Impact of Cyber Hygiene Behavior on Target Suitability using Dual Systems Embedded Dual Attitudes Model

Early stage paper

Harsh Parekh
Louisiana State University
hparek1@lsu.edu

Dr. Andrew Schwarz
Louisiana State University
aschwarz@lsu.edu

ABSTRACT

While the Covid-19 pandemic has emphasized the significance and difficulties of maintaining self-hygiene, the lack of attention given to cyber hygiene in mainstream cyber security literature has become increasingly apparent. Organizational leaders and industry experts in the security domain are urging to make this precautionary behavior a central focus against ever-rising security needs. In this article, we construct an understanding of cyber hygiene from the extant literature. Cyber Hygiene behavior in individuals could be habitual or self-controlled. First, we use the concept of dual systems theory to navigate the two pathways. Second, this research situates that such non-obligation behaviors are subjected to two competing attitudes that can exist simultaneously. Thus, we model dual attitudes within a reflexive and reflective systems framework (Dual Systems Theory). This combined model explains individuals' contradictory actions to their beliefs. Third, we seek to understand the impact of cyber hygiene behavior on target suitability. Overall, the research model explains individuals' influence of attitudes toward cyber hygiene practices can explain their likelihood of getting attacked. This research promises a holistic understanding of cyber hygiene behaviors from antecedents to its consequence.

Keywords

cyber hygiene, self-regulation, dual attitudes model, self-protection, target suitability, dual systems

INTRODUCTION

Security suffers endemic problems despite the increase in security investments due to several vulnerabilities. According to data from the (“Federal Trade Commission (FTC) Report” 2022), consumers lost almost $8.8 billion to fraud in 2022, representing a surge of over 30% from the prior year. The majority of this fraudulent activity was attributable to imposter scams and fake investing schemes. Security literature has had a dominant focus on mandating regulatory frameworks and applying industry standards. Deterrent procedures and preventive security practices have been long recognized as effective IS security need (Straub 1990), however, precautionary approaches are less discussed in the literature compared to the former. The popularity of the deterrence approach has been to deal with consequential issues for organizations. Information systems research is rife with studies that explain intentional damage by individuals (Harrington 1996; Straub and Nance 1990; Willison et al. 2018). However, unintentional damage caused by exposing organizations to security risks remains underexplored (Kwon and Johnson 2013). Such damages are a result of non-malicious users accidentally compromising the confidentiality, integrity, or availability of data or systems.

Security systems consist of technical and social guardians. Technological guardians consist of antivirus technology, intrusion detection systems, and firewalls, whereas, social guardians consist of security staff in an organization (Yar 2005). User behavior towards security and their personal computing is crucial for organizational security. Technological guardians have proven to be ineffective in detecting and preventing insider threats (Wang et al. 2015, 2017) and social guardians are challenged with limited resources against irregularities of cyber-spatial activities.

Thus, there arises a need to cultivate proactive information security behavior among individuals (D’Arcy et al. 2009; Lin et al. 2022). Training interventions in the past have made a note of employee’s current habits to improve their security policy compliance (Puhakainen and Siponen 2010). However, developing training interventions and best practices for precautionary security habits is challenged by situational variability and individual complacency.

Studies have found that individual characteristics (disgruntled employees) and organizational factors both contribute to individual’s malicious behavior (Hsu et al. 2015; Liang et al. 2016; Straub and Nance 1990). Information systems scholars have adopted from an early development in the criminology literature to understand the protective behavior. A potential target can be protected by deterrence, prevention, remedy, and detection (Straub and Welke 1998). An example of non-malicious threat is to compromise organizational credentials making systems vulnerable to attack. Since individuals’ contribution toward the suitability of the target remains unquantified, the actual threat caused by organizational insiders is underreported. More than a third of companies have detected overprivileged users and 60% of them suffer attacks due to phishing on those accounts (“Get the 2020 Cloud Threat Report” 2020).

Technology-assisted solutions help to improve compliance but are often not enough to mitigate all security risks (Cavusoglu et al. 2009; Siponen 2005). Employee’s security policy compliance beliefs are shaped by intrinsic benefit, the safety of resources and rewards (Bulgurcu et al. 2010). These intrinsic benefits constitute contentment, satisfaction, accomplishment and fulfillment about the compliance behavior. Self-protective behavior is not influenced by formal controls such as deterrence, rewards, or monitoring, rather more informal controls like self-control or social control driving such behavior. Self-protective behavior is motivated by factors such as perception of self-efficacy, threat susceptibility, and controllability. Previous studies have found that risk perception leads to precautionary behavior such as using anti-virus software (van Schaik et al. 2017). Self-protective behavior such as keeping antivirus current, installing a firewall and filtering emails can help achieve safe computing practices. Interestingly, messages that promote such pro-security actions by expressing positive consequences instead of applying aversive control are more persuasive (Anderson and Agarwal 2010).

Cyber hygiene is a self-protective behavior that is related to awareness about online security and practices associated with increasing cybersecurity. Motivated offenders look online to exploit poor cyber hygiene behaviors. Some examples of good cyber hygiene practices include avoidance of malicious content (emails, websites, or infected media), applying antivirus software, and updating systems regularly (Maennel et al. 2018). Cyber hygiene is a set of practices, whereas, security awareness is related to knowledge of security. User security behaviors have been categorized into maintaining cyber hygiene and threat response behavior. Many users suffer low awareness about technology-aided security techniques which emerges as a major challenge. A survey of 329 homes reported a majority of users are unable to distinguish between antivirus software and firewall (National cybersecurity alliance report). Users are often aware of the security threats but often lack situation-specific awareness (Jaeger et al. 2021; Moody et al. 2017) and defensive security practices. Cyber-related knowledge, capability, and motivation are factors that are reported to influence such protective behaviors. Effect of habit has been reported to make individuals more susceptible to phishing attacks (Ayaburi and Andoh-Baidoo 2019). While protection motivation theory has been used to explain cyber hygiene behavior evidence of behavior being habitual or deliberate is missing.

RQ1: How does an individual's attitude and IS habits influence their behavior towards cyber hygiene practices?

RQ2: How does individual's cyber hygiene behavior influence their target suitability?

Maintaining cyber hygiene have no formal sanctions or rewards for individuals. However, individuals' moral beliefs or commitments generated by their self-conscious would create informal deterrence to unhygienic behavior. While several security breaches such as the infamous WannaCry ransomware attack was criticized for maintaining a bad cyber hygiene, our understanding of literature fairly limited. Health psychology literature recognizes the value of self-regulation theory in understanding hygiene behaviors. The dual systems model of self-regulation has popularly been used to explain self-control in HCI literature. In this research, we utilize dual systems theory to understand the outcomes of cyber hygiene behavior. In the next section, we present a brief summary of all the components of our theoretical model.

