IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

AN INQUIRY TO CYBERLOAFING AND STRATEGIES TO MINIMIZE ITS INCIDENCE IN THE GOVERNMENT FOR INCREASED PRODUCTIVITY

SANDY JANE M. ALFARO
MPA Candidate, College of Development Management
University of Southern Philippines

Chapter 1

INTRODUCTION

The 21st Century, dubbed as the *Information and Internet* age is supposed to be one of the most advanced and easy-going eras of mankind. This is the time where we have the privilege of having things in just 'one click' as opposed to our ancestors who had to shed blood and sweat to hunt and gather food, or painstakingly write down their thoughts on rock or papyrus. When Berners Lee created the World Wide Web (WWW) or the Internet, it has since tightly linked our daily lives and our manner of doing business with the computer. One of the advantages of the Internet is, it enhances the way we communicate via e-mail and instant messaging. For instance, e-mails have replaced letters. In other words, the Internet works without boundaries thus making knowledge and information sharing accessible at our fingertips. The invention of the Internet was also intended to increase employees' productivity and at the same time encourage better communication and connectivity between stakeholders. This same Intention proliferated even more with the birth of Social Media. According to the Pew Research Center, 90% of young adult uses social media compared to only 12% in 2005, and 77% of the users belong to the age bracket of 30-49 years old. However, too much use of social media or the Internet for personal and non-work activities can be counterproductive. Literatures indicated that the decreasing of productivity as a result of browsing the Internet for personal usage during working hours inhibit employees from completing their task (Ramayah T., 2010). This is known as production deviance (Venkatapathy and Madhumathi, 2016). Another term commonly used is *cyberloafing*. *Cyberloafing* refers to personal usage of Internet for non-work purposes during working hours. The activities may include online news reading, online shopping, social media browsing or other sort of entertainment purposes (Garrett and Danziger, 2008). As a counterproductive behavior *cyberloafing* is dubbed as *cyberslacking* or *cyberslouching* (Weatherbee, 2010).

Grover (2014) found that 64% of a sample of 1,000 workers in the United States surfed the Internet for personal activities during work hours. However, Grover's population focused on workers in private corporations who are using desktop computers. Several researchers have published various policies and technologies to control Internet use at work for personal activity using computers in the office. But, there are no articles specifically on the topic of *Cyberloafing* in government offices using smaller technology devices such as smartphones. Moreover, heads of agencies, management or supervisory personnel as well as Human Resource (HR) personnel, need recommendations to control or monitor employee Internet misuse through *cyberloafing* in smaller personal devices to protect their office and increase employee productivity. Published various policies and technologies to control Internet use at work for personal activity using computers in the office. But, there are no articles specifically on the topic of Cyberloafing in government offices using smaller technology devices such as smartphones. Moreover, heads of agencies, management or supervisory personnel as well as Human Resource (HR) personnel, need recommendations to control or monitor employee Internet misuse through cyberloafing in smaller personal devices to protect their office and increase employee productivity.

PROBLEM STATEMENT

Despite the many advantages of using the Internet in organizations, *cyberloafing* is a potentially serious problem for organizational leaders and HR personnel. Saraç and Çiftçioğlu (2014) estimated that unofficial web surfing costs U.S. employers more than $50 billion a year in lost productivity. The general problem herein is that the overall productivity of an agency can be affected by government employees wasting valuable work time when they are *cyberloafing*. The specific problem is that the heads of agencies or management or supervisory personnel and HR personnel have not established reliable ways to monitor and limit employees' personal usage of the Internet through their smartphones while on the job. Ultimately, this research paper aims to fill the gap in the literature regarding this topic through a focus on the incidences of government employees' *cyberloafing* activities through their mobile phones and gathering the personal opinions or suggestions of Chief Administrative Officers, frontline supervisors or any other management and HR personnel, on how to set up or fortify internet use policies and make them more effective with respect to monitoring and limiting *cyberloafing* while on the job. Therefore, the general research question to answer is: How can the management and/or Human Resource (HR) personnel minimize wasted work time by monitoring and limiting the personal Internet activity of employees who use their smartphones while on the job? This is then followed by these research sub questions:

RQ1: What effective strategies can the Chief Administrative Officers, Human Resource (HR) personnel and other management personnel use to monitor employees so that they are not wasting work time by *cyberloafing* from their smartphones?

