Effects of Personal Factors and Organizational Reinforcing Tools in Decreasing Employee Engagement in Unhygienic Cyber Practices: Perspectives From a Developing Country

Princely Ifinedo, Brock University, Canada*
https://orcid.org/0000-0001-7032-3532
Nigussie Mengesha, Brock University, Canada
https://orcid.org/0000-0001-5673-5733
Rahel Bekele, Addis Ababa University, Ethiopia

ABSTRACT

Employee engagement in unhygienic cyber practices (UCP) is a concern for organizations across the world. The purpose of this paper is to explore the effects of personal and environmental factors in decreasing workers’ engagement in UCP in a developing country. A personal-environment-behavior model was adapted for the study. Data was collected from working MBA students in Ethiopia. The key results show that the personal factor of self-regulation related to acceptable cyber practices decreases workers’ engagement in UCP, while self-efficacy did not. The environmental factor of computer monitoring (CM) decreases workers’ engagement in UCP, while the availability of security education and training awareness (SETA) programs did not. Both CM and SETA have positive effects in improving self-efficacy. Only SETA programs positively impact self-regulation. This study adds to the understanding of end-user security behavior by focusing on UCP with insights from a developing country.

KEYWORDS
Computer Monitoring, Developing Country, IS Security, IS Security Management, Nonmalicious Threat, Self-Efficacy, Self-Regulation, SETA Programs, Unhygienic Cyber Practices

1. INTRODUCTION

The diffusion of the Internet has boosted cyber-based operations for private and public organizations across the world. Internet-adopting organizations entrust workers to use the tool to perform work-related tasks; however, employees often deviate from organizational rules on prescribed cybersecurity
practices and measures (Farshadkhah et al., 2021; Ogbanufe, 2021; Hamidi & Moradi, 2017; The ePolicy Institute, 2017; Ifinedo, 2019; Wang et al., 2020). Organizations that use the Internet for operations, including storing customer data, employee information, and financial records, as well as transmitting data and information to clients and partners, must accept that they share in its increased vulnerability because security incidents and breaches do occur (Anderson & Agarwal, 2010; CyberEdge Group Report, 2020). Unfortunately, the aftermath of security incidents can be devastating for affected organizations (Optimum Security, 2021).

Security incidents with origins in global networks, including the Internet, are indeed pervasive. A survey of 1,200 information systems (IS) security professionals based in 17 countries revealed that 76.7% of participants admitted their organizations experienced one or more successful cyber attacks in 2019, and 81.7% of them predicted that at least one incident would occur in 2020 (CyberEdge Group Report, 2020). Threats to organizational IS, including the Internet, emanate from internal and external sources (Blue Coat Systems Inc., 2015; Ponemon Institute, 2012; Verizon Business Systems, 2019). According to Verizon Business Systems' (2019) report of 41,686 security incidents in private and public organizations worldwide, 34% of such attacks involved an insider.

Insiders are current employees, part-time workers, former employees, and other business associates who have—or have had—access to an organization’s IS resources in the course of performing their work responsibilities (Burns et al., 2018). A report published by the Ponemon Institute (2020) identified three primary insider-threat profiles: employee or contractor negligence, criminal and malicious insiders, and credential theft or imposter risk. The report notes that the global average cost of an insider threat is USD 11.45 million across the three primary insider threat profiles. Furthermore, the percentage of incidents caused by employee or contractor negligence, criminal and malicious insiders, and imposter risk is 63%, 23%, and 14%, respectively (Ponemon Institute, 2020). The high percentage of incidents attributable to employees or contractors suggests a need to focus on their security practices and behaviors.

This study focuses on negligent employees who participate in unsafe or unhygienic cyber practices, such as downloading unauthorized software from the Internet onto work computers and logging into the Internet via unsecured WIFI networks. A recent cybersecurity report on some African countries (KNOWBE4, 2019, p. 6) notes, “more than a quarter of respondents connected their devices to the internet using a free Wi-Fi connection in a public space.” Although these actions seem harmless, they can be exploited by cybercriminals, who may leverage such lapses to harm an organization’s digital resources. Cyber hygiene practices are the precautions and steps users of online digital tools take to maintain, safeguard, and secure data resources from intrusions and external attacks (McAfee.com, 2020; National Cyber Security Alliance 2007, 2020). Here, the term ‘cyber hygiene practices’ refers to the acceptable or favorable notion of the phenomenon, while the term unhygienic cyber practices (UCP) connotes unfavorable and ill-advised acts.

To mitigate employee participation in UCP and related IS-security misbehavior, organizations often deploy technological tools, which practitioners (Barlock et al., 2014; The Security Culture Report, 2017) and researchers (Anderson & Agarwal, 2010; Crossler et al., 2013; Ng et al., 2009; Rhee et al., 2009; Warkentin et al., 2011; Warkentin et al., 2016; Warkentin & Willson, 2009; Workman et al., 2008; Ifinedo, 2014) have since realized are inadequate in containing such concerns. The Security Culture Report (Barlock et al., 2014) notes that “despite the latest technological improvements in security, it is still the employees who often unknowingly invite security breaches through carelessness” (p. 32). Consequently, the role of technical or behavioral approaches to studying IS security issues and safe online practices have been touted (Anderson & Agarwal, 2010; Barlock et al., 2014; Crossler et al., 2013; Ng et al., 2009; Rhee et al., 2009; The Security Culture Report, 2017; Warkentin et al., 2011; Warkentin et al., 2016; Warkentin & Willson, 2009; Workman et al., 2008; Ognaufe, 2021).

Prior research has identified and shown that knowledge of individual characteristics, personal dispositions, and personal factors are pertinent to understanding individuals’ motivation to engage in unacceptable IS security practices and behaviors (Bulgurcu et al., 2010; Hu et al., 2011; Rhee et
al., 2009; Warkentin et al., 2011; Warkentin et al., 2016; Warkentin & Willison, 2009; Workman et al., 2008). Similarly, the reinforcing roles of organizational controlling mechanisms, such as security education and training awareness (SETA) programs (Burns et al., 2018; D’Arcy et al., 2009; Yoo et al., 2018; Yaokumah et al., 2019) and security surveillance technology or computer monitoring (CM) to reinforce the desired security behaviors have been highlighted in prior studies (Chen et al., 2015; D’Arcy et al., 2009; D’Arcy & Hovav, 2008).

Previous research on end-user security behavior has primarily been carried out in the context of IS policy compliance (Cram et al., 2019). Commonly used theoretical perspectives in prior studies include fear appeals and sanctions derived from protection motivation theory (PMT) and general deterrence theory (GDT) (Cram et al., 2019). We did not consider sanctions because previous IS security studies have revealed that GDT is not always effective in reducing violations of IS security rules (Son, 2011; Hu et al., 2011). Instead, intrinsic factors, such as self-control, were more effective than GDT (Son, 2011; Hu et al., 2011). Moreover, IS policy compliance studies have not differentiated between non-malicious and malicious security acts, and few researchers have acknowledged this vital reality (Guo et al., 2011; Lowry et al., 2015). Indeed, researchers (e.g., Warkentin and Willison, 2009; Crossler et al., 2013) have asserted that the management and control of insider threats could be more effective when specific attention is paid to each group’s actions. However, the motivations of insider threat profiles (i.e., negligent, criminal, and imposter) differ (Ponemon Institute, 2020).

Notably, studies examining the direct effects of self-regulation, CM, and SETA programs on IS security behavior or UCP are rare. Our study aims to fill these gaps in the research on end-user security behavior. Specifically, we seek to contribute to the literature by investigating the effects of two individual cognitive factors (i.e., self-efficacy and self-regulation) and two organizational factors (i.e., SETA programs and CM) in reducing employee involvement in UCP. The two related cognitive factors were selected because the literature suggests both effectively enhance behavioral modification and change in individuals (Bandura, 1977; Wood & Bandura, 1989). Additionally, self-efficacy has been identified as an essential predictor of intentions to enact online security measures (LaRose et al., 2005; Ng et al., 2009; Rhee et al., 2009), and it generally facilitates adherence to IS security policies, as a recent meta-analytic study in the area has shown (Cram et al., 2019). Furthermore, self-regulation reduces IS security violations (Hu et al., 2011) and moderates the cost-benefit calculus regarding Internet use compliance (Li et al., 2018). The two organizational security reinforcing mechanisms chosen for this study ensure employees get formal access to necessary information regarding IS security threats, and organizations can monitor or review workers’ computing actions and cyber practices to stimulate desired security behaviors (Chen et al., 2015; D’Arcy & Hovav, 2008; Lowry et al., 2015).

Most of the research in the extant literature enriches our understanding of end-user security behavior, mainly from the perspectives developed or advanced countries. Insights from developing countries in Africa have not been widely represented. It is argued that the diversification of views enhances knowledge. However, only a few studies have explored UCP issues in Africa. For example, Butler and Butler (2015) studied UCP issues in the Republic of South Africa. Likewise, van Rensburg (2021) investigated end-user perceptions on information security issues in the Republic of South Africa. Bongonko (2017) reported that self-efficacy and SETA programs positively influence end-user security behavior in Kenya. Ifinedo et al.’s (2019) study indicates that workers’ positive attitudes toward cyber hygiene decrease participation in UCP, and so do the construct of subjective norms. Ifinedo and Akinnuwesi (2015) compared employees’ engagement in UCP in Nigeria and Canada and found that socio-economic conditions and national cultural factors explain differences in workers’ perceptions. Others have also shown that national factors affect workers’ perceptions of IS security and privacy issues (e.g., Bellman et al., 2004; Ifinedo, 2009; Ameen et al., 2021). Against such a backdrop, it can be argued that findings related to employees’ end-user security behaviors reported in advanced countries may not sufficiently reflect the realities in developing countries. Indeed, researchers have suggested that contexts should be duly considered in research (Fernandez, 2016; Johns, 2017), and their advice was heeded in this research project.
Thus, the current study contributes to the body of research on this topic in the following ways: (a) distinguishing between end-user non-malicious and malicious security practices or acts; (b) enriching the literature with a focus on non-malicious insider behavior in Ethiopia, a developing country in Africa; (c) applying Bandura’s theory of reciprocal determinism (triadic reciprocality), which incorporates the relationships among personal, environment, and behavior factors in the study of end-user security behavior; (d) presenting findings showing that self-regulation and computer monitoring are important in controlling workers’ engagements in UCP; (e) explaining contradictory results in research related to the role of self-efficacy in decreasing worker’s involvement in UCP (Ng et al., 2009; Rhee et al., 2009; Ameen et al., 2021).