CONCEPTUAL AND THEORETICAL MOTIVATION

Cyber Hygiene

The term Cyber Hygiene is borrowed from personal hygiene literature and is broadly perceived as 'creating and maintaining online safety'. Organizations find it challenging to monitor and reward/sanction their employers for safe computing practices and extra role security behaviors (Anderson and Agarwal 2010). The major challenge is with inclusivity of every possible action in security policies. Cyber hygiene is a self-protective behavior that is formally unregulated. From practitioners to academics there have been many attempts to define cyber hygiene, however, most of them have failed in producing a context-independent definition (Kappers et al. 2021; Maennel et al. 2018). The varied nature of these definitions symbolizes that cyber hygiene constitutes an array of different actions. Some of these actions are specialized like effective patch management and keeping a track of system health, while, others are simpler like every day internet use. To address this challenge, Vishwanath et al (2020) conceptualized cyber hygiene as "the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet-enabled devices from being compromised in a cyber-attack" using aspects of personal hygiene. This conceptualization serves as an operational definition that guides the categorization of cyber hygiene that is used in this study. Alternate conceptualization explains cyber hygiene from training context (Pfleeger et al. 2014), employee's perception context (Sheppard et al. 2013), and the technical context (Savold et al. 2017). With such varying contexts, this protective behavior has reportedly generated several outcomes.

Previous research explains different cyber hygiene components without an explicit conceptualization of terminology. For example, Anderson and Agarwal (2010) developed and explained a phenomenon of conscientious cybercitizens as individuals that show precautionary security behavior resulting in safe computing practices. Similarly, proposed taxonomy of protection motivation behaviors such as reporting suspicious behavior, appropriate data entry, secure email and internet use, etc. overlap extensively with cyber hygiene behaviors (Posey et al. 2013). While it is impossible to achieve ideal cyber hygiene behavior through security policies, evaluation of different cyber hygiene outcomes helps organizations maintain a favorable level. Good cyber hygiene behavior reduces victimization experiences (Howell 2021). The cyber hygiene behavior of top management in an organization is often more important due to elevated access rights. Thus, individuals experience different levels of susceptibility and need to maintain good cyber hygiene. Even the degree to which urgency arousal cues in a phishing email invokes feelings in individuals positively influences their phishing susceptibility (Ayaburi and Andoh-Baidoo 2019).

Employees lack awareness of security risks associated with bad hygiene practices such as personal use of social media at work, low self-efficacy, understanding website credentials etc.

(Arachchilage and Love 2014). Such individual differences in people result in different level of susceptibility to online victimization. Individuals are situationally aware or have high computer proficiency reported thwarting their personal activity while accessing a public Wi-Fi network (Maimon et al. 2022). This explains why certain individuals fall prey to multiple socially engineered attacks such as spear phishing. To measure the cyber hygiene construct Vishwanath et al (2020) proposed an 18-item cyber hygiene inventory (CHI) scale that measures five distinct dimensions of cyber hygiene (Vishwanath et al. 2020). Their scale measures human cyber interactions that capture individuals' self-belief about the technology, their cognitively processing ability and their online banking behavior. In this study we utilize those dimensions as a contextual categorization of cyber hygiene scenarios- storage and device hygiene, transmission hygiene, social media hygiene, authentication and credential hygiene, and email and messaging hygiene. Trinkle, Crossler & Warkentin (2014) measure factors influencing employees to play online social network games on company-owned computers which is similar to social media hygiene in our study (Trinkle et al. 2014). Individual differences such as information handling, social media use, password management, mobile device and email use are found to be predictive of attitudes towards cyber hygiene (Neigel et al. 2020).

Dual Systems model

The core tenet of Dual systems theory is that behavior is determined by the interplay between automatic and controlled information processing (Hofmann et al. 2009). Individual information processing can produce impulsive, largely automatic forms of behavior or deliberate, largely controlled forms of behavior. Individual differences are responsible for the selection of information processing systems. Resultant behavior in a *reflective system* is a consequence of the decision process (reasoned action), whereas, in a *reflexive system* is largely governed by habits

(Strack and Deutsch 2004). Both reflexive and reflective systems operate in parallel. In the Cyber hygiene context, it can operate as a result of habits (Baraković and Baraković Husić 2022; Cain et al. 2018) or could be the result of thoughtfully reflective decision making (Howell 2021). Polites et al (2018) have established in their work that both systems of information processing influence self-related processes (Polites et al. 2018). Cyber hygiene behavior is often not obligatory (unlike compliance) and individuals make a choice based on their self-control. From the above conceptualization of cyber hygiene (Vishwanath et al. 2020) we know that it produces self-protective outcomes. Figure 1 represents the discussion so far.

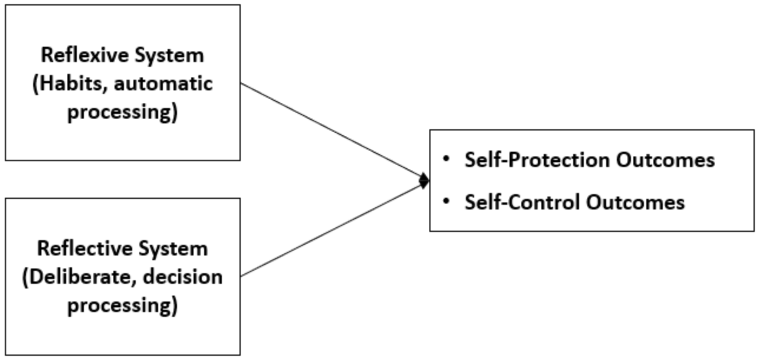
Reflexive System (Habits, automatic processing)
Reflective System (Deliberate, decision processing)
• Self-Protection Outcomes
• Self-Control Outcomes

Figure 1. Dual systems and self-related process outcomes

Dual systems theory has been used in the literature to predict self-related processes (Polites et al. 2018) and self-related outcomes (Metcalfe and Mischel 1999; Soror et al. 2015; Turel and Qahri-Saremi 2016). Soror et al (2015) utilized dual systems perspective to understand the negative consequences of mobile phone use. Similarly, Polites et al (2018) measured social network site (SNS) self-identity with the dual systems theory (Polites et al. 2018). Hu and Xu (2018) utilized dual systems perspective to understand non-compliance behavior and found the interesting role of the reflexive system (self control)(Xu and Hu 2018). Design features of mobile applications have been evaluated from a dual systems perspective to understand their support of digital self-control for its users (Lyngs et al. 2019). Similarly, mindfulness prevents automatic or habitual responses to phishing emails by activation of rational decision-making. Thus, the dual systems perspective is apt to explain an individual's self-control behaviors that are based on hedonic impulses or deliberate evaluations. It has been separately assessed that both habit/automatic use (Ayaburi and Andoh-Baidoo 2019) and thoughtful usage (Howell 2021) leads to victimization experiences. In another research, Turel and Qahri-Saremi (2016) found that people have strong cognitive-emotional preoccupation and weak cognitive-behavioral control on problematic use of social networking services (Turel and Qahri-Saremi 2016). However, to our knowledge, the two systems have not been explored in the same model (narrating different context) to affect victimization.