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

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

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

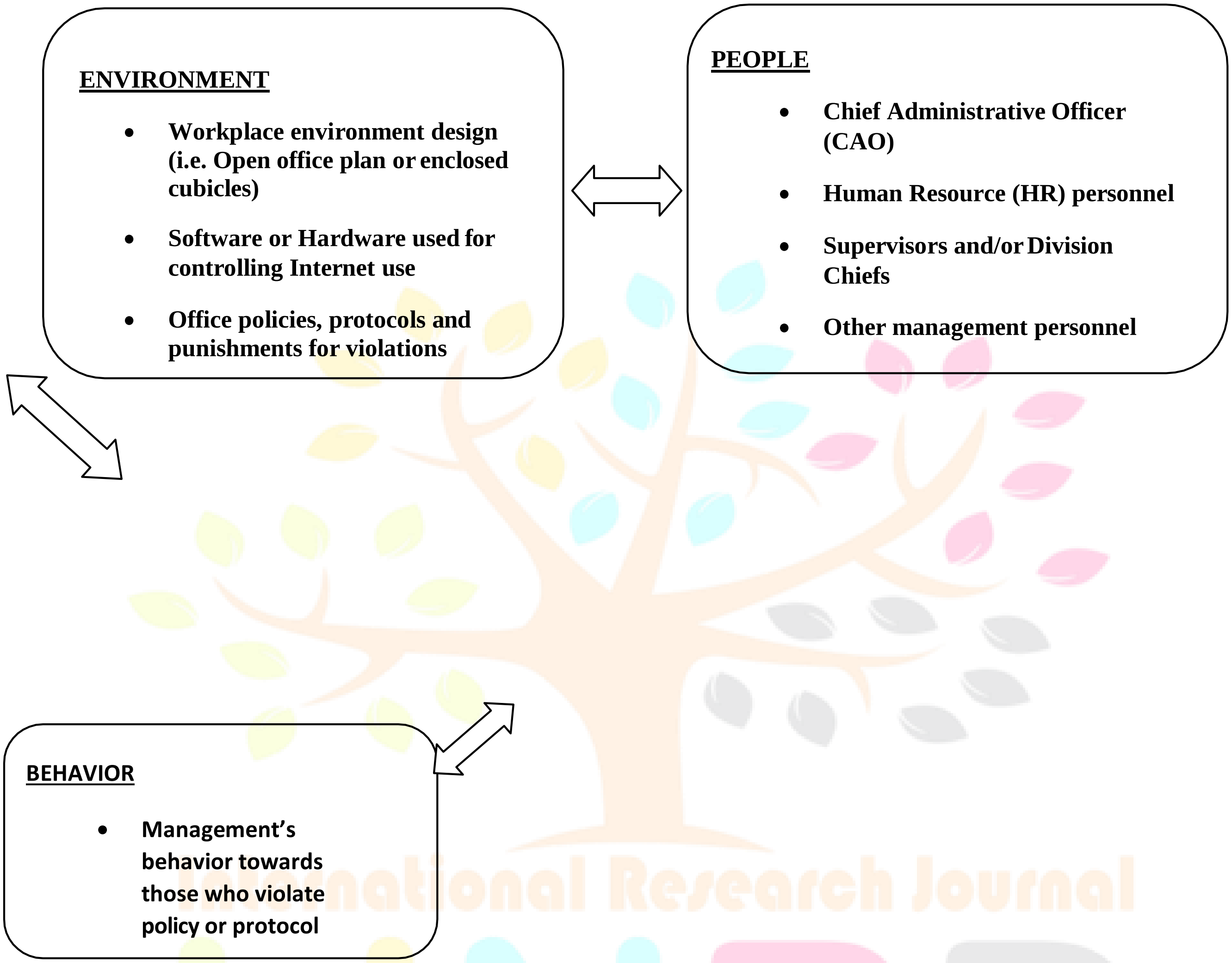
SIGNIFICANCE OF THE STUDY

The purpose of this qualitative phenomenological study was to find reliable ways for government office heads, managers, supervisors and HR personnel to monitor and limit employees' personal use of the Internet through their mobile devices and smartphone technology while on the job. In addition to wasted work time, other major organizational concerns include security threats, policy violations, and the misuse of the Internet during work time, especially when employees use their smartphone to access the office intranet and official e-mail platforms. This research involves exploring ways to limit employees' *cyberloafing* through their personal smartphones while on the job, avoid wasting valuable work time and increasing the agency's overall productivity.

