyberslacking by government and other public sector employees appears to be of a major concern and warrants additional research.

Dissertation Goal

The main goal of this research study was to measure the self-reported extent (i.e. amount of time spent & frequency) to which government employees and their co-workers engage in cyberslacking activities in the workplace, to ascertain the perceived ethical severity of these cyberslacking activities, and to investigate if there are any differences on these measures based on gender, age, level of education, and years working for government. The first specific goal of this research study was to measure government employees' self-reported *frequency* of engagement in cyberslacking activities. Frequency of engagement in cyberslacking activities was measured based on 20 items using a seven-point scale ranging from 1-never to 7-several times a day.

The second goal of this research study was to measure the government employees' reports on their *co-workers' frequency* of engagement in cyberslacking activities. According to Blanchard and Henle (2008), it is difficult to measure self-reported cyberslacking, because employees know that it is undesirable activity, and may not be forthcoming about their abuse of workplace Internet technology. Also, Henle and Blanchard (2008) found that self-reported cyberslacking data was more difficult to obtain. Given that individuals tend to under-report their own engagement in unethical activities and over-report others, this study measured both the employees' self-reported engagement in cyberslacking activities as well as their reporting on co-workers'

engagement in such activities. Thus, the second measure about co-workers tried and sees if triangulation of the measures was made (Spears & Barki, 2010).

The third goal of this research study was to measure government employees' self-reported *amount of time spent* on engagement in cyberslacking activities. Time of engagement in cyberslacking activities was measured based on 20 items using a seven-point scale ranging from 1-never to 7-on average 8 or more hours a day. The fourth goal of this research study was to measure government employees' reports of the *amount of time co-workers spend* on engagement in cyberslacking activities. The fifth goal of this research study was to measure government employees' perceived *ethical severity* of cyberslacking activities (Levy, Ramim, & Hackney, 2013). Perceived ethical severity engagement in cyberslacking activities was measured based on 20 items using a seven-point scale ranging from 1-Highly Unethical to 7-Highly Ethical.

According to Akman and Mishra (2009), "the area of IT ethics has been attracting a lot of attention recently and the most current research on IT ethics are concentrated on either common demographics such as gender, age, education, and experience" (p. 1251). Also, Akman and Mishra (2010) stated, "results indicated that gender has positive impact on average daily time spent on the use of the Internet for communication/e-mailing/chat and information access/downloading/entertainment" (p. 482). Vitak, Crouse, and LaRose (2011) stated that, "being younger, male, and a racial minority positively predict cyberslacking variety and frequency" (p. 1751).

Therefore, the sixth goal of this research study was to determine if there are any significant differences in government employees' self-reported *frequency* of engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job

level, and (e) years working for government. The seventh goal of this research study was to determine if there any significant differences in government employees' reports on *co-workers' frequency* of engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government. The eight goal of this research study was to determine if there any significant differences in government employees' self reported *amount of time spent* on engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government (Akman & Mishra, 2009; Blanchard & Henle, 2008; Levy et al., 2013; Magklaras & Furnell, 2005; Verton, 2000; Whitty, 2002, 2004; Whitty & Carr, 2006).

The ninth goal of this research study was to determine if there any significant differences in government employees' reported on *co-workers' amount of time spent* on engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government (Akman & Mishra, 2009; Blanchard & Henle, 2008; Levy et al., 2013; Magklaras & Furnell, 2005; Verton, 2000; Whitty, 2002, 2004; Whitty & Carr, 2006).

The tenth goal of this research study was to assess the impact of government employees' *reported amount of time spent* (self + co-workers) and *frequency* of engagement (self + co-workers) in cyberslacking activities of their *perceived ethical severity* of such activities (Akman & Mishra, 2009; Blanchard & Henle, 2008; Levy et al., 2013; Magklaras & Furnell, 2005; Verton, 2000; Whitty, 2002, 2004; Whitty & Carr, 2006).

As the use of the Internet at work increases, so does the need to study its misuse (Kim & Byrne, 2011; Hovav et al., 2009). According to Restubog et al. (2011) "there has been little empirical work concerning cyberloafing behavior" (p. 247). According to Jia (2008), there is a necessity to develop more empirical work to know "if cyberslacking replaces other traditional forms of loafing" (p. 93). The claim for more research about cyberslacking is not only to understand the behavior, also to understand the reasons behind it and to identify the levels of severity (Messarra, Karkoulian, & McCarthy, 2011; Venkatraman, 2008). Liberman, Seidman, McKenna, and Buffardi (2011) stated that, future research should include the exploration of "why employees engage in cyberslacking and their affective reactions to cyberslacking [sic]" (p. 2197), while attempting to identify the organizational, social, and personal factors that would affect this behavior.

Research Questions

The main research question (RQ) that this research study was addressed is: to what extent (i.e. amount of time spent & frequency) are government employees self-reported about themselves and their co-workers on engagement in cyberslacking activities in the workplace; how ethically severe, they perceived these cyberslacking activities, as well as if there are any significant differences on these measures based on gender, age, level of education, and years of employment. Moreover, this study analyzed the impact of the aforementioned measures on employees' *perceived ethical severity* of such activities in the public sector. The types of cyberslacking activities that this research study included are: shopping online during work hours, perusing pornographic sites,

visiting SNS for personal use, and using work computers for managing personal data (Henle & Blanchard, 2008; Johnson & Indvik, 2003; Kidwell, 2010; Lara et al., 2006; Lim & Teo, 2005).

The specific research questions that this research study addressed are:

RQ1: What is the government employees' self-reported *frequency of engagement* in cyberslacking activities?

RQ2: What is the government employees' reported *frequency of co-workers' engagement* in cyberslacking activities?

RQ3: What is the government employees' self reported amount of *time spent on engagement* in cyberslacking activities?

RQ4: What is the government employees' reported of *co-workers' amount of time spent on engagement* in cyberslacking activities?

RQ5: What is the government employees' perceived *ethical severity* of engagement in cyberslacking activities?

RQ6: Are there any significant differences in government employees' self-reported frequency of engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?

RQ7: Are there any significant differences in government employees' reported frequency of co-workers' engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?

RQ8: Are there any significant differences in government employees' self-reported amount of time spent engaging in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?

RQ9: Are there any significant differences in government employees' reported the amount of time spent by co-workers engaging in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?

RQ10: What is the impact of government employees' self-reported amount of time spent (self + co-workers) and frequency of engagement (self + co-workers) in cyberslacking activities on their perceived ethical severity of such activities?

Figure 1: Conceptual Model on the Impact of Frequency and Amount of Time Spent on Cyberslacking on Ethical Severity of Such Activities

Relevance and Significance

According to Ugrin and Pearson (2013), "Cyberloafing has become a pervasive problem for many organizations and some researchers have suggested a deterrence approach based on acceptable use policies for Internet-based applications, coupled with mechanisms designed to monitor employee Internet usage and detect unauthorized usage" (p. 812). According to Whitty and Carr (2006), "cyberslacking is the overuse of the Internet in the workplace for purposes other than work" (p. 238). Also, Whitty and Carr (2006) argued that, "cyberslacking can be a problem for companies as this can lead to loss of productivity and could be considered a waste of companies' resources" (p. 238). The problem occurs when employees spend time visiting Websites not related to their job duties (Jefferies, 2000; Nagi, 2006; Whitty & Carr, 2006). This problem not only leads to a loss of productivity and, by extension, a liability to the organization (Block, 2001), it also creates computer network security problems, legal issues, and reductions in data speed across the computer network (Chen, C. C., Chen, J. V., & Yang, 2008). Ugrin and Pearson (2013) stated that, "individually, threats termination and detection mechanisms are effective deterrents against activities like viewing pornography, managing personal finances, and personal shopping, but must be coupled together and actively enforced to dissuade activities like personal emailing and social networking" (p. 812). Millsgy et al. (2001) showed three problems that cyberslacking activities present in the workplace: "(1) the exhaustive use of company resources, (2) productivity and financial loss, and (3) legal liability" (p. 36). Johnson and Rawlins (2008) stated, "cyberloafers and cyberslackers are becoming such a big enough problem in the corporate world that many companies are beginning to crack down" (p. 46). For example,

when employees send or watch pornographic material, this activity affect computer

network, and other employees as a consequence of the interruptions can also cause legal

problems, can increase the potential of inflicting malware on corporate networks

(Johnson & Rawlins, 2008). As a consequence, companies are currently using computer

monitoring systems (Alder, Schminke, Noel, & Kuenzi, 2007) that although beneficial,

may present ethical issues, depending on the regulations of the organization. According

to a study by Ugrin et al. (2008), monitoring employees with low self-control is

beneficial to the organization (Gottfredson & Hirschi, 1990). Individuals with low self-

control are more likely to engage in cyberslacking (Restubog et al., 2011).

Based on the aforementioned findings, the relevance of this study was in tandem

with both for-profit companies as well as government agencies. Additionally, this

problem has significant implications as a consequence of the massive increase in Internet-

based tools in the workplace that area readily available to employees. Also, İnce and Gül

(2011) stated that, "The frequently given voice to these and such like questions at both

academic and organization environment shows that cyberslacking increasingly became a

matter that management has to deal with" (p. 510). Moreover, it appears that there is a

gap in the literature when it comes to understanding the role of self-reported extent (i.e.

amount of time spent & frequency) to which government employees and their co-workers

engage in cyberslacking activities in their workplace, to ascertain the ethical severity of

these cyberslacking activities. Jefferies (2000) stated that,

> As such a huge number of ethical issues are raised. Some such issues include
>
> those of privacy, accuracy, data security, intellectual property rights and
>
> accessibility. However concern for these issues and the actual social and cultural

impact on society of the burgeoning development of a multimedia cyberspace is very often overlooked in most of the 'hype' and 'techno- enthusiasm' that abounds. (p. 1)

Limitations and Delimitations

Limitations

This study presented a limitation with the generalizability of the sample. The participants in this research study represented several agencies of the Executive Branch of the Government of Puerto Rico. Griffiths (2010) mentioned examples of abusive behaviors that employees have engaged in the workplace's Internet, including cybersexual, also he stated, "online friendship/relationship abuse, internet activity abuse, online information abuse, criminal internet abuse" (p. 463). Oswalt et al. (2003) stated, "IT managers must be particularly aware of the legal and ethical issues concerning the use of Internet on the job. IS students must develop a solid background in the ethical use of the Internet" (p. 647). According to Oswalt et al. (2003), the distraction of Internet presents an ethical issue in the workplace. Those statements are related to another limitation for the study. Houston and Tran (2001) stated that, "The problem facing researchers is how to encourage participants to respond, and then to provide a truthful response in surveys. This is another limitation of this study, truthful response in surveys" (p. 70). Furthermore, when their response is related to an unethical activity in the workplace.

Delimitations

      The participants for this research study were representing several agencies of the Executive Branch of the Government of Puerto Rico. The sample was limited to a selected amount and not all the employees in the public sector.

Barriers and Issues

      Ínce and Gül (2011) stated that,

> improvements on Internet in the last 10 years have changed work life radically. The use of Internet is discussed much with its negative ways and positive ways such as accessing data, facilitating marketing, shortening production span, reducing cost and making production more efficient. (p. 507)

Furthermore, Ínce and Gül (2011) showed that, "statistics about results of cyberslacking make being taught that cyberslacking is an organizational problem gradually wide spreading and it needs to be controlled by organizations [sic]" (p. 512). Chen et al. (2008) explained that cyberslacking is not the only problem; also includes computer network security problems, legal issues, and data speed reduction problems across the computer network (Oswalt et al., 2003). Furthermore, Messarra et al. (2011) stated that, "When employees send their coworkers personal e-mails, jokes, etc. the time spent reading these e-mails decreases productivity time and fills up the server capacity with non-productive material" (p. 254). According to Oswalt et al. (2003), companies need more Internet monitoring and filtering tools to reduce those unwanted results that cyberslacking presents. Nonetheless the problem persists, and even increases, because every day there

are more, new multimedia elements that distract employees, while the cost of implementing and monitoring employees increases (Restubog et al., 2011).

This research study has barriers and issues that were necessary to address (Sekaran, 2003). Sekaran (2013) stated: "Identifying the critical issues, gathering relevant information, analyzing the data in ways that help decision making, and implementing the right course of action, are all facilitated by understanding business research" (p. 2). One of the barriers was that many respondents was not want to reveal their misuse of Internet in the workplace because they know it to be unethical (Sekaran, 2003; Ugrin et al., 2008; Zhang et al., 2006). To mitigate this barrier, the survey used in this study ensured the anonymity of the answers along with the measure of the participants' perceptions about their co-workers. By integrating the participants' perceptions of their co-workers, a better triangulation measure was provided indicating overall means across the total sample.

Another barrier of this research study was that employees perceived the survey as an audit of their Internet use and computer behavior. To mitigate this barrier, a letter was included with the survey in order to explain the purpose of the study and the anonymity of the process. Also, the letter included an explanation that the research study was not an investigation of a government agency, rather done for academic research only.

This research study used a Web-based survey instrument to collect the data. According to Sekaran (2003), there are advantages and disadvantages to the use of electronic surveys. Sekaran (2003) stated that, "an electronic questionnaire is easy to administer, can reach globally, very inexpensive, fast delivery and respondents can answer at their convenience like the mail questionnaire" (p. 251). An electronic survey was another potential barrier to this study, because not all people have a computer or a

connection to the Internet (Sekaran, 2003). Given that the focus of this study is on cyberslacking, it is valid to collect data only from those employees who actually have access to work computer, hence, also able to complete the survey instrument online. Thus, to mitigate this barrier, only employees with assigned computer were invited to participate in the study.

Definitions of Terms

Cyberslacking – the overuse of the Internet in the workplace for purposes other than work (Whitty & Carr, 2006)

Government sectors – institutions providing non-profit public services (e.g., universities, local government, etc.) (Akman & Mishra, 2009)

IAUP – Internet Acceptable-Use Policy is a written agreement signed by employees that sets forth the permissible and prohibited workplace uses of the Internet (Mills et al., 2001).

Self-control theory of crime – the theory of how crime is construed, how it should be measured, the kinds of people who are likely to engage in it, and the institutional context within which it is controlled (Gottfredson & Hirschi, 1990)

SNSs – Social Networking Sites is a place in Internet that allow users to post their profiles and create personal networks for exchanging information with others users (Henle & Blanchard, 2008; Johnson & Indvik, 2003; Kidwell, 2010; Lara et al., 2006; Lim & Teo, 2005; Weaver & Morrison, 2008)

Ethics – generally refer to the rules and principles of right and wrong conduct, it therefore boils down to morality and good or bad conduct (Gbadamosi, 2004)

Unethical – deliberate intent to mislead (Thomson, 2001)

Public sector – The adjective 'public' often denotes government at federal, state, and local levels, although it increasingly encompasses nonprofit organizations such as those of civil society or any not what specifically acting in self-interest. A long list of what public sector organizations exists. Colleges and universities, health care organizations, charities, as well as postal offices, libraries, prisons, etc. (Wang, Yan, Chen, & Xing, 2010); according to Akman and Mishra (2009), government sector by definition is public service

Summary

The chapter one of this research study discussed: problem statement, dissertation goal, research questions, relevance and significance, barrier and issues, as well as definition of terms. The research problem that this study addressed was cyberslacking in public sector organizations (Johnson & Chalmers, 2007; Mills et al., 2001; Whitty & Carr, 2006). Slacking in the workplace, due to the introduction of new technologies, is not a recent phenomenon. As additional technology is incorporated into the workplace, new challenges arise.

The main goal of this research study was to measure the self-reported extent (i.e. amount of time spent & frequency) to which government employees and their co-workers engage in cyberslacking activities in the workplace, to ascertain the perceived ethical severity of these cyberslacking activities, and to investigate if there are any differences on these measures based on gender, age, level of education, and years working for government. This chapter also defined the research questions that the research study

addressed. Also, a conceptual model on the impact of frequency and amount of time

spent on cyberslacking on ethical severity of such activities was presented.

