UNIVERSITY OF NAIROBI

FACULTY OF SCIENCE AND TECHNOLOGY, DEPARTMENT OF COMPUTER SCIENCE

FRAMEWORK FOR EVALUATING THE IMPACT OF TECHNOLOGICAL CYBERLOAFING CONTROL ON EMPLOYEE PERFORMANCE: A CASE OF ETHICS AND ANTI-CORRUPTION COMMISSION IN KENYA

BY

PAUL K. MWANGI

P54/73016/2014

SUPERVISOR: MS. SELINA A. OCHUKUT

AUGUST 2021

Submitted in partial fulfillment of the requirements for the Degree of Master of Science in Information Technology Management of the University of Nairobi

DECLARATION

I declare that this is my original work, except where due references are cited, and has not been submitted for any other award in any University.

20/08/21

Paul Kibuku Mwangi

Date

Reg No.: P54/73016/2014

This project report has been submitted in partial fulfillment of the requirement of the Master of Science Degree in Information Technology Management of the University of Nairobi with my approval as the University supervisor.

Atwani

23/08/2021

Ms. Selina Atwani Ochukut

Date

Faculty of Science and Technology

Department of Computer Science

University of Nairobi

DEDICATION

This research work is dedicated to my late father Muthee Kibuku and mother Maria Waruiru for instilling in me the values of discipline and hard work that have made me come this far.

ACKNOWLEDGEMENTS

First, I wish to acknowledge God's grace and presence, without which I could not have accomplished this task. Secondly, I acknowledge the critical role played by my supervisor, Ms. Selina Atwani in this journey. I will forever be grateful for her patience in guiding through the process despite my initial little understanding of research concepts. Thirdly, I recognize the other members of the panel of assessors Mr Eric Ayienga, Dr Andrew Kahonge and Dr Elisha Abade for critics, challenges and guidance during the different assessment sessions which helped sharpen my understanding of the research process and greatly improved the research work. Fourthly, I recognize the role played by my peers in the process, George Njoroge and Easter Wambui by being available for the much needed consultations and encouragement. Finally, I acknowledge and greatly appreciate the role played my wife Alice, daughters Evelyn and Lisa and son Ernest who constantly reminded me of the need to finish school and understood my absence during the research period.

ABSTRACT

Over the years, organizational operations have become highly computerized with almost all processes incorporating aspects of computing in their undertaking. Apart from installing computing infrastructures to facilitate the operations, organizations have integrated internet and email systems to enable communication, linkage to external stakeholders and provide for external information gathering. While these installations are useful in enhancing productivity and efficiency in operations, employees often slack off from work by using the technologies for personal purposes. This behavior, referred to as cyberloafing, has become a challenge to organizations with associated negative consequences. A major consequence of the behavior is that it impacts negatively on employee performance by disrupting official work programs and denying computing resources to official activities. A common mechanism that organizations have adopted to control this behavior is installation of technological control solutions in form of monitoring and filtering systems. There is however no much information on how to evaluate the value of these control systems. To bridge the gap, this study proposed an evaluation framework that can aid in determining their impact on employee performance. The proposed framework was tested using technological cyberloafing control in Ethics and Anti-Corruption Commission (EACC) in Kenya. Data was collected from 116 employees of the institution and analyzed using Statistical Package for the Social Sciences (SPSS) version 27. During the assessment, it was established that the control in EACC has impacted positively on employee performance through reducing cyberloafing and being perceived fair by employees. The study also identified that in order to reduce cyberloafing, the control systems should have capacity to detect any attempts and enforce defined sanctions. Issuing advance notice should also be part of control implementation process for it to be perceived fair by employees. A resulting framework was identified which considers the capability of cyberloafing control to detect, enforce, reduce the behavior and be perceived fair by employees. The study concluded by recommending that as a means of assessing value on ICT investments, organizations need to determine the impact of technological cyberloafing control on employee performance. Detection and enforcement capabilities should also be considered as key technical requirements when these solutions are being acquired and installed.

Keywords: Technological Cyberloafing Control, Cyberloafing, Cyberloafing Control, Employee Performance, Perceived Fairness

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

AUP	Acceptable Use Policies
CCTV	Closed Circuit Television
GDT	General Deterrence Theory
HR	Human Resources
ICT	Information Communication Technology
IS	Information Systems
IT	Information Technology
NG	Next Generation
NWRC	Non-Work Related Computing
PDA	Personal Digital Assistant
SPSS	Statistical Package for the Social Sciences

CHAPTER ONE: INTRODUCTION

1.1 Background

Advances in computing technologies and internet have made their use a daily routine for people and organizations globally (Karaoƚlan Yilmaz *et al.*, 2015). While organizations have adopted these technologies as a way of increasing productivity and efficiency, the facilities have provided employees with opportunities to get off from work and engage the technology on personal non-work activities (Askew *et al.*, 2014). This use of work computing facilities for personal activities during working hours is called cyberloafing (Jia, Jia and Karau, 2013). In different literatures, the behavior is referred to as cyberslacking, non-work related computing (NWRC), cyberbludging, internet deviance, personal internet usage at work, internet abuse and internet addiction disorder. Apart from computers, PDAs have also been used to cyberloaf.

There are different forms of cyberloafing ranging from those regarded as minor acts with little impact and consequences, to those regarded as major with greater impact and heavy consequences in terms of cost and time consumption (Blanchard and Henle, 2008). Minor cyberloafing includes non-work-related emailing, online shopping and business, surfing mainstream news websites, job searching and downloading materials. Major cyberloafing includes downloading music, online abuses, gambling, engaging in blogging and chatting, gaming, streaming adult content and other heavy non-work-related media.

It has been demonstrated that cyberloafing is widespread across sectors and regions, consuming 40%-60% of employees working time(Lim, Koay and Chong, 2020). For instance, seventy-five percent of employees who were alumni of a large university in Asia, disclosed to cyberloaf fifty one minutes in each working day (Lim and Chen, 2012). In another report, employees working in emergency section of a hospital located in Florida indicated that they spend 12 minutes in an hour on Facebook (Black *et al.*, 2013). Other studies have reported that on average, two hours per day are spent by employees while engaging in cyberloafing behavior (Greengard, 2000; Conner, 2015).

Cyberloafing has an impact on organizations with various negative consequences to both the institution and individual employees as identified in various studies (Young, 2001; Whitty and

Carr, 2006; Weatherbee, 2010; Vitak, Crouse and Larose, 2011; Zoghbi-Manrique-De-Lara, 2012). As a major consequence to organizations, this behavior impacts greatly on productivity when employees spend a lot of time cyberloafing and engaging resources that could otherwise be used in productive assignments. It disrupts their schedules and work plans prolonging durations spent on work assignments. Regarding the impact on ICT infrastructure, cyberloafing activities increase security risks on organizational data and network as it opens channels with 'the external world'. It also creates a strain to ICT resources, especially bandwidth, which can greatly impact on effectiveness in facilitation of organizational operations. Apart from being a proliferation in the workplace that can result in penalizing of employees, the behavior can result in non-compliance and lack of participation affecting organizational effectiveness. Another threat of cyberloafing is that it could expose organizations and employees to unnecessary legal situations such as defamation, sexual harassment, dissemination of harmful information, and access to prohibited materials such as music and unlicensed software.

To address this behavioral challenge, organizations have adopted various strategies that can be classified into technological and non-technological. The latter address organizational and personality factors for cyberloafing and include awareness creation, recruitment process, performance measurement, job design and organizational justice (Jian, 2013; Ahmad *et al.*, 2014; Holguin, 2016). Technological control mechanisms, which are the most popularly implemented means of addressing cyberloafing in organizations (Jia, Jia and Karau, 2013), employ electronic monitoring and content filtering to implement defined ICT Acceptable Use Policies (AUPs) (Ugrin and Michael Pearson, 2013).

1.2 Problem Statement

Due to increased over-reliance on electronic technologies at workplaces, there are higher incidents of employees engaging in cyberloafing behavior. Studies have demonstrated a widespread engagement in cyberloafing activities across regions and sectors including government institutions (Greengard, 2000; Nazareth and Choi, 2015; Mackay, 2019). Being a global phenomenon, Kenya's organizations are not an exception. Local studies have identified access to social media at work as a major interference on employee engagement and overall productivity (Munene and Nyaribo, 2013; Mwituria, 2015).

Employees' over-engagement in cyberloafing exposes organizations to a range of threats both internally and externally. A major consequence is that the behavior affects organizational effectiveness through inhibition of productivity both for individual employees and the institution. Additionally, it strains the organizational ICT resources (especially through network bandwidth degradation and congestion). It also exposes organizations to external threats such as network and data security risks and unnecessary legal liabilities arising from employee involvement in illegal online activities. For government institutions, the effect on employee performance can impact greatly on delivery of government services to the citizenly.

Since the use of computers and internet will continue increasing, it is inevitable that control of cyberloafing becomes an important aspect in organizational management. Many organizations have implemented technological control mechanisms in form of electronic monitoring and content filtering systems (Urbaczewski and Jessup, 2002; Wang, Tian and Shen, 2013). Studies have been conducted on assessment of the effectiveness of these controls in reducing cyberloafing(Ugrin and Michael Pearson, 2013; Wang, Tian and Shen, 2013) and their impact on aspects such as employees motivation(Jiang, Siponen and Tsohou, 2020) and job attitude (Alder *et al.*, 2008)). There is however no much research-based literature on the link between implementation of these control systems and employee performance and on evidence whether the solutions are adequately designed to positively impact job performance.

1.3 Research Objectives

The primary objective of this study was proposing a framework for evaluating the impact of technological cyberloafing control on performance of employees. Specifically, the study sought to:

1. Identify the aspects of technological cyberloafing control that impact on employee performance.

2. Propose a framework that can be used to evaluate the impact of technological cyberloafing control on employee performance.
3. Test the evaluation framework using technological cyberloafing control in EACC.

1.4 Research Questions

The study was undertaken with a focus to getting answers to the following questions:

1. What aspects of technological cyberloafing control systems are important when evaluating their impact on employee performance?
2. What is the appropriate framework for evaluating the impact of technological cyberloafing control on employee performance?
3. How does technological control impact on cyberloafing behavior in EACC?
4. How has technological cyberloafing control affected the perceptions of fairness among employees in EACC?
5. What is the impact of technological cyberloafing control on employee performance in EACC?

1.5 Significance of the Study

There is a shortage of information on cyberloafing topic in Kenya be it on extent, antecedents, consequences or strategies for managing the counterproductive behavior. This implies that there is no localized guide on effective ways to address the phenomenon. Since majority of organizations have implemented technological control, the outcome of this study will guide on the necessary configurations for achieving the main goal of this control which is improving employee performance. The resulting framework will also provide a guide for determining the value of the control systems and provide relevant information for decision making on their continued maintenance. For organizations that are yet to acquire a cyberloafing control solution, the outcome of the study will provide a guide on the technical aspects to consider while procuring or developing the solution.

1.6 Scope of the study

Research has been undertaken on antecedents, extent and impact of cyberloafing in organizations. Studies have also been carried out on the different mechanisms of controlling cyberloafing, their effectiveness and impact on organizations and employees.

On technological cyberloafing control, studies could be done on their effectiveness, impact on organizational and employee performance, impact on ICT security, impact on ICT resources utilization among other topics. This research work specifically addressed itself on the impact of technological control on employee performance and used cyberloafing control in one government institution in Kenya (EACC) to establish the relationships and make conclusions.

