RESEARCH ARTICLE:

Evaluation of Managerial Tools for Preventing and Controlling Cyber-Loafing among Administrative Staff: A Case Study of a Selected Municipality in KwaZulu-Natal, South Africa

Nonhlanhla Beata Mkhize[1], Celani John Nyide[2] and Peggy Pinky Mthalane[3]

Received: 12 December 2023 **|** **Revised:** 28 August 2024 **|** **Published:** 16 September 2024

Reviewing Editor: Dr. Folasayo Olalere, The Open University

Abstract

Organisations have implemented systems to address cyber-loafing, but these measures are often insufficient to completely prevent employees from engaging in such activities. Consequently, the manager's role in mitigating cyber-loafing becomes crucial. However, the specific strategies employed by managers to reduce and control cyber-loafing remain unclear. This paper endeavours to evaluate the managerial tools used to prevent and control cyber-loafing among administrative staff in the workplace. Furthermore, it proposes effective measures to mitigate this phenomenon. The study employed a mixed-methods approach, combining qualitative and quantitative research methodologies. Purposive sampling was utilised, with a sample size of 156 administrative staff for the quantitative study and 11 managers and supervisors for the qualitative segment. The quantitative data revealed that administrative staff use company internet and computers to perform cyber-loafing activities. Managers and supervisors can apply various tools, including software monitoring systems, internet policies, and employee monitoring, to control cyber-loafing activities. The general deterrence theory (GDT) framework was used to explain the tools used to curb cyber-loafing in the study under investigation. Additionally, other deterrent mechanisms and organisational control measures were identified and discussed in specific instances. This research contributes to a comprehensive understanding of the role of managers in addressing cyber-loafing and proposes practical tools and strategies that can be implemented by organisations to effectively mitigate this phenomenon. By enhancing managerial approaches to cyber-loafing, organisations can improve productivity and ensure a secure work environment.

Keywords: *administrative staff; cyber-loafing; deterrent mechanisms; general deterrence theory; management tools*

Introduction

Computer technology and the Internet have eased and improved communication across organisations (Jandaghi *et al*., 2015). These technological resources have not only improved communication methods, but they have also boosted productivity and enhanced operational processes. Despite the numerous advantages the Internet has brought to organisations, cyber-loafing remains a serious challenge for many organisations. Taking advantage of the innovation of the Internet, computers, and networks, employees have developed habits of escaping from their work responsibilities and using company resources and the Internet for non-work-related tasks during company hours (Elciyar and Simsek, 2021). The term "cyber-loafing" refers to the practice of employees utilising their work time for non-work-related online activities, such as social media use, web browsing, or checking and replying to personal email. Although the term was first used in 1995, it gained traction in 2002 following the publication of a study on the subject in the Organizational Behaviour Journal. Early studies were primarily concerned with the

[1] Durban University of Technology, nonhlanhla.beata@gmail.com | https://orcid.org/0009-0004-4334-2884
[2] Durban University of Technology, nyidec@dut.ac.za | https://orcid.org/0000-0003-2883-0092
[3] Durban University of Technology, gumedepp@dut.ac.za | https://orcid.org/0000-0001-7003-5311

DUT
DURBAN UNIVERSITY OF TECHNOLOGY
INYUVESI YASETHEKWINI YEZOBUCHWEPHESHE
AFRICAN JOURNAL OF INTER/MULTIDISCIPLINARY STUDIES
OPEN ACCESS

detrimental and ineffectual consequences that a business could experience when its workers engaged in cyber-loafing.

This pattern has escalated to a degree that adversely affects the organisation's productivity, with an increasing number of employees neglecting their tasks to indulge in cyber-loafing (Jandaghi *et al*., 2015). As a result, organisations are faced with a myriad of challenges, which include identity theft, time squandering, and a lack of creativity as a result of employees' fragmented focus during cyber-loafing (Kasap, 2019). Abbasi (2018) asserts that cyber-loafing among staff has cost organisations billions of dollars in production losses, internet costs and internet security issues. This leaves organisations in a vulnerable position, negatively affecting company policy and exposing the company to serious risks of security breaches. Cyber-loafing also affects the employees' abilities and the quality of production in the long run (Abbasi, 2018). It also encourages internet gambling, which wastes useful working hours (Rahimnia and Mazidi, 2015). The Internet and computers will continue to play a pivotal role in the Fourth Industrial Revolution, and companies will continue to face serious problems dealing with cyber-loafing among employees during work hours (Jandaghi *et al*., 2015). It is without a doubt that cyber-loafing jeopardises organisations' efficiencies and security. As a result, managers strive to reduce the risks associated with employee cyberloafing. These dangers include decreased output and the possibility of malware or other security issues.

Organisations are reported to have implemented systems to curb cyber-loafing, such as software programmes designed to monitor, track, and lock illegal use of company internet facilities (Aku, 2017). Unfortunately, these systems do not completely prevent employees from engaging in cyber-loafing; hence, the role of managers in mitigating this act cannot be ignored (Aku, 2017). According to research, managers lack the necessary skills and tactics for minimising workplace cyber-loafing (Abbasi, 2018; Kaptangil, 2021; Toker and Baturay, 2021). Some of these incidents are not properly addressed because of the cost of dealing with or resolving this behaviour in the workplace. This paper argues that managers have not evaluated the effectiveness in reducing and controlling cyber-loafing (Holguin, 2016), nor have they fully investigated the need to discover new ones. Therefore, this study aimed to identify cyber-loafing activities that are common among administrative staff in the workplace, and evaluate existing tools used by managers to prevent and control cyber-loafing among the administrative staff. This was achieved by using a case study of a selected municipality in the province of KwaZulu-Natal in South Africa.

Literature Review

The term cyber-loafing was first used by Kamins in 1995 (Aku, 2017; Elciyar and Simsek, 2021). Cyber-loafing is described as intentional or voluntary activities by employees during working hours, using the company's internet and computer resources for personal activities or activities unrelated to their official assignments, thereby neglecting their duties (Jandaghi *et al*., 2015). To have a better insight into the cyber-loafing challenges in the workplace, it is pivotal to begin with the discourse on the types and categories of cyber-loafing.