CONCEPTUAL FRAMEWORK

Bandura’s (1986) Social Cognitive Theory (SCT) as applied to media attendance and mobile technology (LaRose & Eastin, 2004) was the framework of this study (see **Figure 1**). The SCT was adapted in order to analyze human behavioral changes based on specific environmental factors. Changing the behavior of employees by controlling their personal Internet activity while at work and preventing them from wasting valuable work time is the major objective of this theory (Harris, Marett & Harris, 2013). This theory provides the framework for designing, implementing, and evaluating programs related to research phenomena (Bandura, 1986. The SCT has three interrelated factors: (a) environment, (b) people, and (c) behavior (Bandura, 1986). For the purposes of this paper, *environment* refers to the workplace environment; such as open work spaces or enclosed ones, technological environments that include software or hardware to control internet use for personal activities, or legal environments which refer to policies and punishments. On the other hand, *people* herein pertains to the staff, management personnel, agency heads, HR and other related personnel. Lastly, behavior refer to the behavior of the management towards employees who violate organizational policies and protocols. The SCT has three interrelated factors: (a) environment, (b) people, and (c) behavior (Bandura, 1986). For the purposes of this paper, environment refers to the workplace environment; such as open work spaces or enclosed ones, technological environments that include software or hardware to control internet use for personal activities, or legal environments which refer to policies and punishments. On the other hand, people herein pertains to the staff, management personnel, agency heads, HR and other related personnel. Lastly, behavior refer to the behavior of the management towards employees who violate organizational policies and protocols.

Figure 1. SCT framework applied to this research on controlling or limiting the incidence of *Cyberloafing* in the government workplace



ENVIRONMENT

- Workplace environment design (i.e. Open office plan or enclosed cubicles)
- Software or Hardware used for controlling Internet use
- Office policies, protocols and punishments for violations

PEOPLE

- Chief Administrative Officer (CAO)
- Human Resource (HR) personnel
- Supervisors and/or Division Chiefs
- Other management personnel

BEHAVIOR

- Management's behavior towards those who violate policy or protocol

NATURE OF THE STUDY

This paper makes use of the qualitative phenomenological study with interviews. Qualitative methodology is a way to transform the world through a sequential process that include interviews, conversations, recordings, and writing memos to self (Aluwihare- Samaranayake, 2012). Researchers use open-ended interview questions to interpret a phenomenon by talking directly to the people and observing their behavior and action, as well as to conduct face-to-face interactions over time (Ballaro & O'Neil, 2013). Open-ended interview questions were suitable for this study. The focus of the qualitative methodology is a single phenomenon and using text and images to develop an inquiry strategy (Chikweche & Fletcher, 2012). The qualitative tools for collecting the research data can include the researchers' eyes and ears, as there are benefits from using casual conversations and accidental observations to collect data. Nevertheless, it is important for researchers to know which approach adds value to their research (Maxwell, 2013). Researchers can conduct qualitative research by exploring and comparing ideas to identify the relationship between them; however, researchers should not try to anticipate the relationships among the ideas from the beginning of a study to avoid bias (Marshall, Cardon, Poddar, & Fontenot, 2013).

SCOPE AND LIMITATION

This research is conducted in three (3) government offices in Davao City selected by the proponents, the specific names of which will not be disclosed and only the responses will be documented and shown. The paper makes use of qualitative research methodologies relying heavily on interviews and focused group discussions limited to a only a few participants in observance of the Anti-COVID-19 protocols against close contact, mass gathering and the implementation of only 50% working capacity allowed inside office premises. The proponents collected data specifically from heads, managers and/or supervisors and HR personnel of selected government offices who have been working for the government for more than one (1) year and is occupying regular, *plantilla* position/s. They were selected by the proponents because such types of government personnel can inspire, if not directly implement, the recommendations of this research as part of the policies and/or protocols in their respective offices.