Based on the preceding discussion, this paper attempts to answer the following research questions:

1. **Research question one (RQ1):** What effect do the personal factors of self-efficacy and self-regulation have on decreasing employee involvement in unhygienic cyber practices?

2. **Research question two (RQ2):** What effect does the environmental reinforcing mechanisms of SETA programs and computer monitoring have on decreasing employee involvement in unhygienic cyber practices?

3. **Research question three (RQ3):** What relationships exist among personal and environmental factors in the context of employee involvement in unhygienic cyber practices?

The remainder of the paper is organized as follows. Section 2 has the literature review, which presents background information on end-user IS security behaviors. Section 3 presents the theoretical framework, research model, and formulated hypotheses. Next, Section 4 presents the research methodology, followed by an explanation of the data analysis results in Section 5. Finally, Section 6 includes a discussion of the results and conclusions.

2. **LITERATURE REVIEW**

Recent research has focused attention on cyber-related end-user IS security behaviors by developing taxonomies for categorizing such behaviors (Egelman & Peer, 2015; Lee et al., 2008; Posey et al., 2013; Ifinedo, 2019; Vishwanath et al., 2020). For example, Posey et al. (2013) proposed a scheme classifying IS protection-motivated behaviors, and Egelman and Peer (2015) developed a security behavior intentions scale. Ifinedo (2019) developed a non-malicious IS security deviant behavior taxonomy, and Vishwanath et al. (2020) presented a cyber hygiene inventory. It is noteworthy that these frameworks have items covering unsafe online computing and unhygienic cyber practices.

Previous investigations of antecedents of end-user security behaviors are available (Aytes & Connolly, 2004; Boehmer et al., 2015; Rhee et al., 2009). For instance, Aytes and Connolly (2004), who examined undergraduate students’ risky computing practices (e.g., sharing and changing passwords, not backing up files regularly, and opening emails from unknown senders), found that experience (efficacy) can reduce such practices. Boehmer et al. (2015) showed that the personal responsibility norm—described as self-regulation in their study—was positively related to college students’ online safety behavior (e.g., performing anti-spyware scans and installing a virus from downloaded files). Using a sample of graduate students, Rhee et al. (2009) confirmed that self-efficacy in information security issues explained end-user security practice behaviors (e.g., using anti-virus and anti-spyware software, sending sensitive information via e-mails, backing up files, and using strong passwords).

Studies of safe online security behaviors of home computer users found self-efficacy to be a critical antecedent for intention to perform security-related behavior on the Internet (Anderson & Agarwal, 2010; Liang & Xue, 2010). A study conducted by Liang and Xue (2010), which used business students to represent home users, revealed that participants are more motivated to avoid the threat of spyware if they have confidence (self-efficacy) in using spyware tools. Other studies have used
samples consisting of working professionals and students; for example, Ugrin et al. (2008) found that individuals who have difficulty with self-regulation have higher propensities to use the Internet for non-work-related purposes. Johnston and Warkentin (2010) identified self-efficacy as a determinant for intention to use anti-malware software. Ng et al. (2009) reported that the IS security behavior of “exercising care when reading emails with attachments” of 134 working students in Singapore was positively influenced by self-efficacy.

A survey of computer end-users in the workplace by Guo and colleagues (2011), who used a scenario-based approach with examples, such as installing unauthorized software and using unauthorized portable devices for storing and carrying organizational data, found that the personal factor of perceived identity matching was negatively linked to workers’ intentions to engage in such non-malicious security practices. Using employees based in the U.S., Chen et al. (2015) demonstrated that SETA programs and security monitoring help improve an organization’s security culture. Likewise, D’Arcy and colleagues (2008, 2009), using data samples of working professionals in the U.S. established the indirect effects of SETA programs and CM through sanctions in deterring misuse of organizational IS resources. Another study of workers in South Korea (Yoo et al., 2018) demonstrated that SETA programs positively influence their self-efficacy, which impacts their security compliance intentions. Burns et al. (2018), who surveyed organizational insiders within the U.S., found that SETA initiatives indirectly affect intentions to protect organizational information assets, and a study of full-time employees in the same country (Lowry et al., 2015) revealed that SETA has an effect on computer abuse through organizational trust.

Past studies have elucidated the effects of personal- and organizational-related factors in diminishing the sanctioned security behaviors in which end-users engage. However, more empirical information on the impact of personal- and organizational-related antecedent factors on end-user security behavior relating to UCP in developing countries is needed to contextualize these insights. The present study seeks to fill such gaps in the research on end-user security behavior. In summary, no previous research has employed the selected personal cognitive factors and organizational reinforcing mechanisms in one nomological network, as is done herein, to explore employee involvement in UCP.

3. THEORETICAL FRAMEWORK, RESEARCH MODEL, AND HYPOTHESES

3.1 Theoretical Framework

This study draws from a simplified version of Bandura’s (1986) theory of reciprocal determinism (triadic reciprocity), a model signifying the interrelationships among three factors: personal (how an individual feels), environmental (the context in which the individual exists), and behavioral (how an individual acts). The theoretical model posits that personal cognitive factors and the environment impact a person’s behavior. Bandura’s (1986) conceptualization of complete triadic reciprocal determinism is displayed when a behavior also influences environmental and personal factors. However, this study’s focus is not on complete triadic reciprocal determinism.

Only the unidirectional relationships highlighting the influences of personal and environmental (external reinforcing factors) on behavior are considered in this study. Other researchers (Ng et al., 2009; Rhee et al., 2009) have done likewise. Thus, Figure 1a depicts the triadic interacting determinants of personal, environmental, and behavioral factors in a bidirectional fashion (Wood & Bandura, 1989). As previously indicated, this study’s focus is on the effects of select personal and environmental factors (i.e., self-efficacy, self-regulation, SETA, and computer monitoring) on behavior (i.e., workers’ engagement in UCP; Figure 1b).

The study’s constructs are described as follows. First, self-efficacy refers to one’s ability to organize and execute courses of action required to produce or perform a specific behavior (Bandura, 1977, 1986). Self-efficacy indicates confidence in one’s ability to exercise control over one’s motivation and behavior. Self-regulation refers to an individual’s purposive self-adjustment to achieve a goal (Carver & Scheier, 2004); it is the process of taking control of and evaluating one’s behavior (Wood &
According to Bandura’s (1991) theory of self-regulation, self-regulative mechanisms operate through three subfunctions (i.e., self-monitoring of one’s behavior, self-judging one’s behavior related to personal and environmental standards, and self-reaction to one’s behavior based on these standards). Likewise, Zimmerman’s (2002) three phases of self-regulation include forethought, performance, and self-reflection. Generally, self-regulative processes enhance learning and behavioral adjustments (Bandura, 1991; Carver & Scheier, 2004; Wood & Bandura, 1989; Zimmerman, 2002).

Bandura (1986) signifies the importance of environmental factors in effecting behavioral change. Reinforcements from an individual’s environment can increase personal cognitive beliefs regarding accomplishing a task or goal (Bandura, 1986; Wood & Bandura, 1989). We contend that the provision of SETA programs and CM offers such with respect to encouraging the desired outcome, which, in this study, is diminished involvement in UCP. In the study, behavior is represented by workers’ self-reported involvement in UCP instead of actual behavior because researchers (Corral-Verdugo, 1997) have demonstrated that self-reported behaviors adequately predict actual behaviors. Furthermore, the practical choice to utilize self-reported responses for the study was informed by the reported difficulty in obtaining security-related information from organizations (Guo et al., 2011).

3.2 Research Model and Hypotheses

The study’s research model is shown in Figure 2. Relevant control variables considered in previous academic studies and reports (Ifinedo, 2014; Lowry et al., 2015; The Security Culture Report, 2017) are included. The study’s hypotheses are discussed in the following subsections.

3.2.1 Effect of Personal Factors on Involvement in Unhygienic Cyber Practices

In tune with the dictates of the theory of self-regulation, individuals who can self-monitor, self-reflect, self-judge, and self-react to set standards are more likely to produce desired outcomes (Bandura, 1991; Zimmerman, 2002). Brown (1998) argues that deficits in self-regulatory processes can heighten behavioral disorders. Past studies from diverse disciplines, including healthcare (Bandura, 2005), education (Zimmerman, 1989), and psychology (Brown, 1998), have shown that individuals with high self-regulation are more capable of facilitating goal-directed behavior and achieving desired outcomes than individuals low on such attributes. Similar insights have been offered in the IS security literature. For example, Hu et al. (2011) demonstrated that individuals with high self-control are less likely to violate organizational IS security rules. Li et al. (2018) and Ugrin et al. (2008) found that individuals with high levels of self-regulation are less inclined to misuse the Internet at work. LaRose et al. (2008) showed that higher perceptions of self-regulation regarding online safety are associated with a higher likelihood of performing online protective actions. Accordingly, workers who can self-
regulate regarding UCP would likely view such practices as contrary to personal and organizational standards and less likely to participate in them. Thus, the following hypothesis is proposed:

**H1:** Higher levels of self-regulation regarding acceptable cyber practices decrease employee involvement in unhygienic cyber practices.

Bandura and Adams (1977) note that “the stronger the perceived self-efficacy, the more active the coping efforts.” People with low self-efficacy are generally less likely to complete a task than those with high self-efficacy (Schunk, 1990). In several disciplines, self-efficacy is effective in electing desired outcomes. For example, it increases self-regulated learning (Bandura, 1986; Zimmerman, 1989), promotes favorable health practices (Bandura, 2005; Dolan et al., 2008), and improves work-related performance (Stajkovic & Luthans, 1998). A study conducted by Dolan et al. (2008) showed that higher self-efficacy predicts lower levels of drug abuse. IS researchers (e.g., Compeau et al., 1999) have demonstrated that self-efficacy impacts an individual’s behavioral reactions to IT, and IS security researchers have also shown that self-efficacy facilitates the intention to comply with IS security rules (Bulgurcu et al., 2010; Ifinedo, 2014). Self-efficacy influences favorable computer security behaviors, as well as safe computing and online practices (Anderson & Agarwal, 2010; Ng et al., 2009; Rhee et al., 2009; Workman et al., 2008), and impacts intention to adopt online protective technologies (Lee & Larsen, 2009). Overall, these findings indicate that an individual’s urge to participate in sanctioned cyber practices will be low where self-efficacy is high. Thus, the following hypothesis is proposed:

**H2:** Higher levels of self-efficacy regarding acceptable cyber practices decrease employee involvement in unhygienic cyber practices.