Cyber hygiene as a habitual behavior (Reflexive system)

Not all decisions require thoughtful consideration as some are habitual. Continued use of technology over a long period of time is attributed largely to the habit over conscious intentions (Polites and Karahanna 2013). Literature on information system habits is more recent than reasoned action literature. In the context of IS usage habit is defined as "the extent to which people tend to perform behaviors automatically because of learning" (Limayem et al. 2007). Thus, habit is a mindset that augments perceptual readiness to perform certain kind of behavior (resultant action). Habit is established through an individual's learned responses and helps in the automatic performance of behavior. While habit is largely explored in post-adoption literature it has found relevance in security policy compliance (Yoo and Rao 2014). Habit acts as an important antecedent to security policy compliance and protective behavior (Jenkins et al. 2010; Vance et al. 2012). Similarly, technology habits influence privacy-related protective behavior. People often agree to privacy updates and clauses without weighing the risks involved. Thus, habits generate both negative and positive outcomes for self-related processes.

Although Cyber hygiene habits (CHH) is a popular phrase in non-academic literature it has not been formalized yet in the noteworthy academic literature. Individual differences in CHH have been studied in security literature that builds our understanding of self-related process outcomes. Ayaburi and Andoh-Baidoo (2019) explained how individual's automatic use of communication media leads to their phishing victimization. An important measure in their study separated routine use of media with habitual use and concluded former was benign towards victimization (Ayaburi and Andoh-Baidoo 2019). Awareness of self-protective behavior is found insufficient and habit disruption strategies are recommended to protect from personal information hygiene risks. Habits are driven by prior experiences and time constraints that are required for processing hygiene scenario. Awareness of the environment helps in creating a perception about threat susceptibility which can be processed into habit creation. Situational cues from the cyber environment control individual's hygiene habits more than their decision-making conscious. Habit can be the moderator for actual behavior or can produce direct effect on actual behavior based on the circumstances of intention-behavior relationship (Limayem et al. 2007). Poor cyber hygiene habits can not only comprise personal data but also create macroeconomic security challenges (Anderson and Agarwal 2010). Wairimu, Ayaburi and Andoh-Baidoo (2018) studied influence of cues (attachment, social connectedness and social anxiety) and experiential factors (privacy risk and security self-efficacy) on the habitual use of unfamiliar wireless networks which relates to transmission hygiene. Their findings suggests that connecting to unsecure network as a routine behavior neutralizes individual's perception about associated security and privacy risks (Wairimu et al. 2018). Next, we look into thoughtful or deliberate decision making.

Cyber hygiene as a deliberate behavior (Reflective system)

Contrasting to habit-actuated behavior, cyber hygiene practices are considered a function of an individual’s decision-making ability (Maimon et al. 2022). Rational choice models have been one of the most popular in information systems literature and have given rise to numerous theories. These models situate an understanding of intentional behaviors that are caused by deliberate or conscious decision-making. Reflective systems involve individuals to make thoughtful mindset toward the problem and then reflecting on outcome and process both. Many criminology theories have relied on ration choice assumption (Piquero and Tibbets 2001). These theories perform risk-benefit analysis to determine decision to engage in criminal behavior. When precautionary behavior is achieved through cognitive processing, it is predicted by risk-taking propensity, perceived concern and controlled thinking ability.

Howell (2021) studied cyber hygiene outcomes as a consequence of thoughtfully reflective decision-making. In the model, thoughtfully reflective decision-making was composed of intentionality, forethought, self-reactiveness and self-reflectiveness (Howell 2021). Similarly, privacy decision-making literature has predominately focused on rational processes to understand choices (Adjerid et al. 2018). Privacy calculus literature views an individual’s choice as a tradeoff between benefits of information disclosure and privacy risks from such disclosures. This view acknowledges deliberate individual behavior. The composite effect of normative and behavioral factors generates varying degrees of data protection affecting user’s willingness to reveal personal information. In a low-risk environment, moral belief dominate to explain the intention to commit security policy violation, however, in presence of high risk, the other two- deterrence and self-control dominate in the model (Xu and Hu 2018). Deterrence does not play a role in cyber hygiene behaviors as there are no formal sanctions associated. However, moral beliefs and self-control can explain the decision-making for such protective behaviors. D'Arcy and Devaraj (2012) studied technology misuse decisions as a function of informal sanctions-social desirability pressure and moral beliefs (D'Arcy and Devaraj 2012).

Explicit and Implicit Attitudes

People's attitudes are immediately developed from their past beliefs and then guide corresponding behavior (Fishbein and Ajzen 2011). Rational process theories assume attitudes to be a result of conscious decision-making referred to as explicit attitude. Explicit attitudes perform a deliberate psychological evaluation of the object and can consciously control its expression. Contrary, Implicit attitudes are automatically activated on exposure to the object and are outside of a person's awareness (Greenwald and Banaji 1995; Wilson et al. 2000). While the conceptualization of implicit and explicit attitudes is developed largely in isolation, their competing parallel existence explains certain behavioral outcomes. Such outcomes can be explained as situations in which an individual's explicit judgment about the object is overridden by an automatically actuated implicit attitude. Applying a dual-attitude structure to the cyber hygiene use case, IS users' explicit attitude towards personal social media service use over work computers is overridden by their strong implicit attitude on system exposure. This view explains that attitude change is not necessarily a result of the replacement of pre-existing attitudes, it can be activated in presence of pre-existing via an implicit reaction. We use Wilson, Lindsey and Schooler's (2000) model of dual attitudes to explain parallel existence of reflective and reflexive systems.

IS user behavior is driven by explicit and implicit attitudes simultaneously (Turel et al. 2011). Serenko and Turel (2019) explained a dual attitudes model of system use. In their model, the less studied implicit attitude affects systems use with mediation through IS habit formation (Serenko and Turel 2019). We integrate the dual systems perspective with dual attitudes models as the two operate with conscious and deliberate elaborations. This perspective can oxymoronic situation about individual's processed beliefs and their actions. For example, Govind et al (2019) noted that consumer's possess an explicit attitude towards ethical products, however, their purchase behavior is driven by their implicit attitude (Govind et al. 2019). Individual's personal characteristics and type of IS that defines the scenario context change between the two attitudes. The configuration depends on user's internal motivation to choose a planned or a routine behavior. In a stressful environment where user is consumed with high cognitive activity implicit attitude prevails over explicit. Situations that are not obligatory challenge an individual's self-processes for outcome generation. Situational factors, individual's perception and their prior attitudes explain their actuation of implicit or explicit mechanism. Cyber hygiene behavior is a suitable case as the user's self-control is challenged by their contradictory actions.