Cook (2017) divides cyber-loafing into two components: browsing and emails. Browsing actions involve visiting websites for entertainment, financial services, news, social networking, shopping, sports, and pornography. Emailing involves receiving and sending personal emails using a company computer and the Internet (Kasap, 2019). Interactive cyber-loafing is when individuals play live online games, chat online, make live posts on social networking sites, and download information (Aku, 2017). Cyber-loafing is further categorized into minor and serious cyber-loafing based on the severity of the deviant behaviour (Elciyar and Simsek, 2021). Cyber-loafing typology was developed based on the device or computer in the workplace (Kaptangil, 2021). Various communication tools can be linked to cyber-loafing. Smartphones, smartwatches, and tablets are part of the communication technologies that enable users to access cyberspace. It is important to note that employees do not only need to work on computers to engage in cyber-loafing activities; they can use their personal devices to connect to their company's Wi-Fi and engage in cyber-loafing activities.

Cyber-loafing behaviour can be divided into four categories based on the underlying behavioural intent (Radebe, 2020). These include classifying cyber-loafing as a development behaviour, recovery behaviour, addiction behaviour, or deviant behaviour (Kasap, 2019; Malik *et al*., 2018; Şimşek and Şimşek, 2019). When cyber-loafing compromises an individual's job performance and detrimentally affects organizational productivity and performance, it is classified as deviant behaviour. Cyber-loafing is an additional behavioural concern for individuals who are suffering from internet addiction in their personal lives, often leading problems with their professional lives, such as strained interpersonal relationships and decreased productivity. Cyber-loafing activities that occur due to employee addiction to the Internet are classified as addictive behaviours (Toker and Baturay, 2021). From an organisational perspective, this behaviour is unacceptable as it neutralises employees' work satisfaction and negatively impacts their mental health (Abbasi, 2018). Finally, cyber-loafing behaviour can be considered a development tool if employees use the Internet to learn new things to improve their work conditions (Kaptangil, 2021). Employers can benefit from such activities by developing their innovative skills and enhancing their working abilities, not to mention the positive impact they have on an organisation. In such a case, cyber-loafing is a development performance (Abbasi, 2018).

For the organisation to evaluate control measures, it is important to distinguish between the two types of cyber-loafing based on the severity of the cyber-loafing deeds. These are minor, not severe, and extreme cyber-loafing behaviours (Jandaghi *et al*., 2015). Minor or not severe cyber-loafing activities range from sending or receiving personal emails using the company internet and computer during working hours to reading news on the Internet. On the other hand, actions that are extreme or severe cyber-loafing include playing games, accessing adult websites, logging on to social media, internet banking, shopping online, job searching, downloading non-work-related and personal stuff, and gambling online (Jandaghi *et al*., 2015; Elciyar and Simsek, 2021). Although certain activities are generally perceived as severe or extreme cyber-loafing actions, for example, playing online games and viewing adult websites, cultural perceptions and values are significant determinants in the categorisation of cyber-loafing activities (Sampat and Basu, 2017). Organisations must understand and separate these two types of cyber-loafing to establish appropriate tools for each category and develop measures for controlling or mitigating such behaviour among their employees.

In recent years, the use of internet technology has increased in the workplace to improve employee performance. Cyber-loafing is recognised as a workplace misconduct that impacts employees' performance and efficiency (Dmour *et al*., 2019; Hadlington and Parsons, 2017; Khansa *et al*., 2018). It has been noted that male employees are predisposed to higher cyber-loafing behaviours than female employees (Malik *et al*., 2018). Cyber-loafing can cause serious damage to the company; employees who perceive themselves as powerless in their work environment are likely to engage in cyber-loafing activities. Job satisfaction and organisational justice have been identified as major influences or motives of cyber-loafing in an organisation (Malik *et al*., 2018). An employee's cyber-loafing activities do not depend only on psychological factors but also on other factors like organisational factors, for example, the work environment, and personal ones like the individual needs of the employees (Kaptangil, 2021). An employee who engages in cyber-loafing behaviour not only negatively impacts their organisation financially but also tends to compromise job quality, which violates the expected job standards (Elciyar and Simsek, 2021). Furthermore, it wastes employees' time, which results in a substantial loss of organisational productivity. Kaptangil (2021) states that the loss due to these activities comes in the form of annual costs for the organisation due to security violations, viruses, lower job productivity, identity and information theft, hacking, time-wasting, and nonworking internet usage, and that this represents a significant loss to companies and organisations. There are direct and indirect costs associated with cyber-loafing (Elciyar and Simsek, 2021). Indirect costs result from procedures and actions that destroy brand images, thus leading to a loss of customer loyalty and customers losing trust in the organisation (Dooly, 2021). Many companies do not report cyber-loafing incidents that occur in their work environment, which increase organisational costs (Abbasi, 2018).

Recent studies indicate that organisations have begun to legalise the use of monitoring systems in the workplace to curb cyber-loafing activities (Koay and Poon, 2022). For the organisation to control or determine which strategy works effectively, managers must have a clear understanding of the cyber-loafing phenomenon. As claimed by Kasap (2019), many employees use their company's internet to browse non-work-related websites, and the majority of these individuals send and receive personal emails at the workplace during working hours. It is estimated that employees spend two to three hours a week cyber-loafing, which is equivalent to half an hour a day. A large number of employees engage in cyber-loafing activities to perform their duties, such as news, social media, online shopping, entertainment and lifestyle, sports, and travel (Kasap, 2019). The severity of cyber-loafing behaviour differs from person to person. While some individuals may use the Internet excessively for work purposes, some may misuse it for shopping, personal communication, gaming, or personal business purposes during the time allocated for work (Ozdamli and Ercag, 2021).