Chapter 2

REVIEW OF RELATED LITERATURE

This chapter contains related literature and studies from references like books, journals, Internet articles and publications, and any related readings.

Related Literature

The Internet and e-mail technology are significant assets to an organization if used for supporting work, but the Internet and its accompanying technology are like a double-edged sword, and organizational leaders should be careful when using it (Askewet al., 2014; Otto, Wahl, Lefort, & Frei, 2012).

Cyberloafing

cyberloafing has serious negative implications for organizations related to non-work activities during working time and presents serious challenges to organizational leaders (Rahimnia & Karimi Mazidi,2015). Loafing or slacking refers to deviant behavior, and *cyberloafing* is the main factor that contributes to minimizing productivity (Kuschnaroff & Bayma, 2014). Human resources personnel need to create a balance between *cyberloafing* and productivity (König & Caner de la Guardia, 2014). The term *cyberloafing* refers to many activities, such as non-work- based computer use, Internet abuse, wasting work time, junk computing, online gaming, online shopping, chatting, cellphone texting, and more, but *cyberloafing* is mainly recognized as four activities: (a) personal communications, (b) accessing personal information, (c) personal downloads, and (d) personal e-commerce (Jia, Jia, & Karau, 2013). There are four perspectives on *cyberloafing*, and the first one is lower task performance through work time spent surfing the Internet instead of on work, which results in lower productivity (Achakul & Yolles, 2013; Kuschnaroff & Bayma, 2014). Hence, the relationship between *cyberloafing* and job performance is negative (Moody & Siponen, 2013; Vitak et al., 2011). The second perspective includes a focus on a particular type of *cyberloafing*, such as gaming and social media, as it becomes difficult for employees to return to work if they use both types during working hours because these types of cyberloafing bring pleasure (Weatherbee, 2012). The result is neglected job responsibilities and decreased productivity (Lim, Teo, & Loo, 2002; Vitak et al., 2011).

The third perspective on *cyberloafing* is that the relationship between *cyberloafing* and productivity can be positive when employees' reason for *cyberloafing* is for a work-related task, such as finding ways to market the organization's products (Coker, 2011; Collet, Hine, & du Plessis, 2015). The fourth perspective is the issue of employees' *cyberloafing* after they are done fone depends on this last perspective, there would be no relationship between cyberloafing and task performance. The fourth perspective could also serve as confirmation that *cyberloafing* can be harmful when it becomes addictive (Klotz & Buckley, 2013). Ugrin and Pearson (2013) focused on the *cyberloafing* problem and suggested using an appropriate policy with a deterrence mechanism to control and monitor the violations of employees. A deterrence model can help to overcome various types of *cyberloafing*. For example, threats of termination and detection mechanisms are practical ways to solve cyberloafing problems, including employees viewing pornography, managing personal finances, and doing personal shopping. Although IT innovations continue to grow and change business, social life, and technology, these changes also result in increased opportunities to violate company Internet policies by *cyberloafing* during work time, which leads to lower work quality and quantity (Jian, 2013; Ugrin & Pearson, 2013).

Internet for Non-work Activities

For the purpose of this research the proponents would like to zoom in on social media activities as the *cyberloafing* activity done by government employees using their smartphones. Karaoğlan Yılmaz, Yılmaz, Öztürk, Sezer, and Karademir (2015) confirmed that using smartphone technology during work time for personal purposes affects work productivity and wastes work time. Employees who engage in social media activities during their work time tend to be less productive than those who do not engage in social networking (Andreassen, Torsheim, & Pallesen, 2014b). Health care researchers Black, Light, Paradise Black, and Thompson (2013) studied social media use through smartphones and confirmed that the health care staff studied spent 12 minutes per hour on Facebook. Social media use increased in correlation with increasing patient numbers in the hospital under study (Black et al., 2013). Many online organizations are losing their customers' satisfaction and productivity because of their employees' cyberloafing behavior (Langfred, 2013; Zoghbi-Manrique-De-Lara, 2012). Users in another study spent 74 minutes per day on the web surfing sites such as LinkedIn, Twitter, and Facebook and 81 minutes per day with mobile apps (MacCormick, Dery, & Kolb, 2012).