Routine Activity Theory

Felson and Cohen (1980) developed routine activity theory that explained patterns of routine or lifestyles that provided opportunities for crime. Their study found that structural changes in patterns of routine influenced crime rates. The perspective explains that crime occurs at the convergence of a motivated offender, a suitable target, and the absence of a capable guardian (Felson and Cohen 1980). Information systems scholars have operationalized this perspective to develop a conceptual framework to mitigate insider threats (Padayachee 2016), understand the risk from the offender's perspective (Willison and Backhouse 2006), and develop a situational perspective for crime (Wang et al. 2019). Researchers have more often studied offenders' motivation and lack of guardianship in comparison to the target suitability. From a routine activity perspective, organizational insiders are privileged information system users whose routine patterns converge in time and space with digital valuable assets. The extended routine activity perspective that emphasizes value, inertia, accessibility, and visibility (VIVA) characteristics (refer to table 1 for details on the dimensions) has found a lot of relevance in IS studies (Wang et al. 2019). Pang and Tanriverdi (2022) in a recent study investigated vulnerabilities in the legacy system using the VIVA framework. They found that legacy system accumulated large information over time making them highly valuable to the organizations, whereas, for likely offenders, they offer visibility and accessibility (Pang and Tanriverdi 2022).

Target Suitability

With increasing internet and communication technology penetration, online perpetrators are increasingly finding it suitable to conduct fraudulent activities. One of the key factors for victimization to occur is unwilling victim's exposure to offenders. Individuals' online behavior can potentially diffuse all the defensive security barriers and subject them to a criminal opportunity. Crime drops due to reduced opportunity by intended/unintended improvement in security and unintended effects of routine activities (Tilley et al. 2015). A victim's online careless behavior can send signaling cues to attract likely perpetrators to take advantage of criminal opportunities. A suitable target does not necessarily mean the victim's availability for a criminal event it also accounts for the victim's disposition and can be used to build trust against them (Wilsem 2013). Personal traits such as self-control, self-esteem and attitudes contribute to target visibility and accessibility. Target suitability is a composite measured defined by four elements- value, inertia, visibility and accessibility (VIVA) (Luo et al. 2020; Wang et al. 2015).

Target suitability element	Measure	Self-regulatory and Self-protection outcomes
Phenomenon of this study	Risk of being a target of crime. (Felson and Clarke 1998)	The probability that an individual's controls can lead to victimization in an online environment.

Value	It is a social and economic measure that an offender may have in mind for a target once appropriated. (Yar 2005)	The benefit that can be obtained with security comprises of an individual.
Inertia	It is a measure of how easily the target can be removed or overcome by an offender (Felson and Clarke 1998)	The strength of individual's self-regulation a likely perpetrator would need to overcome with arousal cues or other trust-gaining mechanisms.
Visibility	It is a measure of definite understanding about the existence of the target or its exposure (Yar 2005)	The strength of an individual's self-control so that a likely perpetrator is restricted from any specific whereabouts of the target.
Accessibility	It is a measure of the ability of an offender to get to the target and then get away from the scene of crime (Felson and Clarke 1998)	The strength of an individual's self-regulation so that the likely perpetrator is unable to gain access to target's cyber environment.

Table 1: Target Suitability elements as Self-process outcomes

According to the situational crime perspective, reducing the suitability of the target reduces the opportunity or circumstances of the crime. Clark's opportunity-reducing framework was utilized by Beebe and Rao (2005) to suggest that perceived cost can be increased by increasing perceived effort and perceived risk for a crime opportunity (Beebe and Rao 2005; Yar 2005). Thereby, previous research establishes the importance of target suitability and offers ways to increase the cost. Wang et al (2015) formulated an understanding of various target characteristics (value, inertia, visibility and accessibility) for IS applications. This suitability perspective formed an understanding of which targets are more prone to attack. In another research future target suitability is predicted using the online information about targets' current suitability (Lee et al. 2018). The study concluded that value and ease of removal (inertia) were two major factors for the suitability of the target. Target suitability increases with the complexity of enterprise architectures. It is clear that most studies have explained suitability from an offender perspective and very limited attention has been drawn towards understanding victim's contribution in generating target suitability. In this study, we understand the victim’s contribution toward target suitability from a self-process behavior.

Cyber hygiene behavior and self-regulated outcomes

Criminal victimization is considered a highly aversive and uncontrollable event. Perceived victimization threat can create self-doubt about control over personal safety. Contrary to rational choice outcomes that rely on risk-benefit analysis, self-regulated outcomes are generated from the ability to control impulsive urges for immediate gratification. The controls are exercised based on moral values and situational moral norms (McCullough and Willoughby 2009). Although early literature on self-control did not study victimization risks, late realization of including activity and lifestyle theories gave a better understanding other situational context of victimization. An implicit assumption of self-process theories is that they consider individuals at the locus of evaluation. Self-regulation has been reported to exhibit several positive outcomes such as interpersonal behaviors, healthy living, and mental health (Robson et al. 2020). Self-regulatory behaviors follow a process model of self-monitoring, self-judgment and self-reaction. Self-control failure in individuals makes it harder for them to recognize social cues.

Online behaviors generated as impulsive, or habitual responses fail to recognize social cues. Consumer online routine behavior affects the decision making of likely perpetrator through their visible vulnerabilities (Clarke 1995). Pratt et al 2014 reported self-control to have a stronger effect when predicting non-contact victimization (online victimization) (Pratt et al. 2014). Also, the behavior of an individual with low self-control showcases higher exposure to fraud victimization (Holtfreter et al. 2010). Individuals’ disposition of cautiousness subjects them to lower risk of victimization. Self-regulation failure in phishing emails can be the result of an individual’s judgment failure of email features (Wright and Marett 2010) or automatic use due to arousal cues

(Ayaburi and Andoh-Baidoo 2019). Higher phishing susceptibility is reported outcome of reactive behaviors to the emotional appeals. Luo et al (2020) found target suitability as a significant outcome of low self-control. Thus, exposure to victimization is situated as an outcome of an individual's self-regulation behavior (Luo et al. 2020). Self-regulated process is not a sufficient condition for less likelihood of victimization. While literature claims rational decision-making with self-regulated process is effective to control adverse outcomes from habitual behavior. However, judgment errors in self-regulation could result in adverse outcomes. Thus, reflective systems do not necessarily paint a positive picture of victimization likelihood. Also, self-regulation plays in conjunction with institution-based regulatory controls (industry self-regulation and government legislation) to explain target suitability outcomes.