Chapter 2

Review of the Literature

Introduction

Ínce and Gül (2011) stated that, "Cyberslacking has been gaining more importance with frequent using of Internet using at works. Cyberslacking, a new type of slacking is used with some aims that are related to Internet access supplied to workers in their work place [sic]" (p. 507). According to Odlyzko (2001), "there are repeating patterns in the histories of communication technologies, including ordinary mail, the telegraph, the telephone, and the Internet" (p. 493). Manross and Rice (1986) explained that the introduction of the telephone in the workplace also attracted an increase of the use of telephone technology for personal use, which resulted in slacking and the consequential loss of productivity. Hardy (2003) stated that the "Internet of today is a complex and anarchic-seeming worldwide network of computer networks. Applications such as electronic mail and the World Wide Web seem on their way to becoming as ubiquitous as the telephone and television in earlier generations" (p. 541). At the same time, new concerns arise about the correct use of those technologies. Hardy (2003) mentioned, "The avalanche of unsolicited commercial message (spam) sent over the Internet had grown to serious proportions by the early 2000s, threatening the integrity of computer networks and e-mail systems" (p. 548). Kraemer-Mbula, Tank and Rush (2013) stated that,

The organizational and technological capabilities of cybercriminals will likely advance and grow in the foreseeable future. As the use of cyberspace develops further, new opportunities will open up, for instance in the observed rapid growth in mobile web usage and social media (p. 552).

Brief Historic Background of Computing in the Workplace

In 1970s and 1980s personal computers revolutionized the workplace (Mowery & Simcoe, 2002). This equipment provides individuals with access to innovative online services (Mowery & Simcoe, 2002). According to Whitty and Carr (2006), computers and the Internet are two important instruments in the workplace nowadays, but there is a productivity challenge when employees appropriate them for personal use. According to Lorents, Maris, Morgan, and Neal (2006), "The potential for misuse of computer systems and resources has been an important issue for many years" (p. 45). Misuse of computers and information systems causes millions of dollars in productivity losses for organizations (Oswalt et al., 2003). Studies revealed that most employees know when they misuse computers during work hours; also, it revealed that they know that doing so represents a cost to their employers (Oswalt et al., 2003). According to Oswalt et al. (2003), organizations need to establish new policies to control this problem, however, knowing the magnitude of such misuse is not fully known. Furthermore, Whitty and Carr (2006) extended the definition of computer misuse in the workplace to include cyber-harassment and other illegal behavior.

Oz (1992) mentioned that computer legislation to mitigate unethical uses started in the late 1970s. According to Oz (1992), "the need for ethical behavior among

computer professionals was already recognized by the late 1960s as the use of computers quickly spread in academic and business organizations" (p. 423). As a result of these initiatives, professional organizations instituted their own ethical codes, beginning in the late 1970s (Oz, 1992).

Internet

According to Mowery and Simcoe (2002), "1960-1985 was the birth of Internet self-governance institutions, 1985-1995 was the growth in installed base of PC's and LAN's, and in 1995 to present, the privatization of Internet infrastructure and commercialization of Internet content" (p. 1372). The Internet as it is known today started in 1960 with a United States (US) military's project called the "Advanced Research Projects Agency Network (ARPANET)", its first application was the electronic mail (i.e. e-mail) (Hardy, 2003; Mowery & Simcoe, 2002). Mowery and Simcoe (2002) stated, "The ARPANET network is widely recognized as the earliest forerunner of the Internet" (p. 1372). According to Mowery and Simcoe (2002), two physicists, Tim Berners-Lee and Robert Cailliau, developed the World Wide Web (WWW), the foundation for Hyper Test Transfer Protocol (HTTP), and the early Hyper Text Markup Language (HTML) code. This invention represented an important phase of the Internet (Hardy, 2003; Mowery & Simcoe, 2002).

Advances in digital technology, also, the rapid developments of electronic networks have dramatically accelerated the growth of distributed multimedia systems. Others communications technologies in addition to the distribution of multimedia information on the Internet have grown significantly (Abie, Spilling, & Foyn, 2004). There is a need to protect digital content and the associated usage rights from

unauthorized access, use, in addition to dissemination (Abie et al., 2004). According to

Wallace (2004), "the advance of technology and the introduction of it in the workplace

have been an important subject of debate for centuries" (p. 5). Wallace (2004) mentioned

that, "By the late 1980s, though, and especially in the 1990s after the World Wide Web

made its debut, the Internet set off a wave of creative destruction that affected business

around the world" (p. 1). The emergence of the Internet enabled information sharing and

dissemination, independent of the information, at a low cost (Lamersdorf, Tschammer, &

Amarger, 2004). According to a study by Lamersdorf et al. (2004), this 'new

environment' at that time, allowed access to a growing number of citizens in addition to

customers, to new kinds of businesses that has been continuously exposed. This novelty

is changing the environment where corporations, governments, and communities interact

(Lamersdorf et al., 2004). According to Lamersdorf et al. (2004), the changes are

especially notable in the way information is received, processed, sent, and stored. Such

changes transform the ways that information is managed, the security, integrity, as well

as consistency of it.

Governments have been engaged in deploying information communication

technologies (ICTs) for several decades to increase their efficiency plus effectiveness

(Bhatnagar, 2004). Early applications were focused on building management information

systems for planning and monitoring (Bhatnagar, 2004). According to Bhatnagar (2004),

the record gain resulting from ICTs has been quite dismal. However, the advent of the

Internet plus its use in advocacy, online learning, and fostering participation in it by some

countries, has once again revived the hope that ICTs can deliver value commensurate

with investment into them (Bhatnagar, 2004). This investment includes information and service to citizens (Bhatnagar, 2004).

The continued growth of the Internet in addition to advances in networking technology have fueled a trend towards outsourcing data management, as well as information technology needs to external application service providers (Mykletun, Narasimha, & Tsudik, 2006). As of this writing, organizations depend on outsourcing services, such as applications via the Internet, to run their operations.

Flynn (2001) mentioned that, "The Internet poses particular challenges to traditional legal methods of regulating online behavior" (p. 1). According to Flynn (2001), some theorists argued that the Internet is capable of collective self-regulation that provides reasonable protection for activities on the global net. This argument points to the difficulty in regulating furthermore legislating the use of the Internet or IS, specifically regarding ethics and law.

In terms of regulation, IS is particularly difficult to manage. Davison, Kock, Chismar, and Langford (2001) stated that, "professional ethics in IS concerns a professional's conduct of behavior and practice when carrying out IS-related activities. Such work may include consulting, researching, teaching and writing" (p. 1). According to Davison et al. (2001),

> Professional behavior usually follows implicitly accepted standards, which may be formally stated, while the institutionalization of codes of conduct/practice is common, and many professional bodies have developed such codes for their members to observe. The field of IS is lacking in this respect. (p. 1)

ISs often present virtual spaces that enable important human interaction (Chapman, 2006). By enabling such interaction, systems designers are inherently creating certain ethical structures (Chapman, 2006). According to Chapman (2006), when one creates or implements an IS, one also creates the ethics for a new world of interaction, and such ethics needs specific attention. Legal experts recognize that the Internet challenges the traditional legal approaches towards the regulation of online behavior (Flynn, 2001). Griffiths (2010) mentioned examples of abusive behaviors that employees have engaged in the workplace's Internet, including cybersexual in addition to online friendship/relationship.

Table 1. Summary of Computing History in the Workplace Related Research

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
İnce & Gül, 2011	Survey	266	Locus of control and cyberslacking, cyberslacking and job satisfaction, work inefficiency and cyberslacking, job satisfaction and intention to leave the job	1. Depending on tendency to increase computer and internet using world-wide, it is inevitable that the cyberslacking will be an important matter for organizations. 2. Researches about cyberslacking are negligible in Turkey. 3. Academicians have highly external locus of control and they actualize minor cyberlacking behaviors. 4. Academicians actualize minor cyblerslacking behavior such as

Table 1. Summary of Computing History in the Workplace Related Research

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
				sending and receiving e-mails unrelated to job, entering news web-sites, making holiday and travel reservation and doing individual banking operations generally.
Manross & Rice, 1986	Survey and interviews	88	Users' perceived attributes of an intelligent telephone system, users' attitudes towards the innovation, and perceived impacts of the system	1. Slightly favorable responses toward the innovation and its impacts, but could not identify perceived attributes of the innovation that differentiated between a "successful" and a "failed" adoption of the innovation. 2. Levels of individual usage of the enhanced telephone's functions could not be distinguished by attitudes, and only slightly by the perceived increases in information handling and phone calls. 3. The implementation and the subsequent diffusion of organizational information systems must be seen, theoretically, as a contingent process.

Table 1. Summary of Computing History in the Workplace Related Research

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Hardy, 2003	Review of Literature	There are no sample	N/A	1. Precursors of the Internet 2. Earlier computer networks 3. Origins of the Arpanet 4. Arpanet 5. CSNET and USENET 6. The first internetwork connection 7. CSNET and ARPANET 8. Internet administration under ARPA 9. The world wide web and the dot-com bubble 10. Security, privacy, regulation, commercialization, and post-ARPA internet administration
Mowery & Simcoe, 2002	Review of Literature	N/A	N/A	1. The creation of the Internet drew on many of the same institutions and policies of the post-war US "national innovations system" that were influential in other post-war high-technology industries. 2. The prominent role of Defense Department funding and procurement in the development of

Table 1. Summary of Computing History in the Workplace Related Research

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
				the Internet 3. Internet's rapid development, also have been extended considerably since the early 1990s. 4. The historically central role of US universities in industrial innovation also has shifted somewhat.
Whitty & Carr, 2006	Review of Literature	N/A	N/A	1. The new rules in the workplace over the use of the Internet, clearly need to be communicated to all employees and designed in a manner that, from an objects relations perspective, integrates with a recognition that the Internet is a potential space for play. 2. There is also need for new research that seeks to frame its' observations in a manner that admits an object relations perspective – in doing so we may more effectively target our 'rules' in the workplace to enhance the productive use of the Internet.

Table 1. Summary of Computing History in the Workplace Related Research

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Oz, 1992	Review of Literature	N/A	N/A	1. There is a reason to embark on an effort to form an international code of ethics for IS professionals. 2. The unified code will enhance the public's perception of IS specialists as representing a true, responsible profession. 3. It will also assure the public of the profession's concern for ethical development and implementation of information systems.
Kim & Byrne, 2011	Computer-based Research Participation System	203	Provide a typology of concepts describing internet usage for non-work-related purposes when supposedly working, identify associations between each concept and specific internet activities that capture a contemporary trend of internet use,	1. Internet access has become ubiquitous in corporate and academic settings. Considering the increased number of employees and students who often use computer-mediated communication technology for both work and leisure, it is important to acknowledge that the boundaries between work and leisure have become blurry. 2. Sheds light on internet behaviors

Table 1. Summary of Computing History in the Workplace Related Research

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
			and argue for an initial framework driven by an investigation on how these concepts relate to one another	and contexts where non-work-related internet use is perceived to be inappropriate and relatively negative as well as contexts where it might not be so bad. 3. The study explicated the distinct meanings of each concept and provided a typology as well as a preliminary framework to prevent conceptual confusion in future research. 4. Empirical evidence on perceived differences across seven concepts and analyzed the fit between internet deviant behaviors and concepts in one specific population: college students.

The Productivity Paradox

Strader, Simpson, and Clayton (2009) stated that, "Today's organizations utilize a broad range of computer-related resources, including personal computers, I/O devices, digital storage space, network bandwidth, and software, to provide their employees with tools for communications and increased productivity" (p. 465). At the same time,

computer misuse increases in the workplace, also, in consequence, it negatively impacts productivity (Strader et al., 2009). According to Strader et al. (2009), in 1980s, employees used computers for playing games during work hours, but in 1990s, the misuse extended to activities on the Internet; this expansion has significantly hurt workplace productivity. Johnson and Rawlins (2008) stated that lower productivity represents billions of dollars in losses to organizations when employees spend more than one hour a day on the Internet for personal use.

Johnson and Rawlins (2008) stated, "The U.S. Treasury Department recently monitored the Internal Revenue Services (IRS) workforce's Internet use. They found that activities such as personal e-mail, chat, online shopping, and personal finance and stocks accounted for 51% of employees' time spent online" (p. 44). Also, Johnson and Indvik (2003) stated that, "Corporate America spends approximately $3.5 billion annually for internet access, with at least $1 billion being attributed to employees' personal and cyberslacking activities. The potential negative effects form lost productivity alone represents a multi-billion-dollar issue" (p. 57). This demonstrates how organizations and government agencies lose money when employees' productivity decreases. According to Liao, Luo, Gurung, and Li, (2009), "During the past decade, ubiquitous deployment of the Internet has reshaped the workplace into an interconnected zone strengthening and catalyzing the organization's productivity" (p. 49). The implementation of new technological tools brings new advances to the workplace, but at the same time, it also increases concerns regarding the loss of productivity, which employees fail to consider when misusing these tools (Liao et al., 2009).

Cyberslacking

The use of Internet in the workplace increases every day then, as a result, new productivity challenges are emerging (Kim & Byrne, 2011). According to Whitty and Carr (2006), "cyberslacking" is the overuse of the Internet in the workplace for purposes other than work. With that overuse, new concerns are present during the work hours (Vitak et al., 2011), because it causes billions of dollars in productivity losses (Blanchard & Henle, 2008; Davis, Flott, & Besser, 2002; Lim, 2002; Phillips & Reddie, 2007; Websense, 2006). Scholars explained that loss of productivity is not the only problem; cyberslacking also leads to computer network security problems, legal issues, moreover the drop in data speed across a company's computer network (Chen et al., 2008; Everton, Mastrangelo, & Jolton, 2005). Ugrin and Pearson (2013) stated that,

> Cyberloafing has become a pervasive problem for many organizations and some researchers have suggested that a deterrence approach utilizing acceptable use policies for Internet-based applications coupled with mechanisms designed to monitor employee Internet usage and detect unauthorized usage can be an effective way to reduce it (p. 812).

According to Blanchard and Henle (2008), the problem of wasting work time by browsing the Internet for personal purpose will continue, because every day there are new multimedia elements to distract employees (Restubog, Garcia, Toledano, Amarnani, Tolentino, & Tang, 2011). Ugrin, Pearson, and Odom (2008) explained that it is necessary to examine why individuals misuse the Internet in the workplace. Also, Ugrin et al. (2008) explained the negative impact of individuals' misuse and what are the

mechanisms to minimize it. Thus, this study was built on the foundation of the self-

control theory of crime, which is introduced in the following section (Ugrin et al., 2008).

Table 2. Summary of Cyberslacking Related Research

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Vitak, Crouse, & LaRose, 2011	Reanalysis of data	2134	Cyberslacking variety, communicative cyberslacking	1. The oeuvre of cyberslacking literature has not yet provide a fully comprehensive review of all behaviors that could potentially predict cyberslacking behaviors. 2. Understanding of cyberslacking in a number of important ways, including, but not limited to, its use of a nationally representative sample. 3. The relationship between media habits and cyberslacking remains an understudied area of research, but appears to be playing a significant role in predicting these behaviors.
Blanchard & Henle, 2008	Survey	201	Perceptions of coworker and supervisor norms, external locus of control, and the frequency	1. Cyberloafing is a multi-faceted behavior which is likely to continue in organizations for the foreseeable future.

Table 2. Summary of Cyberslacking Related Research

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
			with which they engaged in cyberloafing	2. It is likely that cyberloafing will become more prominent and not less. 3. Need to better understand what sorts of cyberloafing behaviors employees engage in and how we can minimize the negative effects of cyberloafing on worker productivity while still maintaining a workplace that allows for creativity and trust.
Ugrin, Pearson, & Odom, 2008	Survey	87	Respondents were asked a question about whether or not they would use their company's resources for personal use	1. Awareness of enforcement was the most salient factor, followed by a statement indicating that one could fired for performing non-work-related computing (NWRC), plus the existence of monitoring systems. 2. The results provide evidence that an acceptable use policies (AUP) that defines acceptable Internet usage, imposes potential sanctions, and

Table 2. Summary of Cyberslacking Related Research

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
				implements detection (or monitoring) mechanisms is an important deterrent of Internet abuse.
				3. The study provides valuable insights and considerations for drafting and implementing an AUP in an organization.