Since cyber-loafing negatively impacts employee performance and productivity, organisations have a huge responsibility to control and reduce this behaviour. While organisations have adopted various forms of technical deterrence mechanisms, cyberloafing continues to increase. The manager's role in mitigating this behaviour by employees is not clear, hence the need to evaluate and review the existing cyber-loafing mitigation tools and strategies. The general deterrence theory (GDT) was adopted to investigate and explain possible mechanisms and strategies for preventing and mitigating cyber-loafing activities among employees. This theory is based on an imposed regulatory model and emphasises regulatory principles imposed by organisations on their employees through the threat of sanctioning (Song *et al*., 2021). GDT, as shown in Figure 1, consists of three categories that influence legal behaviour: sanctions, detection, and enforcement. Furthermore, this theory is based on the idea that human behaviour is rational to a degree and may be influenced by incentives, particularly negative incentives such as those found in formal punishments (Song *et al*., 2021).

According to GDT, the prospect of retribution, when weighed against the potential reward of engaging activities, can significantly influence employee intentions and actions (Song *et al*., 2021). GDT has been widely used to explore and explain processes that are aimed at lowering employee participation in unproductive workplace deeds such as cyber-loafing (Song *et al*., 2021). GDT is most used in criminal justice, ethics, and, more recently, cyber-loafing (Ozdamli and Ercag, 2021). It proposes a system in which the consequences of improper behaviour are fully specified, revealed, and punished as a result of qualified discovery methods. According to the GDT, two types of cyber-loafing mitigation strategies that appear to lower cyber-loafing activities are the use of workplace internet policies and electronic monitoring systems (Hassan *et al*., 2015). Using GDT, Ugrin and Pearson (2013) evaluated the effectiveness of appropriate use policies and electronic monitoring in curbing cyber-loafing in the workplace. According to Song *et al*. (2021), individuals tend to act accordingly if the punishment is extreme compared to the benefits derived from the individual's actions. Some scholars have discovered that there is a relationship between the effectiveness of deterrence methods and individual characteristics. Ugrin and Pearson (2013) noted that deterrent mechanisms such as threats of sanctions and termination of employment were effective in preventing some types of cyber-loafing activities. The organisation needs to properly explain to its workers the detrimental effects of cyber-loafing. Increasing awareness among employees of the implications of cyber-loafing on company information security can serve as a tool to mitigate cyber-loafing activities in the workplace (Hadlington and Parsons, 2017). However, findings from Saleh *et al*. (2018) indicate that the certainty of detection and the threat of sanctions and punishments lead individuals to hide their cyber-loafing activities. Due to this, employees prefer to use their smartphones when engaging in cyber-loafing, especially when they are sure of being detected by company monitoring systems.

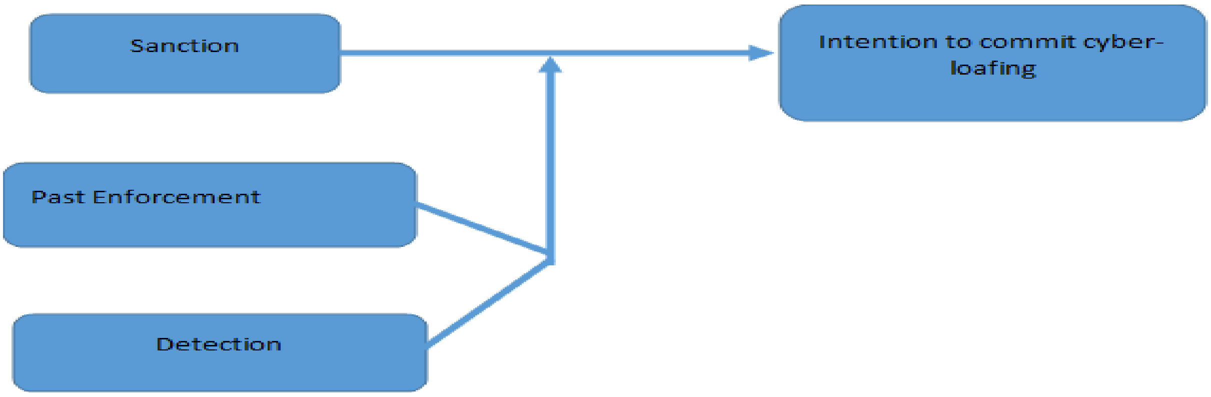

Figure 1: Deterrence model in cyber-loafing (Ugrin and Pearson, 2013)

The sanctioning component of the GDT model is crucial for individuals' trust in its scope. The severity of the promised consequences is a deciding factor in whether or not employees engage in undesirable behaviour, such as cyber-loafing (Hassan *et al*., 2015). In other words, the likelihood of the promised penalties occurring is a major deciding factor in deterring employees from engaging in cyber-loafing activities (Hassan *et al*., 2015; Song *et al*., 2021). For penalties or punishments to be effective as deterrents, they must be immediate and unlikeable (Song *et al*., 2021). Furthermore, from the standpoint of cyber-loafing, organisations that impose more punishments are more likely to have a low number of people involved in cyber-loafing (Hassan *et al*., 2015). When a business has punishments in place, employees are less likely to engage in cyber-loafing. According to this idea, when substantial costs and repercussions are associated with their actions, people tend to avoid actions that could lead to breaking the law or becoming offenders. For instance, the availability of appropriate punishments and awareness of previous enforcement are significant factors. The use of deterrents as a technique for reducing the high rate of cyber-loafing among employees has been criticised for its many flaws. For instance, the rise in Internet abuse has been associated with threats of legal punishment. Furthermore, social norms and observability were said to have a significant impact on the effectiveness of deterrence in reducing employee cyber-loafing (Song *et al*., 2021). However, the perceived certainty and severity of possible cyber-loafing punishments were found to mitigate the impact of observability on employee cyber-loafing. The threat of punishment was almost ineffective at curbing cyber-loafing behaviour among employees due to earlier experience or the possibility of punishment avoidance (Hensel and Kacprzak, 2021). According to Ugrin and Michael (2013), the effect of possible fines on cyber-loafing will be tempered by an increased chance of discovery and evidence of prior enforcement for less abusive manners. This suggests that employees who are aware of formal detection methods are less likely to engage in cyber-loafing operations.