Cyber hygiene behavior and self-protective outcomes

Thoughtfully reflective decision-makers are more likely to adopt self-protective behaviors such as computer privacy (Howell 2021). Protective behaviors are explained using the protection motivation theory which explains an individual's protection based on threat appraisal and coping appraisal. These interests are developed in a defensive response against negative self-view maintaining psychological well-being (Alicke and Sedikides 2009). The self-protection view explains why people make justifiable choices in presence of differential susceptibility. Previous research has urged for exploration and measurement of this justifiable choice. Criminology research on victim self-protection behavior explains the role of victims' resistance in changing crime outcomes. Guerette and Santana (2010) used opportunity theory to report that victim self-protection behavior could change criminal outcomes by 92-93% in some cases (Guerette and Santana 2010). Thus, self-protection behavior can reduce the likelihood of criminal incidents.

Also, from a situational crime perspective, avoidance as a result of self-protection inspires criminal opportunity reduction.

Maimon et al (2022) found that people who possess situational awareness would limit their usage of personal accounts on public WiFi networks (Maimon et al. 2022). Thus, self-protection behavior exists both in the presence or absence of criminal motivation. The concept of forceful (direct defense from perpetrator) and non-forceful resistance (reducing likelihood of criminal event) explains the two outcomes. Hence, outcomes such as reducing suitability are a consequence of such protective behaviors. Individual self-protection can lower their privacy concerns if they establish control over their personal information. Individuals utilize target hardening practices to acquire a sense of safety and assurance outcomes (Beebe and Rao 2005). Self-protection is meant for several perceived outcomes such as reducing the perceived risk of victimization and their corresponding perceived suitability. In our model, we measure target suitability as a self-protection and self-regulation outcome.

RESEARCH MODEL

We build an integrated research model that is representative of all the scenarios in which cyber hygiene behavior can lead to a suitable target. First, we present an integration of dual attitudes within the framework of the dual system. We inspired our theoretical model from Serenko and Turel's (2019) dual attitude model of system use. They pointed out six important differences between IS habits and implicit attitudes (Serenko and Turel 2019). Out of the difference, the expression of habits as a behavioral tendency (extend to which behavior can be performed) and implicit attitudes as psychological evaluation of an object builds an understanding to our model.

H1: Implicit attitude toward online hygiene practices is associated with cyber hygiene habit formation.

Another central tenet of the model of the dual attitude is that implicit attitudes can exist and can have a direct influence on behaviors (Wilson et al. 2000). The link between implicit attitude and behavior is empirically tested in 167 studies. They found that the relationship between implicit attitude on behaviors was not significantly different from explicit attitude (Cameron et al. 2012). This brings us to our next hypothesis.

H2: Implicit attitude towards online hygiene practices influences cyber hygiene behavior formation.

Individual' situational cognitive capacity influences whether explicit attitude will be retrieved or implicit attitude will override. Also, explicit attitudes can be altered easily in comparison with the implicit ones. Self-attributed motives and processes operate when explicit attitudes predict a stronger intention to perform a certain kind of behavior.

H3: Explicit attitude toward online hygiene practices positively influences self-regulation intention.

Psychological reasoning theories such as theory of planned behavior, the theory of reasoned action, and other consistent theories situated an understanding of intention influencing behavior. In our model, we use the self-regulation intention of the reflective system to predict the resultant behavior.

H4: Self-regulation intention of cyber hygiene practices would positively influence cyber hygiene behavior.

In their original conceptualization, Wilson, Lindsey and Schooler (2000) explained how implicit attitude can influence behavior even though the individual is aware of explicit attitude. This explains the moderation effect of cyber hygiene habits on self-regulation intention-behavior effect

(Wilson et al. 2000). Considering rational choice assumption, self-regulation for hygiene maintenance should predict cyber hygiene behavior. However, reflexive systems challenge these assumptions and weaken the effect of intention on behavior. This effect depletion occurs with habit formation. (Limayem et al. 2007) explain how habit formation limits the predictive power of intention and establish role of habit as moderator in the intention-behavior relationship.

H5: Cyber hygiene habits moderate (weaken) the relationship between self-regulation intention and cyber hygiene behavior.

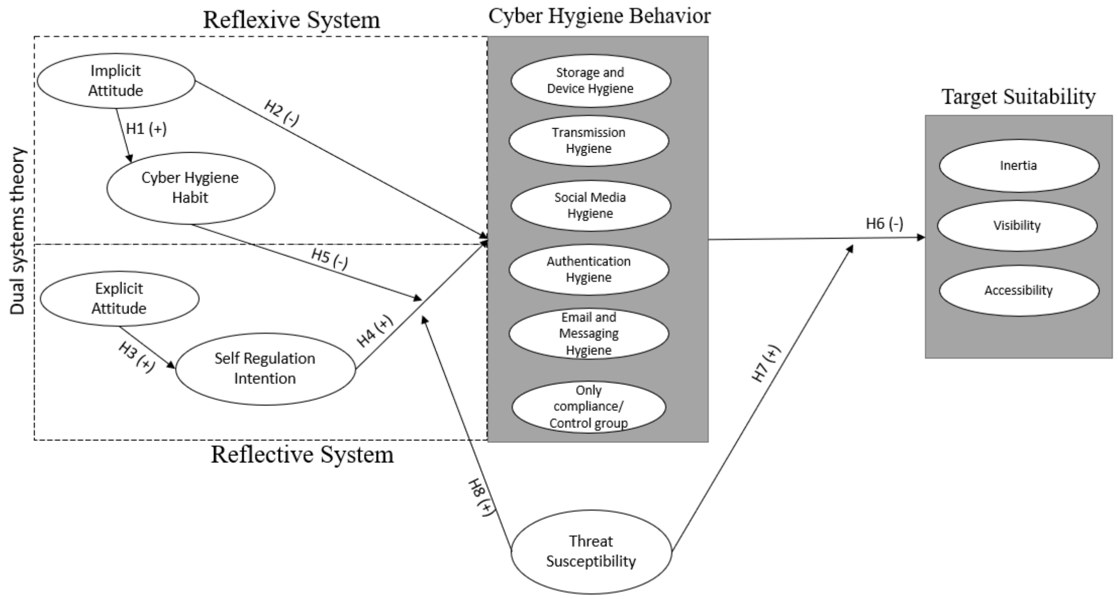

Figure 2. Research Model

Second, we make an understanding of different cyber hygiene contexts based on (Vishwanath et al. 2020)'s classification. From a victim's perspective, criminal outcomes are influenced by the victim's self-protective behavior. Victim behavior is considered preceptory to criminal opportunities. Thus, depending on the cyber hygiene context individual's behavior influences different levels of victimization opportunity.