### 3.2.2 Effect of Environmental Reinforcing Mechanisms on Involvement in Unhygienic Cyber Practices

CM is used to track and review employees’ computing activities to ensure that only authorized tasks are performed (D’Arcy & Hovav, 2008), and this organizational reinforcing mechanism ultimately
strengthens compliance (D’Arcy et al., 2009). Prior researchers have highlighted the critical role of CM in controlling workers’ security behaviors (Urbaczewski & Jessup, 2002). Studies have shown that CM deters employees’ misuse of organizational IS resources (D’Arcy et al., 2009; D’Arcy & Hovav, 2008) and enhances positive corporate security culture (Chen et al., 2015). CM was also found to discourage employees’ unauthorized modification of data (D’Arcy & Hovav, 2008). It is expected that UCP will be low when workers know their computing and cyber activities are being regularly reviewed. Thus, the following hypothesis is proposed:

**H3:** Computer monitoring decreases employee involvement in unhygienic cyber practices.

Observations from related management and social psychology fields have shown that awareness programs, campaigns, and training generally facilitate behavioral change. For instance, Noar (2006) reported that awareness programs and campaigns improve health-related behavioral changes, and Tannenbaum et al. (1991) showed that training improves workers’ expectations and commitment. Formal SETA programs are effective and reinforcing insofar as they educate employees about their roles and expectations regarding IS security requirements (Burns et al., 2018), train workers on why IS security rules compliance is essential (D’Arcy & Hovav, 2008; Yaokumah et al., 2019), change their attitudes toward IS security compliance (Bulgurcu et al., 2010), and enforce IS security rules (D’Arcy et al., 2009; Straub & Welke, 1998). Thus, SETA programs direct workers’ attention to safeguarding organizational IS assets. Therefore, it is expected that employees who have access to SETA programs will more accurately recognize the dangers posed by UCP to organizational IS resources (Lowry et al., 2015). As such, they will be less likely to participate in such practices. Past IS security studies have established that SETA programs are effective in reducing sanctioned computer security practices and intentions to misuse IS (D’Arcy et al., 2009; D’Arcy & Hovav, 2008; Posey et al., 2015; Yoo et al., 2018; Yaokumah et al., 2019) and enhance overall security culture (Chen et al., 2015). Thus, the following hypothesis is proposed:

**H4:** SETA programs decrease employee involvement in unhygienic cyber practices.

### 3.2.3 Relationships Among Personal and Environmental Factors

Self-efficacy can be engendered by training and awareness campaigns, and findings from diverse disciplines have affirmed this claim (Bandura, 2005; Gist et al., 1989; Noar, 2006; Stajkovic & Luthans, 1998; Tannenbaum et al., 1991). For example, Gist et al. (1989) found that individuals with higher levels of self-efficacy perform better on a computer software training program than those with lower self-efficacy. The IS security trade press has also indicated that SETA initiatives improve workers’ competence with safe cybersecurity practices and desirable IS security behaviors (IIROC, 2012; Morgan, 2019). Likewise, findings from academia have shown that SETA initiatives enhance workers’ self-efficacy related to intentions to adhere to prescribed IS privacy and security practices (Posey et al., 2015; Warkentin et al., 2011; Park et al., 2017). Thus, the following hypothesis is proposed:

**H5a:** SETA programs increase workers’ self-efficacy regarding acceptable cyber practices.

Self-efficacy revolves around individuals’ abilities to leverage coping efforts in accomplishing challenging tasks (Bandura, 1977; Bandura & Adams, 1977). This insight implies that an individual’s self-efficacy increases when internal or external coping mechanisms are present. Therefore, when tools like CM deployed to reinforce desired outcomes (e.g., avoid UCP) are in place, an individual’s self-efficacy in such areas is expected to improve. Observations from educational psychology and health education (Gleeson-Kreig, 2006) indicate that self-efficacy is positively related to monitoring (Moos & Azevedo, 2008; Nietfeld et al., 2006). For instance, Nietfeld et al. (2006) revealed that
interventions designed to improve students’ metacognitive monitoring significantly improves their self-regulated learning self-efficacies. Moreover, the management literature shows that performance monitoring positively influences subordinate performance and managerial effectiveness (Larson & Callahan, 1990). Thus, the following hypothesis is proposed:

**H5b:** Computer monitoring increases workers’ self-efficacy regarding acceptable cyber practices.

Individuals’ self-regulative processes (e.g., self-monitoring and self-judgment) are critical for accomplishing challenging goals (Bandura, 1991; Wood & Bandura, 1989); accordingly, mechanisms capable of stimulating such thought processes should enhance an individual’s self-regulation. We contend that training, guidance, awareness programs, and monitoring can generally enhance self-regulation. *Ceteris paribus*, the same supposition should hold for workers’ self-regulation related to engaging in sanctioned cyber practices. Concerning technology-based training, Bell and Kozlowski (2002) found that adaptive guidance and training substantially affect the nature of trainees’ self-regulation. Park et al. (2017) revealed that nursing students’ health information security awareness significantly affects their self-control, a concept related to self-regulation, to protect against disclosing patients’ health information. Insights gleaned from an IS security ethics study (D’Arcy & Hovav, 2008) that CM sensitizes individuals’ judgment and reaction towards engagement in acceptable practices. Thus, the following set of predictions are proposed.

**H6a:** SETA programs increase workers’ self-regulation regarding acceptable cyber practices.

**H6b:** Computer monitoring increases workers’ self-regulation regarding acceptable cyber practices.

4. RESEARCH METHODOLOGY

4.1 Research Context, Study Design, and Participants

To test the research model, we used the survey method, and data were collected in Ethiopia. According to a World Bank Report (2021), “with more than 112 million people [in 2019], Ethiopia is the second-most populous nation in Africa after Nigeria and the fastest growing economy in the region. However, it is also one of the poorest, with a per capita income of $850.” The Internet has diffused widely in the country, and organizations’ use of the tool is increasing (CIA-World Factbook, 2020). It is critical for insights from the country to be investigated; as the Africa Cyber Security Report (2017) noted, “most of the African countries including Ethiopia are now moving to E-services without” (p. 41) adequately considering security issues that could arise from such platforms. At the outset, we discussed IS security issues that could occur when workers ignore cybersecurity guidelines and rules.

In designing the research study, we used items validated in prior research to represent the study’s reflective constructs. For the dependent construct, 37 examples of cyber practices were drawn from three sources (McAfee.com, 2020; National Cyber Security Alliance 2007, 2020). A list containing these items was given to seven individuals (i.e., the three IS professors and four IT professionals acknowledged in the paper) knowledgeable about cybersecurity issues in the research setting. They were asked to choose ten items from the list they believe are prevalent in the country or region. Fifteen highly ranked items from the exercise are shown in Appendix A. However, only ten were included in the study, and four were subsequently dropped due to low item-loadings. The final number of items used to represent UCP in this study was comparable to those reported in closely related works (e.g., Ng et al., 2009; Guo et al., 2011).

A pilot survey of the developed research instrument was pre-tested among twenty students and five professors to enhance the content and face validity of the items. The feedback received improved the wording of items used in the final questionnaire; a suggestion was also made to define unfamiliar terms (e.g., UCP), which we followed in the main survey. For the main study, we collected data from
working professionals enrolled in the MBA programs of two universities (one large and one small) in the nation’s capital, Addis Ababa. To eliminate potential teacher-student relationship bias, two research assistants distributed and collected the questionnaires in the classroom. Participation in the study was voluntary, and students were awarded no academic or other incentives for participating in our study project.

At one location, 150 questionnaires were distributed and 103 returned, and at the other location, 60 of the 90 distributed questionnaires were returned; thus, the combined response rate was 77.6%. We were interested in gauging end-user cyber practices in organizational settings, and home users’ or individuals’ cyber practices were not within the scope of this study. Responses from participants who indicated that they were full-time students were not included. Furthermore, poorly completed (i.e., patterned responses and those too many missing answers) questionnaires were excluded. Responses with more than 20% missing data were excluded per recommendations in the literature (Brick & Kalton, 1996).

A total of 150 valid responses were used for data analysis, and this sample size is comparable to those of other studies investigating similar topics (Ng et al., 2009). To assess the statistical power and minimum sample size required for the study, we used the inverse square root method with a power level of 0.8 and significance level of 0.05 (Kock, 2020); the results indicated that a sample size of 150 observations would suffice.

Participants in the study came from diverse industries, including media, banking, healthcare, education, food, manufacturing, and retail. Some of their job titles include accountant, associate project advisor, branch manager, lead health safety officer, engineer, lecturer, human resources director, and sales manager. There were missing entries in the sample, but, 96 (64%) respondents were male, and 52 (34.7%) were female. Furthermore, 37 (24.7%) of them had already earned other post-graduate degrees. Their average time since starting to use computers was 12.1 years (SD = 5.3). Other characteristics of the participants are shown in Table 1.

4.2 Measurement Development

For UCP (Appendix A), whose sources and inclusion rationale were succinctly discussed in the preceding paragraph, we instructed each participant to “please indicate how often you participate in the [item] listed in Appendix A.” We assessed their responses using a seven-point Likert scale, ranging from “Almost never” (1) to “Almost always” (7), with a not applicable (N/A) option. The measures for self-efficacy were adapted from a previous study (Lin & Huang, 2008), and self-regulation contained items adapted from studies conducted by Bandura (1991) and Williams et al. (1996). The measures used for SETA programs and CM were adapted from a study performed by D’Arcy et al. (2009). The measurement items used for these constructs were assessed on a seven-point Likert scale, ranging from “Strongly disagree” (1) to “Strongly agree” (7), with an N/A option. Mackenzie et al.’s (2005) recommendations for specifying constructs as either reflective or formative were followed. Accordingly, all the constructs in the study were delineated as reflective constructs. The constructs and their items are shown in Table 2 and Appendix A.