The need to monitor and correct incidences of Cyberloafing

Many organizations permit their employees to use their own devices, such as smartphones and tablets, to research corporate data. The employees can use their own devices to connect online without using organizational networks by using their mobile network. In this type of situation, organizational leaders need to adopt monitoring and security strategies, such as blocking websites, tracking e-mails, and reviewing browsing history (Harris & Patten, 2014). Several organizational leaders have used a new plan to control employee *cyberloafing* via a personal device, data streaming, texting, and voice messages. Organizational leaders can use mobile device management systems to monitor and control nearly all functions of personal employee devices and to collect private data (Lee, Crossler, & Warkentin, 2016). Nevertheless, it is difficult to estimate the security risks faced by employees without having real knowledge about a security concept related to the information stored in their smartphones (Lee et al., 2016). The use of smartphones in daily life and at work can lead to increased risks from attacks and breaching opportunities. Although a smartphone is personal property, employees can use it to access personal and work information according to the bring-your-own-device strategy. Many organizational leaders confirmed that using smartphones to access organizational databases reduced operating costs (Harris & Patten, 2014). However, although approximately 75% of large businesses allow employees to connect to the organization's system from personal smartphones, many of these smartphones lack passwords or any security application that could mitigate potential risk (Harris & Patten, 2014). There needs to be a secure system to protect an organization's information and to save working time, especially when employees connect their smartphones to the system directly or through the organization's computer desktop. Rakes, Deane, and Rees (2012) noted a secure IT environment is critical for government institutions, and system protection becomes more difficult because attackers (i.e. hackers) have more knowledge. Using multiple security tools to protect the same system will decrease opportunities for breaches and will help to cover security defects or weaknesses in software by using additional software or hardware that does not have the same gap or defect. However, the need exists to check the positive and negative security features for each security software or hardware and then to cover the negative points by combining the current software with another software or hardware that does not have the same weakness (M. Harris & Patten, 2014). For example, many government departments and commercial companies use the ISO/IEC standards as the optimal choice for providing effective security specifications for a system, as ISO/IEC is a general security language for all company types (Humphreys, 2008). The ISO/IEC standards can help to handle insider threats that would cause vulnerabilities in an organization's system, as it is important to achieve balance in information security systems and to have a good level of monitoring for changes in the system and security risks (Král, 2011). The surveys conducted indicated 35% of security problems in the United States and the United Kingdom were about insider threats, such as fraud (Humphreys, 2008). These threats are a serious problem and may have a negative effect on businesses (Humphreys, 2008).

Strategies and Mechanisms to control Cyberloafing

Organizational control has an association with terms such as managerial control, system control, policy control, and behavior control and represents the possible procedures used to control employees' behavior and engage them to comply with an organization's policies and goals (Piscotty et al., 2016). Employees generally comply with organizational rules and policy when managers force them to do it and when the employees realize there are punishments in place. This strategy depends on employing various types of formal punishments and applying these punishments to employees who violate the rules. If employees realize there is a punishment in place and that punishers will practically apply it to others who commit or violate organizational policy, they will try to avoid repeating undesirable behavior (Piscotty et al., 2016). Leaders can control or minimize employees' undesirable behavior by making them expect various formal punishments if they continue *cyberloafing* during working hours. Although there need to be effective strategies to control cyberloafing in the workplace; including a control strategy and punishment strategy to control the *cyberloafing* phenomenon, supervisors must be near the employees, understand their behavior in depth, and monitor and apply punishments if any violations happen (Piscotty et al., 2016). Setting an effective policy related to Internet use is also important for employees to have clear rules related to using an organization's resources (i.e. time at work, work internet connection etc.) for personal purposes. The prevention strategy is important for deterring employee policy violations. Using preventative technology may help with growing a business, but the technology could cause business owners to lose their reputation and customers due to employees' misuse of the technology in the workplace (Eivazi, 2011). Organizational leaders should follow several steps to start an effective prevention strategy. The first step is to ensure the online policy includes clear points related to an organization's rules and policies (Glassman, Prosch, & Shao, 2015). It is difficult for employers to estimate the risks faced by employees without having real knowledge about a security concept. Therefore, there needs to be training for managers regarding knowledge of security risks and threats possibly associated with violating organizational policy (Drouvelis & Nosenzo, 2013; Bartariya & Rastogi, 2016). Employees also need to have security training and experience in this area before they can identify the risks from using an online service in the workplace (Glassman et al., 2015).