Determining whether the certainty or severity of punishments deters offenders from engaging in rebellious conduct is a contentious issue. Real data from both sides of the argument demonstrates that this aspect of deterrence has been shown to significantly influence the use deterrent techniques to stop cyber-loafing. The severity of sanctions is more important than the certainty of punishment (Ezeh *et al*., 2018). Employee perceptions of the severity of punishments have a negative influence on employee intention to misuse the organisation's internet resources, according to Song *et al*. (2021), but this effect is not seen evident for workers' perceived certainty of sanctions. Similarly, Radebe (2020) found that workers' intentions to break their organisation's internet service security policy were influenced by the perceived severity of punishments, but the perceived certainty of sanctions had no statistically significant effect. In contrast to the foregoing, empirical data suggests that the certainty of punishment, rather than the harshness of sanctions, deters workers from engaging in a rebellious manner such as cyber-loafing. Employees from various organisations had a statistically significant influence on their desire to comply based on the certainty of discovery (Song *et al*., 2021).

Methodology

In this study, the researchers employed a mixed-methods approach, which combines the elements of qualitative and quantitative research approaches. This method was assumed to provide an in-depth understanding of the phenomenon being investigated and to strengthen the validity of the findings (Dudovskiy, 2016). The researchers balanced the limitations of each method, by combining qualitative and quantitative methods, and doing so provided strong evidence, that bolstered thethe findings while ascertaining the achievement of the study's objectives (Creswell, 2017). This study's population consisted of managers, supervisors (12 in total for the qualitative research approach) and administrative personnel from a Customer Service Centre in a selected Municipality within the province of KwaZulu-Natal, South Africa. The sample size was determined through purposive sampling. Considering that this study used mixed-method research, the sample sizes were categorised into quantitative (for research objective 1) and qualitative for research objective 2) as discussed below.

The sample size for the quantitative data was calculated based on a 95% confidence level with an 80% proportion of the target population at 0.005 acceptable margins of error. The formula used for calculation was:

$N = \{Z^2 * \Sigma^2 * [N / (N - 1)] / \{ME^2 + [Z^2 * \Sigma^2 / (N - 1)]\}$. Whereby N= Sample Size; Z= Confidence Level; Σ = Alpha; P= Proportion and ME= Margin of error. The sample size for the administrative staff was 156.

The researchers used Statistical Package for the Social Sciences (SPSS, Version 27) to analyse the quantitative data. Frequencies, cross-tabulation and bivariate statistics were used to analyse the data for the quantitative research strategy (Polit and Beck 2012: 63). The statistical measures, analyses, and trustworthy data interpretation, employed by the researcher concurred with the statistical analysis.

As determined by Nayak and Singh (2021), the rules for selecting the number of respondents to partake in a study depend on the research methodology. According to Patton (1990), there are no specified rules for measuring the sample size in qualitative research. It depends on the dimensions (depth or breadth) in which the researcher seeks to inquire. Hence, the sample size for this study was 12 managers and supervisors, which conforms with Creswell (2017: 58), who indicated that 12 participants (managers and supervisors) suffice for a qualitative study. The researchers used the narrative technique to analyse data acquired through interviews for the qualitative research methodology. Mitchell and Egudo (2003: 6) describe a narrative method as a social science strategy that incorporates the use of storytelling methodology to assist the researcher to gain insight into organisational information and aid in the transmission of diverse tacit information.

Questionnaires were used to obtain quantitative data. Only administrative personnel were given the opportunity to respond to the survey questionnaires in this study. Questionnaires were handed out physically to 156 participants. The questionnaire contained items in the form of a five-point Likert scale. These items were used to identify cyber-loafing activities that are common among administrative staff in the workplace. Moreover, interviews were conducted to acquire qualitative data. Interviews were conducted in person with managers and supervisors to evaluate existing tools used by managers to prevent and control cyber-loafing among the investigated administrative staff. Out of 156 participants, 101 participants responded to the questionnaires, yielding a response rate of 65%. According to Taherdoost (2016), the normal or appropriate sample size for quantitative research studies is 40% of the participants. Therefore, this study's response rate was deemed appropriate. For the qualitative part of this study, a total of 11 participants participated, yielding a response rate of 92%. Kumar (2016) recommends a minimum of 10 participants per qualitative research studies. This means that the findings of this study are based on an acceptable response rate. The researchers then used SPSS, Version 27 to analyse the quantitative data. The researcher used frequencies, cross-tabulation, and bivariate statistics to analyse the data for the quantitative research strategy (Polit and Beck, 2012). Furthermore, the researchers used the narrative technique to analyse data acquired through interviews for the qualitative research methodology.

Cronbach's alpha was utilized for the reliability testing in this study. The main purpose was to test the consistency and reliability of the research questions. The results of this study show that the internal consistency was 0.782, which is a good measure (Taherdoost, 2016). To ensure the study's credibility, the researchers endeavoured to eradicate any bias and generate convincing findings. Triangulation of the data was utilised to check for similarity and diversity of various replies to assess internal consistency and efficient dependability to the investigation. This strategy, according to Dudovskiy (2018), is the rewriting of stories told through interviews. The study's validity was guaranteed by conducting a pre-test. Before the final questionnaires were handed to the participants, the questionnaire was subjected to pretesting to identify errors that may be encountered by the participants (Mohajan, 2018). In terms of ethical clearance, written permission to conduct the study was obtained from the Faculty of Accounting and Informatics Research Ethics Committee (FREC).

Results

This section begins by presenting the quantitative data analysis gathered through the questionnaire. Participants were asked 11 questions. The following activities were identified based on the questions: online shopping, gaming and sports, exploring holiday and travel sites, browsing social media sites, checking weather forecasts, and accessing job search sites, study sites, online news, online magazines, auction sites, and personal e-mails Figure 2 illustrates the cyber-loafing activities prevalent among administrative staff at a selected eThekwini Municipality. The activities were ranked from the most frequently used to the least used. The most prevalent cyber-loafing activities were "accessing job search sites" and "personal e-mails". It can be assumed that staff at the selected municipality are job hunting and checking their e-mails to see if there are any job offerings or notifications that have come through. Figure 2 shows that cyber-loafing was represented in varying percentages depending on the loafing activity.