4.3 Common Method Bias

Common method bias (CMB) was assessed using three techniques: correlation matrix assessment (Pavlou et al., 2007), assessment of full collinearity variance inflation factors (VIFs; Kock, 2015), and Harman’s single-factor test (Podsakoff and Organ, 1986). First, given that none of the study’s constructs are highly correlated (i.e., close to 0.90) in the correlation matrix (Table 3), CMB is unlikely to be a problem for the data. Second, the results show that the full collinearity VIFs for self-efficacy, self-regulation, SETA programs, computer monitoring, and self-reported participation in UCP are 1.37, 1.16, 1.36, 1.52, and 1.12, respectively. These values are below the threshold of 3.3, which is used to indicate the presence of CMB in a model (Kock, 2015). As the constructs’ full collinearity VIFs are below the threshold value, CMB is not problematic for the study’s data. Third, Harman’s
single-factor test was performed using an exploratory factor analysis. The results showed that the variance explained by the largest factor was 37.5%. No single factor explained more than half of the variance in the model. This approach also shows that CMB is not a problem for the data.

5. DATA ANALYSIS

We used partial least squares (PLS), a component-based structural equation modeling technique, for estimation (Gefen & Straub, 2005; Hair et al., 2017). PLS is more appropriate for exploratory studies emphasizing hypothesis testing than covariance-based approaches, which are more suitable for studies highlighting theory development and confirmatory analyses (Gefen & Straub, 2005). We used WarpPLS 7.0 software to perform PLS estimation (Kock, 2014). PLS does not require large sample size or normally distributed data (Hair et al., 2017). However, a sample size of 150 may not be large enough, so we conducted a Shapiro-Wilk test for data normality. The results show that the study’s measures were not normally distributed, thus confirming PLS’s suitability for this study (Hair et al., 2017). PLS recognizes two models (i.e., measurement and structural), which are discussed in the following subsections.

| Variable | Category | Number | Percent | Variable | Category | Number | Percent |
|----------|----------|--------|---------|----------|----------|--------|---------|
| Age      | Less than 20 years | 1 | 0.7% | 21 - 30 years | 77 | 51.3% |
|          | 21 - 30 years     | 77 | 51.3% |          | 41 - 50 years | 15 | 10.0% |
|          | 41 - 50 years     | 15 | 10.0% |          | 51 - 60 years | 5 | 3.3% |
|          | 51 - 60 years     | 5 | 3.3% |          | 61 years and above | 0 | 0.0% |
|          | 61 years and above | 0 | 0.0% |          | Missing   | 1 | 0.7% |
| Work tenure | Less than 1 year | 0 | 0.0% | 1-3 years | 71 | 47.3% |
|          | 1-3 years         | 71 | 47.3% |          | 4-6 years    | 41 | 27.3% |
|          | 4-6 years         | 41 | 27.3% |          | 7-10 years   | 22 | 14.7% |
|          | 7-10 years        | 22 | 14.7% |          | 11 years and above | 6 | 4.0% |
|          | 11 years and above | 6 | 4.0% |          | Missing     | 10 | 6.7% |
| Education | Secondary education | 0 | 0.0% | ISSP | Yes | 39 | 26.0% |
|          | Vocational education | 0 | 0.0% |      | No | 45 | 30.0% |
|          | Bachelor's degree | 112 | 74.7% |      | Don't know | 59 | 39.3% |
|          | Master's degree | 37 | 24.7% |      | Missing | 7 | 4.7% |
|          | Missing | 1 | 0.7% |      |      |      |         |
| Size     | Less than 10 | 17 | 11.3% |      | Very low | 7 | 4.7% |
|          | 11 - 50 | 12 | 8.0% |      | Low | 3 | 2.0% |
|          | 51 - 250 | 15 | 10.0% |      | Somewhat low | 19 | 12.7% |
|          | 251 - 500 | 29 | 19.3% |      | Undecided | 26 | 17.3% |
|          | 501 - 1000 | 16 | 10.7% |      | Somewhat high | 54 | 36.0% |
|          | 1001 - 4999 | 13 | 8.7% |      | High | 19 | 12.7% |
|          | More than 5000 | 21 | 14.0% |      | Very high | 15 | 10.0% |
|          | Do not know | 18 | 12.0% |      | Missing | 7 | 4.7% |
|          | Missing | 9 | 6.0% |      |      |      |         |
5.1 Measurement Model Assessment

In assessing item reliability, a Cronbach’s alpha of 0.70 is considered adequate (Gefen & Straub, 2005; Hair et al., 2017; Kock, 2014). The values reported in Table 3 show that the study’s item reliabilities are sufficient. To assess convergent validity, the following criteria are used. First, item loading values should be 0.7 (Fornell & Larcker, 1981); however, 0.6 is acceptable (Gefen & Straub, 2005). Second, composite reliability indicators should be 0.7 or greater. Third, individual items should load more strongly on intended constructs than on other constructs. Fourth, the construct’s average variance extracted (AVE) should be at least 0.5 to confirm that the construct-related variance is higher than the error variance (Hair et al., 2017). All entries in Tables 3 and 4 indicate satisfactory levels of convergent validity, except for the AVE for UCP (0.46), which is close to 0.5.

To achieve discriminant validity, it is recommended that the square root of AVE for a construct be larger than all other cross-correlations (Fornell & Larcker, 1981). Entries in Table 3 meet these requirements. Additionally, recommended robust checks were used. We used the heterotrait-monotrait ratio of correlations (HTMT) to assess the robustness of discriminant validity (Henseler et al., 2015). HTMT ratios lower than 0.90 are considered good and best if the ratios are above 0.85. Furthermore, p-values (one-tailed) for HTMT ratios are good if values lower than 0.05 are obtained. The results shown in Appendix B offer further support for the discriminant validity of the study’s constructs.

Table 2. Constructs and Measurement Items

| Construct          | Identification | Item                                                                 |
|--------------------|----------------|----------------------------------------------------------------------|
| Self-efficacy      | Sef1           | I have basic knowledge on how to avoid *unhygienic cyber practices*. |
|                    | Sef2           | I find it easy to implement preventive measures against *unhygienic cyber practices*. |
|                    | Sef3           | I have the skills and expertise to avoid engaging in *unhygienic cyber practices*. |
| Self-regulation    | Sre1           | I take it upon myself not to engage in *unhygienic cyber practices*. |
|                    | Sre2           | I self-monitor my activities to make sure I do not inadvertently engage in *unhygienic cyber practices*. |
|                    | Sre3           | If I found myself engaging in *unhygienic cyber practices*, I would be very upset. |
|                    | Sre4           | Engagements in *unhygienic cyber practices* are unacceptable to me. |
| Computer monitoring| Mon1           | I believe that my organization monitors its employees’ cyber practices and engagements. |
|                    | Mon2           | I believe that employee work-related computing activities are monitored by my organization. |
|                    | Mon3           | I believe that my organization monitors computing activities to ensure that employees are performing only explicitly authorized tasks. |
|                    | Mon4           | I believe that my organization reviews logs of employees’ computing activities on a regular basis. |
| SETA programs      | Set1           | My organization provides training to help employees improve their awareness of computer and information security issues. |
|                    | Set2           | My organization provides employees with education on computer issues. |
|                    | Set3           | My organization educates employees on their computer security responsibilities. |
|                    | Set4           | In my organization, employees are briefed on the consequences of engaging in *unhygienic cyber practices*. |
Table 3. Descriptive Statistics, Item Reliability, AVEs, and Inter-construct Correlations

|       | Mean  | SD   | COM  | CRA   | AVE   | SEFF | SREG  | SETA  | MONI  | UCP   |
|-------|-------|------|------|-------|-------|------|-------|-------|-------|-------|
| SEFF  | 4.51  | 1.54 | 0.90 | 0.84  | 0.75  | 0.87 | 0.16  | 0.32  | 0.29  | -0.15 |
| SREG  | 5.08  | 1.70 | 0.86 | 0.79  | 0.62  | 0.16 | 0.79  | 0.13  | -0.03 | -0.07 |
| SETA  | 3.75  | 1.87 | 0.94 | 0.91  | 0.78  | 0.32 | 0.13  | 0.88  | 0.46  | -0.13 |
| MONI  | 4.21  | 1.83 | 0.93 | 0.90  | 0.76  | 0.29 | -0.03 | 0.46  | 0.87  | -0.23 |
| UCP   | 3.28  | 2.01 | 0.84 | 0.78  | 0.46  | -0.15| -0.07 | -0.13 | -0.23 | 0.68  |

Note: SEFF = Self-efficacy, SREG = Self-regulation, MONI = Computer monitoring, SETA = SETA programs, COM = composite reliability; CRA = Cronbach’s alpha; AVE = average variance extracted; SD = Standard deviation

Table 4. Item Loadings and Cross-loadings

|       | Self-efficacy | Self-regulation | SETA programs | Computer monitoring | UCP |
|-------|---------------|-----------------|---------------|---------------------|-----|
| Seff1 | 0.868         | 0.16            | 0.281         | 0.286               | -0.22|
| Seff2 | 0.904         | 0.206           | 0.272         | 0.288               | -0.124|
| Seff3 | 0.828         | 0.036           | 0.267         | 0.187               | -0.03|
| Sreg1 | 0.172         | 0.854           | 0.108         | 0.025               | -0.058|
| Sreg2 | 0.192         | 0.832           | 0.142         | 0.059               | -0.148|
| Sreg3 | 0.081         | 0.772           | 0.029         | -0.113              | 0.023|
| Sreg4 | 0.026         | 0.701           | 0.122         | -0.081              | -0.035|
| Seta1 | 0.273         | 0.188           | 0.864         | 0.335               | -0.102|
| Seta2 | 0.269         | 0.097           | 0.887         | 0.344               | -0.043|
| Seta3 | 0.291         | 0.084           | 0.883         | 0.483               | -0.12|
| Seta4 | 0.282         | 0.085           | 0.908         | 0.448               | -0.205|
| Mon1  | 0.317         | 0.013           | 0.393         | 0.855               | -0.265|
| Mon2  | 0.281         | 0.016           | 0.422         | 0.903               | -0.236|
| Mon3  | 0.201         | 0.021           | 0.38          | 0.906               | -0.223|
| Mon4  | 0.231         | -0.159          | 0.398         | 0.831               | -0.077|
| UCP_3 | -0.139        | -0.171          | -0.085        | -0.175              | 0.664|
| UCP_4 | -0.166        | -0.083          | -0.115        | -0.16               | 0.756|
| UCP_5 | -0.051        | 0.004           | -0.005        | -0.102              | 0.69|
| UCP_6 | -0.185        | -0.036          | -0.09         | -0.146              | 0.634|
| UCP_9 | 0.013         | 0.029           | -0.188        | -0.186              | 0.656|
| UCP_2 | -0.061        | -0.034          | -0.063        | -0.176              | 0.67|
| UCP_1 | 0.032         | -0.172          | 0.024         | 0.048               | 0.445|
| UCP_7 | 0.118         | -0.075          | 0.025         | 0.046               | 0.325|
| UCP_8 | 0.031         | 0.084           | -0.107        | -0.11               | 0.44|
| UCP_10| -0.008        | -0.083          | -0.194        | -0.054              | 0.381|