CHAPTER TWO: LITERATURE REVIEW

2.1 Concept and Typologies of Cyberloafing

The term cyberloafing was initially used in a seminar paper by Lim of National Singapore University in the year 2002 (Lim, 2002). It consists of two parts: ‘cyber’ and ‘loafing’. ‘cyber’ is commonly used as a prefix for phrases based on computer sciences which refer to computers as tools. ‘loafing’ is gotten from the word ‘loafer’ which refers to a person who wastes time. Cyberloafing is simply the act of wasting time by engaging in unexpected activities using a computer or other computing facilities such as internet and email. In an office setup, time is normally wasted by enganging in personal affairs instead of undertaking official assignments. Cyberloafing involves deliberate use of IT for non-work affairs during defined working hours and while in the workplace (Jandaghi *et al.*, 2015).

Cyberloafing activities have been classified into various categories. Lim (2002) classified them into browsing and emailing. According to him, browsing activities are actions such as visiting websites for purposes of reading and watching news, social networking, entertainment, shopping, financial services, pornography and sports among other non-wok related activities. Emailing involves the receipt, reading and exchange of non-work related emails. Blau, Yang and Ward-Cook (2006) introduced another category of cyberloafing activities called interactive internet activity which included online gaming, chats, social networks live posts, and downloading of information and materials. Blanchard and Henle (2008) classified the activities into serious and minor cyberloafing. The latter includes common internet usage at work and emailing while the former includes pornography viewing, music and video downloads, online gaming and gambling. Mastrangelo, Everton and Jolton (2006) classified cyberloafing as nonproductive and counterproductive computer use. Nonproductive use happens through activities that are unproductive, but do not have the potential to be destructive to the organization such as chatting, gaming, or shopping. Counterproductive use happens when there is engagement in behavior that conflicts with the organization’s norms and work schedules, such as transmission or downloading of pornography, creation of computer viruses, trafficking of drugs, downloading copy-written materials and sexual harassment.

The definitions and classifications imply that cyberloafing involves both waste of time and engagement of employer ICT facilities. The resultant effect is a negative impact on employee performance. Application of any control mechanism meant to address the behavior must therefore result in improved or high employee job performance.

2.2 Mechanisms for Controlling Cyberloafing

The mechanisms applied by organization in controlling cyberloafing activities can broadly be classified into technological and non-technological.

2.2.1 Non-technological mechanisms

At organizational governance level, Acceptabe Use Policies (AUPs) (also called electronic use policies or internet use policies) define the use, misuse and implications on 'illegal' engagements of office tools to facilitate cyberloafing such as internet and email misuse (Pearson and Ugrin, 2008; Holguin, 2016). Organizations also engage management practices to assist in controlling cyberloafing. These include rigorous recruitment, performance measurement, job design and organizational justice (Jian, 2013; Ahmad *et al.*, 2014; Holguin, 2016). Another non-technological mechanism used by organizations is creating employee awareness and training on the impacts and consequences of cyberloafing (Ifinedo, 2012).

2.2.2 Technological mechanisms

These mechanisms are aimed at achieving effective monitoring, filtering, blocking and reporting of cyberloafing activities. They have proved useful over time (Wang, Tian and Shen, 2013) and therefore have been implemented in many organizations (Urbaczewski and Jessup, 2002). Monitoring involves control systems that observe, regulate and records individuals' activities when engaging internet and other computing infrastructures. Filtering is preventing the access, transmission, and delivery of undesirable information (Bertino, Ferrari and Perego, 2005). Sheriff and Ravishankar (2012) identified the different forms of monitoring and filtering as:

i. **Packet sniffing** - this involves use of software programs that scrutinize all the information that passes through the network to which it is connected. They can be setup with or without filters and can monitor online activities including sites visited, mails sent and received internet telephony and audio, video or textual downloads.

ii. **Desktop monitoring** – in this technique, devices are installed on the computer and are able to intercept the signals and replicate what the user is seeing or typing on the desktop.

iii. **Closed Circuit Cameras (CCTVs)** - used in the workplace to monitor employees' activities. In an organizational setup, they are mainly used for security surveillance purposes.

iv. **Internet monitoring and content filtering systems** – these are systems that monitor, inspect and control billions websites visited by employees in the workplace. They also inspect emails and other internet-based communications and provides web security against malware, spyware and viruses. These solutions which are mainly configure as web proxies and internet firewalls, are the common technological cyberloafing control mechanisms used in organizations. Examples of these solutions are Cisco Umbrella, Barracuda Web Security, Untangle NG Firewall, FortiGuard, Sophos Web Filter and WebTitan (TrustRadius, 2021). This study was mainly focused on this category of technological cyberloafing controls.

2.3 Requirements for an Effective Technological Cyberloafing Control System

Researchers have described technological cyberloafing control systems as deterrence mechanisms that are theoretically premised on the General Deterrence Theory (GDT) (D'Arcy, Hovav and Galletta, 2009; Ugrin and Michael Pearson, 2010; Hassan, Reza and Farkhad, 2015). The theory posits that success of such mechanisms is determined by their capability to guarantee detection of unacceptable actions and provide for severe punishment (Gibbs, 1977). This implies that the effectiveness of a deterrence system can be measured by the twin parameters of perceived sanction certainty (probability of detection and punishment) and perceived sanction severity level (enforcement criteria). The accuracy of this formula is supported by the argument that individuals who perceive that there is a high possibility of being detected and severely punished are less likely to be engaged in objectionable behavior (Cheng *et al.*, 2014). They will always disregard the potential benefits of the behavior on weighing against the potential punishment (Rahimnia and Karimi Mazidi, 2015).

In regard to IS monitoring systems, their success is pegged on capability to increase perceptions of the certainty and severity of punishment for misuse (D'Arcy, Hovav and Galletta, 2009).

According to Ugrin and Michael Pearson (2013), a high potential to be caught (probability of detection) and perceived certainty of sanctions (likelihood of enforcement) increases the deterrence power of cyberloarfing control systems and makes them more effective. In determining the effectiveness of cyberloafing sanctions (as implemented in electronic monitoring systems) towards different cyberloafing activities, the two researchers found that it is only when both detection and enforcement are provided for that the monitoring system is able to effectively enforce sanctions and reduce employees' intention to engage in all forms of cyberloafing. The loafing activities included viewing pornography, personal finances management, shopping, emailing and social networking. Without enforcement guarantee, the system could only control viewing pornography, personal finances management and shopping. Their research model (figure 1) was adopted by Hassan, Reza and Farkhad (2015) in a study involving employees of a Tehran subway station with similar results on the role of detection and enforcement in determining the effectiveness of implementing anti-cyberloafing policies and sanctions by means of electronic monitoring.

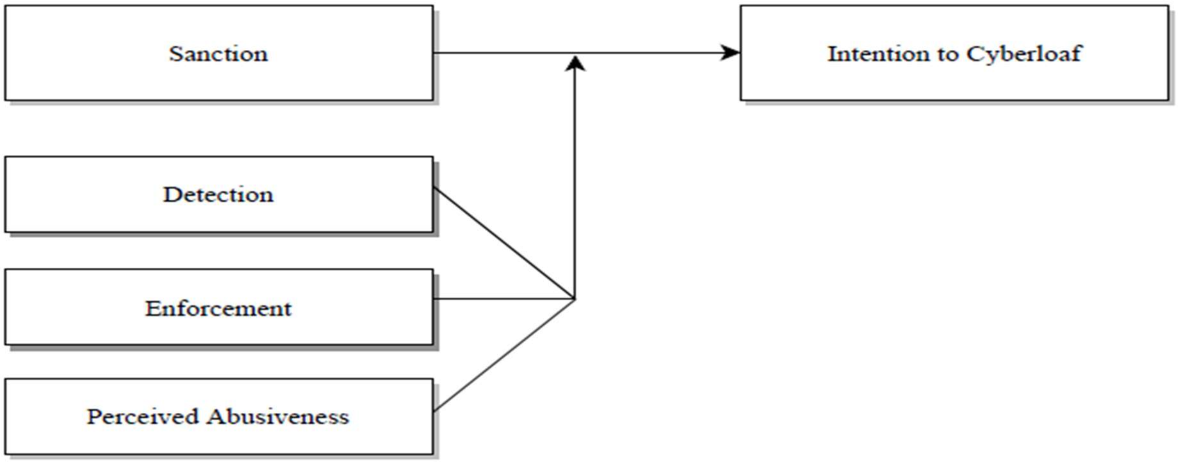

Figure 1: Ugrin and Pearson Framework

Another study involving administration personnel in a Spanish University (Zoghbi-Manrique-De-Lara and Olivares-Mesa, 2010) concluded that control systems (comprising of proximity and monitoring) can only be effective in reducing cyberloafing activities if punishment is integrated as part of the setup. This confirms that apart from putting in place detection mechanisms (monitoring system), enforcement (punishment) must be part of a cyberloafing control mechanism for it to be effective.

The studies establish that technological cyberloafing control systems fit well within deterrence mechanisms and their effectiveness is determined by capability to guarantee detection of cyberloafing behavior and provide for enforcement of defined sanctions (AUPs).

2.4 Effect of Advance Notice on Application of Technological Cyberloafing Control

Although most organizations employ silent covert monitoring as a strategy of detecting employee deviant behaviors, worker's advocacy groups insist that as a bare minimum, the subjects should be informed of the intention to monitor before it is applied (Alder, Noel and Ambrose, 2006). Hovorka-Mead *et al.* (2002) established that informing employees in advance before engaging in monitoring impacts positively on their perception of procedural fairness by making them feel valued and their privacy respected . Having prior information on monitoring also provides deterrence against the objectionable behavior and makes employees modify their internet and email activities to avoid being detected and punished (Kim and Choi, 2005; Alder, Ambrose and Noel, 2006).

2.5 Technological Cyberloafing Control and Fairness Perception

Application of monitoring and filtering controls is often associated with perceptions of unfairness which could result in reduced loyalty and resentment by employees making them underperform (Urbaczewski and Jessup, 2002; Khansa *et al.*, 2017). A study on the association between internet monitoring and job performance (Jiang, 2020) established that monitoring results in a reduction of intrinsic work motivation which in turn results in reduced job performance. In a study investigating the influence of advance notice, organizational trust and justification on job attitudes, Alder, Ambrose and Noel, (2006) placed internet monitoring fairness as a mediating variable (figure 2) and established that it has a positive impact on employees' job attitudes that included satisfaction, commitment and intentions to achieve a high turnover.