Self-Control Theory of Crime

According to Gottfredson and Hirschi (1990), "the theory of crime has

implications for how crime itself is construed, how it should be measured, the kind of

people who are likely to engage in it, and the institutional context within which it is

controlled" (p. 4). They explained that there are two key factors for predicting criminal

behavior: self-control opportunity and the second one is the opportunity (Gottfredson &

Hirschi, 1990). These lacks of self-control occur when employees engage in the misuse

of Web tools in the workplace (Kim & Byrne, 2011). Restubog et al. (2011) argued that

there is a relationship between low self-control in addition to a vulnerability factor that

results in counterproductive behaviors such as cyberslacking. Ugrin et al. (2008) as well

as Vitak et al. (2011) presented a relationship between their two studies that will be used

in developing a profile of the type of employee who has a propensity for cyberslacking.

Ethical Use of the Internet

Oswalt et al. (2003) stated: "IT managers must be particularly aware of the legal and ethical issues concerning the use of Internet on the job. IS students must develop a solid background in the ethical use of the Internet" (p. 647). According to Oswalt et al. (2003), the distraction of Internet presents an ethical issue in the workplace. According to Messarra et al. (2011), employees need to be educated about the ethical use of the Internet in the workplace. Young (2010) stated, "with continued use, education and training can help increase employee accountability and ethical integrity when online" (p. 1469). Furthermore, Chen et al. (2008) explained that Internet misuse in the workplace presents ethical issues that could be turn into online crimes.

According to Gbadamosi (2004), ethics has generally been used to refer to the rules and principles of right or wrong conduct. Levy et al. (2013) stated that, "however, it appears that very limited attention has been given to investigating the ethical severity of cyber-security attacks and emerging employees' unethical behaviors within the context of growing organizational Web-based systems" (p. 1). Also, Chen et al. (2008) argued that, "the deviant use of Internet technology in the workplace can pose various risks to a corporation" (p. 88). Furthermore, they showed that this misuse might be linked with an engagement of unethical activities. Those unethical activities are or can become cyber crimes (Chen et al., 2008).

Block (2001) asked two critical questions, "is cyber (or any other kind of) slacking on the job immoral? Is it akin to theft?" (p. 226). That shows the necessity to understand the ethical severity of cyberslacking. Liberman et al. (2011) argued that:

While our list of non-Internet loafing activities were minor in severity and only

resulted in production deviance, it is important to examine in future research

whether cyberloafing is related to other more extreme forms of deviant workplace

behavior such as theft. (p. 2197)

Cyberslacking activities may be severe as a theft; however, currently there is limited

documented research on such issues (Friedman, 2000; Liberman et al., 2011).

Table 3. Summary of Ethical Use of the Internet

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Oswalt & Elliot, 2003	Review of Literature	N/A	N/A	1. IT managers must grasp the seriousness of the legal and ethical issues that cyberslacking brings to the workplace environment. 2. Reduction of cyberslacking will help prevent lost employee productivity, reduce employer liability, improve company security, and minimize the drain on company resources.
Messarra, Karkoulian, & McCarthy, 2011	Survey	254	Examine the impact of four internet monitoring policies on cyberslacking and work satisfaction.	1. Results indicated that having a free Internet access had a positive relation with cyberlacking and monitoring policies, it is nevertheless Lebanese companies.

Table 3. Summary of Ethical Use of the Internet

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
Young, 2010	Review of literature	N/A	Former model	1. There is a growing attitude that employees are more open to using work computers from online banking to reading the news and we may need to rethink what is appropriate and inappropriate Internet use. 2. Employee Internet abuse has created significant productivity, financial, and legal problems among organizations.
Levy, Ramim, & Hackney, 2013	Survey	1100	Ethical severity of five common cyber-security attacks.	1. The study reveal that the majority of users (90%) reported their sense of severity as unethical across all five cyber-security attacks, while only a small minority of users (3.24%) reported these cyber-security attacks to be ethical. 2. A small number of individuals appeared unethical, we believe institutions should advertise very strong sanctions for those who are caught to ensure that the overall

Table 3. Summary of Ethical Use of the Internet

Study	Methodology	Sample	Instrument/ Constructs	Main findings or contribution
				attitude towards e-learning remains highly credible.
				3. Executives should be aware that the vast majority of e-learners are indeed ethical and should be treated as such without imposing collateral actions that reduces the moral of those who strive to be ethical at all times.

What is Known and Unknown

On a daily basis, cyberslacking is a problem in all organizational sectors, public and private. There is a need to integrate Internet monitoring systems, however, the financial investments required to implement such systems may not be feasible for every organization (Alder et al., 2007; Bhatnagar, 2004; Johnson & Chalmers, 2007; Oswalt et al., 2003; Sweeper et al., 2000). Ergun and Polat (2012) stated that, "nevertheless, considering the impacts of cyberslacking on organizations, it is clear that there is a need for new studies which would be quite useful in terms of organizations" (p. 1). Furthermore, other new studies are necessary to uncover the extent (i.e. amount of time spent & frequency) of cyberslacking, along with employees' perceptions about the ethical severity level of such behaviors as it appear that some employees do not find such cyberslacking activities to be unethical at all (Liberman et al., 2011). According to

Liberman et al. (2011), new cyberslacking studies will help to understand new modalities of this behavior with different scenarios or other organizational sectors, i.e. public and private.

In organizations, supervisors know that their employees are engaging in the misuse of the Internet, but they only attack the problem by using different types of punishments or policies that are rarely enforced (Weatherbee, 2010; Whitty & Carr, 2006). Moreover, it is clear that additional research studies are needed to investigate and analyze the extent (i.e. amount of time spent & frequency) to which employees and their co-workers engage in cyberslacking activities in their workplace, along with assessing if there are any demographic indicators that may be able to explain differences in such misuse that affects the productivity in the workplace (Weatherbee, 2010; Whitty & Carr, 2006).

Chapter 3

Research Methodology

Introduction

This research study was exploratory in nature with a model testing as well. This

research study measured the frequency, time spent, and perceived ethical severity of

cyberslacking activities, both self-reported and reported about that of co-workers.

According to Sekaran (2003), the process of research includes "observation, preliminary

data gathering, problem definition, theoretical framework, generation of hypothesis,

scientific research design, data collection, analysis and interpretation, deduction, report

writing, report presentation, managerial decision making" (p. 56). Cyberslacking

behaviors that were surveyed included a collection of activities indicated in prior

literature, such as: shopping online during work hours, perusing pornographic sites,

visiting SNS for personal use, and using work computers for managing personal data, all

have been reported in prior literature (Henle & Blanchard, 2008; Johnson & Indvik,

2003; Kidwell, 2010; Lara et al., 2006; Lim & Teo, 2005; Mills et al., 2001; Vitak et al.,

2011; Websense, 2006).

Proposed Study Participants

The participants in this research study were representing several agencies of the

Executive Branch of the Government of Puerto Rico. The participants were employees of

the agencies and they received a message in their workplace e-mail accounts. The e-mail

message described the purpose of the research study and list the respective instructions to voluntary participate in the study. The sample included individuals from government agencies, and with an anticipated response rate of 25% or at least 150 participants minimum, which is typical for survey-based research (Fowler, 2995). These participants included employees of different ages, genders, educational levels, job levels, and varying years of working for government. An online anonymous survey was distributed using a commercial product, such as Google Forms. The Uniform Resource Locator (URL) of the Web-based survey instrument was sent by e-mail to the employees of the government agency requesting them to participate in the research study. Moreover, an e-mail message was sent to the participants from the head of the agency to request their voluntary participation in the study in order to help increase participation in this research.

Study Measures

This research study used a quantitative survey instrument to collect the data (Sekaran, 2003). The survey instrument (See Appendix A) have six sections: (a) self cyberslacking activity frequency; (b) co-workers' cyberslacking activity frequency; (c) self cyberslacking activities time; (d) co-workers' cyberslacking activities time; (e) ethical severity of cyberslacking activities; and (f) demographic information. The first four sections of the quantitative survey contained 20 cyberslacking activities documented in prior literature (Henle & Blanchard, 2008; Johnson & Indvik, 2003; Kidwell, 2010; Lara et al., 2006; Lim & Teo, 2005). To assess the measured variables, the survey instrument items have a seven-point Likert scale to facilitate the participants identifying the activity and the perceived ethical severity respectively.

Cyberslacking Activities

The measure of frequency, time spent, and perceived ethical severity was based on 20 cyberslacking activities on which study participants were asked to report. Participants were asked to self-report their cyberslacking activity frequency, report their co-workers' cyberslacking activity frequency, self-report cyberslacking activity time, report their co-workers' cyberslacking activity time, and report their perceived ethical severity of the 20 cyberslacking activities (Blanchard & Henle, 2008; Henle & Blanchard, 2008; Johnson & Indvik, 2003; Kidwell, 2010; Kim & Byrne, 2011; Lara et al., 2006; Lim & Teo, 2005; Vitak et al., 2011). Table 4 outlines the list of the 20 cyberslacking activities found in prior literature that was used for this study measures.

Table 4. Cyberslacking Activities (CA)

Item	Cyberslacking activities	Item Source(s)
CA1	Check non-work related email	Blanchard & Henle, (2008); Kim & Byrne, (2011); Lara et al., (2006); Lim, (2002); Lim & Teo, (2005)
CA2	Send non-work related email	Blanchard & Henle, (2008); Kim & Byrne, (2011); Lara et al., (2006); Lim, (2002); Lim & Teo, (2005); Vitak et al., (2011)
CA3	Visit general news sites	Blanchard & Henle, (2008); Kidwell, (2010); Kim & Byrne, (2011); Lim, (2002); Lim & Teo, (2005)
CA4	Visit stock or investment related Websites	Blanchard & Henle, (2008); Kim & Byrne, (2011); Lim, (2002); Lim & Teo, (2005)
CA5	View sports-related Websites	Blanchard & Henle, (2008); Kim & Byrne, (2011); Lim, (2002); Lim

Table 4. Cyberslacking Activities (CA)

Item	Cyberslacking activities	Item Source(s)
		& Teo, (2005)
CA6	Visit banking- or finance-related Websites	Blanchard & Henle, (2008); Kim & Byrne, (2011); Lim, (2002)
CA7	Shop online for personal goods	Blanchard & Henle, (2008); Kidwell, 2010; Kim & Byrne, (2011); Lim & Teo, (2005); Vitak et al., (2011)
CA8	Visit online auctions sites (e.g., eBay)	Blanchard & Henle, (2008); Kim & Byrne, (2011)
CA9	Send/receive instant messaging	Blanchard & Henle, (2008); Kim & Byrne, (2011); Lim & Teo, (2005); Vitak et al. (2011)
CA10	Participate in online games	Blanchard & Henle, (2008); Kim & Byrne, (2011); Lim & Teo, (2005); Vitak et al., (2011)
CA11	Participate in chat rooms	Blanchard & Henle, (2008); Kim & Byrne, (2011)
CA12	Visit newsgroups or bulletin boards	Blanchard & Henle, (2008); Kim & Byrne, (2011)
CA13	Book vacations/travel	Blanchard & Henle, (2008); Kim & Byrne, (2011)
CA14	Visit virtual communities	Blanchard & Henle, (2008); Kim & Byrne, (2011)
CA15	Maintain a personal Web page	Blanchard & Henle, (2008); Kidwell, (2010); Kim & Byrne, (2011)
CA16	Download music	Blanchard & Henle, (2008); Kim & Byrne, (2011)
CA17	Visit job-hunting or employment-related Websites	Blanchard & Henle, (2008); Kim & Byrne, (2011); Lim & Teo,

Table 4. Cyberslacking Activities (CA)

Item	Cyberslacking activities	Item Source(s)
		(2005)
CA18	Visit gambling Websites	Blanchard & Henle, (2008); Kim & Byrne, (2011)
CA19	Read blogs	Blanchard & Henle, (2008); Kim & Byrne, (2011); Vitak et al., (2011)
CA20	View sexually explicit Websites	Blanchard & Henle, (2008); Kim & Byrne, (2011); Lim, (2002); Lim & Teo, (2005)

Frequency of Cyberslacking Activities

In this section, the frequency of participants' cyberslacking activities are reviewed based on prior literature (Akman & Mishra, 2009; Blanchard & Henle, 2008; Magklaras & Furnell, 2005; Verton, 2000; Whitty, 2002; Whitty, 2004; Whitty & Carr, 2006). To measure frequency, the survey presented a seven-point Likert scale that included: 1-never, 2-once a month, 3-every other week, 4-once a week, 5-several days a week, 6-once a day, and 7-several times a day (Lim & Teo, 2005). According to each cyberslacking activity, participants selected their corresponding frequency of activity (see items SCAF1 to SCAF20 in Appendix A) and the frequency of that of their co-workers (see items CCAF1 to CCAF20 in Appendix A).

Time Spent on Cyberslacking Activities

To measure the amount of time spent on cyberslacking activities, the research study used a seven-point Likert scale also based on the aforementioned literature. For amount of time spent, the scale included: 1-never, 2- on average about 15 minutes a day,

3- on average about 30 minutes a day, 4- on average about 1 hour a day, 5- on average

about 2 to 4 hours a day, 6- on average about 5 to 7 hours a day, 7- on average 8 or more

hours a day. According to each cyberslacking activity, participants selected their

corresponding amount of time spent on each activity (see items SCATx1 to SCATx20 in

Appendix A) and the amount of time that they perceived their co-workers spent on each

cyberslacking activity (see items CCATx1 to CCATx20 in Appendix A).

Perceived Ethical Severity of Cyberslacking Activities

In this section, the measure of perceived ethical severity of cyberslacking

activities was reviewed and proposed based on prior literature (Oswalt et al., 2003; Levy

et al., 2013; Vitak et al., 2011). Each of the previously discussed 20 activities was divided

and participants selected how ethically severe they considered each cyberslacking activity

in the workplace during their work hours (Block, 2001; Gattiker & Kelley, 1999; Johnson

& Rawlins, 2008). To measure level of perceived ethical severity on each cyberslacking

activity, the measure had a seven-point Likert scale following Levy et al. (2013), which

include the scale of: 1-highly unethical, 2-unethical, 3-somewhat unethical, 4-neither, 5-

somewhat ethical, 6-ethical, 7-highly ethical. According to each cyberslacking activity,

participants will select their corresponding level of perceived ethical severity of each

activity (see items ESCA1 to ESCA20 in Appendix A).

Demographic Information

In this section, the demographics measures of participants' gender, age, highest

education degree achieved, job level, and years of work in the public sector was based on

prior literature (Akman & Mishra, 2009; Fiore & Nelson, 2003; Garrett & Danziger,

2008; Gruber, 1999). According to Ergun and Polat (2012), "gender may affect the

frequency and duration of cyberslacking as well as types of cyberslacking engaged and perceptions of cyberslacking" (p. 7). Moreover, Levy et al. (2006) stated, "females are more ethical than males, individuals become more ethical with age and graduates appear to be more ethical" (p. 10). Thus, this research study collected gender information to identify how the measured constructs are different and if there is consistency of such gender issue as reported in prior literature also in the context organizations in the public sector (Henle & Blanchard, 2008; Weatherbee, 2010). The study by Messarra et al. (2011) revealed that younger employees tend to engage more in cyberslacking, and that males tend to engage more in than females. Previous studies have shown other demographic factors, such as years in the organization and educational level to be important factors in the ethical abuse of work-owned technology (Lim & Teo, 2005). Accordingly, each participant was provided with survey items asking to report (anonymously) their corresponding demographic information (see items F1 to F5 in Appendix A).

Validity and Reliability

Internal Validity

Straub (1989) stated that internal validity of a study refers to "whether the observed effects could have been caused by or correlated with a set of unhypothesized and/or unmeasured variables" (p. 151). Also, according to Ellis and Levy (2009), "internal validity refers to the likelihood that the results of the study actually mean what the researcher indicates they mean" (p. 332). King and Jun (2005) stated: "survey research is a major presence in Information Systems (IS)" (p. 881). Also King and Jun

(2005) argued: "therefore, this method has the potential to produce generalizable results that can be applied to populations other than the sample tested. However, such potential needs to be carefully assessed and "designed into" the study" (p. 881). Thus, in this investigation, a panel of 10 experts was invited to review the measures (Appendix A). The members of the expert panel were professionals that have academic degrees and extensive experience in cybersecurity, information systems, ethics, as well as the legal field. The expert panel group received an explanation of the purpose of this research study. They were asked to validate the instrument according to their knowledge and experience in their respect professional field by providing feedback in improving the language, wording, as well as activities proposed.