Note: The UCP items are presented in loadings table to demonstrate their distinct nature from the items used to represent the reflective constructs.
5.2 Structural Model Assessment

After assessing the measurement model validity, the hypotheses were tested using WarpPLS software, which provides information on several model fit and quality indices (Kock, 2020). To obtain satisfactory predictive and explanatory quality, it is recommended that the p-values of the average path coefficient, average $R^2$, and average adjusted $R^2$ should be below 0.05 (Kock, 2020). Furthermore, the average full collinearity VIF and average block VIF should be 3.3 or lower (Kock, 2020). The global fit measure of Tenenhaus’ goodness of fit (GoF) should be satisfactory; namely, GoF is large if it is equal to or greater than 0.36, medium if it is equal to or greater than 0.25, and small if it is equal to or greater than 0.1 (Wetzels et al., 2009). The values presented in Table 5 show that the proposed research model exhibits adequate predictive and explanatory power.

The results of the structural model, including the amount of variance explained ($R^2$), path coefficients ($\beta$), and path significance (p-value), are presented in Figure 3. The results show that SETA programs and CM explain 16% and 6% of self-efficacy and self-regulation, respectively. Self-efficacy, self-regulation, SETA programs, CM, and the control variables explain 21% of the variance in employee self-reported involvement participation in UCP. An $R^2$ of 0.20 and above is adequate (Hair et al., 2017). Five out of eight hypotheses were supported. Namely, the results of the analysis indicate that hypotheses H1, H3, H5a, H5b, and H6a are supported, while H2, H4, and H6b are unsupported by the data. A summary of the hypothesis tests is presented in Table 6.

Regarding the control variables, the results indicate that the frequency of UCP involvement of workers in small-sized organizations is higher than in larger organizations. Males and workers with

Table 5. Structural Model Fit and Quality Indices

| Measure                          | Obtained value | Assessment criteria |
|----------------------------------|----------------|--------------------|
| Average path coefficient (APC)   | 0.148, $p = 0.016$ | p-value should be below 0.05 |
| Average $R^2$                    | 0.142, $p = 0.019$ | p-value should be below 0.05 |
| Average adjusted $R^2$           | 0.115, $p = 0.038$ | p-value should be below 0.05 |
| Average block VIF                | 1.122           | Acceptable if less than 3.3 |
| Average full collinearity VIF    | 1.290           | Acceptable if less than 3.3 |
| Tenenhaus GoF                    | 0.339           | Small if $\leq 0.1$; Medium if $\leq 0.25$; Large if $\leq 0.36$ |

Figure 3. The PLS results (Note: * significant at $p < 0.05$ level; ** significant at $p < 0.01$ level; ns = not significant)
more computer knowledge are more likely to engage in UCP. The availability of formal IS policies, data collection locations, age, and computer usage years did not appear to influence UCP engagement for the study’s participants.

6. DISCUSSIONS AND CONCLUSION

6.1 Findings

By focusing on viewpoints from a developing country in Africa, this study empirically investigated how personal cognitive factors and organizational reinforcing mechanisms can reduce workers’ involvement in UCP. Our data analysis produced both expected and unexpected results; we will begin by discussing the unsupported hypotheses.

To some degree, inconsistent results may indicate the potential effect of context (Johns, 2017). The result showing that SETA programs do not decrease workers’ involvement in UCP (H4) is counterintuitive because such programs are initiated to accomplish such an objective (D’Arcy et al., 2009). We believe this unexpected result in our study may be due to extraneous influences. Indeed, a post hoc analysis of the data shows that SETA programs reduced involvement in UCP for participants from organizations with IS security policies (N = 39); the presence of IS security policies in organizations, to an extent, indicate the availability of security awareness and education (D’Arcy et al., 2009; KNOWBE4, 2019; Lowry et al., 2015; Posey et al., 2015). Furthermore, the relationships between SETA programs and UCP engagement were not statistically significant for participants who indicated they did not have IS policies or were unaware of the existence of such in their organizations (N = 104).

Thus, the preponderance of participants with no IS policies in their organizations, as well as the respondents’ low average score of 3.75 for SETA programs availability compared to the other constructs’ scores (Table 3), might have caused the low explanatory power in the relationship between SETA programs and the dependent construct. Abraha (2015), who conducted a study in the research context of Ethiopia, noted that the “majority of the respondents (77.1%) also said that they do not have any organizational structure specifically dedicated to dealing with cybercrime threats,” which supports our explanation. Broadly, our result in this aspect seems to affirm observations suggesting that a lack of resources in developing countries does not bode well for cyber and IS security postures (Ifinedo, 2009; Ifinedo & Akinnuwesi, 2015; Ameen et al., 2021). This is because SETA programs are expensive (Morgan, 2019), and organizations in Ethiopia, which is not considered a rich country (World Bank Report, 2021), may struggle to implement such programs.

| Hypotheses | Path coefficient | Significance (p-value) | Status |
|------------|-----------------|------------------------|--------|
| H1: Self-regulation (-)→ UCP | -0.17 | 0.05 | Supported |
| H2: Self-efficacy (-)→ UCP | -0.11 | 0.09 | Not supported |
| H3: Computer monitoring (-)→ UCP | -0.23 | 0.01 | Supported |
| H4: SETA programs (-)→ UCP | 0.04 | 0.16 | Not supported |
| H5a: SETA programs → Self-efficacy | 0.24 | 0.01 | Supported |
| H5b: Computer monitoring → Self-efficacy | 0.25 | 0.01 | Supported |
| H6a: SETA programs → Self-regulation | 0.20 | 0.01 | Supported |
| H6b: Computer monitoring → Self-regulation | -0.13 | 0.10 | Not supported |

Note: (-)→ = Negative relationship; → = Positive relationship
Admittedly, self-efficacy is widely reported to be imperative for favorable IS security behaviors in developed contexts (Ng et al., 2009; Rhee et al., 2009; Lee & Larsen, 2009; Ifinedo, 2014). The result in our research context indicating that the participants’ self-efficacy relating to acceptable cyber practices does not reduce workers’ engagement in UCP is not unexpected (e.g., Abraha, 2015; KNOWBE4, 2019). Indeed, recent reports (KNOWBE4, 2019; The African Report, 2021) have indicated that end-users on the African continent do not possess sufficient knowledge of UCP and related IS security issues. A cross-cultural study of cybersecurity compliance among workers in developing and developed countries carried out by Ameen et al. (2021) showed that national contexts matter, and employees in developing countries do not believe they have “confidence in their ability to deal with a security threat… and they do not feel comfortable with doing so without assistance” (p. 13). This background information helps to explain the lack of support for H2.

Another interesting finding of this study concerns the lack of support for the relationship between CM and self-regulation (H6b). Hair et al. (2010) suggests that it is possible to accept the hypothesized path’s coefficient (β) of -0.13 at the p < 0.10 level; had we done so, the prediction would have been supported. However, as the beta’s direction is inconsistent with our prediction, we did not accept the result. This particular result suggests that workers with low self-regulation regarding acceptable cyber practices are more likely to be positively impacted by CM than their high self-regulation counterparts. This proposition is in line with observations made by Urbaczewski and Jessup (2002), who indicated that electronic monitoring tends to yield differing outcomes for high- and low-performance individuals. Zimmerman (2002) described self-regulation in terms of performance, among other elements. Regardless, more research is needed to ascertain the nature of this relationship in the context of UCP involvement.

Regarding RQ1, the result shows that higher levels of self-regulation regarding acceptable cyber practices decrease employee involvement in UCP, which supports H1. Thus, employees who possess higher levels of purposive self-evaluation and adjustment towards acceptable cyber practices and can self-judge their behavior are less likely to participate in UCP. This finding is similar to observations reported elsewhere (LaRose et al., 2008; Li et al., 2018; Ugrin et al., 2008).

Regarding RQ2, H3 is supported, suggesting that CM decrease employee involvement in UCP. This finding affirms the viewpoint indicating that workers’ participation in ill-advised cyber-related practices can be controlled by a mechanism ensuring that their computing and cyber practices are being routinely monitored. This finding lends credence to evidence in studies highlighting the importance of CM in improving security culture postures (Chen et al., 2015), discouraging sanctioned computing practices, and reducing IS security violations (D’Arcy et al., 2009; D’Arcy & Hovav, 2008; Urbaczewski & Jessup, 2002).

Regarding RQ3, the results show that employee self-efficacy related to acceptable cyber practices is increased by SETA programs and CM, which supports H5a and H5b, respectively. Thus, workers’ self-efficacy regarding acceptable cyber practices positively benefitted from the provision of SETA programs in their organizations (Burns et al., 2018; D’Arcy et al., 2009). This insight shows that workers’ perceptions of their self-efficacy regarding cyber-related practices was enhanced by reinforced training, awareness, and other guidance on the issue. Our finding agrees with espoused insights in the trade press and academic publications, signifying the critical role of SETA initiatives in increasing employee cybersecurity knowledge (KnowBe4, 2018; Posey et al., 2015). Hence, an individual worker’s cognitive beliefs about avoiding UCP is enhanced when his or her computing and cyber activities are regularly monitored. This result concurs with similar findings and observations in the extant literature (Larson & Callahan, 1990; Moos & Azevedo, 2008; Nietfeld et al., 2006).