H6: Cyber hygiene behavior can negatively influence victimization likelihood (target suitability).

Individual differences in threat susceptibility play a role in explaining cybercrime victimization (Cheng et al. 2020). These differences are a result of an individual's perceived IT efficacy, their perceived safety on internet and coping ability. Also, previous victimization experiences shape up their susceptibility perception. Thus, the effect of cyber hygiene behavior on target suitability can be amplified by the moderator variable of threat susceptibility. High-risk environments would have higher cyber hygienic behavior that will lower the likelihood of crime. Similarly, intention to perform self-regulative cyber hygiene practices will be amplified in a high risk environment leading to higher extent of cyber hygiene behavior.

H7: Threat susceptibility moderates (amplifies) the effect of cyber hygiene behavior on the suitability of the target.

H8: Threat susceptibility moderates (amplifies) the effect of self-regulation intention on cyber hygiene behavior.

METHODOLOGY

Due to unreliable data (social desirability bias) from personal questionnaires we need to consider scenario-based cross-sectional survey (D'Arcy et al. 2009; Siponen and Vance 2010; Vance et al. 2015).

Step1) Pilot study: We administered a pilot study with graduate students at a large public university in southern USA. We made an adaptation of cyber hygiene scale developed by (Vishwanath et al. 2020) to scenarios to test their cyber hygiene behavior. Seventy-two students participated in the survey with 70 valid responses. The survey contained objective screening questions for each of the six cyber hygiene type followed by subjective set of question to understand their level of chosen cyber hygiene engagement. This pilot study is intended to help improve the quality of the survey instrument and have content validity.

Findings from pilot: Across all the cyber hygiene types, lack of past experience with a similar scenario and technical negligence were two main barriers for evaluating their cyber hygiene. For example, reporting a suspicious email could not be evaluated as several students reported being unaware of possible ways of reporting. We learn to develop scenarios that have routine relevance and technical simplicity for the respondents. Second, students also reported "lack of context" for some scenarios which helped us re-design those specific measures. Third, the rationale for practicing and not practicing certain type of cyber hygiene are not same in most of the scenarios. Thus, separate evaluation is necessary to understand a complete perspective. Fourth, a good number of scenarios were reported to be habitual rather being deliberate. Fifth, lack of self-regulatory outcomes is a primary reason to not follow cyber hygiene practices. Sixth, self-protective outcomes are a key reason to maintain cyber hygiene practices. The findings from the pilot help us better design scenarios. Although the level of analysis for this research possesses different characteristics as compared to university students, it was helpful to seek validation before performing main study.

Step 2) Expert panel and Pre-test: After approval of the baseline scenario and the model, like many other studies using this study design, we should convene an expert review panel. As cyber hygiene literature is not well established within the field of security. The DRW workshop will help accomplish this step.

Step 3) Main study: A priori power analysis to determine how many responses are necessary to achieve the required effect size. Scenario based factorial survey administered with industry professionals on (Mturk/Qualtrics online survey).

EXPECTED OUTCOMES & IMPLICATIONS

We have multifold contribution with this article. First, to construct our extant understanding about cyber hygiene, mainly from criminology literature. Previous studies fail to build validation on antecedents and consequence of cyber hygiene. Second, to understand what motivates such behavior in individuals. Previous focus on similar behaviors have been contextually constrained such as home users safe computing, phishing susceptibility and consequences. A complete explanation of all different types of such behaviors is missing (Vishwanath et al. 2020). Third, theoretically contribution lies in integration of two theories that have similar orientation (dual systems thinking and dual attitudes model). Several previous research have exclusively explained them but the integration is unique to this study. Fourth, building an understand of target suitability as a result of such non-obligatory behaviors. Security research has dominantly focused on offender motivation and have produced various empirical evidence to deter the resultant behaviors. However, the quantification of individual's contribution to suitability of targets as a result of their day-to-day hygiene is missing.

Several practical implications can be promised from the results of this study. First, an understanding of influence of attitudes on cyber hygiene behaviors and how habits are formed can help organizations build personalized trainings based on employee's implicit and explicit mindset. Second, understanding of how habits can suppress self-regulation intentions in individuals can help divert attention towards employee's cyber hygiene habits. The model can be used to devise strategies to prevent habituation. Third, different contextual cyber hygiene behaviors are manipulated in the study design which can help organizations get specific insights about different cyber hygiene scenarios. Fourth, contribution of cyber hygiene behavior in explaining target suitability will add insights to the organizational policies for inclusion of hygiene behaviors. Fifth, contextual factors shape up employee's attitudes towards the company which can initiate potential for several research outcomes.

REFERENCES

Adjerid, I., Peer, E., and Acquisti, A. 2018. "Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making," *MIS Quarterly* (42:2), pp. 465–488.

Alicke, M. D., and Sedikides, C. 2009. "Self-Enhancement and Self-Protection: What They Are and What They Do," *European Review of Social Psychology* (20:1), pp. 1–48.

Anderson and Agarwal. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), p. 613.

Arachchilage, N. A. G., and Love, S. 2014. "Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective," *Computers in Human Behavior* (38), pp. 304–312.

Ayaburi, E., and Andoh-Baidoo, F. K. 2019. *Understanding Phishing Susceptibility: An Integrated Model of Cue-Utilization and Habits*, presented at the ICIS 2019 Proceedings. 43.

Baraković, S., and Baraković Husić, J. 2022. "Cyber Hygiene Knowledge, Awareness, and Behavioral Practices of University Students," *Information Security Journal: A Global Perspective*, pp. 1–24.

Beebe, N. L., and Rao, H. R. 2005. "Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security," in *Proceedings of the 2005 SoftWars Conference, Las Vegas, NV.*

Bulgurcu, Cavusoglu, and Benbasat. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), p. 523.

Cain, A. A., Edwards, M. E., and Still, J. D. 2018. "An Exploratory Study of Cyber Hygiene Behaviors and Knowledge," *Journal of Information Security and Applications* (42), pp. 36–45.

Cameron, C. D., Brown-Iannuzzi, J. L., and Payne, B. K. 2012. "Sequential Priming Measures of Implicit Social Cognition: A Meta-Analysis of Associations With Behavior and Explicit Attitudes," *Personality and Social Psychology Review* (16:4), pp. 330–350.

Cavusoglu, Huseyin, Raghunathan, S., and Cavusoglu, Hasan. 2009. "Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems," *Information Systems Research* (20:2), pp. 198–217.

Cheng, C., Chan, L., and Chau, C. 2020. "Individual Differences in Susceptibility to Cybercrime Victimization and Its Psychological Aftermath," *Computers in Human Behavior* (108), p. 106311.

Clarke, R. V. 1995. "Situational Crime Prevention," *Crime and Justice* (19), pp. 91–150.