External Validity

According to Leedy and Ormord (2005), external validity of a study refers to the "extent to which its results apply to situations beyond the study itself" (p. 105). King and He (2005) stated: "generalizability of sample results to the population of interest, across different measures, persons, settings, or times" (p. 882). To ensure that the data of this study have a good representation of government agencies sample and the population, the demographics variables of gender, age, educational level, job level, as well as years in the organization (the government agency) were compared between the data collected and the actual known data of the agencies surveyed.

Instrument Validity

According to Straub (1989), instrument validation refers to a "prior and primary process in confirmatory empirical research" (p. 162). The quantitative survey instrument that was used in this research study was validated to ensure its design (Straub, 1989).

First, an expert panel of professionals was asked to review and validate the quantitative survey instrument. As such, the expert panel validated the instrument items and the constructs assessed. Although items from previously published work were used in the initial draft of the survey instrument, expert review was also conducted to add validity (Blanchard & Henle, 2008; Kim & Byrne, 2011; Lara et al., 2006; Lim, 2002; Lim & Teo, 2005; Vitak et al., 2011).

Reliability

According to Straub (1989), "reliability is a statement about the stability of individual measures across replications from the same source of information" (p. 160). Furthermore, Straub (1989) stated, "findings based on a reliable instrument are better supported, and parameter estimates are more efficient" (p. 160). Sekaran (2003) stated that Cronbach's Alpha is a useful or effective coefficient to indicate how well the items in a set correlate to one another. Cronbach's Alpha values ranging from 0.0 to 1.0, where higher value indicate a higher reliability of the construct. This research study used Cronbach's Alpha to assess the reliability of each of the measured constructs. An acceptable valid Cronbach's Alpha for a construct is usually one that is over 0.7 (Sekaran, 2003).

Data Collection and Analysis

Data Collection

According to Sekaran (2003), "data collection methods are an integral part of research design" (p. 223). King and Jun (2005) stated that, "survey research is a major presence in Information Systems (IS)" (p. 881). This research study used a quantitative

anonymous Web-based survey instrument to collect the data. The survey was distributed via e-mail and data was collected using Google Forms. No specific identifiable information was collected. Furthermore, Houston and Tran (2001) stated that, "the problem facing researchers is how to encourage participants to respond, and then to provide a truthful response in surveys" (p. 70). Eddy, D'Abate, and Thurston (2010) stated that, "this snowball effect allowed us to: select individuals who work in office settings and who are expected to be doing work during work hours" (p. 643). Therefore, if there were too few responses, the research study originally planned to use a data collect process called snowball (Eddy et al., 2010), that asks 10 people that answered the survey to ask another set of 10 colleagues in their office to take part. This process was repeated until the expected number of responses was achieved.

Pre-Analysis Data Preparation

This research study measured cyberslacking activity in the public sector. After collecting the data and prior to any analysis, it was necessary to conduct a data cleansing to ensure the data is free of any irregularities prior to full analysis (Levy, 2006). According to Levy (2006), "a pre-analysis data screening deals with the process of detecting irregularities or problems with the collected data" (p. 150). This research study evaluated the accuracy of data collected from the survey. The study also ensured that the Web-based instrument had all items required to eliminate missing data. Moreover, this research study used Mahalanobis Distance to identify multivariate outliers. According to Levy (2008), "Mahalanobis distance was performed to detect outliers in the data collected" (p. 1667).

Proposed Analysis

According to Sekaran (2003), "in the data analysis we have three objectives: getting a feel for the data, testing the goodness of data, and testing the hypotheses developed for the research" (p. 306). Sekaran (2003) indicated that, the first objective will include the mean, range, standard deviation, and variance. This research study used data collected to address the RQs indicated in Chapter 1. For the corresponding statistical analysis of each question, it was necessary to follow the statistical analysis mentioned by Sekaran (2003). Also, according to Sekaran (2003), it is essential to include a frequency distribution for the demographic variables. Thus, the data analysis included a tabulation to compute the percentage of time of those cyberslacking activities based on gender, age, level of education, job level, and years working for government, as well as the percentage of frequency of those activities and how many participants consider those activities unethical. Moreover, this research study used means of the aggregated constructs scores for all five constructs to analyze RQ1-RQ6, graph the results of covariance (ANCOVA) using Statistical Package for Social Sciences (SPSS) for RQ6-RQ9. According to Mertler and Vannatta (2012), ANCOVA was used to analyze the differences when controlled by the demographic indicators as noted in RQ6-RQ9. The ANCOVA is different to ANOVA, but Mertler and Vannatta (2012) stated, "ANCOVA additionally controls for a variable (covariate) that may influence the DV" (p. 15).

Ordinal Logistics Regression (OLR) and Multiple Linear Regression (MLR) were used to answer RQ10. Mertler and Vannatta (2012) stated: "multiple regression identifies the best combination of predictors (IVs) of the dependent variable" (p. 14). The regression equation was used to make the predictions (Sprinthall, 2007). Also, Mertler

and Vannatta (2012) stated: "logistic regression may be used to predict values on a DV of two or more categories" (p. 293). Furthermore, they stated: "logistic regression specifies the probabilities of the particular outcomes (e.g., *pass* and *fail*) for each participant or case involved" (p. 293). Moreover, MLR is based on linearity, and OLR allows the ability to look for non-linear relationship between the IVs and the DV. Thus, this study used both MLR and OLR to further understand the relationships between the IVs and the DV.

Resources

In developing this research study, it was necessary to identify all the resources that helped ensure its success. To collect the data, it was necessary to identify the public sector agencies that participated in the survey. The survey was distributed using Google Forms to collect the data, which also was used to develop the necessary data reports. The selected agencies provided the necessary Internet and computer connections to each participant, also a personal computer was used to storage the data that Google Form collected, then use SPSS to analyze the data, as well as Microsoft Word to write and documented the results.

Chapter 4

Results

Overview

This chapter presents the data analysis and the results of this research investigation. The organization of this chapter is according to the chapter three. The results include: analysis, findings, and a list of the answers for the research questions. A pre-analysis data screening was made. This research study used Cronbach's Alpha to assess the reliability of each of the measured constructs. An acceptable valid Cronbach's Alpha for a construct is usually one that is over 0.7 (Sekaran, 2003). Also, this research study used Mahalanobis distance to identify multivariate outliers. Results of the MLR and OLR analyses were presented.

This research study used a quantitative survey instrument to collect the data (Sekaran, 2003). The survey instrument in Appendix A has six sections: (a) self cyberslacking activity frequency; (b) co-workers' cyberslacking activity frequency; (c) self cyberslacking activities time; (d) co-workers' cyberslacking activities time; (e) ethical severity of cyberslacking activities; and (f) demographic information. The first four sections of the quantitative survey contained 20 cyberslacking activities from prior literature (Henle & Blanchard, 2008; Johnson & Indvik, 2003; Kidwell, 2010; Lara et al., 2006; Lim & Teo, 2005). To assess the measured variables, the survey instrument items have a seven-point Likert scale to facilitate the participants identifying the activity and the perceived ethical severity respectively. The online anonymous survey was distributed

using Google Forms. The Uniform Resource Locator (URL) of the Web-based survey instrument was sent by e-mail to the employees of the government agencies requesting them to participate in the research study. Moreover, an e-mail message was sent to the participants from the head of the agencies to request their voluntary participate in the study in order to help increase participation in this research.

The main research question (RQ) that this research study addressed was: to what extent (i.e. amount of time spent & frequency) are government employees self-report about themselves and their co-workers on engagement in cyberslacking activities in the workplace; how ethically severe they perceive these cyberslacking activities to be, as well as if there are any significant differences on these measures based on gender, age, level of education, and years of employment. The specific research questions that this research study addressed were:

RQ1: What is the government employees' self-reported *frequency of engagement* in cyberslacking activities?

RQ2: What is the government employees' reported *frequency of co-workers' engagement* in cyberslacking activities?

RQ3: What is the government employees' self reported amount of *time spent on engagement* in cyberslacking activities?

RQ4: What is the government employees' reported of *co-workers' amount of time spent on engagement* in cyberslacking activities?

RQ5: What is the government employees' perceived *ethical severity* of engagement in cyberslacking activities?

RQ6: Are there any significant differences in government employees' self-reported frequency of engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?

RQ7: Are there any significant differences in government employees' reported frequency of co-workers' engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?

RQ8: Are there any significant differences in government employees' self-reported amount of time spent engaging in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?

RQ9: Are there any significant differences in government employees' reported the amount of time spent by co-workers engaging in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?

RQ10: What is the impact of government employees' self-reported amount of time spent (self + co-workers) and frequency of engagement (self + co-workers) in cyberslacking activities on their perceived ethical severity of such activities?

Data Collection and Analysis

Pre-Analysis Data Screening

According to Levy (2006), "a pre-analysis data screening deals with the process

of detecting irregularities or problems with the collected data" (p. 150). This research

study evaluated the accuracy of data collected from the survey. This study ensured that

the Web-based instrument have all items required to eliminate missing data. Moreover,

all records were reviewed for response-sets (i.e. when participants marked the exact same

score for all items without reading the survey). The cases with response-set of above 95%

similar score across all items measured were identified, which resulted in 19 records that

were deleted, providing a total of 183 usable cases. This research study used Mahalanobis

Distance to identify multivariate outliers. According to Levy (2008), "Mahalanobis

distance was performed to detect outliers in the data collected" (p. 1667). Table 5 details

the values that resulted from the Mahalanobis Distance Analysis.

Table 5. Mahalanobis Distance Extreme Values

			Case Number	**CaseID**	**Value**
Mahalanobis Distance	Highest	1	153	169	180.61319
		2	156	173	180.49310
		3	172	191	179.85264
		4	55	55	178.95600
		5	33	33	174.98223

Demographic Analysis

The pre-analysis data screening was completed and 183 usable responses were

available for the analyses. The data showed that 62 or 33.9% of the respondents were

males, and 121 or 66.1% were females, while 106 or 57.9% were between the ages of 40

to 59. In academic level 67 or 36.6% of the respondents had bachelor's degree and 105 or

57.4% were not supervising other employees. The demographic details of the sample

collected are presented in Table 6.

Table 6. Descriptive statistics of population (N=183)

Item	Frequency	Percentage (%)
Gender		
Male	62	33.9
Female	121	66.1
Age		
18 to 24	1	0.5
25 to 29	12	6.6
30 to 39	57	31.1
40 to 49	63	34.4
50 to 59	43	23.5
60 to 64	6	3.3
65 or older	1	.5
Academic Level		
None	0	0
High school diploma	0	0
Associates degree	12	6.6
Bachelor's degree	67	36.6
Master's degree	65	35.5
Professional degree	9	4.9
Doctoral degree	30	16.4
Job Level		
Supervising	78	42.6
No Supervising	105	57.4
Years in Government		
1 or less years	1	.5
1 to 5 years	33	18.0
6 to 10 years	29	15.8
11 to 15 years	34	18.6
16 to 20 years	27	14.8
21 or more	59	32.2

Internal Validity

Straub (1989) stated that internal validity of a study refers to "whether the observed effects could have been caused by or correlated with a set of unhypothesized and/or unmeasured variables" (p. 151). Also, according to Ellis and Levy (2009), "internal validity refers to the likelihood that the results of the study actually mean what the researcher indicates they mean" (p. 332). King and Jun (2005) stated that, "survey research is a major presence in Information Systems (IS)" (p. 881). Also King and Jun (2005) argued that, "therefore, this method has the potential to produce generalizable results that can be applied to populations other than the sample tested. However, such potential needs to be carefully assessed and "designed into" the study" (p. 881). Thus, in this investigation, a panel of 10 experts was invited to review the proposed measures (Appendix A). The members of the expert panel were professionals that have academic degrees and extensive experience in cybersecurity, information systems, ethics, as well as the legal field. They validated the instrument according to their knowledge and experience in their respect professional field by providing feedback for improving the language, wording, as well as activities proposed. Several minor word changes were preformed as a result of the expert panel process before proceedings to deploy the survey to the participants.

External Validity

According to Leedy and Ormord (2005), external validity of a study refers to the "extent to which its results apply to situations beyond the study itself" (p. 105). King and He (2005) stated that, "generalizability of sample results to the population of interest, across different measures, persons, settings, or times" (p. 882). To ensure that the data of

this study have a good representation of government agencies population, the demographics variables of gender, age, educational level, job level, as well as years in the organization of government agencies were collected.

Instrument Validity

According to Straub (1989), instrument validation refers to a "prior and primary process in confirmatory empirical research" (p. 162). The quantitative survey instrument was validated to ensure its design (Straub, 1989). An expert panel of 10 professionals was asked to review and validate the quantitative survey instrument. As such, the expert panel validated the instrument items and the constructs assessed. The expert panel submitted their recommendations and the instrument was adjusted according to the feedback. Items from previously published work were used in the survey instrument to add validity (Blanchard & Henle, 2008; Kim & Byrne, 2011; Lara et al., 2006; Lim, 2002; Lim & Teo, 2005; Vitak et al., 2011).

Reliability

According to Straub (1989), "reliability is a statement about the stability of individual measures across replications from the same source of information" (p. 160). Furthermore, Straub (1989) stated, "findings based on a reliable instrument are better supported, and parameter estimates are more efficient" (p. 160). Sekaran (2003) stated that Cronbach's Alpha is a useful or effective coefficient to indicate how well the items in a set correlate to one another. Cronbach's Alpha values ranging from 0.0 to 1.0, where higher value indicate a higher reliability of the construct. This research study used Cronbach's Alpha to assess the reliability of each of the measured constructs. An acceptable valid Cronbach's Alpha for a construct is usually one that is over 0.7

(Sekaran, 2003). Table 7 provides an overview of the Cronbach's Alpha. According to

Table 7, all constructs have acceptable reliability, given that all of measured constructs

demonstrated Cronbach's Alpha above 0.7, while four of the five constructs had

Cronbach's Alpha of over 0.85, indicating very high reliability.

Table 7. Results of Reliability Analysis

Variable	No. of Items	Cronbach's Alpha
SCAF	20	0.773
CCAF	20	0.933
SCAT	20	0.864
CCAT	20	0.940
ESCA	20	0.967

In order to preform the analyses to address the research questions of this study, first data

aggregation was conducted. Given the assumption that the items were linearly

distributed, all five constructs were aggregated linearly following the Eq. 1 to Eq. 5 as

noted below. Given that each item in each construct used a scale of 1-7, the range of the

aggregated scores of the constructs were from 20 to 140 (See Figure 2). Table 8 provides

the means of the aggregated constructs scores for all five constructs: SCAF, SCAT,

CCAF, CCAT, and ESCA.