As hypothesized in H6b, SETA programs improved self-regulation regarding acceptable cyber practices. This result implies that employees’ self-regulative processes related to engagement in UCP are significantly impacted by SETA programs, suggesting that such training, awareness, exposure, and guidance helps adjust workers’ cognitive beliefs about such concerns. Hence, self-evaluation of acceptable cyber practices in the organization, self-judgment on such matters, and self-reaction to
ensure commitment to acceptable standards are favorably nurtured by SETA programs. Our finding for the effect of SETA initiatives on self-regulation is similar to observations made by others (Bell & Kozlowski, 2002; Park et al., 2017).

6.2 Theoretical Contributions

Our study contributes to research on motivational antecedents of acceptable end-user security behavior using the example of workers’ involvement in UCP. We introduce Bandura’s (1986) theory of reciprocal determinism with its personal-environment-behavior conceptualization as a viable theoretical framework to study end-user security behavior related to UPC. Our results provide partial support for the suitability of Bandura’s theory of reciprocal determinism to end-user security research. This study demonstrates that other than sanctions and fear appeals, personal cognitive factors and organizational reinforcing tools could effectively manage and control UCP.

We empirically demonstrate that personal cognitive factors of self-efficacy and self-regulation are important in reducing employee involvement in UCP. To the best of our knowledge, this study is among the first to examine the effect of self-regulation on UCP engagement. Our findings are pertinent given that prior IS security studies have amplified the critical roles of sanctions and fear appeals in driving compliance. Our study shows that personal cognitive beliefs related to one’s competence, skills, and abilities to self-evaluate, self-judge, and self-adjust in the area of acceptable cyber engagement can motivate or shape employees’ end-user security behavior.

Our study provides empirical evidence supporting the significance of CM in reducing employee involvement in UCP. Although the construct of SETA programs was not found to reduce UCP involvement directly, it does so indirectly through their cognitive beliefs of self-efficacy and self-regulation related to acceptable cyber engagement. Our study provides initial evidence to support the importance of CM in elevating a worker’s self-regulative process in the context of UCP involvement. We also demonstrate that CM and SETA programs positively enhance employee self-efficacy on the subject. This study is among the first of its kind to explore these hypothesized relationships in the context of employee involvement in UCP.

Using empirical data from an under-researched region, we broaden perspectives, thereby enriching insights in the IS security sub-domain. For example, our data analysis offered an insight suggesting that an employee’s self-efficacy related to engagement in acceptable cyber practices might hinge on contextual influences. Similarly, SETA programs’ availability and their impact on reducing workers’ involvement in UCP might be contextual. Thus, where an individual is located might have a bearing on his or her ability to deal with UCP and related IS security issues (e.g., Bellman et al., 2004; Ifinedo, 2019; KNOWBE4, 2019; The African Report, 2021; Ameen et al., 2021).

Methodologically, we used self-reported behavior, compared to the putative construct of “intention” commonly used in most of the previous studies (Cram et al., 2019). Our utilization of multiple examples of UCP for the study could guide researchers seeking to explore similar phenomena; more precisely, our UCP examples offer a foundation for future inquiries to build upon and expand.

6.3 Practical Implications

The findings of our study also have implications for practitioners. Our results advance the viewpoint suggesting that technical (e.g., employing technology to monitor employee cyber activities at work) and personal cognitive factors (e.g., self-regulation and self-efficacy) are viable alternatives for organizations to consider where other approaches (e.g., sanctions) do not successfully prevent or reduce ill-prescribed security practices. Undoubtedly, CM has several issues (e.g., ethical, legal, and privacy concerns) associated with its use (Gumbus & Grodzinsky, 2008; Miller & Weckert, 2000); nonetheless, our result shows that managers could benefit from investing and deploying such tools to monitor workers’ cyber engagements in work environments.

Given the importance of self-regulation in the study, managers could evaluate their workers’ self-regulative attributes to determine who has low or high self-regulation with acceptable cyber-related
engagements. Those found to have low self-control could be provided with specialized psychological training to improve their cognitive belief deficits. Likewise, high self-control workers could be trusted to perform more delicate and sensitive tasks in the organization (e.g., work with intellectual property data stored online) since their high self-regulative processes would guide them against engaging in ill-advised cyber practices that could harm organizational interests.

This study also suggests that organizations could continue to use the two reinforcing mechanisms of SETA programs and CM to help reduce employee involvement in UCP. Security training and awareness programs enhance self-efficacy, so they are needed in organizations where workers engage in any form of UCP. Given the importance of rewards—monetary or non-monetary—in enhancing compliant security behavior (Chen et al., 2012), they could be provided to workers to stimulate their self-efficacy related to acceptable cyber practices. Furthermore, given the increasing importance of team-based approaches in controlling cybersecurity incidents (IIROC, 2012), workers with high self-efficacy in cyber practices could be given memberships in such teams or tasked to take leadership roles in such sub-groups. Our study indicates that the need exists for cyber and IS security awareness knowledge to be transferred from regions of the world where it is available to parts of the world (e.g., Sub-Saharan Africa) lacking such knowledge. The provision of financial resources to improve cyber security awareness and education in the region could also be considered (The African Report, 2021).

Small businesses face resource constraints. Our data suggest that small-sized organizations in the research location or comparable settings could seek various forms of assistance (e.g., financial or technical) to help manage the disproportionate occurrence of UCP among their workers. Instituting SETA programs incurs financial costs (Morgan, 2019), which small firms may not be able to afford. The need also exists for male workers to be carefully sensitized to the dangers of UCP. Our results suggest that practitioners should pay more attention to managing the cyber and computing activities of workers more knowledgeable about computers because such workers are more likely to engage in UCP.

### 6.4 Limitations and Future Study

This study has limitations. For parsimony, we used four constructs to represent personal and environmental factors; admittedly, other antecedent factors (e.g., outcome expectancy and peer influence) that may affect workers’ involvement in UCP were not selected. Future research could incorporate such factors to fill this gap. We used self-reported responses for analysis because of the difficulty in obtaining security-related information in organizations. We cannot ascertain whether social desirability bias exists in the collected data. Future research could use workers’ actual computer logs, if possible, to mitigate such concerns.

Data were collected from one cohort of insiders (i.e., employees). It is unlikely that the findings reported herein could be generalized to all categories of insiders. Future studies could use different groups of workers to improve the generalizability of conclusions. As the data were collected in one country, we caution against generalizing the study’s findings to all countries in its region or elsewhere. Comparative studies could be commissioned in the future to enrich the insights gained from this study. We used cross-sectional data, which is known to have shortcomings; future inquiries in the area could use longitudinal data to offer additional insights. Workers’ tasks and job complexities may affect the types of UCP to which workers are exposed; however, we did not control for them in the study. Attention should be paid to such concerns in future work. Using the Delphi study approach could be more rewarding for generating UCP in research locations; others could consider utilizing such an approach in the study. We did ask participants whether they had SETA programs in their work environments; future studies should consider asking such a question.

To generate further insights, Bandura’s triadic reciprocal determinism with bidirectional paths could be used in future studies. For example, it could be illuminating to know whether UCP prevalence in an organization lessens workers’ self-efficacy regarding such matters and if UCP prevalence might reflect contexts where security training or monitoring are lacking. Results from our study call for
future research to be conducted to determine whether deploying CM to control employee involvement in UCP is less effective for workers with high self-regulation.

7. CONCLUSION

Curbing workers’ involvement in UCP is a critical issue for managers worldwide, including those in Sub-Sahara Africa. Although research from other parts of the world has examined the influence of personal cognitive and environmental factors on UCP engagement, studies from the African continent, such as the current effort, are rare. We drew from a simplified version of Bandura’s triadic reciprocality theory. Our results show that workers’ self-regulation decreases the urge to engage in UCP. Employees are less likely to be involved in UCP when their organizations monitor their computers or other work-related IT tools. The findings also reveal that workers’ self-efficacy regarding acceptable cyber practices do not decrease UCP engagement, a result highlighting reality in the research context, which departs from perspectives reported in advanced countries.

The favorable roles of computer monitoring and the availability of SETA programs in enhancing workers’ self-efficacy related to acceptable cyber practices were demonstrated by our study. Likewise, our results show that SETA programs positively impact workers’ self-regulation regarding acceptable cyber security practices. Few researchers have investigated such relationships in end-user security behavior research. This study draws managers’ attention to relevant personal cognitive and organizational reinforcing tools to consider in controlling and managing workers’ behaviors regarding acceptable cyber security practices. Future studies are needed to examine the roles of other pertinent sub-factors, such as social norms, rewards, national IT policies, personal attitudes, and outcome expectancy. Overall, this study contributes to the growing body of research on UCP and end-user security behavior with viewpoints from an under-explored region of the world.

ACKNOWLEDGMENT

This research is supported by a grant (REB File No. 18-204) received from Brock University, Canada. The authors are grateful for the assistance we received from the following individuals: Ms. Meseret Ayano, Mr. Kennedy Odishika, Dr. Salehu Anteneh, Dr. Mesfin Fikre, Prof. Anteneh Ayanso, Prof. Faith-Michael Uzoka, and Prof. Olumide Longe.

FUNDING AGENCY

Publisher has waived the Open Access publishing fee.
REFERENCES

Abraha, H. (2015). The state of cybercrime governance in Ethiopia. Center for Global Communication Studies. Retrieved from https://www.researchgate.net/publication/322234805_THE_STATE_OF_CYBERCRIME_GOVERNANCE_IN_ETHIOPIA

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers’ data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. Computers in Human Behavior, 114, 106531. doi:10.1016/j.chb.2020.106531

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. Management Information Systems Quarterly, 34(3), 613–643. doi:10.2307/25750694

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. Journal of Organizational and End User Computing, 16(3), 22–40. doi:10.4018/joeuc.2004070102

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84(2), 191–215. doi:10.1037/0033-295X.84.2.191 PMID:847061

Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. Prentice-Hall.