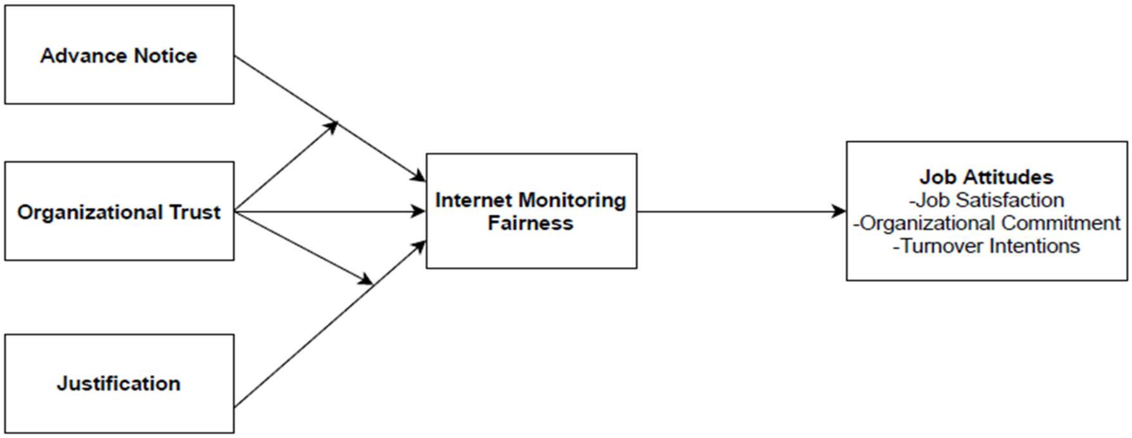

Figure 2: Alder, Ambrose and Noel Model

Research has suggested that perception of procedural fairness among employees in implementation of cyberloafing control is improved by providing for quotas of unrestricted access. These breaks provide mental refreshment sessions for employees enabling them to gain a greater impetus to undertake their tasks by offering relaxation and re-energizing moments (Henning *et al.*, 1997; Coker, 2013). The provision also helps to create the social norms that work time is for work-related activities and cyberloafing can only be exercised during quota breaks (Glassman, Prosch and Shao, 2015).

A cyberloafing control system is also perceived unfair if it doesn't provide relevant information and feedback. A study on design of a system to manage employees access to internet (Kim and Choi, 2005) recommends that the system should warn users that there will be monitoring, recording and analyzing of their navigation of the internet. Despite providing some considerable deterrence against intention to access objectionable materials, this warning presents some respect for privacy. The researchers also recommended that the system should provide customized deny messages to be displayed to users. Such messages should state the reason for denial and how to request for access. The feedback could also include a link to the organizations usage policies (Glassman, Prosch and Shao, 2015)

Implementation of an electronic monitoring and control system should be done in such a manner that it does not result in perceptions of unfairness among employees which could impact negatively on their performance.

2.6 Technological Cyberloafing Control and Employee Performance

Currently there is no much literature primarily on the direct link between cyberloafing control and employee performance. However, there is a lot of literature confirming a negative impact of technological cyberloafing control on employees cyberloafing behavior (Pearson and Ugrin, 2008; Henle, Kohut and Booth, 2009; Zoghbi-Manrique-De-Lara and Olivares-Mesa, 2010; Ugrin and Michael Pearson, 2013). Additionally, studies have identified that over-engagement on cyberloafing impacts employee performance negatively (Li and Chung, 2006; Bock and Ho, 2009; Askew, 2013). This then implies that usage of technological cyberloafing control will most likely impact employee performance positively, mediated by reduced cyberloafing. Such a relationship is identified in a study on anti-cyberloafing internet monitoring and employees performance (Jiang, 2020). The study investigated the relationship between internet monitoring, cyberloafing behavior, employee motivation and the ultimate impact on performance.

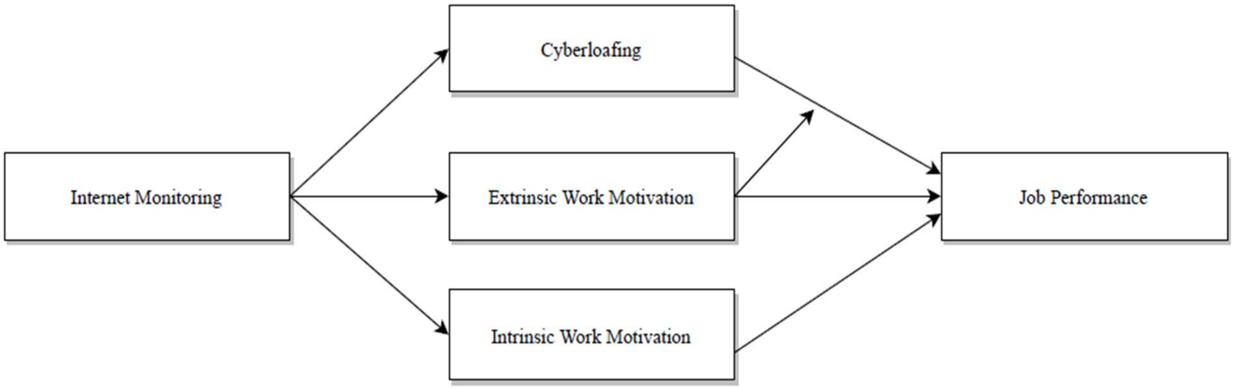

Figure 3: Jiang Model

The researcher established that anti-cyberloafing internet monitoring decreased both cyberloafing and intrinsic work motivation. The decrease in cyberloafing activies results in increased performance while the decrease in intrinsic work motivation results in decreased performance.

2.7 Conceptual Framework

The reviewed literature identifies that determinants of effective technological cyberloafing control are detection probability and enforcement likelihood. Issuing of a notice prior to implementing control may also reduce cyberloafing and improve employee's perception of fairness. The literature also identifies the effect of cyberloafing control on employee performance to not only be determined by its reduction of cyberloafing but also the perception of fairness in controlling the behavior. Based on the review, a framework was proposed as presented in figure 4.

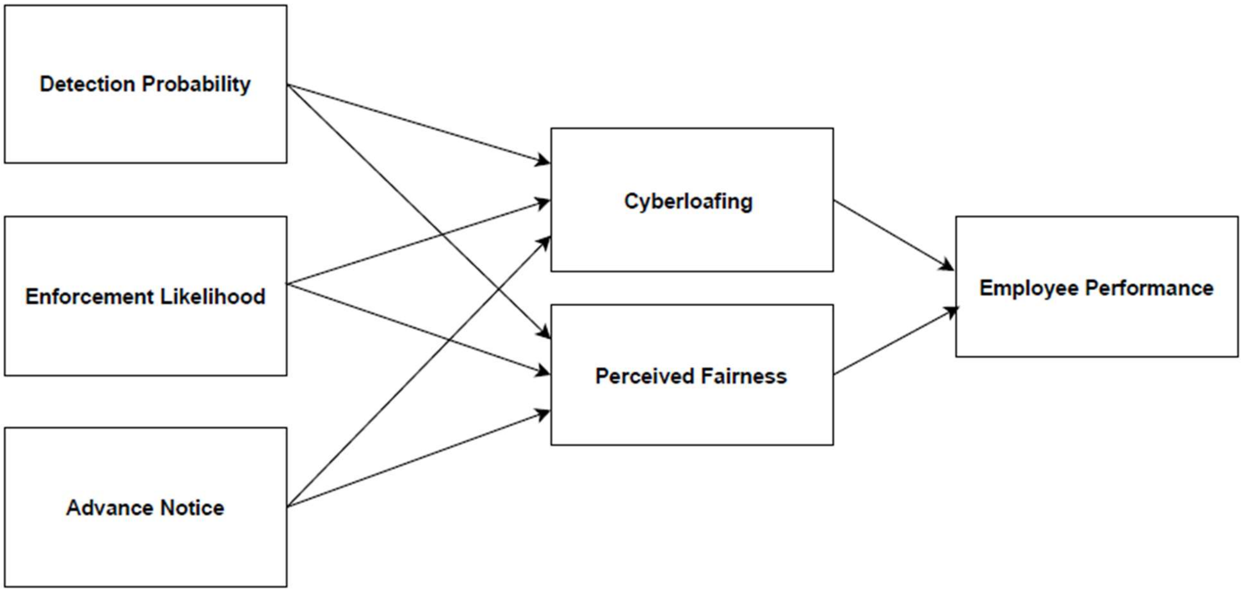

Figure 4: Proposed Evaluation Framework

Table 2.1:Variables definition and measures

Variable	Type	Definition	Measures	Scale
Detection Probability	Independent	Chance of being caught engaging in cyberloafing (Ugrin and Michael Pearson, 2013)	Detection chance when browsing, accessing social media, downloading, streaming and emailing (Ugrin and Michael Pearson, 2013)	five-point likert scale
Enforcement Likelihood	Independent	Likelihood of being punished (Ugrin and Michael Pearson, 2013)	Blocking likelihood, reporting likelihood, past enforcement (D’Arcy, Hovav and Galletta, 2009; Ugrin	five-point likert scale

			and Michael Pearson, 2013)	
Advance Notice	Independent	The period between when employees are notified about a decision and when the consequences of the decision take effect (Brockner *et al.*, 1994)	Notice period (Brockner *et al.*, 1994)	Five-levels scale
Cyberloafing	Mediating	Use of work computing facilities for personal activities during working hours (Jia, Jia and Karau, 2013)	Frequency of engaging in disallowed browsing, social media, downloading materials, streaming and emailing (Askew, 2013)	Five-levels scale
Perceived Fairness	Mediating	Perceived processes and procedures fairness (Colquitt, 2001)	Fair design, consistence, personal treatment (Colquitt, 2001)	five-point likert scale
Employee Performance	Dependent	Extent to which tasks are performed by employees (Koay, Soh and Chew, 2017)	Completing tasks on time, fulfilling responsibilities, work planning, taking up new responsibilities, engagement on non-work activities (Koopmans *et al.*, 2014; Jiang, 2020)	five-point likert scale

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

Research Methodology is the systematic way to solve a research problem (C. R. Kothari, 2004). It defines the steps adopted to address the research problem alongside the logic behind the choices. This section therefore defines the adopted research design, target population and selection of respondents, how information was collected from respondents and how the collected information was analyzed.

3.2 Research Design

A research design is a procedural plan adopted by the researcher to answer research questions validly, objectively, accurately and economically (Kumar, 2011). It refers to the strategy applied in ensuring that the components of the study are integrated in a logical manner. The study employed descriptive research design to gather data and establish facts and relationships between cyberloafing control and employee performance.

Data was collected from the employees of Ethics and Anti-Corruption Commission (EACC) in Kenya. The main reason for choosing a single institution is that the category of the systems under review should possess similar technical capabilities to achieve the target of improved employee performance. The only reason why their performance may vary in different institutions is the manner they are configured and the applied licenses. The results of the study will therefore most likely provide a reflection of the situation across institutions and systems. The chosen institution has a relatively high number of employees which provides for reliable sampling.

3.3 Study Population

Population is a complete set of persons or objects with common characteristic as established through a sampling criteria defined by a researcher. In this study, the respondents were drawn from employees of Ethics and Anti-Corruption Commission (EACC). The choice of the population was influenced by the criticality of the services offered in the institution that require high concentration and performance by employees. The institution has highlighted improving staff competencies and performance as key activities in the current strategic plan 2018-2023. The institution has a total of 704 employees spread across 5 directorates and working from 13 different offices across the country.

3.4 Sample Population and Sampling

Sampling is the process of statistically selecting a subset of the population of interest in a research to aid in making the required observations and inferences (Bhattacherjee, 2012). A sample must be truly representative for the derived inferences to be generalized back to the population.

A sample of 158 employees in EACC was picked from the total employee population of 704. The number was determined through application of the formula provided by Yamane (1967).

Yamane's Formula: $n = \frac{\mathrm{N}}{1+\mathrm{N}(e)^2}$

where ***n*** is sample size, **N** is the total population and ***e*** is the level of precision

Applying the formula on a population of 704 employees and adopting a level of precision of (+ or -)7%

$n = \frac{704}{1+704(0.07)^2}$ = 158 employees

Stratified sampling was applied to ensure that all offices are considered while random sampling was used to pick employees to provide required information on their interaction with the control and the impact on performance.