Eq. 1: $\quad SCAF = SCAF_1 + SCAF_2 + \ldots + SCAF_{20}$

Eq. 2: $\quad CCAF = CCAF_1 + CCAF_2 + \ldots + CCAF_{20}$

Eq. 3: $\quad SCAT = SCAT_1 + SCAT_2 + \ldots + SCAT_{20}$

Eq. 4: $\quad CCAT = CCAT_1 + CCAT_2 + \ldots + CCAT_{20}$

Eq. 5: $\quad ESCA = ESCA_1 + ESCA_2 + \ldots + ESCA_{20}$

Figure 2 and Table 8 addresses RQ1 to RQ5. Figure 2 illustrates the means of the

aggregated constructs scores of the five constructs.
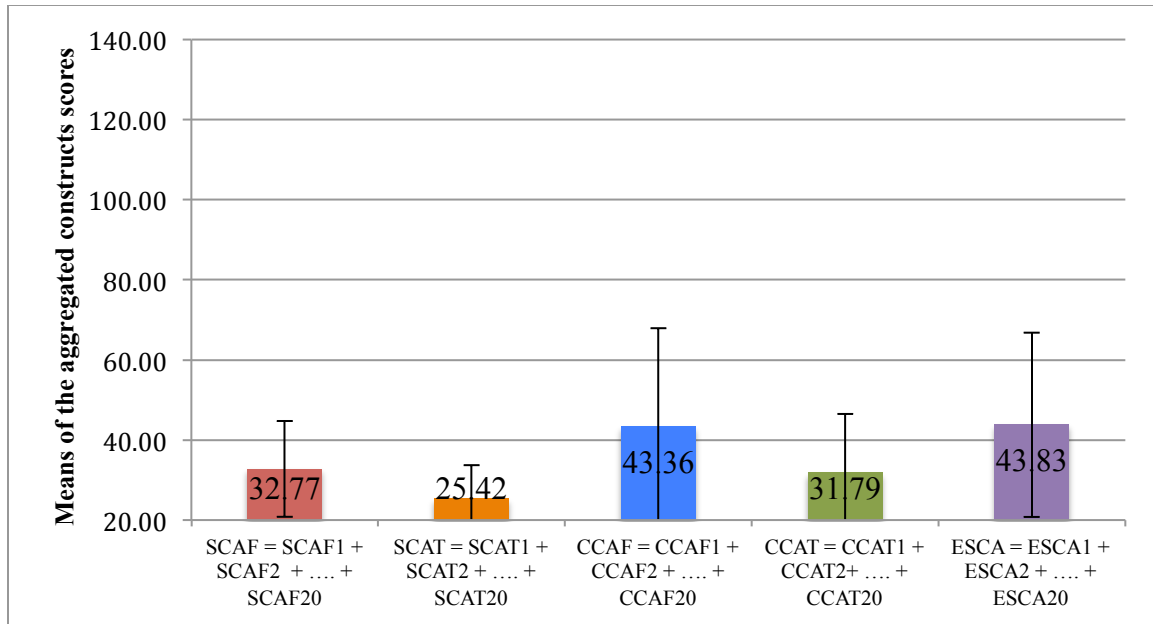
Figure 2: Means of the Aggregated Constructs Scores for all Five Constructs

Table 8. Results of the Means of the Aggregated Constructs Scores for all Five Constructs

Constructs	Means of the Aggregated Constructs Scores	Standard Deviation
SCAF	32.77	11.95
CCAF	43.36	24.59
SCAT	25.42	8.37
CCAT	31.79	14.71
ESCA	43.83	23.05

Figures 3, 4, 5, 6, and 7 illustrate the means and standard deviations of ESCA for the demographic of gender, age, education, job level, and years in the government.
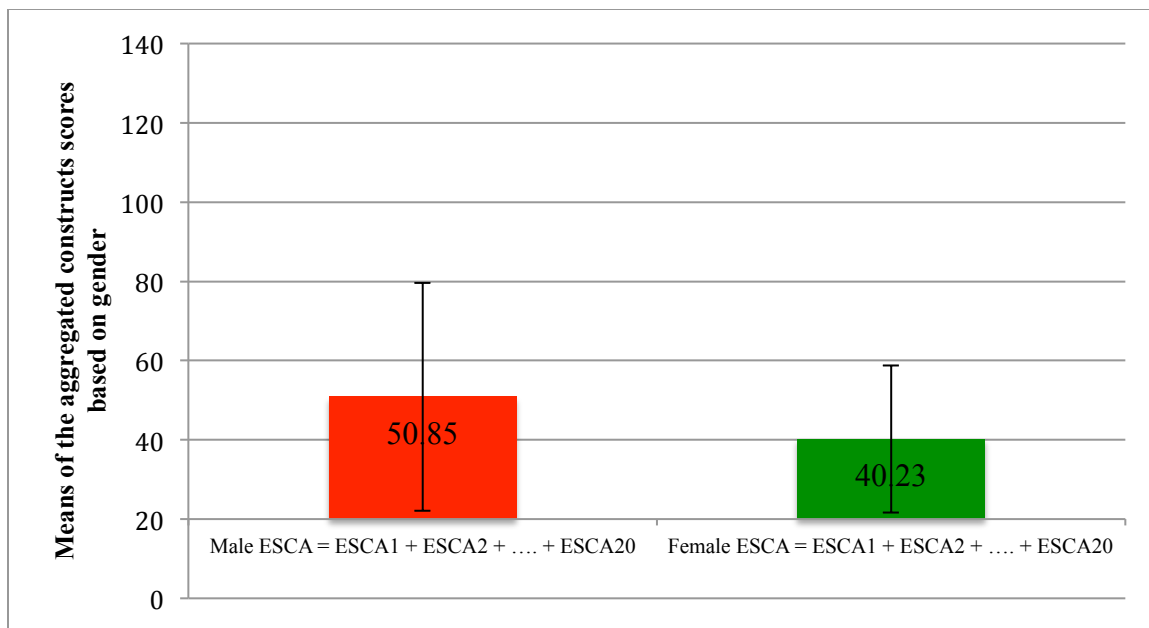
Figure 3: Means of the Aggregated Constructs Scores for Ethical Severity Cyberslacking Activity based on gender
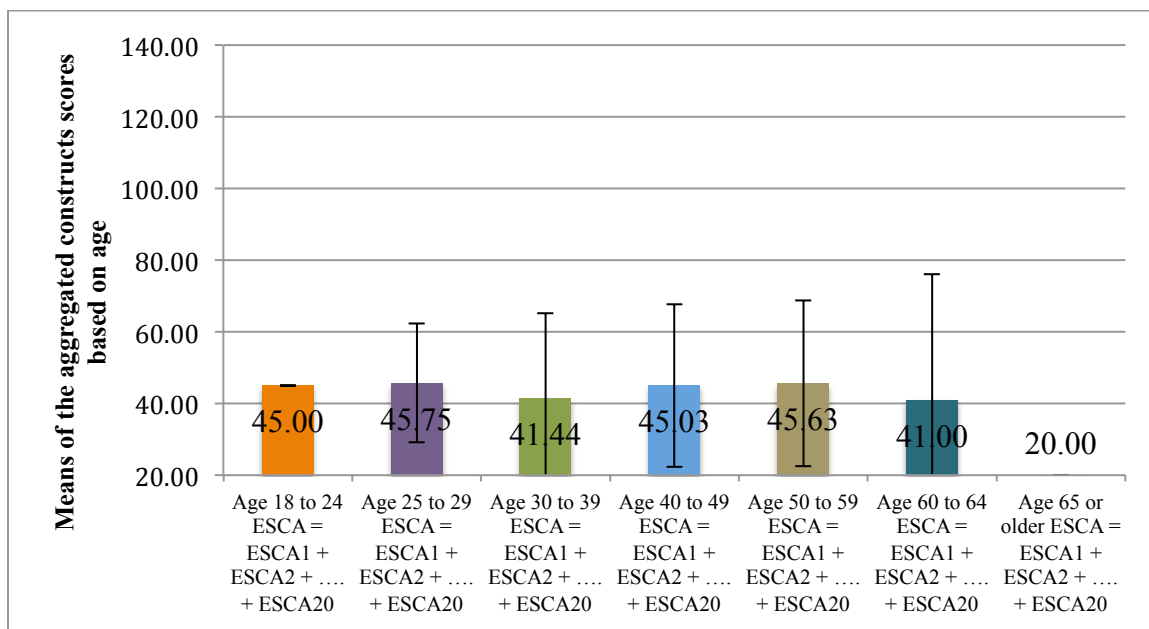
Figure 4: Means of the Aggregated Constructs Scores for Ethical Severity Cyberslacking Activity based on age
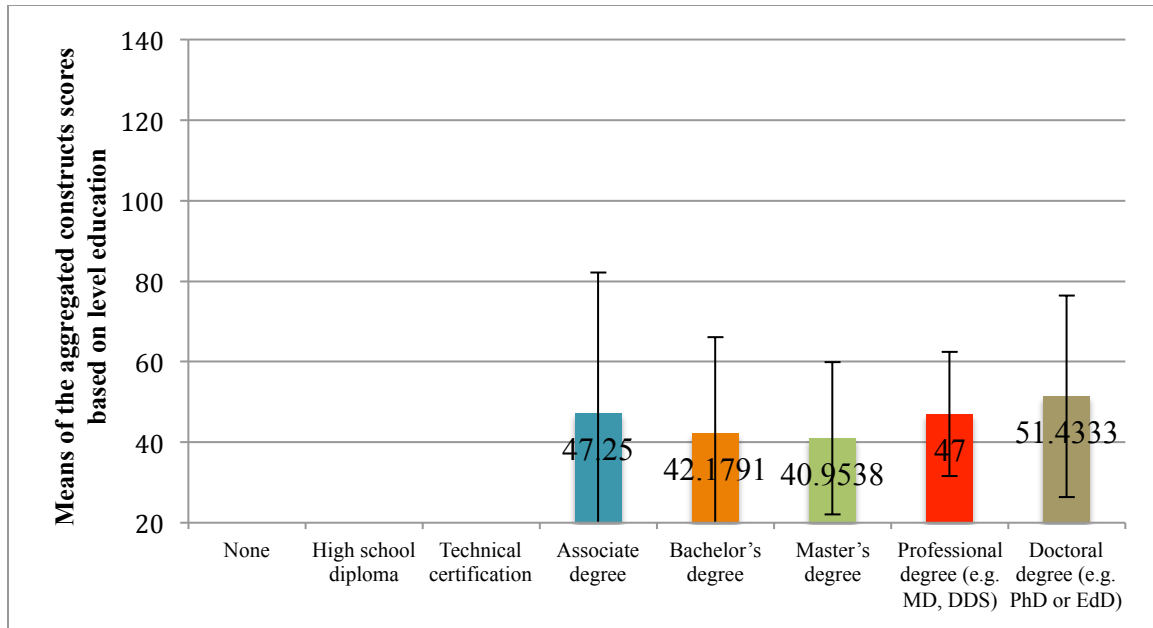
Figure 5: Means of the Aggregated Constructs Scores for Ethical Severity Cyberslacking Activity based on Level Education
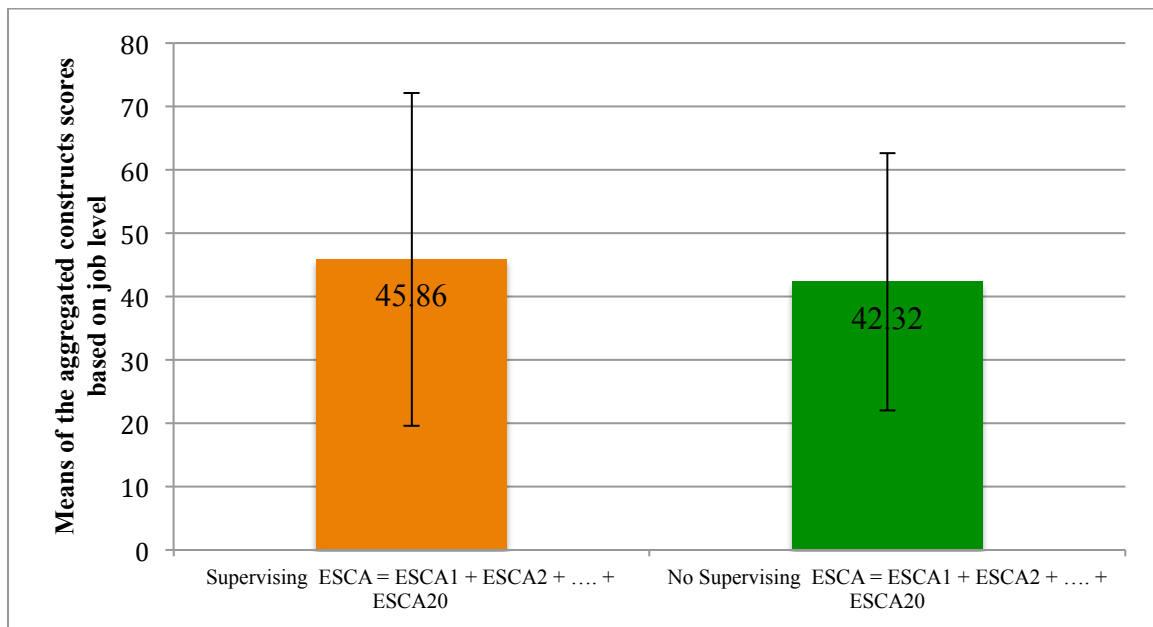
Figure 6: Means of the Aggregated Constructs Scores for Ethical Severity Cyberslacking Activity based on Job Level
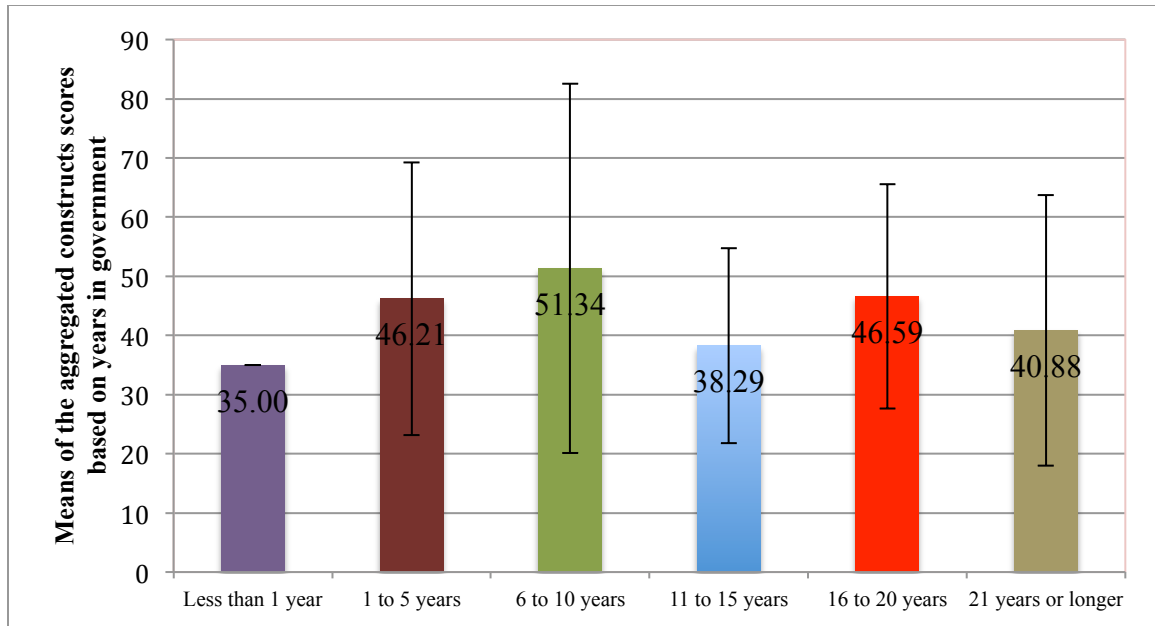
Figure 7: Means and Standard Deviations of Ethical Severity Cyberslacking Activities based on Years in Government

This research study used analysis of covariance (ANCOVA) to answer RQ6-RQ9. According to Mertler and Vannatta (2012), ANCOVA was used to analyze the differences when controlled by the demographic indicators. The ANCOVA is different to ANOVA, but Mertler and Vannatta (2012) stated, "ANCOVA additionally controls for a variable (covariate) that may influence the DV" (p. 15). Tables 9, 10, 11, and 12 present an overview of the ANCOVA of the demographic of SCAF, CCAF, SCAT, and CCAT with ESCA as dependent variable.