Bandura, A. (1991). Social cognitive theory of self-regulation. Organizational Behavior and Human Decision Processes, 50(2), 248–287. doi:10.1016/0749-5978(91)90022-L

Bandura, A. (2005). The primacy of self-regulation in health promotion. Applied Psychology, 54(2), 245–254. doi:10.1111/j.1464-0597.2005.00208.x

Bandura, A., & Adams, N. E. (1977). Analysis of self-efficacy theory of behavioral change. Cognitive Therapy and Research, 1(4), 287–310. doi:10.1007/BF01663995

Barlock, S., Buffomante, T., & Rica, F. (2014). Cyber security: It’s not just about technology. Retrieved from https://assets.kpmg/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf

Bell, B. S., & Kozlowski, S. W. J. (2002). Adaptive guidance: Enhancing self-regulation, knowledge, and performance in technology-based training. Personnel Psychology, 55(2), 267–306. doi:10.1111/j.1744-6570.2002.tb00111.x

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. The Information Society, 20(5), 313–324. doi:10.1080/01972240490507956

Blue Coat Systems Inc. (2015). Research shows workers ignoring known cyber risks, surfing adult content and downloading unapproved apps. Retrieved from https://pressreleases.responsesource.com/news/87288/research-shows-workers-ignoring-known-cyber-risks-surfing-adult-content/

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. Behaviour & Information Technology, 34(10), 1022–1035. doi:10.1080/0144929X.2015.1028448

Bogonko, B. (2017). An investigation on the techno-human influence on examination information security management: A case of three Kenyan universities (MSc. Thesis). United States International University - Africa. Retrieved from http://erepo.usiu.ac.ke/11732/3532

Brick, J., & Kalton, G. (1996). Handling missing data in survey research. Statistical Methods in Medical Research, 5(3), 215–238. doi:10.1177/096228029600500302 PMID:8931194

Brown, J. M. (1998). Self-regulation and the addictive behaviors. In Treating addictive behaviors (2nd ed.). Plenum Press.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. Management Information Systems Quarterly, 34(3), 523–548. doi:10.2307/25750690
Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2018). Intentions to comply versus intentions to protect: A vie theory approach to understanding the influence of insiders’ awareness of organizational seta efforts. *Decision Sciences, 49*(6), 1187–1228. doi:10.1111/deci.12304

Butler, R., & Butler, M. (2015). The password practices applied by south african online consumers: Perception versus reality. *South African Journal of Information Management, 17*(1). Advance online publication. doi:10.4102/sajim.v17i1.638

Carver, C. S., & Scheier, M. F. (2004). Self-regulation of action and affect. In K. D. Vohs & R. F. Baumeister (Eds.), *Handbook of self-regulation: Research, theory, and applications* (pp. 13–39). The Guilford Press.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems, 55*(3), 11–19. doi:10.1080/08874417.2015.11645767

CIA-World Factbook. (2020). *Country report – Ethiopia*. Retrieved from https://www.cia.gov/library/publications/the-world-factbook/geos/et.html

Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *Management Information Systems Quarterly, 23*(2), 145–158. doi:10.2307/249749

Corral-Verdugo, V. (1997). Dual ‘realities’ of conservation behavior: Self-reports vs observations of re-use and recycling behavior. *Journal of Environmental Psychology, 17*(2), 135–145. doi:10.1006/jevp.1997.0048

Cram, W. A., D’Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *Management Information Systems Quarterly, 43*(2), 525–554. doi:10.25300/MISQ/2019/15117

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101. doi:10.1016/j.cose.2012.09.010

CyberEdge Group Report. (2020). *2020 cyberthreat report defense*. Retrieved from https://cyber-edge.com/wp-content/uploads/2020/03/CyberEdge-2020-CDR-Report-v1.0.pdf

D’Arcy, J., & Hovav, A. (2008). Does one size fit all? Examining the differential effects of is security countermeasures. *Journal of Business Ethics, 89*(1), 59–71. doi:10.1007/s10551-008-9909-7

D’Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98. doi:10.1287/isre.1070.0160

Dolan, S. L., Martin, R. A., & Rohsenow, D. J. (2008). Self-efficacy for cocaine abstinence: Pretreatment correlates and relationship to outcomes. *Addictive Behaviors, 33*(5), 675–688. doi:10.1016/j.addbeh.2007.12.001 PMID:18191329

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. doi:10.1145/2702123.2702249

Farshadkhah, S., Van Slyke, C., & Fuller, B. (2021). Onlooker effect and affective responses in information security violation mitigation. *Computers & Security, 100*, 102082. doi:10.1016/j.cose.2020.102082

Fernández, W. D. (2016). Commentary on Davison and Martinsons’ ‘context is king! Considering particularism in research design and reporting’. *Journal of Information Technology, 31*(3), 265–266. doi:10.1057/s41265-016-0004-8

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *JMR, Journal of Marketing Research, 18*(1), 39–50. doi:10.1177/002224378101800104

Gefen, D., & Straub, D. W. (2005). A practical guide to factorial validity using pls-graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16*, 91–109. doi:10.17705/1CAIS.01605
Gist, M. E., Schwoerer, C., & Rosen, B. (1989). Effects of alternative training methods on self-efficacy and performance in computer software training. *The Journal of Applied Psychology, 74*(6), 884–891. doi:10.1037/0021-9010.74.6.884

Gleson-Kreig, J. M. (2006). Self-monitoring of physical activity: Effects on self-efficacy and behavior in people with type 2 diabetes. *The Diabetes Educator, 32*(1), 69–77. doi:10.1177/0145721705284285 PMID:16439495

Gumbus, A., & Grodzinsky, F. (2008). Ethical and managerial implications of internet monitoring. In M. L. Mackenzie & S. L. Rosenberg (Eds.), *Emerging Business Theories for Educators and Practitioners*. Cambridge Scholars Press.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203–236. doi:10.2753/MIS0704-1222280208

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Sage.

Hamidi, H., & Moradi, S. (2017). Analysis of consideration of security parameters by vendors on trust and customer satisfaction in e-commerce. *Journal of Global Information Management, 25*(4), 32–45. doi:10.4018/JGIM.2017100103

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. doi:10.1007/s11747-014-0403-8

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54–60. doi:10.1145/1953122.1953142

Ifinedo, P. (2009). Information technology security concerns in global financial services institutions: Do socio-economic factors differentiate perceptions? *International Journal of Information Security and Privacy, 3*(2), 68–83. doi:10.4018/ijisp.2009040105

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69–79. doi:10.1016/j.im.2013.10.001

Ifinedo, P. (2019). End user nonmalicious, counterproductive computer security behaviors: Concept, development, and validation of an instrument. *Security & Privacy, 2*(3), e66. doi:10.1002/spy2.66

Ifinedo, P., & Akinnuwaesi, B. A. (2014). Employees’ non-malicious, counterproductive computer security behaviors (ccsb) in Nigeria and Canada: An empirical and comparative analysis. Paper presented at the 2014 IEEE 6th International Conference on Adaptive Science & Technology (ICAST), Ota, Nigeria.

Ifinedo, P., Mengesha, N., & Longe, O. (2019). Factors that influence workers’ participation in unhygienic cyber practices: A pilot study from Nigeria. Paper presented at the Information and Communication Technologies for Development. Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D. ICT4D 2019. IFIP Advances in Information and Communication Technology, Dar es Salaam, Tanzania. doi:10.1007/978-3-030-19115-3_25

IIROC. (2012). *Cybersecurity best practices guide for IIROC dealer members*. Retrieved from https://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf

Johns, G. (2017). Reflections on the 2016 decade award: Incorporating context in organizational research. *Academy of Management Review, 42*(4), 577–595. doi:10.5465/amr.2017.0044

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *Management Information Systems Quarterly, 34*(3), 549–566. doi:10.2307/25750691

KnowBe4. (2018). Security awareness training deployments deter, defeat hackers. Retrieved from https://www.knowbe4.com/hubfs/SecurityAwarenessTrainingDeploymentsDeterDefeatHackers.pdf

KnowBe4. (2019). *Whitepaper: African cybersecurity research report*. Retrieved from https://www.knowbe4.com/hubfs/African%20Cybersecurity%20Research%20Report.pdf

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration, 11*(4), 1–10. doi:10.4018/ijec.2015100101
Kock, N. (2020). Warppls© user manual: Version 7.0. ScriptWarp Systems.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM, 51*(3), 71–76. doi:10.1145/1325555.1325569

Larson, J. R., & Callahan, C. (1990). Performance monitoring: How it affects work productivity. *The Journal of Applied Psychology, 75*(5), 530–538. doi:10.1037/0021-9010.75.5.530

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445–454. doi:10.1080/01449290600879344

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of smb executives’ decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177–187. doi:10.1057/ejis.2009.11

Li, H., Luo, X., Zhang, J., & Sarathy, R. (2018). Self-control, organizational context, and rational choice in internet abuses at work. *Information & Management, 55*(3), 358–367. doi:10.1016/j.im.2017.09.002

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394–413. doi:10.17705/1jais.00232

Lin, T.-C., & Huang, C.-C. (2008). Understanding knowledge management system usage antecedents: An integration of social cognitive theory and task technology fit. *Information & Management, 45*(6), 410–417. doi:10.1016/j.im.2008.06.004

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193–273. doi:10.1111/isj.12063

MacKenzie, S. B., Podsakoff, P. M., & Jarvis, C. B. (2005). The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. *The Journal of Applied Psychology, 90*(4), 710–730. doi:10.1037/0021-9010.90.4.710 PMID:16060788

McAfee.com. (2020). McAfee security tips: 13 ways to protect your system. Retrieved from https://community.mcafee.com/t5/Consumer-Documents/McAfee-Security-Tips-13-Ways-to-Protect-Your-System/ta-p/549205

Miller, S., & Weckert, J. (2000). Privacy, the workplace and the internet. *Journal of Business Ethics, 28*(3), 255–265. doi:10.1023/A:1006232417265

Moos, D. C., & Azevedo, R. (2008). Monitoring, planning, and self-efficacy during learning with hypermedia: The impact of conceptual scaffolds. *Computers in Human Behavior, 24*(4), 1686–1706. doi:10.1016/j.chb.2007.07.001

Morgan, S. (2019). Global cybersecurity spending predicted to exceed $1 trillion from 2017-2021. Retrieved from https://cybersecurityventures.com/cybersecurity-market-report/

National Cyber security Alliance. (2007). *Stay safe online*. Retrieved from https://www.nist.gov/system/files/documents/itl/NCSA-DOC-NOI-Response-08012011.pdf