D’Arcy, J., and Devaraj, S. 2012. “Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model: Employee Misuse of Information Technology Resources,” *Decision Sciences* (43:6), pp. 1091–1124.

D’Arcy, J., Hovav, A., and Galletta, D. 2009. “User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach,” *Information Systems Research* (20:1), pp. 79–98.

“Federal Trade Commission (FTC) Report.” 2022. *Federal Trade Commission Report*. (https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022).

Felson, M., and Clarke, R. V. 1998. *Opportunity Makes the Thief: Practical Theory for Crime Prevention*, (1. publ.), Police Research Series, London: Home office, Policing and Reducing Crime Unit.

Felson, M., and Cohen, L. E. 1980. “Human Ecology and Crime: A Routine Activity Approach,” *Human Ecology* (8:4), pp. 389–406.

Fishbein, M., and Ajzen, I. 2011. *Predicting and Changing Behavior*, (0 ed.), Psychology Press. (https://doi.org/10.4324/9780203838020).

“Get the 2020 Cloud Threat Report.” 2020. (https://www.oracle.com/security/cloud-threat-report/, accessed February 23, 2023).

Govind, R., Singh, J. J., Garg, N., and D’Silva, S. 2019. “Not Walking the Walk: How Dual Attitudes Influence Behavioral Outcomes in Ethical Consumption,” *Journal of Business Ethics* (155:4), pp. 1195–1214.

Greenwald, A. G., and Banaji, M. R. 1995. “Implicit Social Cognition: Attitudes, Self-Esteem, and Stereotypes.,” *Psychological Review* (102:1), pp. 4–27.

Guerette, R. T., and Santana, S. A. 2010. “Explaining Victim Self-Protective Behavior Effects on Crime Incident Outcomes: A Test of Opportunity Theory,” *Crime & Delinquency* (56:2), pp. 198–226.

Harrington, S. J. 1996. “The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions,” *MIS Quarterly* (20:3), p. 257.

Hofmann, W., Friese, M., and Strack, F. 2009. “Impulse and Self-Control From a Dual-Systems Perspective,” *Perspectives on Psychological Science* (4:2), pp. 162–176.

Holtfreter, K., Reisig, M. D., Leeper Piquero, N., and Piquero, A. R. 2010. “Low Self-Control and Fraud: Offending, Victimization, and Their Overlap,” *Criminal Justice and Behavior* (37:2), pp. 188–203.

Howell, J. 2021. *Self-Protection in Cyberspace: Assessing the Processual Relationship Between Thoughtfully Reflective Decision Making, Protection Motivation Theory, Cyber Hygiene, and Victimization*, University of South Florida ProQuest Dissertations Publishing.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., and Lowry, P. B. 2015. “The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness,” *Information Systems Research* (26:2), pp. 282–300.

Huth, C. L., Chadwick, D. W., Claycomb, W. R., and You, I. 2013. “Guest Editorial: A Brief Overview of Data Leakage and Insider Threats,” *Information Systems Frontiers* (15:1), pp. 1–4.

Jaeger, L., Eckhardt, A., and Kroenung, J. 2021. “The Role of Deterrability for the Effect of Multi-Level Sanctions on Information Security Policy Compliance: Results of a Multigroup Analysis,” *Information & Management* (58:3), p. 103318.

Jenkins, J. L., Durcikova, A., Ross, G., and Nunamake, J. F. 2010. *Encouraging Users to Behave Securely: Examining the Influence of Technical, Managerial, and Educational Controls on Users' Secure Behavior*, presented at the ICIS 2010 Proceedings. 150.

Kappers, W., Glassman, A., and Wills, M. 2021. "CYBER INSURANCE EFFECTS ON CYBER HYGIENE: DOES THE HOMEOSTATIC EFFECT APPLY?," *Issues In Information Systems*. (https://iacis.org/iis/2021/4_iis_2021_1-8.pdf).

Kwon, J., and Johnson, M. E. 2013. "Health-Care Security Strategies for Data Protection and Regulatory Compliance," *Journal of Management Information Systems* (30:2), pp. 41–66.

Lee, J., de Guzman, M. C., Talebi, N., Korni, S. K., Szumigala, D., and Rao, H. R. 2018. "Use of Online Information and Suitability of Target in Shoplifting: A Routine Activity Based Analysis," *Decision Support Systems* (110), pp. 1–10.

Liang, N. (Peter), Biros, D. P., and Luse, A. 2016. "An Empirical Validation of Malicious Insider Characteristics," *Journal of Management Information Systems* (33:2), pp. 361–392.

Limayem, Hirt, and Cheung. 2007. "How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance," *MIS Quarterly* (31:4), p. 705.

Lin, C., Wittmer, J. L. S., and Luo, X. (Robert). 2022. "Cultivating Proactive Information Security Behavior and Individual Creativity: The Role of Human Relations Culture and IT Use Governance," *Information & Management* (59:6), p. 103650.

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), p. 173.

Luo, X. (Robert), Li, H., Hu, Q., and Xu, H. 2020. "Why Individual Employees Commit Malicious Computer Abuse: A Routine Activity Theory Perspective," *Journal of the Association for Information Systems* (21), pp. 1552–1593.

Lyngs, U., Lukoff, K., Slovak, P., Binns, R., Slack, A., Inzlicht, M., Van Kleek, M., and Shadbolt, N. 2019. "Self-Control in Cyberspace: Applying Dual Systems Theory to a Review of Digital Self-Control Tools," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow Scotland Uk: ACM, May 2, pp. 1–18. (https://dl.acm.org/doi/10.1145/3290605.3300361).

Maennel, K., Mäses, S., and Maennel, O. 2018. "Cyber Hygiene: The Big Picture," in *Secure IT Systems* (Vol. 11252), Lecture Notes in Computer Science, N. Gruschka (ed.), Cham: Springer International Publishing, pp. 291–305. (https://doi.org/10.1007/978-3-030-03638-6_18).

Maimon, D., Howell, C. J., Jacques, S., and Perkins, R. C. 2022. "Situational Awareness and Public Wi-Fi Users' Self-Protective Behaviors," *Security Journal* (35:1), pp. 154–174.

McCullough, M. E., and Willoughby, B. L. B. 2009. "Religion, Self-Regulation, and Self-Control: Associations, Explanations, and Implications.," *Psychological Bulletin* (135:1), pp. 69–93.

Metcalfe, J., and Mischel, W. 1999. "A Hot/Cool-System Analysis of Delay of Gratification: Dynamics of Willpower.," *Psychological Review* (106:1), pp. 3–19.

Moody, G. D., Galletta, D. F., and Dunn, B. K. 2017. "Which Phish Get Caught? An Exploratory Study of Individuals′ Susceptibility to Phishing," *European Journal of Information Systems* (26:6), pp. 564–584.