Table 9. Analysis of the Covariance of SCAF with ESCA as Dependent Variable

ANCOVA of SCAF		
Demographics	**F**	**Sig.**
Gender	3.63	.059
Age	.594	.442
Education	1.108	.294
Job Level	1.336	.250
Years in Government	.477	.491

*- p<0.05, ** - p<0.01, *** - p<0.001

Table 10. Analysis of the Covariance of CCAF with ESCA as Dependent Variable

ANCOVA of CCAF			
Demographics	**F**	**Sig.**	
Gender	5.286	*.023*	*
Age	.013	.909	
Education	.407	.525	
Job Level	4.138	*.044*	*
Years in Government	1.555	.215	

* - p<0.05, ** - p<0.01, *** - p<0.001

Table 11. Analysis of the Covariance of SCAT with ESCA as Dependent Variable

ANCOVA of SCAT		
Demographics	**F**	**Sig.**
Gender	3.825	.052
Age	.446	.505
Education	2.807	.096
Job Level	.890	.347
Years in Government	1.337	.249

* - p<0.05, ** - p<0.01, *** - p<0.001

Table 12. Analysis of the Covariance of CCAT with ESCA as Dependent Variable

ANCOVA of CCAT			
Demographics	**F**	**Sig.**	
Gender	6.326	*.013*	*
Age	.001	.969	
Education	.811	.369	
Job Level	2.878	.092	
Years in Government	1.379	.242	

* - p<0.05, ** - p<0.01, *** - p<0.001

Multiple Linear Regression (MLR)

Multiple Linear Regression (MLR) was used to answer the research question RQ10. Mertler and Vannatta (2012) stated that, "multiple regression identifies the best combination of predictors (IVs) of the dependent variable" (p. 14). The regression equation was used to make the predictions of the ESCA construct (Sprinthall, 2007). The RQ10 was: What is the impact of government employees' self-reported amount of time spent (self + co-workers) and frequency of engagement (self + co-workers) in cyberslacking activities on their perceived ethical severity of such activities? In order to preform the MLR analysis, data aggregation was conducted using linear means scoring, given that the data demonstrated both acceptable normality and linearity. The result for predicting the DV (ESCA) from the four IV predictors (SCAF, SCAT, CCAF, & CCAT) was found that SCAT was the only significant (p<.01) IV, with a positive regression weight. This result presents that ESCA increases significantly as scores on SCAT increases. Furthermore, SCAF, CCAF, and CCAT were not significant predictors of ESCA, however, it appears that CCAT was borderline, and may require further

investigation, especially as it has a negative coefficient. Table 13 provides an overview of

the MLR with the coefficients and significance.

Table 13. Multiple Linear Regression (MLR) Analysis Results (n=183)

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	T	Sig.
1	(Constant)	21.595	5.608		3.851	*.000***
	SCAF	.071	.207	.037	.346	.730
	SCAT	.876	.287	.318	3.056	*.003***
	CCAF	.158	.129	.168	1.224	.223
	CCAT	-.290	.211	-.185	-1.375	.171

* - p<0.05, ** - p<0.01, *** - p<0.001

The portion of the variance in ESCA that was explained by SCAF, SCAT, CCAF, and

CCAT in combination was R^2 = .111, or 11.1%, which appears to be relatively very low.

The results showed that SCAT has the more significance value with a solid coefficient

value. In the opposite side, the results showed that CCAT have a negative value with no

significance, which means that as CCAT increases, the value of ESCA decreases,

although not significantly. Moreover, SCAF and CCAF were also found not to be

significant predictors of ESCA.

Ordinal Logistic Regression (OLR)

Ordinal Logistic Regression (OLR) was made to test the prediction of the

dependent variable (ESCA) based on the four independent variables (SCAF, SCAT,

CCAF, & CCAT). The results are somewhat consistent with the results of the MLR

analysis. The OLR showed that SCAF (p=.08) and SCAT (p=.03) were significant. The

overall model for predicting ESCA based on the four predictors (SCAF, SCAT, CCAF, &

CCAT) showed: -2 Log Likelihood = 1371.767, x^2(4) = 28.650 p<.001. Table 14

provides an overview of the OLR Model Significance. The result shows that it is very

significance with a value of p<.001.

Table 14. Ordinal Logistic Regression Model Significance

Model	-2Log Likelihood	Chi-Square	df	Sig.
Intercept Only	1371.767			
Final	1343.117	28.650	4	*.000 ****

* - p<0.05, ** - p<0.01, *** - p<0.001

The results of the OLR analysis showed that only two predictors (SCAF &

SCAT) are significant and this indicated that these independent variables were significant

predictors of ESCA. The results indicated that CCAF and CCAT are not significant

predictors of ESCA. However, CCAT was also found here to be negatively related to

ESCA, as was provisory found in MLR. Table 15 provides an overview of the results of

the OLR Parameter Estimates.

Table 15. Ordinal Logistic Regression (OLR) Parameter Estimates

	Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
SCAF	0.029	0.016	3.056	1	*0.08 **	-0.003	0.061
SCAT	0.05	0.023	4.731	1	*0.03 **	0.005	0.096
CCAF	0.01	0.01	1.024	1	0.311	-0.01	0.03
CCAT	-0.018	0.017	1.115	1	0.291	-0.05	0.015

* - p<0.05, ** - p<0.01, *** - p<0.001

Findings

The self reported frequency of engagement in cyberslacking activities of this

research study is represented by the Means of the Aggregated Constructs Scores for all

Five Constructs = 32.77 with a Standard Deviation = 11.95 (See Table 8). The co-

workers reported frequency of engagement in cyberslacking activities is represented by

the Means of the Aggregated Constructs Scores for all Five Constructs = 43.36 with a

Standard Deviation = 24.59 (See Table 8). The results of this research study showed the

self reported amount of time of engagement in cyberslacking activities represented by the

Means of the Aggregated Constructs Scores for all Five Constructs = 25.42 with a

Standard Deviation = 8.37 (See Table 8). Also, the results showed the Co-workers'

reported amount of time of engagement in cyberslacking activities represented by the

Means of the Aggregated Constructs Scores for all Five Constructs = 31.79 with a

Standard Deviation = 14.71 (See Table 8). Furthermore, this research study presented the

employees' perceived ethical severity of engagement in cyberslacking activities

represented by the Means of the Aggregated Constructs Scores for all Five Constructs =

43.83 with a Standard Deviation = 23.05 (See Table 8). The results of this research study

showed that there are no significant differences in government employees' self-reported

frequency of engagement in cyberslacking activities based on gender, age, level of

education, job level, and years working for government. On other hand, the results

presented that there are significant differences in government employees reported

frequency of co-workers' engagement in cyberslacking activities based on gender with

p=.023 and job level with p=.044. The results indicated that there are not significant

differences in government employees self-reported amount of time spent engaging in

cyberslacking activities based on gender, age, level of education, job level, and years

working for government. Also, there is a significant differences in government

employees' reporting the amount of time spent by co-workers engaging in cyberslacking

activities based on gender with p=.013.

MLR analysis shows that there is an inverse relationship, although not significant, between SCAT and ESCA. SCAT was found to be the most significant and influential construct (p=.003). The coefficient value of SCAF is negligible that result in none significance. OLR analysis shows that SCAF and SCAT are significant predictors of ESCA. The result of SCAF is not to far from SCAT like indicated by MLR. The strongest coefficient in OLR results was found to be SCAT with a significance of p=.03 and the second strongest coefficient is SCAF with a significance of p=.08. CCAT is negative coefficient with none significance which means that the more they report the more less ethical they are. The coefficient of CCAF is negligible that result in none significance.

Summary of the Results

This chapter presented the results and the analysis of them in order to answer the research questions of the study. The analysis started with a pre-analysis of the data for a screening data purpose. Following this pre-analysis, a Mahalanobis Distance was made to identify multivariate outliers. The result shows that there was five multivariate outliers identified, which resulted in 183 usable cases. This analysis was followed by a demographic analysis to examine more information about the participants. The result presents that 62 or 33.9% of the respondents were males and 121 or 66.1% were females. Internal, external, and instrument validity was performed to ensure the validity of the study. This research study used Cronbach's Alpha to assess the reliability of each of the measured constructs. The Cronbach's Alpha values shows that all constructs have strong reliability, because all of them are above 0.7.

The study performed MLR, OLR and ANCOVA analysis to answer the research questions. MLR analysis shows that there are inverse relationship between SCAT and ESCA. SCAT is the most influential that result in more significance $p=.003$. The coefficient value of SCAF is negligible that result in none significance. OLR analysis shows that SCAF and SCAT are significant predictors of ESCA. The result of SCAF is not to far from SCAT in the MLR. The strongest coefficient that was found in the OLR was SCAT with a significance of $p=.03$ and the second strongest coefficient is SCAF with a significance of $p=.08$. CCAT has negative coefficient with none significance, however, it means that the more they report to perceive their co-workers spent on each cyberslacking activities, the less ethical they are. The coefficient of CCAF is negligible that result in none significance.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

This chapter begins with conclusions drawn from the results of this study. The ten research questions were answered and implications of the study are shown. The contributions of this study to the Information Systems body of knowledge by empirically identifying the role of amount of time spent and frequency of cyberslacking on individuals' perceived ethical severity of IS in the workplace are presented. The main goal of this research study was to measure the self-reported extent (i.e. amount of time spent & frequency) to which government employees and their co-workers engage in cyberslacking activities in the workplace, to ascertain the perceived ethical severity of these cyberslacking activities, and to investigate if there are any differences on these measures based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government. The population of this study was 183 government employees of different agencies of the public sector.

The first specific goal of this research study was to measure government employees' self-reported *frequency* of engagement in cyberslacking activities. Frequency of engagement in cyberslacking activities was measured based on 20 items using a seven-point scale ranging from 1-never to 7-several times a day. The results indicated that the self reported frequency of engagement in cyberslacking activities of this research study is

the Means of the Aggregated Constructs Scores for all Five Constructs is equal to 32.77 with a Standard Deviation of 11.95.

The second goal of this research study was to measure the government employees' reports on their *co-workers' frequency* of engagement in cyberslacking activities. The results indicated that the co-workers reported frequency of engagement in cyberslacking activities is the Means of the Aggregated Constructs Scores for all Five Constructs is equal to 43.36 with a Standard Deviation of 24.59. The third goal of this research study was to measure government employees' self-reported *amount of time spent* on engagement in cyberslacking activities. Time of engagement in cyberslacking activities was measured based on 20 items using a seven-point scale ranging from 1-never to 7-on average 8 or more hours a day. The results indicated that the self reported amount of time of engagement in cyberslacking activities is the Means of the Aggregated Constructs Scores for all Five Constructs is equal to 25.42 with a Standard Deviation of 8.37.

The fourth goal of this research study was to measure government employees' reports of the *amount of time co-workers spend* on engagement in cyberslacking activities. The results indicated that co-workers' reported amount of time of engagement in cyberslacking activities is the Means of the Aggregated Constructs Scores for all Five Constructs is equal to 31.79 with a Standard Deviation of 14.71. The fifth goal of this research study was to measure government employees' perceived *ethical severity* of cyberslacking activities. Perceived ethical severity engagement in cyberslacking activities was measured based on 20 items using a seven-point scale ranging from 1-Highly Unethical to 7-Highly Ethical. This research study showed that the employees' perceived ethical severity of engagement in cyberslacking activities is the Means of the Aggregated

Constructs Scores for all Five Constructs is equal to 43.83 with a Standard Deviation of 23.05.

The sixth goal of this research study was to measure if there is any significant differences in government employees' self-reported frequency of engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government. The results of this research study showed that there are no significant differences in government employees' self-reported frequency of engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government. The seventh goal of this research study was to measure if there any significant differences in government employees' reported frequency of co-workers' engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government. The results showed that there are significant differences in government employees reported frequency of co-workers' engagement in cyberslacking activities based on gender with p=.023 and job level with p=.044.

The eighth goal of this research study was to determine if there any significant differences in government employees' self-reported amount of time spent engaging in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government. The results indicated that there are not significant differences in government employees self-reported amount of time spent engaging in cyberslacking activities based on gender, age, level of education, job level, and years working for government. The ninth goal of this research study was to determine if there any significant differences in government employees' reported the amount of time spent

by co-workers engaging in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government. The results indicated that there is a significant differences in government employees' reported the amount of time spent by co-workers engaging in cyberslacking activities based on gender with p=.013.

The tenth goal of this research study was to determine the impact of government employees' *reported amount of time spent* (self + co-workers) and *frequency* of engagement (self + co-workers) in cyberslacking activities of their *perceived ethical severity* of such activities. MLR analysis shows that there are inverse relationship between SCAT and ESCA. SCAT is the most influential that result in more significance p=.003. The coefficient value of SCAF is negligible that result in none significance. OLR analysis shows that SCAF and SCAT are significant predictors of ESCA. The result of SCAF is not to far from SCAT in the MLR. The strongest coefficient that was found in the OLR was SCAT with a significance of p=.03 and the second strongest coefficient is SCAF with a significance of p=.08. CCAT has negative coefficient with none significance, however, it means that the more they report to perceive their co-workers spent on each cyberslacking activities, the less ethical they are. The coefficient of CCAF is negligible that result in none significance.

Implications

This research study has significant implications as a consequence of the massive increase in Internet-based tools in the workplace that area readily available to employees. According to Gottfredson and Hirschi (1990), "the theory of crime has implications for

how crime itself is construed, how it should be measured, the kind of people who are likely to engage in it, and the institutional context within which it is controlled" (p. 4). They explained that there are two key factors for predicting criminal behavior: self-control opportunity and the second one is the opportunity (Gottfredson & Hirschi, 1990). These lacks of self-control occur when employees engage in the misuse of Web tools in the workplace (Kim & Byrne, 2011). This investigation contribute to the Information Systems body of knowledge by empirically identifying the role of amount of time spent and frequency of cyberslacking on individuals' perceived ethical severity of IS in the workplace.

Study Limitations

This study presented a limitation with the generalizability of the sample. The participants in this research study represented only several agencies of the Executive Branch of the Government of Puerto Rico. According to Oswalt et al. (2003), the distraction of Internet presents an ethical issue in the workplace. Another limitation was that agencies do not want that their employees participate in this type of study because they admit that their employees are engage in cyberslacking activities. Houston and Tran (2001) stated that, "the problem facing researchers is how to encourage participants to respond, and then to provide a truthful response in surveys. This is another limitation of this study, truthful response in surveys" (p. 70). Furthermore, when their response is related to an unethical activity in the workplace. The bureaucracy of the process in the government to participate in this type of research study was another limitation. Furthermore, unions in the government agencies was another limitations, because several

agencies do not want to exposed their employees to this type of study. Finally, the quantity of questions in the survey was another limitation.

Recommendations for Future Research

There are many areas for future research that was identified based on the results of this investigation. The first recommendation is that this investigation could be replicated with a short version of the survey. The second recommendation is to replicate the survey with cyberslacking activities only using personal mobile devices. The third recommendation for future research study is to determine the impact of government employees' *reported amount of time spent* (self + co-workers) and *frequency* of engagement (self + co-workers) in cyberslacking activities of their *perceived cyber security severity* of such activities.

Summary

The main research question (RQ) that this research study addressed was: to what extent (i.e. amount of time spent & frequency) are government employees self-report about themselves and their co-workers on engagement in cyberslacking activities in the workplace; how ethically severe, they perceive these cyberslacking activities, as well as if there are any significant differences on these measures based on gender, age, level of education, job level, and years of employment. The specific research questions that this research study addressed were:

RQ1: What is the government employees' self-reported *frequency of engagement* in cyberslacking activities?

RQ2: What is the government employees' reported *frequency of co-workers' engagement* in cyberslacking activities?

RQ3: What is the government employees' self reported amount of *time spent on engagement* in cyberslacking activities?

RQ4: What is the government employees' reported of *co-workers' amount of time spent on engagement* in cyberslacking activities?

RQ5: What is the government employees' perceived *ethical severity* of engagement in cyberslacking activities?

RQ6: Are there any significant differences in government employees' self-reported frequency of engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?

RQ7: Are there any significant differences in government employees' reported frequency of co-workers' engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?

RQ8: Are there any significant differences in government employees' self-reported amount of time spent engaging in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?

RQ9: Are there any significant differences in government employees' reported the amount of time spent by co-workers engaging in cyberslacking activities

based on (a) gender, (b) age, (c) level of education, (d) job level, and (e)

years working for government?

RQ10: What is the impact of government employees' self-reported amount of time

spent (self + co-workers) and frequency of engagement (self + co-workers)

in cyberslacking activities on their perceived ethical severity of such

activities?