The distribution of participants across offices was based on percentage of employees in each office as presented in table 3.1.

Table 3.1: Sample distribution

Office	**No of employees**	**Employee Percentage**	**Participants**
Nairobi	458	65.05682%	102
Isiolo	21	2.982955%	5
Machakos	22	3.125%	5

Bungoma	21	2.982955%	5
Mombasa	25	3.551136%	6
Kisumu	24	3.409091%	5
Garissa	21	2.982955%	5
Eldoret	23	3.267045%	5
Kisii	21	2.982955%	5
Malindi	21	2.982955%	5
Nakuru	23	3.267045%	5
Nyeri	24	3.409091%	5
Total	**704**	**100%**	**158**

3.5 Data Collection Methods

The study used a structured questionnaire to collect data on employee's interaction with the control system and its impact on performance. Kumar (2011) defines a questionnaire as a written list of questions to which answers are recorded by respondents. Being structured, the questionnaire provided uniform collection of categorized sets of data. This method is suitable because:

1. It enables a wide reach and therefore increases the chance of meeting the targeted sample population.
2. It is less expensive.
3. It is free from interviewer's bias.
4. It provides respondents with enough time to give well thought responses

3.6 Dealing with Biasness

Bias is any process at any stage of inference in research which tends to produce results or conclusions that differ systematically from the truth (Yarborough, 2021). To avoid desirability bias where research respondents answer questions in a manner that will be seen favorable to the researcher, anonymity was considered while designing and distributing the questionnaire with the identity of the researcher and respondents not disclosed. To avoid selection bias, participants were identified using random sampling. The questionnaire was also issued to staff in different positions irrespective of job rankings. To protect the study from agreement bias where respondents have a tendency to go with a positive response option, the questionnaire was designed in a manner to avoid questions that imply that there is a right answer. In some areas, there was a mix of positively and negatively worded questions.

3.7 Validity and Reliability Testing

Validity is the capability of a data collection instrument to measure what it is supposed to (C. Kothari, 2004). The study considered both construct validity (capability to account for scores) and content validity (capability to adequately cover the topic of study). To achieve construct validity, the questionnaire was divided into sections as per the variables in the conceptual framework. To enhance content validity, five randomly selected supervisors in EACC were engaged to discuss the questionnaire and their views incorporated.

Reliability refers to the repeatability, stability or internal consistency of a data collection instrument (Kumar, 2011). A pre-study was undertaken involving 10% of the sample population (16 in number) as recommended by Sekaran (2006) to measure the questionnaire's reliability. SPSS was used to run the reliability test by obtaining Cronbach Alpha of each variable.

It was established that Enforcement Likelihood variable's Cronbach's Alpha was 0.488 which is way below the recommended minimum of 0.7. A review of the three measures of the variable (blocking, reporting and past enforcement) established that past enforcement measure was not suitable because on discarding it Cronbach alpha for the item rose to 0.768. The measure was therefore removed from the tool. The results of the reliability test were as per table 3.2

Table 3.2: Results of reliability test

Variable	**Cronbach's Alpha**	**N**
Detection Probability	0.903	5
Enforcement Likelihood (with enforcement history)	0.488	3

Enforcement Likelihood (without enforcement history)	0.768	2
Cyberloafing	0.732	5
Fairness	0.841	3
Performance	0.808	5

3.8 Data Analysis

Data analysis is the process of inspecting, cleaning, describing, condensing and evaluating collected data with an aim of discovering useful information for purposes of making conclusions and supporting decisions. Quantitative data collected in the study was analyzed using SPSS in three steps:

a. Analysis of respondents – To establish the broadness and diversity of respondents, analysis of their personal data was carried out including gender, age, education level, length of service and their directorate or department in the institution.
b. Descriptive analysis – This involved describing, summarizing and discovering patterns in the information gathered from respondents mainly using frequency distribution tables.
c. Inferential analysis – This involved analyzing data on sets of variables for purposes of discovering relationships and prediction. Regression analysis was carried out where joint significance approach was applied as it is appropriate when mediation is involved (MacKinnon *et al.*, 2002). Two levels of regression were conducted involving the relationship between independent variables and mediating variables and that between mediating variables and the dependent variable.

CHAPTER FOUR: RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents and discusses the results obtained after analyzing the collected data. Analysis was done in three stages: respondent's biodata analysis; descriptive analysis and inferential analysis. Statistical Package for the Social Sciences (SPSS) version 27 was used to carry out the analysis and results presented in tables and charts.

4.2 Questionnaire Return Rate

A total of 116 questionnaires were returned representing 73% of the 158 number that were issued. Table 4.1 below presents the distribution of returned questionnaires per office.

Table 4.1: Questionnaire return per office

Office	**Issued**	**Returned**	**Percentage**
Nairobi	102	67	66%
Isiolo	5	5	100%
Machakos	5	5	100%
Bungoma	5	5	100%
Mombasa	6	6	100%
Kisumu	5	5	100%
Garissa	5	3	60%
Eldoret	5	5	100%
Kisii	5	3	60%
Malindi	5	4	80%
Nakuru	5	5	100%
Nyeri	5	3	60%
Totals	**158**	**116**	**73%**

4.3 Respondents Information

Data was collected from diverse respondents among EACC employees. In Section A of the questionnaire, they were required to provide personal information on gender, age, education level, length of service and the directorate or department they are placed in the institution. The provided information is presented in the charts below as a broad description of their diversity.