Accessing personal e-mails was rated the highest among other activities at 96.04%. It can then be concluded that the investigated participants were busy with personal e-mails instead of performing daily duties. Accessing job search sites at 91.08% was the second-highest cyber-loafing activity. The combined results for accessing personal e-mails and job searches further suggest that staff are accessing e-mails to establish if there are any job offers in their e-mail inbox. Accessing social media sites was rated at 81.18% in third place. This finding suggests that staff were busy on social media, possibly interacting with their friends and family during working hours, which may hinder productivity. The fourth-rated activity was accessing weather forecast sites and online news was rated at 79.2%, according to Figure 2. The pursuit of studies was also rated highly at 78.21%. This finding could be attributed to the fact that the investigated administrative staff are pursuing their studies for better opportunities, either within or outside the municipality. Visiting holiday, travel, and auction sites ranged from 70% to 71%. This finding suggests that the activity is active within the organisation but less prevalent than accessing job sites and personal e-mails. Online shopping, gaming, and sports, as well as online magazines, were less popular. The aforementioned findings suggest that the participants are dissatisfied with their jobs and demotivated since they are using company resources (internet and computer) to search for jobs or check their e-mails. Checking personal e-mails is also linked to doing personal business while at work and using company resources.

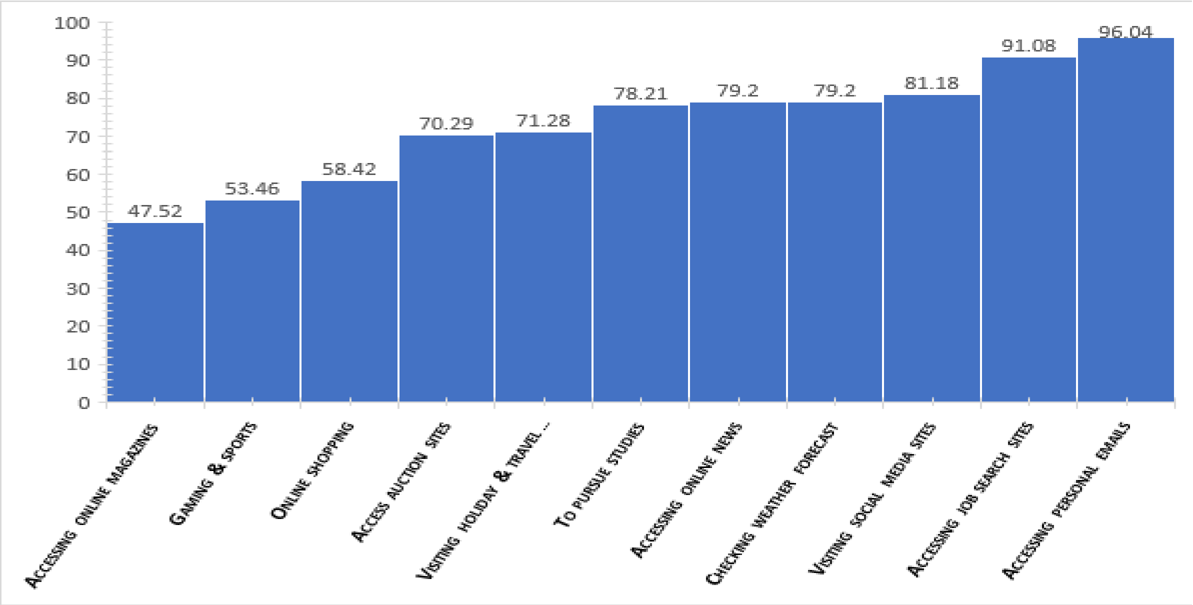

Figure 2: Summary of cyber-loafing activities

Existing Tools Used by Managers to Prevent and Control Cyber-Loafing

This section presents qualitative responses that sought to identify cyber-loafing activities common among administrative staff.

Monitoring internet usage during working hours

Managers and supervisors were asked how they monitored internet usage during employees' working hours. The findings revealed necessity for establishing consensus on the timing and methods for monitoring internet usage. However, Anonymous 1 stated that "*as an employer, it is important to check and monitor the usage of the Internet by my teams to report to my superiors. There is a system in place currently. Our employees are currently working from home and have been given routers with limited data for a month. Once an employee submits a request for more data during the month, we start monitoring. We give our employees enough data for work a month; that is how we monitor.*" Furthermore, it appears that internet monitoring is delegated to the Computer and Information Technology Department. This was confirmed by Anonymous 7, who mentioned that "*managers do not usually monitor, but the Information Computer Technology department monitors through its software to check for any possible violation of the policy.*" Wu *et al*. (2021) also believe that organisations use various mechanisms to monitor internet use. Some organisations use the Internet or desktop surveillance tools to monitor internet use, which the Computer and Information Technology Department largely administers.

Reaction to misuse of the Internet

Participants were questioned about how they reacted when they walked around and observed administrative staff conducting personal business on their company computers during working hours. Based on the responses, it is evident that cyber-loafing is not an acceptable practice. Anonymous 2 and 8 stated clearly that cyber-loafing is not permitted at the customer care of the selected municipality. Anonymous 2 mentioned that "*administrative staff are aware that they are not allowed to conduct personal business on the company's property. Should they be caught, they will be disciplined and/or dismissed*."

Internet usage policy

The responses gathered about the availability of an internet usage policy and its adequateness to reduce cyber-loafing activities in the organisation indicate differing views from the participants. The majority acknowledged the existence of an internet policy within the organisation but challenged its adequacy. Anonymous 4, for example, was quoted saying, "*We do have a company policy in place, and it is given to every employee who joins the organisation. I do not think it is adequate. After all, once an employee signs the policy, it is put on file because it is something people do not value*." According to Hadlington and Parsons (2017), not having an internet policy as an organisation in this technological era exposes one or the entire organisation to cyber risks. However, in a study by Rahimnia and Mazidi (2015), only 40% of managers believed that the Internet policy was sufficient for deterring cyber-loafing. This means that managers must largely place more value on the Internet policy as a cyber-loafing deterrent.