Cyberslacking behaviors that were included in the survey were a collection of

activities indicated in prior literature, such as: shopping online during work hours,

perusing pornographic sites, visiting SNS for personal use, and using work computers for

managing personal data, that previous studies have presented (Henle & Blanchard, 2008;

Johnson & Indvik, 2003; Kidwell, 2010; Lara et al., 2006; Lim & Teo, 2005; Mills et al.,

2001; Vitak et al., 2011; Websense, 2006). Analysis of covariance (ANCOVA), as well

as Ordinal Logistics Regression (OLR) and Multiple Linear Regression (MLR) analyses

were used to address the research questions. Mertler and Vannatta (2012) stated:

"multiple regression identifies the best combination of predictors (IVs) of the dependent

variable" (p. 14). In MLR the results showed that SCAT have the more significance value

with a solid coefficient value. In the opposite side, the results showed that CCAT have a

negative value with no significance, which means that as CCAT increases, the value of

ESCA decreases, although not significantly. Moreover, SCAF and CCAF were also

found not to be significant predictors of ESCA. In OLR the results indicated that CCAF

and CCAT are not significant predictors of ESCA. However, CCAT was also found here

to be negatively related to ESCA, as was provisory found in MLR.

Subsequent to the analysis of this research study, the results were presented and conclusions were examined. The study includes the discussion of the implications and limitations that was identified. Furthermore, recommendations for future research were presented and extend the Information Systems body of knowledge by empirically identifying the role of amount of time spent and frequency of cyberslacking on individuals' perceived ethical severity of IS in the workplace.

Appendix A

Quantitative Survey Instrument

General Instructions

Dear Participant:

As a Ph.D. student at Nova Southeastern University, I am conducting research for my dissertation to investigate cyberslacking activities in the public sector. My co-investigator and mentor for this study is Dr. Yair Levy, Professor of Information Systems and Cybersecurity at Nova Southeastern University, Graduate School of Computer and Information Sciences.

I would appreciate your time in participating in this quantitative research survey. The survey is divided into six sections and will take approximately 15-20 minutes to complete. All information gathered during this study will be protected and will not be distributed for any other use than academic research. Furthermore, the survey does not collect any personal identification information and is completely anonymous.

This survey is completely voluntary. Please, you are asked to kindly participate only once in the survey. If you have any questions, you can contact me via wilnelia@nova.edu. Thank you for your time and your participation in this anonymous survey. To start the survey, click on the following link: [link going here]

Respectfully,

Wilnelia Hernández-Castro, Ph.D. Candidate
Nova Southeastern University
Graduate School of Computer and Information Sciences

Section A. Self Cyberslacking Activity Frequency (SCAF)

Please estimate the frequency of **your** cyberslacking activities during work hours as you recall during the course of a typical month. How often do **you** estimate that you engage in the following activities at work over the course of a typical month? Please mark the frequency using the scale from (1) Never to (7) several times a day.

Item								
SCAF1	I check non-work related emails	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF2	I send non-work related emails	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF3	I visit general news Websites	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF4	I visit stock or investment-related Websites	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF5	I view sports-related Websites	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF6	I visit my banking or finance- related Websites	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF7	I shop online for personal goods	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF8	I visited online auction sites (e.g. eBay)	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF9	I send/receive instant messaging (IMs)	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF10	I participate in online games	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF11	I participate in chat rooms	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF12	I visit	Never	Once a	Every	Once a	Several	Once a	Several

		Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
	newsgroups or bulletin boards	(1)	month (2)	other week (3)	week (4)	days a week (5)	day (6)	times a day (7)
SCAF13	I book vacations/travel	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF14	I visit virtual communities	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF15	I work on maintaining my personal Web page or Website	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF16	I download music	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF17	I visit job hunting or employment-related Websites	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF18	I visit gambling Websites	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF19	I read blogs	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
SCAF20	I view sexually explicit Websites	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)

Section B. Co-Workers' Cyberslacking Activity Frequency (CCAF)

Please estimate the frequency of **your co-workers'** cyberslacking activities during work hours as you recall during the course of a typical month. How often do you estimate that **your co-workers** engage (in general – on average) in the following activities in the workplace during work hours over the course of a typical month? Please mark the frequency using the scale from (1) Never to (7) Almost every day.

Item								
CCAF1	My co-workers check non-work related email	Never (1)	Once a month (2)	Every other week (3)	Once a week (4)	Several days a week (5)	Once a day (6)	Several times a day (7)
CCAF2	My co-workers	Never	Once a	Every	Once a	Several	Once a	Several

		Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
	send non-work related email							
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF3	My co-workers visit general news sites	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF4	My co-workers visit stock or investment-related Websites	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF5	My co-workers view sports-related Websites	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF6	My co-workers visit banking or finance-related Websites	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF7	My co-workers shop online for personal goods	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF8	My co-workers visit online auctions sites (e.g. eBay)	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF9	My co-workers send/receive instant messaging	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF10	My co-workers participate in online games	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF11	My co-workers participate in chat rooms	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF12	My co-workers visit newsgroups or bulletin boards	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF13	My co-workers book vacations/travel	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF14	My co-workers visit virtual communities	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF15	My co-workers maintain a	Never	Once a month	Every other	Once a week	Several days a	Once a day	Several times a

	personal Web page	(1)	(2)	week (3)	(4)	week (5)	(6)	day (7)
CCAF16	My co-workers download music	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF17	My co-workers visit job hunting or employment-related sites	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF18	My co-workers visit gambling Websites	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF19	My co-workers read blogs	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCAF20	My co-workers view sexually explicit Websites	Never	Once a month	Every other week	Once a week	Several days a week	Once a day	Several times a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)

Section C. Self Cyberslacking Activities Time (SCATx)

Please estimate the amount of time (in hours) of **your** cyberslacking activities during work hours as you recall during the course of a typical workday. How often do you estimate that **you** engage in the following activities at work over the course of a typical workday? Please mark the frequency using the scale from (1) Never to (7) on average 8 or more hours a day.

Item								
SCATx1	I check non-work related email	Never	On average about 15 minutes a day	On average about 30 minutes a day	On average about 1 hour a day	On average about 2 to 4 hours a day	On average about 5 to 7 hours a day	On average 8 or more hours a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
SCATx2	I send non-work related email	Never	On average about 15 minutes a day	On average about 30 minutes a day	On average about 1 hour a day	On average about 2 to 4 hours a day	On average about 5 to 7 hours a day	On average 8 or more hours a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
SCATx3	I visit general news sites	Never	On average about 15 minutes	On average about 30 minutes	On average about 1 hour a day	On average about 2 to 4 hours a	On average about 5 to 7 hours a	On average 8 or more hours a

		(1)	a day (2)	a day (3)	(4)	day (5)	day (6)	day (7)
SCATx4	I visit stock or investment-related Websites	Never	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)
SCATx5	I view sports-related Websites	Never	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)
SCATx6	I visit banking or finance-related Websites	Never	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)
SCATx7	I shop online for personal goods	Never	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)
SCATx8	I visit online auctions sites (e.g. eBay)	Never	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)
SCATx9	I send/receive instant messaging	Never	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)
SCATx10	I participate in online games	Never	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)
SCATx11	I participate in chat rooms	Never	On average about	On average about	On average about 1	On average about 2	On average about 5	On average 8 or

			15 minutes a day (1)	30 minutes a day (2)	hour a day (3)	to 4 hours a day (4)	to 7 hours a day (5)	more hours a day (6)	(7)
SCATx12	I visit newsgroups or bulletin boards	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
SCATx13	I book vacations/travel	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
SCATx14	I visit virtual communities	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
SCATx15	I maintain a personal Web page	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
SCATx16	I download music	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
SCATx17	I visit job hunting or employment-related sites	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
SCATx18	I visit gambling Websites	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
SCATx19	I read blogs	Never	On	On	On	On	On	On

			average about 15 minutes a day (1)	average about 30 minutes a day (2)	average about 1 hour a day (3)	average about 2 to 4 hours a day (4)	average about 5 to 7 hours a day (5)	average 8 or more hours a day (6)	(7)
SCATx20	I view sexually explicit Websites	Never (1)	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)	

Section D. Co-Workers' Cyberslacking Activities Time (CCATx)

Please estimate the amount of time (in hours) of **your co-workers'** cyberslacking activities during work hours as you recall during the course of a typical workday. How often do you estimate that **your co-workers** engage in the following activities at work over the course of a typical workday? Please mark the frequency using the scale from (1) Never to (7) 8 or more hours a day.

Item									
CCATx1	My co-workers check non-work related email	Never (1)	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)	
CCATx2	My co-workers send non-work related email	Never (1)	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)	
CCATx3	My co-workers visit general news sites	Never (1)	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)	
CCATx4	My co-workers visit stock or investment-related Websites	Never (1)	On average about 15 minutes a day (2)	On average about 30 minutes a day (3)	On average about 1 hour a day (4)	On average about 2 to 4 hours a day (5)	On average about 5 to 7 hours a day (6)	On average 8 or more hours a day (7)	
CCATx5	My co-	Never	On	On	On	On	On	On	

			average about 15 minutes a day	average about 30 minutes a day	average about 1 hour a day	average about 2 to 4 hours a day	average about 5 to 7 hours a day	average 8 or more hours a day
	workers view sports related Websites		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCATx6	My co-workers visit banking or finance-related Websites	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
CCATx7	My co-workers shop online for personal goods	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
CCATx8	My co-workers visit online auction sites (e.g. eBay)	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
CCATx9	My co-workers send/receive instant messaging	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
CCATx10	My co-workers participate in online games	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
CCATx11	My co-workers participate in chat rooms	Never	On average about 15 minutes a day (1)	On average about 30 minutes a day (2)	On average about 1 hour a day (3)	On average about 2 to 4 hours a day (4)	On average about 5 to 7 hours a day (5)	On average 8 or more hours a day (6)	(7)
CCATx12	My co-workers visit newsgroups or bulletin boards	Never	On average about 15 minutes a day	On average about 30 minutes a day	On average about 1 hour a day	On average about 2 to 4 hours a day	On average about 5 to 7 hours a day	On average 8 or more hours a day

		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCATx13	My co-workers book vacations/travel	Never	On average about 15 minutes a day	On average about 30 minutes a day	On average about 1 hour a day	On average about 2 to 4 hours a day	On average about 5 to 7 hours a day	On average 8 or more hours a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCATx14	My co-workers visit virtual communities	Never	On average about 15 minutes a day	On average about 30 minutes a day	On average about 1 hour a day	On average about 2 to 4 hours a day	On average about 5 to 7 hours a day	On average 8 or more hours a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCATx15	My co-workers maintain a personal Web page	Never	On average about 15 minutes a day	On average about 30 minutes a day	On average about 1 hour a day	On average about 2 to 4 hours a day	On average about 5 to 7 hours a day	On average 8 or more hours a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCATx16	My co-workers download music	Never	On average about 15 minutes a day	On average about 30 minutes a day	On average about 1 hour a day	On average about 2 to 4 hours a day	On average about 5 to 7 hours a day	On average 8 or more hours a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCATx17	My co-workers visit job hunting or employment-related sites	Never	On average about 15 minutes a day	On average about 30 minutes a day	On average about 1 hour a day	On average about 2 to 4 hours a day	On average about 5 to 7 hours a day	On average 8 or more hours a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCATx18	My co-workers visit gambling Websites	Never	On average about 15 minutes a day	On average about 30 minutes a day	On average about 1 hour a day	On average about 2 to 4 hours a day	On average about 5 to 7 hours a day	On average 8 or more hours a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCATx19	My co-workers read blogs	Never	On average about 15 minutes a day	On average about 30 minutes a day	On average about 1 hour a day	On average about 2 to 4 hours a day	On average about 5 to 7 hours a day	On average 8 or more hours a day
		(1)	(2)	(3)	(4)	(5)	(6)	(7)
CCATx20	My co-workers view sexually explicit	Never	On average about 15	On average about 30	On average about 1 hour a	On average about 2 to 4	On average about 5 to 7	On average 8 or more

	Websites		minutes a day (2)	minutes a day (3)	day (4)	hours a day (5)	hours a day (6)	hours a day (7)
		(1)						

Section E. Ethical Severity of Cyberslacking Activities (ESCA)

Please rate your level of agreement with the following statements, as they apply to the following cyberslacking activities. Please mark the ethical severity level using the scale from (1) Highly Unethical to (7) Highly Ethical.

Item								
ESCA1	Checking non-work related email	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA2	Sending non-work related email	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA3	Visiting general news Websites	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA4	Visiting stock or investment-related Websites	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA5	Viewing sports-related Websites	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA6	Visiting banking or finance-related Websites	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA7	Shopping online for personal goods	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA8	Visiting online auction sites (e.g. eBay)	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA9	Sending/ receiving instant messages (IMs)	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA10	Participating in online games	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA11	Participating in chat rooms	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA12	Visiting newsgroups or bulletin boards	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)

ESCA13	Booking vacations/ travel	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA14	Visiting virtual communities	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA15	Working on maintaining a personal Web page	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA16	Downloading music	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA17	Visiting job hunting or employment-related Websites	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA18	Visiting gambling Websites	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA19	Reading blogs	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)
ESCA20	Viewing sexually explicit Websites	Highly Unethical (1)	Unethical (2)	Somewhat Unethical (3)	Neither (4)	Somewhat Ethical (5)	Ethical (6)	Highly Ethical (7)

Section F. Demographic Information

Please select according to your characteristics:

F1. What is your gender?
    a. Male
    b. Female

F2. What is your age group?
    a. 18 to 24
    b. 25 to 29
    c. 30 to 39
    d. 40 to 49
    e. 50 to 59
    f. 60 to 64
    g. 65 or older

F3. What is the highest education degree you have achieved?
    a. None

b. High school diploma
c. Technical certification
d. Associate degree
e. Bachelor's degree
f. Master's degree
g. Professional degree (e.g. MD, DDS)
g. Doctoral degree (e.g. PhD or EdD)

F4. Is your job includes supervising other employees?
a. Yes
b. No

F5. How long have you worked in the public sector?
a. less than 1 year
b. 1 to 5 years
c. 6 to 10 years
d. 11 to 15 years
e. 16 to 20 years
f. 21 years or longer

Appendix B

Authorization Letter

OCALARH

Estado Libre Asociado de Puerto Rico
Oficina de Capacitación y Asesoramiento en Asuntos
Laborales y de Administración de Recursos Humanos

Harry O. Vega Díaz
Director

13 de junio de 2014

Sra. Wilnelia Hernández Castro
[...]
[...]
[...]   '27

Estimada señora Hernández:

Espero que al recibo de la presente se encuentre bien. Con el propósito de colaborar con usted en el trabajo investigativo que desea realizar como parte de su Disertación Doctoral, nos pusimos en contacto con personal de varias agencias gubernamentales para que puedan asistirle en el proceso.

Adjunto, la información de las personas contacto en la Oficina de Capacitación y Asesoramiento

ayuda necesaria para que pueda completar de manera satisfactoria su investigación.

Le deseo el mayor de los éxitos en su gestión de Disertación Doctoral y agradecemos su interés e iniciativa de contar con nuestra Agencia.

Estamos siempre a sus órdenes.

Cordialmente,

Harry O. Vega Díaz
Director

PO Box 8476 San Juan, Puerto Rico 00910-8476 • Teléfono (787) 274-4300 • Fax (787) 250-1145 • www.ocalarh.pr.gov

Appendix C

IRB Approval Memo

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

NSU

MEMORANDUM

To: Wilnelia Hernandez-Castro

From: Ling Wang, Ph.D.
Institutional Review Board

Date: May 20, 2014

Re: *An Empirical Assessment of Employees Cyberslacking in the Public Sector*

IRB Approval Number: wang04151402

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

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

2)   ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3)   AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

Appendix D

University of Puerto Rico at Mayagüez Campus IRB Approval Memo

CPSHI/IRB 00002053
University of Puerto Rico – Mayagüez Campus
Dean of Academic Affairs
Call Box 9000
Mayagüez, PR 00681-9000

March 18, 2015

Wilnelia Hernandez Castro

Dear Ms. Hernandez:

As a member of the Institutional Review Board of the University of Puerto Rico - Mayagüez Campus, I have considered the Review Application for your project titled An Empirical Assesment of Employee Cyberslacking in the Public Sector (Protocol num. 20150320E). After an evaluation of your protocol, I have determined that according to Category 2 of 45.CFR.46.101(b).