4.3.1 By gender

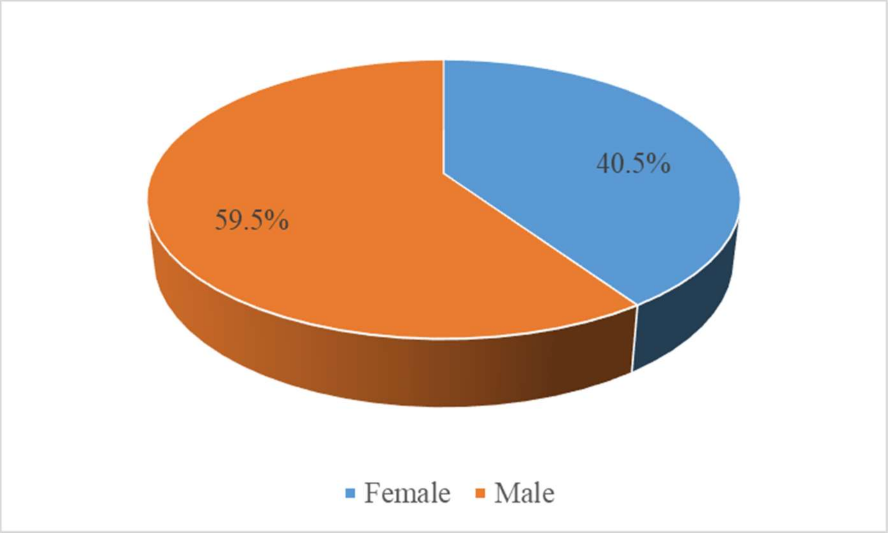

Figure 5: Respondents by gender

4.3.2 By directorate or department

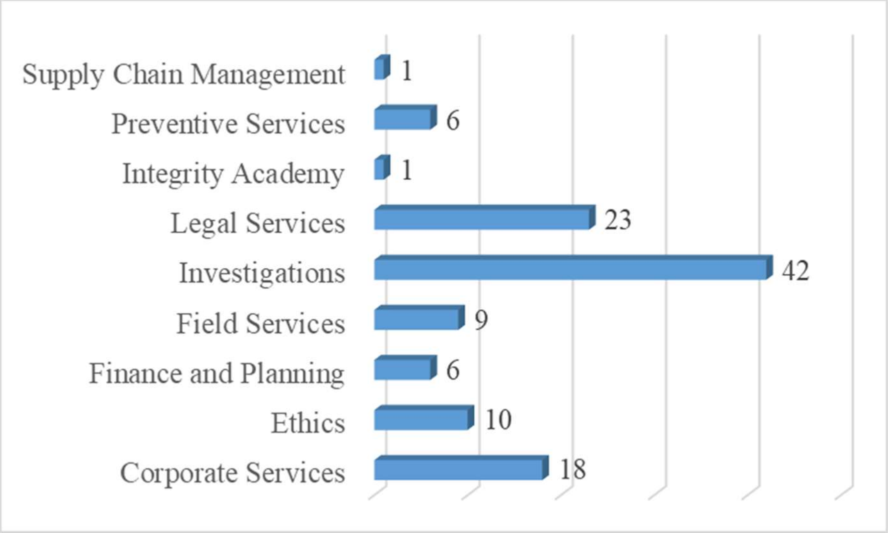

Figure 6: Respondents by directorate or department

4.3.3 By length of service

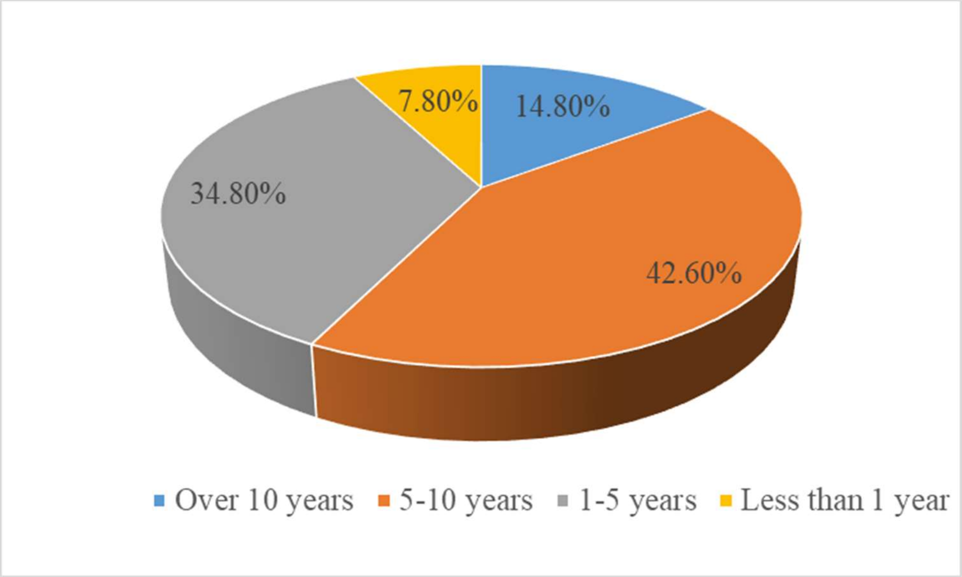

Figure 7: Respondents by length of service

4.3.2 By age

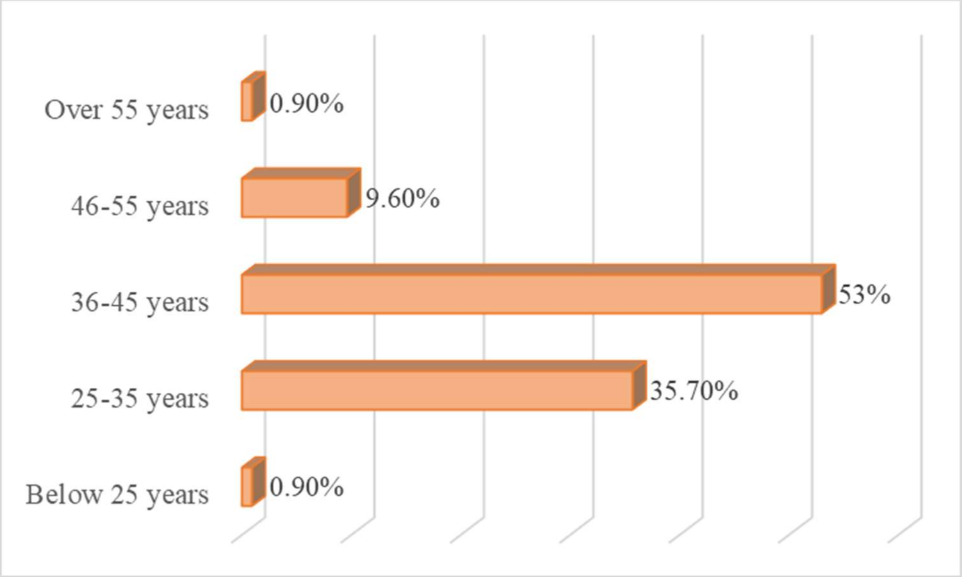

Figure 8: Respondents by age

4.3.5 By Level of education

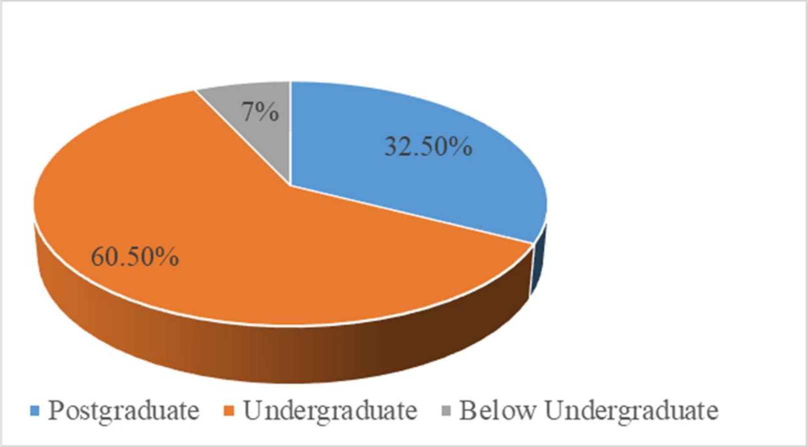

Figure 9: Respondents by level of education

4.4 Descriptive Statistics

This section describes the data collected on sections covering the various variables in the study as captured in sections B to E of the questionnaire. In the analysis, respondents who answered “Strongly Agree” and “Agree” in the five items likert scale are combined to represent agreement while those who answered with “Strongly Disagree” and “Disagree” are combined to represent disagreement.

4.4.1 Detection Probability

The Cyberloafing control system in EACC will most likely detect attempts by employees to cyberloaf by browsing non-job related websites, accessing social media, downloading non-work related materials, video streaming and accessing personal emails during working hours. Table 4.2 presents the percentages on possibility of detection per loafing behavior.

Table 4.2: Detection probability results

I Will be detected attempting to cyberloaf through:	**Agree**	**Disagree**	**Neutral**	**Total**
Browsing	80.2%	12%	7.8%	100%
Accessing social media	73.8%	10.3%	15.5%	100%

Downloading materials	81.9%	6%	12.1%	100%
Video streaming	80.2%	6.9%	12.9%	100%
Accessing personal mails	66.4%	13.8%	19.8%	100%

4.4.2 Enforcement Likelihood

89.6% of respondents confirmed that the control system blocks attempts to cyberloaf while 84.4% indicated that the system reports to management any of their attempts to cyberloaf. This confirms that the control system is able to enforce sanctions against the behavior. Table 4.3 presents the percentages on likelihood of enforcement

Table 4.3: Enforcement likelihood results

Enforcement action	**Agree**	**Disagree**	**Neutral**	**Total**
Will be blocked	89.6%	2.6%	7.8%	100%
Will be reported	84.4%	4.3%	11.3%	100%

4.4.3 Advance Notice

The analysis established that EACC most likely did not issue notice before introducing cyberloafing control to employees as 84.1% of the respondents indicated they were not given any notice. Table 4.4 presents the response on advance notice.

Table 4.4: Advance notice period results

Notice Period	**No.**	**Percentage**
No notice	95	84.1%
Up to 1 week	10	8.8%
1-2 weeks	2	1.8%
2-4 weeks	5	4.4%
One month or more	1	0.9%
Total	**113**	**100.0**

4.4.4 Cyberloafing Level

Analysis of response on cyberloafing activities shows that there is very little engagement in the behavior in all its five forms. Only a little engagement in personal emailing during working hours is reported. Table 4.5 presents the summary on cyberloafing engagement results.

Table 4.5: Engagement in cyberloafing activities results

Category	**Never**	**Rarely**	**Sometimes**	**Frequently**	**Constantly**	**Total**
Browsing	73.9%	22.6%	2.6%	0.9%	0%	100%
Social media	53%	35.7%	7%	4.3%	0%	100%
Downloading	70.4%	23.5%	5.2%	0.9%	0%	100%
Streaming	65.2%	26.1%	7%	1.7%	0%	100%
Emailing	30.4%	41.7%	22.6%	3.5%	1.7%	100%

4.4.5 Fairness Perception

Implementation of cyberloafing control in EACC has been done in a fair manner. 61.8% indicated that the application of control is applied consistently across all employees, 69.6% said the control process is fair and 73% confirmed that the control system is fair to them individually. Table 4.6 presents the details

Table 4.6: Perception of control fairness

Your response on	**Agree**	**Disagree**	**Neutral**	**Total**
Control is applied consistently across employees	61.8%	15.7%	22.6%	100%
Control process is fair	69.6%	5.2%	25.2%	100%
Control is fair to me	73%	6.1%	20.9%	100%

4.4.6 Employee Performance

According to the collected data, majority of employees are able to finish tasks within allocated time (89.6%), they meet requirements of their responsibilities (97.3%), are able to plan work well (96.5%), take up new responsibilities (96.7%) and are not involved in non-work activities (91.3%). Table 4.7 presents the details on employee performance

Table 4.7: Employee performance results

Category	**Agree**	**Disagree**	**Neutral**	**Total**
I'm able to finish work within time	89.6%	2.6%	7.8%	100%
I'm able to fulfil responsibilities	97.3%	0%	2.7%	100%
I'm able to plan work	96.5%	0%	3.5%	100%
I take new responsibilities	96.7%	1.7%	1.7%	100%
I'm not involved in non-job related activities	91.3%	0.9%	7.8%	100%

4.5 Cross-Validation of Performance Data

To confirm the validity of employee performance data provided by the respondents, a cross-validation was carried out by collecting the same data from supervisors. Census sampling was employed with the questionnaire issued to all 25 supervisors. 19 questionnaires were returned representing 76%. The comparison of means between the two samples is as per table 4.8

Table 4.8: Comparison of performance data: respondents against supervisors

Question	**Mean**	
	Respondents	**Supervisors**
Adequately complete assigned tasks within expected timeframes	4.32	4.06
Fulfil the responsibilities specified in their job descriptions	4.50	4.13
Plan their work sufficiently well	4.44	3.81
Always ready to take up any new job responsibilities as may be allocated from time to time	4.47	4.00
Don't involve themselves in non-job related activities during working hours	4.37	3.69

Overall	4.42	3.94

Strongly Disagree=1 Disagree=2 Neutral=3 Agree=4 Strongly Agree=5

The comparison shows that there is some variation between information provided by the respondents and that provided by the supervisors. Regression analysis was carried out based on both sets of data on employee performance. To apply supervisor's data, means per directorate were calculated and used to replace respondent's data on employment questions.

4.6 Inferential Statistics

The study conducted regression analysis to establish the significance, strength and direction of relationships and impacts between independent, mediating and dependent variables. Joint significance approach (MacKinnon *et al.*, 2002) was used where analysis was conducted in two stages: regression between independent variables and mediating variables; regression between mediating variables and dependent variables.

4.6.1 Regression analysis between advance notice, detection probability, enforcement likelihood and cybeloafing

The findings are as presented in Table 4.9.

Table 4.9: Regression analysis between independent variables and Cyberloafing

Model summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error**
1	.901^a	.813	.806	.256
a. Predictors: (Constant), Advance Notice, Detection Probability, Enforcement Likelihood				

Coefficients^a						
		Unstandardized Coefficients		**Standardized Coefficients**		
Model		**B**	**Std. Error**	**Beta**	**t**	**Sig.**
1	(Constant)	-.456	.258		-1.765	.080
	Detection Probability	-.317	.103	-.214	-3.078	.003
	Advance Notice	.368	.060	.502	6.115	.000

	Enforcement Likelihood	-.401	.113	-.302	-3.549	.000
a. Dependent Variable: Cyberloafing						

The findings in Table 4.9 shows that r=0.901. This indicates that advance notice, detection probability and enforcement likelihood have a strong relationship with cyberloafing in EACC. In addition, R^2 was 0.813 which indicate that 81.3% of the changes in cyberloafing in EACC are accounted for by advance notice, detection probability and enforcement likelihood.

Using the coefficients findings in Table 4.9, the multiple regression equation was:

Y= -0.456 - 0.317 DP + 0.368 AN – 0.401 EL

Where;

Y = Cyberloafing
DP = Detection Probability
AN = Advance Notice
EL = Enforcement Likelihood

The findings showed that when advance notice, detection probability and enforcement likelihood are held constant, the regression coefficient for cyberloafing in EACC was -0.456. It was however established that unit changes in detection probability and enforcement likelihood would lead to negative and significant change in cyberloafing in EACC as shown by regression coefficient of -0.317 and -0.401 respectively. This shows that detection probability and enforcement likelihood will significantly affect cyberloafing albeit negatively. In addition, the study established that unit change in advance notice would lead to positive and significant changes in cyberloafing in EACC as shown by regression coefficient of 0.368.

4.6.6 Regression analysis between advance notice, detection probability, enforcement likelihood and perceived fairness

Table 4.10: Regression analysis between independent variables and Perceived Fairness

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error**

1	.332[a]	.110	.086	.945
a. Predictors: (Constant), Advance Notice, Detection Probability, Enforcement Likelihood				

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-0.298	0.312		-0.955	.234
	Detection Probability	0.341	0.402	0.366	0.848	.398
	Advance Notice	0.118	0.023	0.139	5.130	.000
	Enforcement Likelihood	0.408	0.517	0.377	0.789	.432
a. Dependent Variable: Perceived Fairness						

The findings in Table 4.10 shows that r=0.332. This indicates that advance notice, detection probability and enforcement likelihood have a weak relationship with perceived fairness in EACC. In addition, R^2 was 0.110 which indicate that only 11% of the changes in perceived fairness in EACC are accounted for by advance notice, detection probability and enforcement likelihood.

Using the coefficients findings in Table 4.10, the multiple regression equation was:

Y= -0.298 + 0.341 DP + 0.118 AN + 0.408 EL

Where;

Y = Perceived fairness
DP = Detection Probability
AN = Advance Notice
EL = Enforcement Likelihood

The findings showed when advance notice, detection probability and enforcement likelihood are held constant, the regression coefficient for perceived fairness in EACC was -0.298. The study established that advance notice has a weak, positive and significant relationship with perceived fairness in EACC as shown by regression coefficient of 0.118 and a p-value of 0.00 which was less than 0.05.

However, the study established insignificant relationship between detection probability and enforcement likelihood and perceived fairness in EACC as shown by significances of .398 and .432 which are greater than recommended 0.05.