Communication of internet usage policy

The findings indicated that most participants agreed that the Internet usage policy was clearly articulated and communicated within the organisation the feedback indicated a necessity for improved dissemination of the Internet policy among the staff. As highlighted by Anonymous 2, "*Annually, the organisation offers online Code of Business Conduct and Ethics training to existing and new employees*." Anonymous 3 added, "*Yes, the policy is well communicated and implemented*." Anonymous 4 mentioned that, "*I think it is well articulated because most people are aware of the consequences of playing on the Internet with company computers*." This is despite Anonymous 7's response "*The Computer and Information Technology Department frequently sends communications to us concerning this issue. It is well articulated, I guess*." Given the above finding, Abubakar and Al-zyoud (2021) maintain that it is essential to regularly inform employees of any policies and procedures their company employs and require them to formally acknowledge receipt the communiqué each time it is circulated. This is the only legally sound way to hold them accountable for the new policies and procedures that have been implemented. The Computer and Information Technology Department frequently sends us communications concerning this issue.

Enforcement and implementation of internet usage policy

Participants were also asked how their organisation enforced and implemented the Internet usage policy. The quantitative questions required several participants to figure out the implementation and enforcement of the internet usage policy. However, responses from the interviewed participants revealed a different scenario. For example, Anonymous 1 said, "*Internet usage is not one of the factors that we tend to focus on. Once an employee submits the request for more data, we process it, and should the person continue finishing their date before the month ends in three consecutive months. We then take measures to enforce policies on that employee, not the organisation as a whole*." Anonymous 2 stated, "*Through training and e-mails*," and Anonymous 5 mentioned, "*We always receive e-mails reminding us of cyber threats from the Computer and Information Technology department*." While Anonymous 3 was quoted saying "*monitoring was done in the form of writing or verbal communique*." Anonymous 7 said, "*Sometimes people are monitored online and reprimanded for abusing the Internet*." Anonymous 8 indicated, "*We have seen some websites being blocked, so I guess that is how the organisation is enforcing compliance with its computer and information technology usage policy*." Anonymous 9 mentioned that "*People are trained first and made to sign the usage policy*." Anonymous 10 was also quoted, saying, "*I do not exactly know how this is done, or maybe I have not come across such an exercise*." Anonymous 11 indicated that, "*the policy is communicated to people*." Based on the quantitative questions above, it is evident that participants have no knowledge about the enforcement or implementation of internet usage policies. Although policies are in place, the interviews' findings reveal inadequate enforcement and implementation of internet usage policies.

Blocking of websites

Based on the findings, all the participants confirmed that blocking websites was an effective strategy for mitigating cyber-loafing activities. In light of this, Anonymous 1 commented, "*there should be sites blocked. For example, YouTube, Employees may want to watch videos even during their lunch break. Those videos may lead to time and data consumption."* Anonymous 3 mentioned, *"it is the most effective way of mitigating cyber-loafing activities and it is used by most advanced institutions nationwide,"* Anonymous 4 responded, "*it is the best way to prevent the waste of resources,"* Anonymous 5 commented, *"I think it is a commendable effort because you will not have trouble with any person on the Internet,"* Anonymous 8 added, *"it is a good strategy; people are playing around with the Internet, and it is costing the company money,"* In line with the above findings, Abubakar and Al-zyoud (2021) said that the leaders of organisations must embrace monitoring and security techniques such as the blocking of websites, the tracking of e-mails and the examination of browser histories. Wu *et al.* (2021: 26) further confirmed that to combat cyberslacking, several companies have implemented multiple regulations and preventative measures, such as mobile compartments, restricting websites, and providing reminders to employees.

Electronic monitoring systems

The majority of the participants confirmed that electronic monitoring systems were used in the organisation to block employees from accessing certain websites. This was confirmed by anonymous 1, who responded, *"yes, there are electronic systems that are effectively monitored,"* and Anonymous 2, who confirmed, *"yes, there are,"* As explained in the answer above, *"our employees are blocked from accessing YouTube and we find that strategy effective,"* Anonymous 3 agreed, *"yes. I have come across them,"* Anonymous 6 said, "*yes and regarding their effectiveness, I think it is effective,"* On the other note, Anonymous 7 and 8 were not sure, respectively, as they said, "*I don't know, I have not heard of such monitoring system,"* and "*I am not sure if these systems are in place,"* To confirm the above findings, Wu *et al.* (2021: 44) highlighted that one efficient strategy for lowering the amount of time spent cyber-loafing is to implement operant conditioning with software that filters the Internet and monitors user activity.

Internet abuse and disciplinary procedures

The structured interview further strengthened qualitative findings by asking managers and supervisors if they had ever taken disciplinary action against an employee for abusing internet and computer usage. This was the first time anyone had encountered such a situation, according to the findings. However, the responses confirmed the possibility of disciplinary measures in such a case. For instance, Anonymous 1 responded, *"I have never been in a formal disciplinary hearing with an employee regarding the abuse of the Internet,"* Anonymous 2 claimed, "*no, I have not; however, Human Resources Department takes care of that part should it happens,"* Anonymous 5 said, *"no one has approached me or reported any form of abuse,"* Anonymous 6 said, "*people are protecting each other; you will never see any person reporting another person,"* Anonymous 9 added, "*it is very tricky and very rare to see a person reporting someone. If that reporter is known, it might cause tension between the people*," Moreover, Anonymous 11 confirmed, *"I have never seen anyone reporting on such issues before. I think they are covering for each other,"* Perceived certainty and severity of possible cyber-loafing punishments mitigated the impact of observability on employee cyber-loafing. Once employees understand that there are punishment protocols for violating organisational policies, they will refrain from committing unacceptable and deviant behaviours (Wu *et al.,* 2021: 55).