A study in the United Kingdom showed that computer users spend an average of 31.4 hours per month Internet browsing and 5.4 hours using their mobile devices for web browsing (Ofcom, 2015). It also indicated that people use their smartphone 61% more than their desktop computer because of its portability (Ofcom, 2015). However, despite the many advantages related to using e-mail and Internet tools, its misuse at work has created new financial and legal challenges for employers (Piscotty et al., 2016). Employers have many concerns regarding the misuse of online services from their employees and therefore tend to adopt an electronic monitoring strategy to protect their business interests and minimize or prevent potential risks to online services at work by employees (Piscotty et al., 2016). Some concerns center on the prospect of making employees feel uncomfortable, even though organizational leaders have the right to monitor employees when they are using organizational resources, such as computers and devices (Glassman et al., 2015). Sarpong and Rees (2014) focused on the big-brother effect in the workplace. The qualitative study involved exploring any fears, discomfort, and stress caused by using a monitoring system during working hours. Managers can use monitoring systems to have an overview of their employees' activities during work hours. In Sarpong and Rees's (2014) study, the managers and non-managers who participated in this study confirmed that they did not have any concerns regarding the electronic monitoring strategy. Organizational policy should include discussing the monitoring system with employees before applying it. Employers can block websites, monitor e-mails, and retrieve browsing histories; however, monitoring personal mobile devices has two opposing views (Glassman et al., 2015). One view is an employer's right to monitor employees' use of personal devices, especially for measuring job performance and protecting organizational data for security purposes (Glassman et al., 2015; Kidwell, 2010; Lee et al., 2016). Another view is employees' right to reject a monitoring strategy that includes their own devices because the aim of monitoring is to control and monitor employees' personal data (Lim et al., 2002). A monitoring strategy is a control mechanism used to control or monitor employees' information during working hours. Controlling employee information privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Lee et al., 2016, p. 5). However, the agreement needed is a contract between employees and organizational leaders that serves as confirmation of employees' acceptance of a monitoring strategy and relinquishment of their mobile privacy to their organizational leaders (Glassman et al., 2015; Kidwell, 2010; Lee et al., 2016). A monitoring strategy may save work time and improve job performance (Carnevale & Smith, 2013). The foundation of performance expectancy is the adoption of a specific technology that will improve job performance, as organizational leaders must monitor and control personal devices to keep organizational data safe and to save work time (Carnevale & Smith, 2013). However, a balance is necessary between the monitoring system and employee privacy (Lee et al., 2016).

In summary, the literatures presented herein defined what is *cyberloafing* and in what context is a non-work related activity considered as such. It then proceeds to show the cost of *cyberloafing* in terms of being unproductive at work and its other consequences such as potential security breaches on the part of the organization. All of the above created the necessity for those in management to come up with mechanisms and strategies to control *cyberloafing* activities. The strategies found by the proponents include preventive and electronic monitoring, which still have some sensitive areas like employee privacy that the management has to resolve before it can come up with a solid Internet use policy. Thus, the researchers aim to find reliable and actionable ways to limit incidences of *cyberloafing* in the government by conducting interviews with those in authority, and focus group discussion as is shown in Chapter 3 of this paper.

Chapter 3

METHODOLOGY

Presented in this chapter is the research design, sources of data, data gathering instruments, and procedure of the study.

Research Design

For this study the proponents used a qualitative research methodology with interviews to shed light on the research problem. Qualitative research involves making a connection between a story and ideas that develop at a site.

Research Locale and Participants

This study was conducted in Davao City, Davao del Sur, Philippines. In particular, it was in three (3) selected government agencies in the city and all of which are National Government agencies. The participants included a Chief Administrative Officer (CAO), Human Resource (HR) personnel, supervisors, division chiefs and/or on-site managers, and all other personnel who are part of the responding agencies' management or are in the position to influence or inspire organizational policies and practices. In total it has ten (10) respondents who are part of the skeletal work force at the time the research was conducted.