4.6.6 Regression analysis between Cyberloafing and Employee Performance

Table 4.11: Regression analysis between Cyberloafing and Employee Performance

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error**
1	-.731[a]	.534	.530	.285
a. Predictors: (Constant), Cyberloafing				

Coefficients[a]						
		Unstandardized Coefficients		**Standardized Coefficients**		
Model		**B**	**Std. Error**	**Beta**	**t**	**Sig.**
1	(Constant)	3.031	.109		27.807	.000
	Cyberloafing	-.806	.052	-.731	-15.500	.000
a. Dependent Variable: Employee Performance						

The findings in Table 4.11 shows that r=-0.731. This indicates that there is a strong and negative relationship between cyberloafing and employee performance in EACC. In addition, R^2 was 0.534 which indicate that 53.4% of the changes in employee performance in EACC are accounted for by cyberloafing.

Using the coefficients findings in Table 4.11, the multiple regression equation was:

Y= 3.031 - 0.806 CL

Where;

Y = Employee performance

CL = Cyberloafing

The findings showed when cyberloafing is held constant, the regression coefficient for employee performance in EACC was 3.031. The study established that unit changes in cyberloafing would lead to negative and significant change in employee performance in EACC as shown by regression coefficient of -0.806.

4.6.6 Regression Analysis for Perceived Fairness and Employee Performance

Table 4.12: Regression analysis between Perceived Fairness and Employee Performance

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error
1	.836[a]	.699	.696	.28390

a. Predictors: (Constant), Perceived Fairness

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.703	.110		24.528	.000
	Perceived Fairness	.459	.028	.836	16.116	.000

a. Dependent Variable: Employee Performance

The findings in Table 4.12 shows that r=0.836. This indicates that perceived fairness has a strong relationship with employee performance in EACC. In addition, R^2 was 0.699 which indicate that 69.9% of the changes in employee performance in EACC are accounted for by perceived fairness.

Using the coefficients findings in Table 4.12, the multiple regression equation was:

Y= 2.703 + 0.459 PF

Where;

Y = Employee performance

PF = Perceived Fairness

The findings showed when perceived fairness is held constant, the regression coefficient for employee performance in EACC was 2.703. It was established that unit changes in perceived fairness would lead to positive and significant change in employee performance in EACC as shown by regression coefficient of 0.459.

4.6.6 Regression analysis between cyberloafing and employee performance based on performance data from supervisors.

Table 4 13: Regression analysis between Cyberloafing and Employee Performance (based on supervisor's performance data)

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error**
1	-.591[a]	.513	.580	.281
a. Predictors: (Constant), Cyberloafing				

Coefficients[a]						
		Unstandardized Coefficients		**Standardized Coefficients**		
Model		**B**	**Std. Error**	**Beta**	**t**	**Sig.**
1	(Constant)	3.721	.104		21.807	.000
	Cyberloafing	-.713	.056	-.681	-14.900	.000
a. Dependent Variable: Employee Performance						

The findings in Table 4.13 shows that r=-0.591. This indicates that cyberloafing has a strong and negative relationship with employee performance in EACC. In addition, R^2 was 0.513 which indicate that 51.3% of the changes in employee performance in EACC are accounted for by cyberloafing.

Using the coefficients findings in Table 4.13, the multiple regression equation was:

Y= 3.721 - 0.713 CL

Where;

Y = Employee performance

CL = Cyberloafing

The findings showed when cyberloafing is held constant, the regression coefficient for employee performance in EACC was 3.721. The study established that unit changes in cyberloafing would lead to negative and significant change in employee performance in EACC as shown by regression coefficient of -0.713.

4.6.6 Regression analysis between perceived fairness and employee performance based on performance data from supervisors

Table 4 14: Regression analysis between Perceived Fairness and Employee Performance (based on supervisors performance data)

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error**
1	.810[a]	.629	.683	.27410
a. Predictors: (Constant), Perceived Fairness				

Coefficients[a]						
		Unstandardized Coefficients		**Standardized Coefficients**		
Model		**B**	**Std. Error**	**Beta**	**t**	**Sig.**
1	(Constant)	2.403	.130		24.008	.000
	Perceived Fairness	.402	.023	.796	15.993	.000
a. Dependent Variable: Employee Performance						

The findings in Table 4.14 shows that r=0.810. This indicates that there is a strong relationship between perceived fairness and employee performance in EACC. In addition, R^2 was 0.629 which indicate that 62.9% of the changes in employee performance in EACC are accounted for by perceived fairness.

Using the coefficients findings in Table 4.14, the multiple regression equation was:

Y= 2.403 + 0.402 PF

Where;

Y = Employee performance

PF = Perceived Fairness

The findings showed when perceived fairness is held constant, the regression coefficient for employee performance in EACC was 2.403. It was established that unit changes in perceived fairness would lead to positive and significant change in employee performance in EACC as shown by regression coefficient of 0.402.

4.7 Summary of Results and Resulting Framework

The findings establish that Detection Probability, Enforcement Likelihood and Advance Notice impact on Cyberloafing behavior with regression coefficients of -0.456, -0.401 and 0.368 respectively. The significance of the impacts was identified as 0.003, 0.000 and 0.000 respectively which is less than 0.05 as recommended. The three relationships are therefore retained in the final proposed framework.

The analysis also established that Advance Notice has a significant relationship with Perceived Fairness at a coefficient of 0.118 and significance of 0.000. This relationship was therefore retained in the final framework. However, it was established that there is no significant impact on Perceived Fairness by both Detection Probability and Enforcement Likelihood as the analysis resulted in significance measures of 0.398 and 0.432 respectively which are far greater than the recommended 0.05. The two relationships were therefore dropped in the final framework.

Finally, it was established that both Cyberloafing and Perceived Fairness have a significant impact on Employee Performance at regression coefficients of -0.713 and 0.402 respectively (based on employee performance data collected from supervisors). The significance of the impacts for both was 0.000 and therefore the two relationships were retained in the final framework.

The resulting final proposed framework was as presented in figure 10

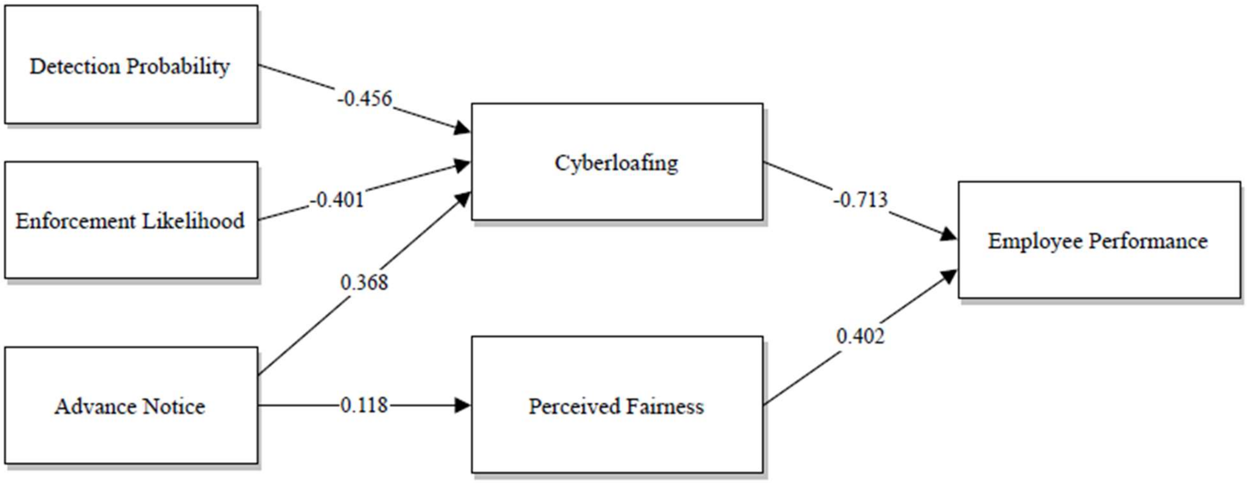

Figure 10: Resulting framework

CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

In the previous chapters of this study report, the research problem was defined, a theoretical background for the study was presented and a framework for establishing the impact of cyberloafing control on employee performance proposed. The framework was then tested using technological cyberloafing control in Ethics and Anti-Corruption Commission (EACC) Kenya resulting in a resultant framework. This chapter concludes the study through self-assessment by discussing the achievement of objectives and answers to the research questions. On the basis of the study findings, we also recommend considerations during implementation of technological cyberloafing control in institutions and suggest further research areas that should be considered on technological cyberloafing control.

5.2 Linking the Study Results to Objectives and Research Questions

Objective 1 of the study was to identify the aspects of technological cyberloafing control that impact on employee performance**.** Related research question was "What considerations should be taken into account when evaluating the impact of technological cyberloafing control on employee performance?"**.** The objective was achieved through a review of various literatures related to effectiveness of cyberloafing control systems, relationship between cyberloafing behavior and employee performance, the effect of control on employee's fairness perception and ultimate impact on their performance. From the review, it was established that the important aspects in establishing the relationship between cyberloafing control and employee performance are their detection capability, their capacity to enforce anti-loafing sanctions, pre-implementation notice and the effect of control on employee's fairness perception and cyberloafing levels.

Objective 2 was to propose a framework that can be used to evaluate the impact of technological cyberloafing control on employee performance. The related research question was "What is the appropriate framework for evaluating the impact of technological cyberloafing control on employee performance?"**.** The aspects identified in objective 1 were considered as constructs for the study and transformed into variables. Their relationships were established by review of different frameworks and models where they have been applied in previous research. This resulted in designing of the proposed framework presented as figure 4 in chapter two.

Objective 3 was to test the proposed evaluation framework using technological cyberloafing control in EACC. The related research questions were: “How does technological cyberloafing control impact on cyberloafing behavior in EACC?”; “How has technological cyberloafing control affected the perceptions of fairness among employees of EACC?” and “What is the impact of technological cyberloafing control on employee performance in EACC?**”.** The proposed framework’s variables were operationalized and measures identified. Data collection instrument in form of a structured questionnaire was designed, validated and used to collect data from a sample of EACC employees. The collected data was analyzed and relationships between the variables identified through regression.

It was established that implementation of technological cyberloafing control has resulted in reduction of engagements in the behavior in EACC necessitated mainly by the system’s capability to guarantee detection and enforce sanctions (blocking and reporting). Despite a majority of EACC employees reporting that they were not given advance notice before the control was applied, it was generally felt that the control’s implementation has been fair across the institution. This implies that other than advance notice, there are other factors in the implementation process that could have contributed to it’s being perceived fair. Finally, the study established that technological cyberloafing control has resulted in increase of employee performance necessitated by reduced cyberloafing and perceptions of fairness in the process. This is well illustrated by the regression coefficients of -0.713 and 0.402 for cyberloafing and perceived fairness respectively against employee performance.

Regression analysis also identified that Detection Probability and Enforcement Likelihood do not have a significant impact on mediating variable Perceived Fairness. The two relationships were therefore dropped in the final framework presented as figure 10 in chapter four.