Discussion

This study focused on employees who engage in non-work-related activities or use the computer and internet for personal purposes. Common cyber-loafing activities, including online shopping, social networking, gambling, and sending personal emails, among others, were identified and discussed (Jandagh *et al*., 2015). The identification of cyber-loafing activities was achieved by employing the five-factor model of personality and the theory of interpersonal behaviour (TIB). Several studies have connected cyber-loafing activities with these theories (Hassan *et al*., 2015; Song *et al*., 2021). Elciyar and Simsek (2021) categorise cyber-loafing into minor and serious cyber-loafing based on the severity of the defiant behaviour. Jandaghi *et al*. (2015) and Elciyar and Simsek (2021) point out that non-severe or minor cyber-loafing activities include sending and receiving personal emails and reading news using company resources during working hours. Accessing adult websites, logging on to social media, internet banking, online shopping, and gambling are some of the cyber-loafing activities that are considered extreme or severe (Jandaghi *et al*., 2015; Elciyar and Simsek, 2021).

The results of this study demonstrate that there were major and minor cyber-loafing activities amongst the investigated administrative staff. These cyber-loafing activities are summarised in Figure 2 The figure revealed that accessing personal emails were ranked highest amongst cyber-loafing activities. Other top activities ranged from 70 to 81%, including accessing travel sites, social media sites, study sites, online news, auction sites, and weather forecasts. The least popular activities were accessing online magazines, gaming and sports, and online shopping. All these social and personal sites, if misused, do not add value to the work of administrative staff. In line with the above findings, cyber-loafing is divided into two components: browsing and emails (Cook, 2017). Browsing actions involve visiting websites for entertainment, financial services, news, social networking, shopping, sports, and pornography. To support the preceding result, Aku (2017) stated that e-mailing is another sort of cyber-loafing behaviour that entails receiving and sending e-mails for personal purposes via the company computer and Internet.

Tools that are commonly used by managers as control measures against cyber-loafing were discussed in the literature review. Most studies that investigated a similar phenomenon adopted the general deterrence theory (GDT) to identify and explain these tools. Other deterrent mechanisms, such as organisational control mechanisms were also used in other instances. Organisational control was found by Abbasi (2018), Hassan *et al*. (2015), and

Song *et al*. (2021) to be closely associated with managerial control, system control, policy control, and behaviour control. According to the study's findings, managers and supervisors have strategies in place to combat cyber-loafing among administrative staff. Managers and supervisors closely monitor their employees by walking around them during their work hours. As a result, they have an Information Technology Department that is responsible for controlling and blocking websites and monitoring computer usage. Monitoring software keeps track of how much time employees spend on corporate computers engaging in non-work-related activities (Aku, 2017). The application saves browser history, keystrokes, and websites visited (Jandaghi *et al*., 2015; Elciyar and Simsek, 2021). Unauthorized internet activity can be monitored by recording keystrokes. The selected municipality's customer service has an internet usage policy that inform their employees about the consequences of breaking it. According to the literature, well-written policies will encourage positive usage while discouraging activities like cyber-loafing (Abbasi, 2018). Policies promote the flow of information and boost output (Hassan *et al*., 2015). Users will be able to understand and work within the policies' parameters. According to Song *et al*. (2021), organisations primarily use the GDT as control mechanisms and strategies for preventing and mitigating employee cyber-loafing. This study's results contradict this; not a single participant from management or administration witnessed or reported staff any instances of staff being charged with violating internet policy. Hence, cyber-loafing takes place within the organisation.

The research was carried out at the customer care centre of a selected municipality in KwaZulu-Natal, South Africa. The findings are, therefore, based on a single department. Given that cyber-loafing is a global challenge, other departments and sectors might offer further insights. As a result, it is suggested that the generalisation of the result be done with caution. There is a need for a comparative analysis of private, parastatal, and government institutions on mechanisms used to control cyber-loafing activities. This study did not investigate staff performance in cyber-loafing activities. Further studies are recommended to investigate how cyber-loafing activities affect employee performance. The study was based on a customer care setup where employees deal with customer complaints. Thus, more studies should investigate other areas unrelated to customer care.

Conclusion

Cyber-loafing has become a standard practice being carried out by employees in many organisations. This study corroborates the existing literature that cyber-loafing activities are common in the workplace, including among administrative staff at a customer care centre in a selected municipality. Despite the existence of mitigating mechanisms implemented by management at the investigated site, cyber-loafing is still prevalent. This is a clear indication that the implementation of these tools falls short. The theory of interpersonal behaviour aided the researcher in connecting cyber-loafing to the theory's components. However, to explain the increase in technology and its components, the theory must be revisited. The study relies heavily on GDT in identifying tools to control cyber-loafing. However, for the theory to remain relevant, some tools must be reviewed.

References

Abbasi, H. A. 2018. Organizational Information Security: Strategies to Minimize Workplace Cyberloafing for Increased Productivity. Doctoral Dissertation, Walden University.

Abubakar, A. M. and Al-zyoud, M. F. 2021. Problematic Internet Usage and Safety Behavior: Does Time Autonomy Matter? *Telematics and Informatics*, 56: 1-11.

Aku, A. 2017. Role of Middle Managers in Mitigating Employee Cyberloafing in the Workplace. Doctoral Dissertation, Walden University.

Cook, A. W. 2017. Cyberloafing, Job Satisfaction, and Employee Productivity: A Quantitative Study. Doctoral Dissertation, Northcentral University.

Creswell, J. D. 2017. Mindfulness Interventions. *Annual Review of Psychology*, 68(1): 491-516.

Dmour, M. M., Bakar, H. S. and Hamzah, M. R. 2020. Antecedent, Consequences and Policies View of Cyberloafing among the Employees. Available: https://iopscience.iop.org/article/10.1088/1742-6596/1529/2/022016/pdf (Accessed 18 May 2023).

Dooly, V. P. 2021. Strategies to Monitor and Deter Cyberloafing in Small Businesses: A Case Study. Doctoral Dissertation, Walden University.