National Cybersecurity Alliance. (2020). Online safety basics. Retrieved from https://staysafeonline.org/stay-safe-online/online-safety-basics/

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users’ computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815–825. doi:10.1016/j.dss.2008.11.010

Nietfeld, J. L., Cao, L., & Osborne, J. W. (2006). The effect of distributed monitoring exercises and feedback on performance, monitoring accuracy, and self-efficacy. *Metacognition and Learning, 1*(2), 159–179. doi:10.1007/s10409-006-9595-6

Noar, S. M. (2006). A 10-year retrospective of research in health mass media campaigns: Where do we go from here? *Journal of Health Communication, 11*(1), 21–42. doi:10.1080/10810730600461059 PMID:16546917

Ogbanufe, O. (2021). Enhancing end-user roles in information security: Exploring the setting, situation, and identity. *Computers & Security, 108*, 102340. doi:10.1016/j.cose.2021.102340

Park, E. H., Kim, J., & Park, Y. S. (2017). The role of information security learning and individual factors in disclosing patients’ health information. *Computers & Security, 65*, 64–76. doi:10.1016/j.cose.2016.10.011
Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. Management Information Systems Quarterly, 31(1), 105–136. doi:10.2307/25148783

Podsakoff, P. M., & Organ, D. (1986). Self-reports in organizational research: Problems and prospects. Journal of Management, 12(4), 531–544. doi:10.1177/014920638601200408

Ponemon Institute. (2012). The human factor in data protection. Retrieved from https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf

Ponemon Institute. (2020). Cost of an insider breach report. Retrieved from https://www.ibm.com/account/reg/uk-en/signup?formid=urx-42429

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders’ motivation to protect organizational information assets. Journal of Management Information Systems, 32(4), 179–214. doi:10.1080/07421222.2015.1138374

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders’ protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. Management Information Systems Quarterly, 37(4), 1189–1210. doi:10.25300/MISQ/2013/37.4.09

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users’ information security practice behavior. Computers & Security, 28(8), 816–826. doi:10.1016/j.cose.2009.05.008

Schunk, D. H. (1990). Goal setting and self-efficacy during self-regulated learning. Educational Psychologist, 25(1), 71–86. doi:10.1207/s15326985ep2501_6

Security, O. (2021). The 21 biggest data breaches of the 21st century. Retrieved from https://optimumsecurity.ca/21-biggest-data-breach-of-21-century/

Stajkovic, A. D., & Luthans, F. (1998). Self-efficacy and work-related performance: A meta-analysis. Psychological Bulletin, 124(2), 240–261. doi:10.1037/0033-2909.124.2.240

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. Management Information Systems Quarterly, 22(4), 441–469. doi:10.2307/249551

Systems, V. B. (2019). 2019 data breach investigations report. https://enterprise.verizon.com/resources/reports/dbir/

Tannenbaum, S. I., Mathieu, J. E., Salas, E., & Cannon-Bowers, J. A. (1991). Meeting trainees’ expectations: The influence of training fulfillment on the development of commitment, self-efficacy, and motivation. The Journal of Applied Psychology, 76(6), 759–769. doi:10.1037/0021-9010.76.6.759

The African Report. (2021). Cybersecurity: Companies in africa need to do more to fight off attacks, says Kaspersky. Retrieved from https://www.theafricareport.com/61897/cybersecurity-companies-in-africa-need-to-do-more-to-fight-off-attacks-says-kaspersky

The ePolicy Institute. (2017). 2007 electronic monitoring & surveillance survey. Retrieved from http://www.epolicyinstitute.com/2007-survey-results

The Security Culture Report. (2017). In depth insights into the human factor. Retrieved from https://get.clt.re/security-culture-report-2017/

Ugrin, J. C., Pearson, J. M., & Odom, M. D. (2008). Cyber-slacking: Self-control, prior behavior and the impact of deterrence measures. Review of Business Information Systems, 12(1), 75–88. doi:10.19030/rbis.v12i11.4399

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

van Rensburg, S. K. J. (2021). End-User Perceptions on Information Security: Pragmatic Lessons on Social Engineering Attacks in the Workplace in Gauteng, South Africa. Journal of Global Information Management, 29(6), 1–16. doi:10.4018/JGIM.293290
Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems, 128*, 113160. doi:10.1016/j.dss.2019.113160

Wang, F., Shan, G. B., Chen, Y., Zheng, X., Wang, H., Mingwei, S., & Hailhua, L. (2020). Identity authentication security management in mobile payment systems. *Journal of Global Information Management, 28*(1), 189–203. doi:10.4018/JGIM.2020010110

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*(3), 267–284. doi:10.1057/ejis.2010.72

Wetzels, M., Odekerken-Schröder, G., & van Oppen, C. (2009). Using pls path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *Management Information Systems Quarterly, 33*(1), 177–195. doi:10.2307/20650284

Williams, G. C., Grow, V. M., Freedman, Z. R., Ryan, R. M., & Deci, E. L. (1996). Motivational predictors of weight loss and weight-loss maintenance. *Journal of Personality and Social Psychology, 70*(1), 115–126. doi:10.1037/0022-3514.70.1.115 PMID:8558405

Wood, R., & Bandura, A. (1989). Social cognitive theory of organizational management. *Academy of Management Review, 14*(3), 361–384. doi:10.2307/258173

World Bank Report. (2021). *The World Bank in Ethiopia*. Retrieved from https://www.worldbank.org/en/country/ethiopia/overview#:~:text=With%20more%20than%20112%20million,middle%2Dincome%20status%20by%202025

Yaokumah, W., Walker, D. O., & Kumah, P. (2019). SETA and security behavior: Mediating role of employee relations, monitoring, and accountability. *Journal of Global Information Management, 27*(2), 102–121. doi:10.4018/JGIM.2019040106

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems, 108*, 107–118. doi:10.1016/j.dss.2018.02.009

Zimmerman, B. (1989). A social cognitive view of self-regulated academic learning. *Journal of Educational Psychology, 81*(3), 329–339. doi:10.1037/0022-0663.81.3.329

Zimmerman, B. J. (2002). Becoming a self-regulated learner: An overview. *Theory into Practice, 41*(2), 64–70. doi:10.1207/s15430421tip4102_2
APPENDIX A

UCP items and their descriptive statistics

| ID   | Item                                                      | Mean | SD  |
|------|-----------------------------------------------------------|------|-----|
| UCP_1 | Using weak passwords at work                             | 3.23 | 1.95 |
| UCP_2 | Not updating work-related passwords regularly            | 3.87 | 2.10 |
| UCP_3 | Not logging out of secure systems after use              | 3.21 | 1.94 |
| UCP_4 | Not always treating sensitive organization data carefully | 3.06 | 1.88 |
| UCP_5 | Allowing others to use one’s work laptop                 | 2.59 | 2.03 |
| UCP_6 | Downloading unauthorized software onto work computer     | 3.20 | 2.11 |
| UCP_7 | Disclosing work-related passwords to others              | 2.56 | 2.11 |
| UCP_8 | Not backing up work files                                | 3.87 | 2.08 |
| UCP_9 | Logging into unsecure networks outside work, e.g. WIFI   | 3.77 | 2.13 |
| UCP_10| Using unauthorized or personal USB at work                | 3.94 | 2.05 |
| UCP_11| Storing work files in cloud without authorization        |      |     |
| UCP_12| Opening attachments in unsolicited emails                |      |     |
| UCP_13| Pasting or sticking computer passwords on office desks   |      |     |
| UCP_14| Visiting non-related websites at work                    |      |     |
| UCP_15| Not updating anti-virus and/or anti-spyware software at work |      |     |

Note: a) The items in *italics* are not included in the data analysis.
b) The items in **bold** font are used in final data analysis.
### APPENDIX B

| HTMT ratios   | p values (one-tailed) for HTMT ratios |
|---------------|---------------------------------------|
| **SELF**      | **SELF**                              |
| SREG          | SREG <0.001                           |
| SETA          | SETA <0.001 <0.001                    |
| MONI          | MONI <0.001 <0.001 <0.001             |
| UCP           | UCP <0.001 <0.001 <0.001 <0.001       |
| **(good if < 0.90, best if < 0.85)** | **(good if < 0.05)** |

**Princely Ifinedo** is a Professor at Brock University, Canada. He holds a Ph.D. in Information Systems (IS) from University of Jyväskylä, Finland, an MBA from the Royal Holloway, University of London, UK, an M.Sc. from Tallinn University of Technology, Estonia, a B.Sc. from the University of Port-Harcourt, Nigeria, and a Diploma (Education) from the University of British Columbia, Canada. His research includes ERP Success, IS Security Management, IS adoption in business and healthcare, E-government, E-business, E-learning, and IS in developing countries and transiting economies. He has presented research at various international IS conferences, contributed chapters to several books/encyclopedias, and published in several reputable journals such as I&M, JCIS, IJIM, JSS, JGIM, DATABASE, CHB, JOCEC, JITM, IMDS, EIS, IJITDM, JITD, JITM, JBTIM, JISP, and Internet Research. He has authored over 100 peer-reviewed publications. He is affiliated with AIS and ASAC.

**Nigussie Mengesha** is an Assistant Professor of Information Systems at the Goodman School of Business, Brock University in Canada. Dr. Nigussie Mengesha received his PhD in Information Systems from the University of Oslo in Norway, and MSc in Information Science from Addis Ababa University in Ethiopia. Dr. Mengesha’s research areas include IT and Strategy, Data Analytics, Information Systems Development and Integration, Open-Source Software, Security, and ICT4D. He has published in Information Technologies and International Development (ITID), Electronic Journal of Information Systems in Developing Countries (EJISD), African Journal of Information Systems (AJIS), International Journal of Information Systems and Social Change (IJSSC), and major international conferences in information systems such as International Conference on Information Systems (ICIS) and International Federation of Information Processing (IFIP) WG9.4.

**Rahel Bekele** is currently an Associate Professor in the School of Information Science at Addis Ababa University. She received her Masters in Information Science from Addis Ababa University and a doctorate in Computer Science from the University of Hamburg, Germany. She is actively engaged in ICT for Development research projects. Her current research interests include software development methods in the context of usability, mobility, and security. She has published in many journals including the British Journal of Educational Technology and SINET: Ethiopian Journal of Science and Technology, and many regional and international conferences in Information Systems and Technology.