5.3 Comparison of Findings With Previous Studies

From the study findings, technological cyberloafing control impacts on employee's performance through reduction of engagement in cyberloafing, not being perceived unfair and issuing pre-implementation advance notice. This is in concurrence with a number of previous studies in the area of cyberloafing control as identified in literature. In their studies, Zoghbi-Manrique-De-Lara and Olivares-Mesa (2010) and Ugrin and Michael Pearson (2013) identify that technological cyberloafing control results in reduction of cyberloafing while Jiang, Siponen and Tsohou (2020) established that internet monitoring results in improved staff performance by reducing cyberloafing behavior. Alder, Ambrose and Noel (2006) established that issuing advance notice results in a perception on fairness regarding application of internet monitoring among employees. The findings that detection capability, enforcement likelihood and advance notice are important aspects in determining the success of technological cyberloafing control are in tandem with previous studies (Alder, Ambrose and Noel, 2006; Ugrin and Michael Pearson, 2013).

5.4 Recommendations

Based on the study findings and those of related previous research, it is recommended that organizations need to put in place technological control measures against cyberloafing, since they have been proven to be effective. The fairness of their implementation should also be considered in order to bring about a positive impact on employee performance. To achieve fairness, the implementation process should not only include advance notice but also integrate unrestricted quotas and feedback as suggested in other literature (Henning *et al.*, 1997; Coker, 2013; Glassman, Prosch and Shao, 2015).

It is also recommended that during procurement, implementation and development of the control systems, detection capability, enforcement likelihood and advance notice should be considered as mandatory technical requirements. This is because they have been identified as key requirements for effectiveness of the solutions.

Finally, investments in IT systems must be justified through establishing their value towards organizational performance (Lin, 2007). It is therefore important that institutions determine the value of investing in technological cyberloafing control systems. This can best be achieved through evaluating their impact on employee performance which is the main casualty of engagement in cyberloafing behavior. It is therefore recommended that organizations regularly evaluate the impact of application of technological control on staff performance.

5.4 Limitations of the Study and Suggestions for Future Research

The study only focused on the value of technological cyberloafing control on employee performance. Apart from affecting performance, cyberloafing behavior also impacts on other aspects of organization ICT such as IT resources performance and security. Research should also be carried out on the impacts of technological control on these aspects. The framework was only tested using data collected from one public sector institution in Kenya. To validate the proposed framework further, it should be tested using data on control in other organizations both in public and private sector.

REFERENCES

Ahmad, S. I. A.-S. *et al.* (2014) ‘The Mediating Influence of Job Satisfaction on the Relationship between HR Practices and Cyberdeviance Ahmad’, *Journal of Marketing and Management*, 5(1).

Alder, G. S. *et al.* (2008) ‘Employee reactions to internet monitoring: The moderating role of ethical orientation’, *Journal of Business Ethics*. doi: 10.1007/s10551-007-9432-2.

Alder, G. S., Ambrose, M. L. and Noel, T. W. (2006) ‘The Effect of Formal Advance Notice and Justification on Internet Monitoring Fairness: Much About Nothing?’, *Journal of Leadership & Organizational Studies*, 13(1). doi: 10.1177/10717919070130011101.

Alder, G. S., Noel, T. W. and Ambrose, M. L. (2006) ‘Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust’, *Information and Management*, 43(7). doi: 10.1016/j.im.2006.08.008.

Askew, K. (2013) ‘The relationship between cyberloafing and task performance and an examination of the theory of planned behavior as a model of cyberloafing’, *Dissertation Abstracts International: Section B: The Sciences and Engineering*, 73(12-B(E)), p. No Pagination Specified. Available at: http://ovidsp.ovid.com/ovidweb.cgi?T=JS&CSC=Y&NEWS=N&PAGE=fulltext&D=psyc8&AN=2013-99120-471%5Cnhttp://opurl.bib.umontreal.ca:9003/sfx_local?sid=OVID:psycdb&id=pmid:&id=doi:&issn=0419-4217&isbn=9781267518965&volume=73&issue=12-B%28E%29&spage=No&pages=No+P.

Askew, K. *et al.* (2014) ‘Explaining cyberloafing: The role of the theory of planned behavior’, *Computers in Human Behavior*, 36, pp. 510–519. doi: 10.1016/j.chb.2014.04.006.

Bertino, E., Ferrari, E. and Perego, A. (2005) ‘Web content filtering’, in *Web and Information Security*, pp. 112–132. doi: 10.4018/978-1-59140-588-7.ch006.

Bhattacherjee, A. (2012) *Social Science Research: principles, methods, and practices*, *Textbooks collection*. doi: 10.1186/1478-4505-9-2.

Black, E. *et al.* (2013) ‘Online social network use by health care providers in a high traffic patient care environment’, *Journal of Medical Internet Research*, 15(5). doi: 10.2196/jmir.2421.

Blanchard, A. L. and Henle, C. A. (2008) ‘Correlates of different forms of cyberloafing: The role of norms and external locus of control’, *Computers in Human Behavior*, 24(3), pp. 1067–1084. doi: 10.1016/j.chb.2007.03.008.

Blau, G., Yang, Y. and Ward-Cook, K. (2006) ‘Testing a measure of cyberloafing’, *Journal of Allied Health*, 35(1), pp. 9–17.

Bock, G. W. and Ho, S. L. (2009) ‘Non-work related computing (NWRC)’, *Communications of the ACM*, 52(4), pp. 124–128. doi: 10.1145/1498765.1498799.

Brockner, J. *et al.* (1994) ‘Interactive Effects of Procedural Justice and Outcome Negativity on Victims and Survivors of Job Loss’, *Academy of Management Journal*, 37(2). doi: 10.5465/256835.

Cheng, L. *et al.* (2014) ‘Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory’, *Computers in Human Behavior*, 38, pp. 220–228. doi: 10.1016/j.chb.2014.05.043.

Coker, B. L. S. (2013) ‘Workplace Internet Leisure Browsing’, *Human Performance*. doi: 10.1080/08959285.2013.765878.

Colquitt, J. A. (2001) ‘On the dimensionality of organizational justice: A construct validation of a measure.’, *Journal of Applied Psychology*, 86(3). doi: 10.1037//0021-9010.86.3.386.

Conner, C. (2015) ‘Wasting time at work: The epidemic continues’, *Forbes*. Available at: http://www.forbes.com/sites/cherylsnappconner/2015/07/31/wasting-time-at-work-the-epidemic-continues/#9523b953ac16.

D’Arcy, J., Hovav, A. and Galletta, D. (2009) ‘User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach’, *Information Systems Research*. doi: 10.1287/isre.1070.0160.

Gibbs, J. P. (1977) ‘Crime, Punishment, and Deterrence.’, *American Journal of Sociology*, 83(1). doi: 10.1086/226534.

Glassman, J., Prosch, M. and Shao, B. B. M. (2015) ‘To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure’, *Information and Management*. doi:

10.1016/j.im.2014.08.001.

Greengard, S. (2000) *The high cost of cyberslacking*, *Workforce, volume 79, number 12*. Available at: https://www.workforce.com/2000/12/01/the-high-cost-of-cyberslacking/.

Hassan, H. M., Reza, D. M. and 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). doi: 10.5539/ibr.v8n3p91.

Henle, C. A., Kohut, G. and Booth, R. (2009) 'Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing: An empirical test of justice theory', *Computers in Human Behavior*. doi: 10.1016/j.chb.2009.03.005.

Henning, R. A. *et al.* (1997) 'Frequent short rest breaks from computer work: Effects on productivity and well-being at two field sites', *Ergonomics*. doi: 10.1080/001401397188396.

Holguin, E. S. (2016) *Strategies Functional Managers Use to Control Cyberloafing Behaviors*, *ProQuest Dissertations and Theses*. doi: 10.1111/j.1467-8616.2008.00521.x Malik,.

Hovorka-Mead, A. D. *et al.* (2002) 'Watching the detectives: Seasonal student employee reactions to electronic monitoring with and without advance notification', *Personnel Psychology*, 55(2). doi: 10.1111/j.1744-6570.2002.tb00113.x.

Ifinedo, P. (2012) 'Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory', in *Computers and Security*, pp. 83–95. doi: 10.1016/j.cose.2011.10.007.

Jandaghi, G. *et al.* (2015) 'Cyberloafing Management in Organizations', *Iranian Journal of Management Studies*, 8(3), pp. 335–349. doi: 10.22059/ijms.2015.52634.

Jia, H., Jia, R. and Karau, S. (2013) 'Cyberloafing and personality: The impact of the Big Five traits and workplace situational factors', *Journal of Leadership and Organizational Studies*, 20(3), pp. 358–365. doi: 10.1177/1548051813488208.

Jian, G. (2013) 'Understanding the Wired Workplace: The Effects of Job Characteristics on Employees' Personal Online Communication at Work', *Communication Research Reports*, 30(1), pp. 22–33. doi: 10.1080/08824096.2012.746221.

Jiang, H. (2020) ‘Understanding the impact of cyberloafing-related internet monitoring on employee job performance: A field experiment’, *40th International Conference on Information Systems, ICIS 2019*, pp. 1–15.

Jiang, H., Siponen, M. and Tsohou, A. (2020) ‘A field experiment for understanding the unintended impact of internet monitoring on employees: Policy satisfaction, organizational citizenship behaviour and work motivation’, in *27th European Conference on Information Systems - Information Systems for a Sharing Society, ECIS 2019*.

Karaoǐlan Yilmaz, F. G. *et al.* (2015) ‘Cyberloafing as a barrier to the successful integration of information and communication technologies into teaching and learning environments’, *Computers in Human Behavior*, 45, pp. 290–298. doi: 10.1016/j.chb.2014.12.023.

Khansa, L. *et al.* (2017) ‘To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls’, *Journal of Management Information Systems*. doi: 10.1080/07421222.2017.1297173.

Kim, S. and Choi, I. (2005) ‘A case study on the development of employee Internet management system’, in *Lecture Notes in Computer Science*. doi: 10.1007/11424857_131.

Koay, K. Y., Soh, P. C. H. and Chew, K. W. (2017) ‘Antecedents and consequences of cyberloafing: Evidence from the Malaysian ICT industry’, *First Monday*, 22(3). doi: 10.5210/fm.v22i3.7302.

Koopmans, L. *et al.* (2014) ‘Construct validity of the individual work performance questionnaire’, *Journal of Occupational and Environmental Medicine*, 56(3). doi: 10.1097/JOM.0000000000000113.

Kothari, C. (2004) *Research methodology: methods and techniques*, *New Age International*. doi: http://196.29.172.66:8080/jspui/bitstream/123456789/2574/1/Research%20Methodology.pdf.

Kothari, C. R. (2004) *Research Methodology: Methods & Techniques*, *New Age International (P) Ltd*. doi: 10.1017/CBO9781107415324.004.

Kumar, R. (2011) *Research Methology: A Step-by-Step Guide for Beginners*, *Igarss 2014*. doi: 10.1007/s13398-014-0173-7.2.

Li, S. M. and Chung, T. M. (2006) ‘Internet function and Internet addictive behavior’, *Computers in Human Behavior*, 22(6). doi: 10.1016/j.chb.2004.03.030.

Lim, P. K., Koay, K. Y. and Chong, W. Y. (2020) ‘The effects of abusive supervision, emotional exhaustion and organizational commitment on cyberloafing: a moderated-mediation examination’, *Internet Research*. doi: 10.1108/INTR-03-2020-0165.

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

Lim, V. K. G. and Chen, D. J. Q. (2012) ‘Cyberloafing at the workplace: Gain or drain on work?’, *Behaviour and Information Technology*, 31(4), pp. 343–353. doi: 10.1080/01449290903353054.

Lin, B. W. (2007) ‘Information technology capability and value creation: Evidence from the US banking industry’, *Technology in Society*, 29(1). doi: 10.1016/j.techsoc.2006.10.003.