Research Rationale

The responses to the interview questions helped the proponents gain insight into the following general and supplemental research questions: How can the management and/or Human Resource (HR) personnel minimize wasted work time by monitoring and limiting the personal Internet activity of employees who use their smartphones while on the job?

RQ1: What effective strategies can the Chief Administrative Officers, Human Resource (HR) personnel and other management personnel use to monitor employees so that they are not wasting work time by *cyberloafing* from their smartphones?

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

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

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

Sampling Technique

Purposive sampling was used in this study. It is a sampling technique in which the researchers rely on their own judgment when choosing members of the population to participate in the study (Research Methodology, 2011). The researchers chose the participants based on their role in the government office they are working in and their direct influence in the formation and implementation of internal policies and protocols whether preventive, corrective or evaluative in nature.

Research Instrument, Data Gathering and Storage

Research Instrument, Data Gathering and The research's ten (10) participants were the sources of the primary data obtained with the help of questionnaires containing open-ended questions serving as a guide to in-depth interviews with them. On the other hand, secondary and supporting data were gathered from the Focus Group Discussion (FGD) that the researchers had among themselves. The researchers and questionnaires disseminated via e-mail were the instruments used in gathering the primary data, while only the researchers' among themselves make up the secondary data. In terms of the process of gathering information, the participants were predetermined according to their position, official appointment or designation, and length of service as discussed in Chapter 1's Scope and Limitation section and in this chapter's Sampling technique section. After which, the participants were asked to fill out Informed Consent forms (Annex A). Upon agreeing to participate in the research, said respondents were sent questionnaires via e-mail and asked to fill them out, then, the scanned copies of which were sent back to the proponents. The participants are interviewed on site by the researcher/s assigned with that particular government office for any follow up questions and the participants' answers were recorded using the researcher's smartphone/s. Once the interviews were done, the researchers had a virtual FGD through Google Meet and they were able to identify some common themes. Lastly, in storing the data, the proponents used a secure cloud storage device accessible only to the proponents called Google Drive, to digitally keep scanned copies of the questionnaires filled out by the respondents.

Ethical Consideration

It was voluntary to participate in this study. The researchers put out a disclaimer in the questionnaires distributed to the chosen respondents and they also discussed with the participants the purpose of the study and confidentiality as an ethical consideration. In addition, pseudonyms were used in lieu of the participants' names for their protection and confidence. As researchers, the proponents took note of the sensitive and emotional nature of the research participants; making sure they were not forced to share information they were unwilling to disclose. Finally, the respondents were treated with respect and their dignities and identities left uncompromised throughout the duration of this research.

Trustworthiness of the Study

The trustworthiness of a qualitative study depends on three things 1) credibility, 2) confirmability, and 3) dependability.

Credibility. Credibility relates to the degree to which the study reflects the real values of the respondents or the "importance of reality" (Moon et. al, 2006). It aims to guarantee the trustworthiness of the study. The researchers ensured that what was documented or noted in this paper was what the respondents or research participants attempted to express.

Conformity. It relates to results relying exclusively on the respondents and the circumstances of the research and not on the bias, motivation, concern, and viewpoint of the inquirers (Guba as quoted by Moon et. al, 2006). The questionnaires handed out were designed to be open-ended and the style of questioning during the interviews were meant to explore in order to guarantee that the respondents' narratives will be captured completely.

Dependability. This relates to the accuracy of study results and methods' records (Sandelwoski, 1986). The researchers thoroughly reviewed the research findings to ensure consistency so that its readers and other research groups would be able to understand and know if this paper is dependable as a reference for a further study or their own distinct papers.

REFERENCES

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

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

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

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

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

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

Demirci, K., Orhan, H., Demirdas, A., Akpınar, A., & Sert, H. (2014). Validity and reliability of the Turkish version of the smartphone addiction scale in a younger population. Bulletin of Clinical Psychopharmacology, 24, 226-234. doi:10.5455/bcp.20140710040824 29

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

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

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

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

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

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

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

Jia, H., Jia, R., & Karau, S. (2013). Cyberloafing and personality: The impact of the big 30 five traits and workplace situational factors. Journal of Leadership & Organizational Studies, 20, 358-365. doi:10.1177/1548051813488208

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

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

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