Dudovskiy, J. 2016. The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance. *eBook Journal of Mixed Methods Research,* 4(1): 6-16.

Elciyar, K. and Simsek, A. 2021. An Investigation of Cyberloafing in a Large-Scale Technology Organization from the Perspective of the Theory of Interpersonal Behavior. *Journal of Communication and Media Technologies*, 11(2): 1-15.

Ezeh, L. N., Etodike, C. E. and Chukwura, E. N. 2018. Abusive Supervision and Organizational Cynicism as Predictors of Cyber-Loafing among Federal Civil Service Employees in Anambra State, Nigeria. *European Journal of Human Resource Management Studies*, 1(2): 1-18.

Hadlington, L. and Parsons, K. 2017. Can Cyberloafing and Internet Addiction Affect Organizational Information Security? *Cyberpsychology, Behavior and Social Networking*, 20(9): 567-571.

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): 91-98.

Hensel, P. G. and Kacprzak, A. 2021. Curbing Cyberloafing: Studying General and Specific Deterrence Effects with Field Evidence. *European Journal of Information Systems*, 30(2): 219-235.

Holguin, E. S. 2016. Strategies Functional Managers Use to Control Cyberloafing Behaviors. Doctoral Dissertation, Walden University.

Jandaghi, G., Alvani, S. M., Zarei Matin, H. and Fakheri Kozekanan, S. 2015. Cyberloafing Management in Organizations. *Iranian Journal of Management Studies*, 8(3): 335-349.

Kaptangil, I. 2021. Covid-19 Pandemic: Reflections on Organizational Life and Employee Psychology. In: Grima, S., Özen, E. and Boz, H. eds. *Contemporary Issues in Social Science: Contemporary Studies in Economic and Financial Analysis, Volume 106*. Leeds: Emerald Publishing Limited, 221-238.

Kasap, Y. 2019. Cyberloafing Behavior in the Workplaces and Management Practices. Doctoral Dissertation, The Institute of Social Scinece of Ankara Yıldırım Beyazıt University.

Khansa, L., Barkhi, R., Ray, S. and Davis, Z. 2018. Cyberloafing in the Workplace: Mitigation Tactics and their Impact on Individuals' Behavior. *Information Technology and Management*, 19: 197-215.

Koay, K. Y. and Poon, W. C. 2022. Understanding Students' Cyberslacking Behaviour in e-Learning Environments: Is Student Engagement the Key? *International Journal of Human–Computer Interaction*, 39(13): 2573-2588.

Kumar, D. 2016. *Building Sustainable Competitive Advantage: Through Executive Enterprise Leadership*. London: Routledge.

Malik, J., Rodriguez, J., Weisbloom, M. and Petridis, H. 2018. Comparison of Accuracy between a Conventional and Two Digital Intraoral Impression Techniques. *International Journal of Prosthodontics*, 31(3): 107-113.

Mitchell, M. C. and Egudo, M. 2003. A Review of Narrative Methodology. Available: https://www.webpages.uidaho.edu/css506/506%20Readings/Review%20of%20Narritive%20Methodology%20Australian%20Gov.pdf (Accessed 15 June 2023).

Mohajan, H. K. 2018. Qualitative Research Methodology in Social Sciences and Related Subjects. *Journal of Economic Development, Environment and People*, 7(1): 23-48.

Nayak, J. K. and Singh, P. 2021. *Fundamentals of Research Methodology Problems and Prospects*. New Delhi: Publishers and Distributors.

Ozdamli, F. and Cavus, N. 2021. Knowledge Sharing Technologies in Higher Education: Preferences of CIS Students in Cyprus. *Education and Information Technologies*, 26(2): 1833-1846.

Patton, M. Q. 1990. *Qualitative Evaluation and Research Methods*. 2nd ed. New York: SAGE Publications, Inc.

Polit, D. F. and Beck, C. T. 2013. Is there Still Gender Bias in Nursing Research? An Update. *Research in Nursing and Health*, 36(1): 75-83.

Radebe, T. G. 2020. Psychological Well-Being and Coping in the Context of Employee Stress. Doctoral Dissertation, North-West University.

Rahimnia, F. and Mazidi, A. R. K. 2015. Functions of Control Mechanisms in Mitigating Workplace Loafing; Evidence from an Islamic Society. *Computers in Human Behavior*, 48: 671-681.

Saleh, M., Daqqa, I., Abdul Rahim, M. B. and Sakallah, N. 2018. The Effect of Cyberloafing on Employee Productivity. *International Journal of Advanced and Applied Sciences*, 5(4): 87-92.

Sampat, B. and Basu, P. A. 2017. Cyberloafing: The Di(sguised) Gital Way of Loafing on the Job. *IUP Journal of Organizational Behavior*, 16(1): 19-37.

Şimşek, A. and Şimşek, E. 2019. Beneficial and Detrimental Effects of Cyberloafing in the Workplace. *Journal of Organizational Behavior Review*, 1(1): 97-114.

Song, M., Ugrin, J., Li, M., Wu, J., Guo, S. and Zhang, W. 2021. Do Deterrence Mechanisms Reduce Cyberloafing When It Is an Observed Workplace Norm? A Moderated Mediation Model. *International Journal of Environmental Research and Public Health*, 18(13): 1-16.

Taherdoost, H. 2016. Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management (IJARM)*, 5(2): 18-27.

Toker, S. and Baturay, M. H. 2021. Factors Affecting Cyberloafing in Computer Laboratory Teaching Settings. *International Journal of Educational Technology in Higher Education*, 18(1): 1-24.

Ugrin, J. C. and Pearson, J. M. 2013. The Effects of Sanctions and Stigmas on Cyberloafing. *Computers in Human Behavior*, 29(3): 812-820.

Wu, J., Mei, W., Ugrin, J., Liu, L. and Wang, F. 2021. Curvilinear Performance Effects of Social Cyberloafing Out of Class: The Mediating Role as a Recovery Experience. *Information Technology and People*, 34(2): 581-598.