Mackay, J. (2019) *The State of Work Life Balance in 2019*, *Rescue Time Blog*. Available at: https://blog.rescuetime.com/work-life-balance-study-2019/.

MacKinnon, D. P. *et al.* (2002) ‘A comparison of methods to test mediation and other intervening variable effects’, *Psychological Methods*, 7(1). doi: 10.1037/1082-989X.7.1.83.

Mastrangelo, P. M., Everton, W. and Jolton, J. A. (2006) ‘Personal use of work computers: Distraction versus destruction’, in *Cyberpsychology and Behavior*, pp. 730–741. doi: 10.1089/cpb.2006.9.730.

Munene, A. G. and Nyaribo, Y. M. (2013) ‘Effect of Social Media Pertication in the Workplace on Employee Productivity’, *International Journal of Advances in Management and Economics*, 2(2), pp. 141–150. Available at: http://www.managementjournal.info/index.php/IJAME/article/view/266.

Mwituria, E. (2015) ‘THE IMPACT OF SOCIAL NETWORKS ON EMPLOYEE PRODUCTIVITY IN COMMERCIAL BANKS IN KENYA: A CASE STUDY OF NIC BANK KENYA’, *Igarss 2014*, (1), pp. 1–5. doi: 10.1007/s13398-014-0173-7.2.

Nazareth, D. L. and Choi, J. (2015) ‘A system dynamics model for information security management’, *Information and Management*, 52(1), pp. 123–134. doi: 10.1016/j.im.2014.10.009.

Pearson, J. M. and Ugrin, J. C. (2008) ‘Exploring Internet abuse in the workplace: how can we maximize deterrence efforts?’, *Review of Business*, 28(2), pp. 29–40. Available at: http://xt6nc6eu9q.search.serialssolutions.com/?SS_Source=3&genre=article&sid=ProQ:&atitle=Exploring+Internet+Abuse+in+the+Workplace%253A+How+Can+We+Maximize+Deterrence+Efforts%253F&title=Review+of+Business&issn=0034-6454&date=2008-01-01&volume=28&issue=2&.

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

Sekaran, U. (2006) *Research method of business: A skill-building approach*, *Writing*. doi: http://www.slideshare.net/basheerahmad/research-methods-for-business-entire-ebook-by-uma-sekaran.

Sheriff, D. A. M. and Ravishankar, M. G. (2012) ‘The Techniques and Rationale of E-Surveillance Practices in Organizations’, *International Journal of Multidisciplinary Research*, 2. Available at: http://zenithresearch.org.in/images/stories/pdf/2012/Feb/ZIJMR/21_ZEN_VOL2ISSUE2_FEB12.pdf.

TrustRadius (2021) *Web Content Filtering Products*. Available at: https://www.trustradius.com/web-content-filtering#products (Accessed: 20 July 2021).

Ugrin, J. C. and Michael Pearson, J. (2010) ‘Understanding the effect of deterrence mechanisms on cyberloafing: Exploring a general deterrence model with a social perspective’, in *ICIS 2010 Proceedings - Thirty First International Conference on Information Systems*.

Ugrin, J. C. and Michael Pearson, J. (2013) ‘The effects of sanctions and stigmas on cyberloafing’, *Computers in Human Behavior*, 29(3), pp. 812–820. doi: 10.1016/j.chb.2012.11.005.

Urbaczewski, A. and Jessup, L. M. (2002) ‘Does electronic monitoring of employee internet usage work?’, *Communications of the ACM*, 45(1), pp. 80–83. doi: 10.1145/502269.502303.

Vitak, J., Crouse, J. and Larose, R. (2011) ‘Personal Internet use at work: Understanding cyberslacking’, in *Computers in Human Behavior*, pp. 1751–1759. doi: 10.1016/j.chb.2011.03.002.

Wang, J., Tian, J. and Shen, Z. (2013) ‘The effects and moderators of cyber-loafing controls: An empirical study of Chinese public servants’, *Information Technology and Management*, 14(4), pp. 269–282. doi: 10.1007/s10799-013-0164-y.

Weatherbee, T. G. (2010) ‘Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy’, *Human Resource Management Review*, 20(1), pp. 35–44. doi: 10.1016/j.hrmr.2009.03.012.

Whitty, M. T. and Carr, A. N. (2006) ‘New rules in the workplace: Applying object-relations theory to explain problem Internet and email behaviour in the workplace’, *Computers in Human Behavior*, 22(2), pp. 235–250. doi: 10.1016/j.chb.2004.06.005.

Yamane, T. (1967) ‘Statistics, An Introductory Analysis, 1967’, *New York Harper and Row CO. USA*.

Yarborough, M. (2021) ‘Moving towards less biased research’, *BMJ Open Science*, 5(1). doi: 10.1136/bmjos-2020-100116.

Young, K. S. (2001) *Employee Internet Abuse: A Comprehensive Plan To Increase Your Productivity and Reduce Liability*, *Netaddiction.Com*. Available at: www.netaddiction.com/articles/business.pdf.

Zoghbi-Manrique-De-Lara, P. (2012) ‘Reconsidering the boundaries of the cyberloafing activity: The case of a university’, *Behaviour and Information Technology*, 31(5), pp. 469–479. doi: 10.1080/0144929X.2010.549511.

Zoghbi-Manrique-De-Lara, P. and Olivares-Mesa, A. (2010) ‘Bringing cyber loafers back on the right track’, *Industrial Management and Data Systems*. doi: 10.1108/02635571011069095.

APPENDICES

Appendix 1: Respondents Questionaire

EVALUATING THE IMPACT OF TECHNOLOGICAL CYBERLOAFING CONTROL ON EMPLOYEE PERFORMANCE: A CASE OF ETHICS AND ANTI-CORRUPTION COMMISSION IN KENYA

Dear participant,

The information being collected through this questionnaire is for purpose of fulfilling the requirements of a Master's Degree in Information Technology Management (Msc.ITM) in the University of Nairobi by undertaking a research project on the impact of technological cyberloafing control on employee performance. The information provided will strictly be used for the research work and will be treated as confidential data. Your anonymity is respected and provided for and therefore you are not required to indicate your name in the questionnaire.

While participation in this data collection is purely voluntary, you are humbly requested to participate and assist in completion of the research.

The exercise should take you between 3-5 minutes.

Kindly answer the questions by ticking the boxes provided or writing brief statements as will be applicable.

SECTION A: BACKGROUND INFORMATION

1. Which directorate or department are you placed in the organization?

Investigations □

Legal Services □

Ethics and Leadership □

Field Services □

Preventive Services □

Corporate Support Services □

Finance and Planning □

Supply Chain Management □

Internal Audit □ National Integrity Academy □

2. In which office are you based

Nairobi □ Nakuru □

Mombasa □ Machakos □

Kisumu □ Malindi □

Eldoret □ Garissa □

Isiolo □ Bungoma □

Kisii □ Nyeri □

3. For how long have you worked with EACC?

Over 10 years □ 5-10 years □

1-5 years □ Less than 1 year □

4. Age bracket?

Below 25yrs □ 25yrs-35yrs □ 36yrs-45yrs □

46yrs-55yrs □ Over 56yrs □

5. Your gender?

Male □ Female □

6. Level of education?

Postgraduate □ Undergraduate □ Secondary/High School □

SECTION B: DETECTION PROBABILITY

7. On the statement below, please indicate the extent to which you agree or otherwise with the stated regarding the possibility of being detected by internet, email and ICT facilities usage monitoring and control system in EACC when attempting to use ICT facilities in the categorized manner

I will be caught by the monitoring and control system in EACC if I attempt to do the following during working hours:	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
a) Browsing non-work related websites e.g shopping, pornography, drugs, betting and games websites					
b) Visiting social media platforms e.g facebook, twitter.					
c) Downloading non-work related materials e.g music, movies					
d) Visiting video sharing sites e.g youtube					
e) Checking personal non-work related emails					

SECTION D: ENFORCEMENT LIKELIHOOD

8. On the statements below, please indicate the extent to which you agree or otherwise with the stated regarding the enforcement options employed by the monitoring and control system in EACC after detecting internet, email and ICT facilities misuse

STATEMENTS	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
The monitoring and control system will block access to objectionable websites and materials on detecting attempts to access them					
The monitoring system will report to management/supervisor any attempts to misuse internet, email and other ICT facilities for disciplinary action					

SECTION C: ADVANCE NOTICE

9. On the statement below, please make a choice of your experience regarding being advised in advance that your internet, email and ICT resources engagement will be monitored and controlled in EACC.

STATEMENT	**No Notice given**	**One week or less**	**1 – 2 weeks**	**2- 4 weeks**	**One month or more**
What notice period were you given before monitoring and control of your internet and email activities was initiated in EACC?					

SECTION E: CYBERLOAFING

10. Please rate the frequency with which you engage in the listed activities in office during working hours

Activity	**Never**	**Rarely (few times per month)**	**Sometimes (few times per week)**	**Frequently (few times per day)**	**Constantly**
a) Browsing non-work related websites e.g shopping, pornography, drugs, betting and games websites					
b) Visiting social media platforms e.g facebook, twitter.					
c) Downloading non-work related materials e.g music, movies					
d) Visiting video sharing sites e.g youtube					
e) Checking personal non-work related emails					

SECTION F: PERCEIVED FAIRNESS

11. On the statements below, please indicate the extent to which you agree or otherwise with the stated regarding the fairness of monitoring and control of internet, email and other ICT facilities in EACC

STATEMENTS	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Monitoring and control of internet, email and other ICT facilities usage is applied consistently across all employees					
Process of monitoring and control of internet, email and other ICT resources usage is fair					
I find monitoring and control of usage of internet, email and other ICT facilities in EACC process fair to me					

SECTION G: EMPLOYEE PERFORMANCE

For each of the following statements, pick the extent to which you agree or disagree with its description of how you undertake your work activities

STATEMENTS	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I adequately complete assigned tasks within expected timeframes					
I fulfil the responsibilities specified in my job descriptions					

I plan my work sufficiently well					
I'm always ready to take up any new job responsibilities as may be allocated from time to time					
I don't involve myself in non-job related activities during working hours					

Thank you for taking your time to respond

Appendix 2: Supervisor's Questionnaire

EVALUATING THE IMPACT OF TECHNOLOGICAL CYBERLOAFING CONTROL ON EMPLOYEE PERFORMANCE: A CASE OF ETHICS AND ANTI-CORRUPTION COMMISSION IN KENYA

Dear participant,

The information being collected through this questionnaire is for purpose of fulfilling the requirements of a Master's Degree in Information Technology Management (Msc.ITM) in the University of Nairobi by undertaking a research project on the impact of technological cyberloafing control on employee performance. The information provided will strictly be used for the research work and will be treated as confidential data. Your anonymity is respected and provided for and therefore you are not required to indicate your name in the questionnaire.

While participation in this data collection is purely voluntary, you are humbly requested to participate and assist in completion of the research.

The exercise should take you about 3 minutes.

EMPLOYEE PERFORMANCE

For each of the following statements, pick the extent to which you agree or disagree with its description of how the staff under you undertake their work

STATEMENTS	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
They adequately complete assigned tasks within expected timeframes					
They fulfil the responsibilities specified in their job descriptions					
They plan their work sufficiently well					

They are always ready to take up any new job responsibilities as may be allocated from time to time					
They don’t involve themselves in non-job related activities during working hours					