Remember that any modifications or amendments to the approved protocol or its methodology must be reviewed and approved by the IRB before they are implemented. The IRB must be informed immediately if an adverse event or unexpected problem arises related to the risk to human subjects. The IRB must likewise be notified immediately if any breach of confidentiality occurs.

We appreciate your commitment to uphold the highest standards of human research protections and remain.

Sincerely,

Dr. Rafael A. Boglio Martínez
President, Institutional Review Board (IRB)
University of Puerto Rico,
Mayagüez Campus
Office: Celis 108
Tel.: (787) 832-4040 Ext. 6277
Web Page: http://www.uprm.edu/cpshi/

Telephone: (787) 832 - 4040 x 6277, 3807, 3808 -- **Fax:** (787) 831-2085 --**Webpage:** www.uprm.edu/cpshi
Email: cpshi@uprm.edu

References

Abie, H., Spilling, P., & Foyn, B. (2004). A distributed digital rights management model for secure information-distribution systems. *International Journal of Information Security*, *3*(2), 113-128.

Akman, I., & Mishra, A. (2009). Ethical behavior issues in software use: An analysis of public and private sectors. *Computers in Human Behavior, 25*(6), 1251-1257.

Alder, G. S., Schminke, M., Noel, T. W., & Kuenzi, M. (2007). Employee reactions to Internet monitoring: The moderating role of ethical orientation. *Journal of Business Ethics*, *80*(3), 481-498.

Bhatnagar, S. (2004). *E-government: from vision to implementation: A practical guide with case studies*. Thousand Oaks, CA: Sage Publications, Inc.

Bennett, J., Owers, M., Pitt, M., & Tucker, M. (2010). Workplace impact of social networking. *Property Management*, *28*(3), 138-148.

Blanchard, A., & Henle, C. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior, 24*(3), 1067-1084.

Block, W. (2001). Cyberslacking, business ethics and managerial economics. *Journal of Business Ethics, 33*(3), 225-231.

Burrus, D. (2010). Social networks in the workplace: The risk and opportunity of Business 2.0. *Strategy & Leadership*, *38*(4), 50-53.

Chapman, C. (2006). Fundamental ethics in information systems. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, *USA*, *8*, 210b.

Chen, J. V., Chen, C. C., & Yang, H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *Industrial Management & Data Systems*, *108*, 87–106.

Cyberslacking at work continues to threaten productivity: Survey zeroes in on newest "internet distractions." (2000, March 6). *Business Wire*.

D'Arcy, J., & Hovav, A. (2009). An integrative framework for the study of information security management Research. In J. Gupta, & S. Sharma (Eds.) *Handbook of Research on Information Security and Assurance* (pp. 55-67). Hershey, PA: Information Science Reference.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence perspective. *Information Systems Research*, *20* (1), pp. 79-98.

Davis, R. A., Flett, G. L., & Besser, A. (2002). Validation of a new scale for measuring problematic internet use: Implications for pre-employment screening. *CyberPsychology & Behavior*, *5*, 331–345.

Davison, R., Chismar, W., Kock, N, & Langford, D. (2001). Professional ethics in information systems. *Proceeding of the 34ᵗʰ Annual Hawaii International Conference on System Sciences*, *USA*, *8*, 8036.

Dorantes, C., Hewitt, B., & Goles, T. (2006). Ethical decision-making in an IT context: The roles of personal moral philosophies and moral intensity. *Proceedings of the 39ᵗʰ Annual Hawaii International Conference on System Sciences, USA,* 1-10.

Eddy, E. R., D'Abate, C. P., & Thurston, Jr. P. W. (2010). Explaining engagement in personal activities on company time. *Personnel Review*, *39*(5), 639–654.

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

Ergun, D., & Polat, G. (2012). Cyberloafing phenomenon in organizations: Determinants and impacts. *Journal of eBusiness and eGovernment studies, 4*(2), 1–15.

Everton, W. J., Mastrangelo, P. M., & Jolton, J. A. (2005). Personality correlates of employees' personal use of work computers. *CyberPsychology & Behavior*, *8*(2), 143–153.

Fang, J., Shao, P., & Lan, G. (2009). Effects of innovativeness and trust on web survey participation. *Computers in Human Behavior*, *25*(1), 144-152.

Fiore, R. N., & Nelson, H. L. (2003). *Recognition, responsibility, and rights: Feminist ethics and social theory*. Lanham, MD: Rowman & Littlefield.

Floyd J. , & Fowler, Jr. (1995). *Improving survey questions. design and evaluation.* Massachusetts, BSN: SAGE Publications, Inc.

Flynn, T. (2001). Ethics, law and technology: A case study in computer-mediated communication. *International Symposium on Technology and Society*, *USA,* 125.

Friedman, W. H. (2000). Is the answer to Internet addiction Internet interdiction? *Proceedings of the Association for Information Systems, USA, 1562-1567.*

Garrett, R., & Danziger, J. (2008). On cyberslacking: Workplace status and personal Internet use. *CyberPsychology & Behavior, 11*(3), 2008.

Gattiker, U., & Kelley, H. (1999). Morality and computers: Attitudes and differences in moral judgments. *Information Systems Research*, *10*(3), 233-254.

Gbadamosi, G. (2004). Academic ethics: What has morality, culture and administration got to do with its measurement? *Management Decision, 42*(9), 1145–1161.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.

Government of Puerto Rico, Department of Labor and Human Resources, Bureau of Labor Statistics, Labor Force and Special Studies Divisions. (2012). *Employment and Unemployment Puerto Rico 2011 average calendar year.* Retrieved from http://www.dtrh.gobierno.pr/pdf/empleo_y_desempleo_en_puerto_rico_promedio _anio_natural_2011.pdf

Greenfield, D. N., & Davis, R. A. (2002). Lost in cyberspace: The web@work. *CyberPsychology and Behavior, 5*, 347–353.

Greengard, S. (2002). The high cost of cyberslacking. *Workforce, 12*, 22–24.

Griffiths, M. (2003). Internet abuse in the workplace: Issues and concerns for employers and employment counselors. *Journal of Employment Counseling, 40*, 87–96.

Gruber, S. (1999). Communication gone wired: Working toward a "practiced" cyberfeminism. *Information Society, 15*(3), 199−208.

Hardy, H. E. (2003). Internet, history and development of. *Encyclopedia of International Media and Communications, Volume 2*.

Henle, C. A., & Blanchard, A. L. (2008). The interaction of work stressors and organizational sanctions on cyberloafing. *Journal of Managerial Issues*, *20*(3), 383-400.

Houston, J., & Tran, A. (2001). A survey of tax evasion using the randomized response technique. *Advances in taxation*, *13*, 69–94.

Ínce, M., & Gül, H. (2011). The relation of cyber slacking behaviors with various organizational outputs: Example of Karamanoğlu Mehmetbey University. *European Journal of Scientific Research*, *52*(4), 507–527.

Jefferies, P. (2000). Multimedia, cyberspace and ethics. *2000 IEEE Conference on Information Visualization*, 99-104.

Jia, H. H. (2008). *Relationships between the big five personality dimensions and cyberloafing behavior* (Master's thesis). Available from ProQuest Dissertation and Theses database. (UMI No. 3320314)

Johnson, J., & , K. W. (2007). Identifying employee internet abuse. *40th Annual Hawaii International Conference on System Sciences*, 1-9.

Johnson, P. R., & Indvik, J. (2003). The organizational benefits of reducing cyberslacking in the workplace. *Journal of Organizational Culture, Communications, and Conflict, 8*(2), 55−62.

Johnson, P. R., & Rawlins, C. (2008). Employee internet management: Getting people back to work. *Journal of Organizational Culture, Communications, and Conflict*, *12*(1), 43-49.

Katz, J. E. (2004). Telephone. *International Encyclopedia of the Social & Behavioral Sciences*.

Kidwell, R. E. (2010). Loafing in the 21st century: Enhanced opportunities -- and remedies -- for withholding job effort in the new workplace. *Business Horizons*, *53*(6), 543-552.

Kim, S. J., & Byrne, S. (2011). Conceptualizing personal web usage in work contexts: A preliminary framework. *Computers in Human Behavior*, *27*(6), 2271-2283.

King, W., & Jun, H. (2005). External validity in IS survey research. *Communications of the Association for Information Systems*, *16*, 880-894.

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, *80*(3), 541–555.

Lamersdorf, W., Tschammer, V., & Amarger, S. (2004). *Building the e-service society: e-commerce, e-business, and e-government*. Norwell, MA: Kluwer Academic Publishers.

Lara, P. Z., Tacoronte, D. V., & Ding, J. T. (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.

Leedy, D. P., & Ormrod, E. J. (2005). *Practical research: Planning and design (8th ed.)*. Upper Saddle River, NJ: Pearson Prentice Hall.

Leiwo, J., & Heikkuri, S. (1998). An analysis of ethics as foundation of information security in distributed systems. *Proceedings of 31st Annual Hawaii International Conference on System Sciences*, *USA*, *6*, 213.

Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science Publishing.

Levy, Y. (2008). An empirical development of critical value factors (CVF) of online learning activities: An application of activity theory and cognitive value theory. *Computers & Education*, *51*(4), 1664–1675.

Levy, Y., & Ramim, M. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology, 8*(4), 24-34.

Levy, Y., Ramim, M. M., & Hackney, R.A. (2013). Assessing ethical severity of e-learning systems security attacks. *Journal of Computer Information Systems, 53*(3), 75-84.

Liao, Q., Luo, X., Gurung, A., & Li, L. (2009). Workplace management and employee misuse: Does punishment matter? *Journal of Computer Information Systems, 50*(2), 49-59.

Liberman, B., Seidman, G., McKenna, K. Y. a., & Buffardi, L. E. (2011). Employee job attitudes and organizational characteristics as predictors of cyberloafing. *Computers in Human Behavior*, *27*(6), 2192–2199.

Lim, V., & Teo, T. (2005). Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. *Information & Management*, *42*(8), 1081-1093.

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.

Lorents, A. C., Maris, J. M., Morgan, J. N., & Neal, G. L. (2006). Ethics of computer use: A survey of student attitudes. *Academy of Information and Management Sciences Journal, 9*(2), 45-60.

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security, 24*(5), 371-380.

Malachowski, D. (2005). *Wasted time at work costing companies billions.* Retrieved July 15, 2011, from http://www.salary.com/careers/layoutscripts/crel_display.asp?tab=cre&cat=nocat&ser=Ser374&part=Par555

Manross, G. G., & Rice, R. E. (1986). Don't hang up: Organizational diffusion of the intelligent telephone. *Information & Management*, *10*(3), 161-179.

Mertler, C., & Vannatta, R.A. (2012). *Advanced and multivariate statistical methods: Practical application and interpretation (5th ed.)*. Glendale, CA:Pyrczak Publishing.

Messarra, L. C., Karkoulian, S., & McCarthy, R. (2011). To restrict or not to restrict personal internet usage on the job. *Education, Business and Society: Contemporary Middle Eastern Issues*, *4*(4), 253-266.

Mills, B. Y., Hu, B. O., Beldona, S., & Clay, J. (2001). Cyberslacking! *Cornell Hotel and Restaurant Administration Quarterly,* 34-47.

Morris, M. G., & Venkatesh, V. (2000). Age differences in technology adoption decisions: Implications for a changing workforce. *Personnel Psychology, 53*(2), 375−403.

Mowery, D. C., & Simcoe, T. (2002). Is the Internet a US invention? — an economic and technological history of computer networking. *Research Policy*, *31*(8-9), 1369-1387.

Mykletun, E., Narasimha, M., and Tsudik, G. (2006). Authentication and integrity in outsourced databases. *Transaction Storage 2*(2), 107-138.

Nagi, K. (2006). Solving ethical issues in eLearning. *Japan Tappi Journal*, *60*(1), 11-20.

Odlyzko, A. (2001). Internet pricing and the history of communications. *Computer Networks*, *36*(5-6), 493–517.

Oswalt, B., Florence, E.H., & Austin, S. F. (2003). Cyberslacking -- legal and ethical issues. *International Association for Computer Information Systems* (pp. 646-652).

Oz, E. (1992). Ethical standards for information systems professionals: A case for a unified code. *MIS Quarterly*, *16*(4), 423-433.

Phillips, J., & Reddie, L. (2007). Decisional style and self-reported email use in the workplace. *Computers in Human Behavior*, *23*(5), 2414-2428.

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

Scheuermann, L. S., & Langford, H. P. (1997). Perceptions of Internet abuse, liability, and fair use. *Perceptual and Motor Skills, 85*, 847–850.

Sekaran, U. (2003). *Research methods for business. A skill building approach (4ᵗʰ ed.).* New York, NY: John Wiley and Sons.

Sekaran, U. (2013). *Research methods for business. A skill building approach (6ᵗʰ ed.).* New York, NY: John Wiley and Sons.

Smith, F. C. (1997). Ethical responsibilities and legal liabilities professionals of network security. *Proceedings of the 13ᵗʰ Annual Computer Security Applications Conference. USA*, 239-250.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management, *34*(3), 503–522.

Sprinthall, R. C. (2007). Basic statistical analysis (8ᵗʰ ed.). Boston, MA: Allyn & Bacon.

Stahl, B. C., Rogerson, S., & Wakunuma, K. J. (2009). Future technologies: The matter of emergent ethical issues in their development. *2009 Computation World: Future Computing, Service Computation, Cognitive, Adaptive, Content, Patterns*, 603-607.

Stewart, E. (2000). Internet acceptable use policies: Navigating the management, legal, and technical issues. *Security Management, 9*, 46–52.

Strader, T. J., Simpson, L. A., Clayton, S. R. (2009). Using computer resources for personal activities at work - employee perceptions of acceptable behavior. *Journal of International Technology and Information Management*, *18*(3/4), 465–476.

Straub, D. W. (1989). Validating instruments in MIS Research. *MIS Quarterly*, *13*(2), 147-169.

Sweeper, M., Boos, W., Hakesley, S., & Thurston, K. (2000). Users to clean up their email security views. *Security*, *19*(5), 385-387.

Thomson, a. (2001). Ethics in computer software design and development. *Computers and Electronics in Agriculture*, *30*(1-3), 85–102

Ugrin, J. C., & Pearson, J. M. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior*, *29*, 812–820.

Ugrin, J. C., Pearson, J. M., & Odom, M. D. (2008). Cyber-slacking: Self-control, prior behavior and the impact of deterrence measures, *12*(1), 75-88.

Venkatraman, S. (2008). *The "darth" side of technology use: Cyberdeviant workplace behaviors*. (Doctoral dissertation). Available from ProQuest Dissertation and Theses database. (UMI No. 3334183)

Verton, D. (2000). Employers ok with e-surfing. *Computerworld*, *34*(1), 16.

Vitak, J., Crouse, J., & LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, *27*(5), 1751-1759.

Wang, Z., Yan, R., Chen, Q., & Xing, R. (2010). Data mining in nonprofit organizations, government agencies, and other institutions. *International Journal of Information Systems in the Service Sector*, *2*(3), 42–52.

Weatherbee, T. G. (2010). Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. *Human Resource Management Review*, *20*(1), 35-44.

Websense, Inc. Web@Work (2006). Retrieved August 20, 2011, from http://www.securitymanagement.com/archive/library/websense_technofile0906.pdf.

Whitty, M. T. (2002). Big brother in Australia: Privacy and surveillance of the Internet in the Australian workplace. *Internet Research 3.0: Net/Work/Theory,* Netherlands.

Whitty, M. T. (2004). Should filtering software be utilized in the workplace? Australian employees' attitudes towards Internet usage and surveillance of the Internet in the workplace. *Surveillance and Society, 2*(1), 39–54.

Whitty, M. T., & Carr, A. N. (2006). New rules in the workplace: Applying object-relations theory to explain problem Internet and email behavior in the workplace. *Computers in Human Behavior, 22*, 235-250.

Young, K. (2010). Policies and procedures to manage employee Internet abuse. *Computers in Human Behavior*, *26*(6), 1467–1471.

Zhang, D., Oh, L. B., Teo, H. H. (2006). An experimental study of the factors influencing non-work related use of IT resources at workplace. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences,* 206a.

Zhang, Y. (2005). Age, gender, and Internet attitudes among employees in the business world. *Computers in Human Behavior, 21*, 1−10.