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., and Hancock, G. M. 2020. "Holistic Cyber Hygiene Education: Accounting for the Human Factors," *Computers & Security* (92), p. 101731.

Padayachee, K. 2016. "An Assessment of Opportunity-Reducing Techniques in Information Security: An Insider Threat Perspective," *Decision Support Systems* (92), pp. 47–56.

Pang, M.-S., and Tanriverdi, H. 2022. "Strategic Roles of IT Modernization and Cloud Migration in Reducing Cybersecurity Risks of Organizations: The Case of U.S. Federal Government," *The Journal of Strategic Information Systems* (31:1), p. 101707.

Pfleeger, S. L., Sasse, M. A., and Furnham, A. 2014. "From Weakest Link to Security Hero: Transforming Staff Security Behavior," *Journal of Homeland Security and Emergency Management* (11:4), pp. 489–510.

Piquero, A. R., and Tibbets, S. G. (eds.). 2001. *Rational Choice and Criminal Behavior: Recent Research and Future Challenges*, (0 ed.), Routledge. (https://doi.org/10.4324/9780203822371).

Polites, G. L., and Karahanna, E. 2013. "The Embeddedness of Information Systems Habits in Organizational and Individual Level Routines: Development and Disruption," *MIS Quarterly* (37:1), pp. 221–246.

Polites, G. L., Serrano, C., Thatcher, J. B., and Matthews, K. 2018. "Understanding Social Networking Site (SNS) Identity from a Dual Systems Perspective: An Investigation of the Dark Side of SNS Use," *European Journal of Information Systems* (27:5), pp. 600–621.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly* (37:4), pp. 1189–1210.

Pratt, T. C., Turanovic, J. J., Fox, K. A., and Wright, K. A. 2014. "SELF-CONTROL AND VICTIMIZATION: A META-ANALYSIS: SELF-CONTROL AND VICTIMIZATION," *Criminology* (52:1), pp. 87–116.

Puhakainen and Siponen. 2010. "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), p. 757.

Robson, D. A., Allen, M. S., and Howard, S. J. 2020. "Self-Regulation in Childhood as a Predictor of Future Outcomes: A Meta-Analytic Review.," *Psychological Bulletin* (146:4), pp. 324–354.

Savold, R., Dagher, N., Frazier, P., and McCallam, D. 2017. "Architecting Cyber Defense: A Survey of the Leading Cyber Reference Architectures and Frameworks," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, New York, NY, USA: IEEE, June, pp. 127–138. (http://ieeexplore.ieee.org/document/7987188/).

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., and Kusev, P. 2017. "Risk Perceptions of Cyber-Security and Precautionary Behaviour," *Computers in Human Behavior* (75), pp. 547–559.

Serenko, A., and Turel, O. 2019. "A Dual-Attitude Model of System Use: The Effect of Explicit and Implicit Attitudes," *Information & Management* (56:5), pp. 657–668.

Sheppard, B., Crannell, M., and Moulton, J. 2013. "Cyber First Aid: Proactive Risk Management and Decision-Making," *Environment Systems and Decisions* (33:4), pp. 530–535.

Siponen, M. T. 2005. "An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice," *European Journal of Information Systems* (14:3), pp. 303–315.

Siponen and Vance. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), p. 487.

Soror, A. A., Hammer, B. I., Steelman, Z. R., Davis, F. D., and Limayem, M. M. 2015. "Good Habits Gone Bad: Explaining Negative Consequences Associated with the Use of Mobile Phones from a Dual-Systems Perspective: Good Habits Gone Bad," *Information Systems Journal* (25:4), pp. 403–427.

Strack, F., and Deutsch, R. 2004. "Reflective and Impulsive Determinants of Social Behavior," *Personality and Social Psychology Review* (8:3), pp. 220–247.

Straub, D. W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255–276.

Straub, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), p. 45.

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), p. 441.

Tilley, N., Farrell, G., and Clarke, R. V. 2015. *Target Suitability and the Crime Drop*, London: Palgrave Macmillan UK. (http://link.springer.com/10.1007/978-1-137-52502-4).

Trinkle, B. S., Crossler, R. E., and Warkentin, M. 2014. "I'm Game, Are You? Reducing Real-World Security Threats by Managing Employee Activity in Online Social Networks," *Journal of Information Systems* (28:2), pp. 307–327.

Turel, O., and Qahri-Saremi, H. 2016. "Problematic Use of Social Networking Sites: Antecedents and Consequence from a Dual-System Theory Perspective," *Journal of Management Information Systems* (33:4), pp. 1087–1116.

Turel, Serenko, and Giles. 2011. "Integrating Technology Addiction and Use: An Empirical Investigation of Online Auction Users," *MIS Quarterly* (35:4), p. 1043.

Vance, A., Lowry, P. B., City University of Hong Kong, Eggett, D., and Brigham Young University. 2015. "Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *MIS Quarterly* (39:2), pp. 345–366.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3–4), pp. 190–198.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., and Chin, J. 2020. "Cyber Hygiene: The Concept, Its Measure, and Its Initial Tests," *Decision Support Systems* (128), p. 113160.

Wairimu, J., Ayaburi, E., and Andoh-Baidoo, F. K. 2018. *Individual's Security and Privacy Behavior on the Use of Unfamiliar Wireless Networks: Habituation Theory Perspective*, presented at the Thirty ninth International Conference on Information Systems, San Francisco 2018.

Wang, J., Gupta, M., and Rao, H. R. 2015. "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications," *MIS Quarterly* (39:1), pp. 91–112.

Wang, J., Li, Y., and Rao, H. R. 2017. "Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences," *Information Systems Research* (28:2), pp. 378–396.

Wang, J., Shan, Z., Gupta, M., and Rao, H. R. 2019. "A Longitudinal Study of Unauthorized Access Attempts on Information Systems: The Role of Opportunity Contexts," *MIS Quarterly* (43:2), pp. 601–622.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101–105.

Willison, R., and Backhouse, J. 2006. "Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective," *European Journal of Information Systems* (15:4), pp. 403–414.

Willison, R., Warkentin, M., and Johnston, A. C. 2018. "Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives: Examining the Influence of Disgruntlement on Computer Abuse Intentions," *Information Systems Journal* (28:2), pp. 266–293.

Wilsem, J. van. 2013. "Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization," *Journal of Contemporary Criminal Justice* (29:4), pp. 437–453.

Wilson, T. D., Lindsey, S., and Schooler, T. Y. 2000. "A Model of Dual Attitudes.," *Psychological Review* (107:1), pp. 101–126.

Wright, R. T., and Marett, K. 2010. "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived," *Journal of Management Information Systems* (27:1), pp. 273–303.

Xu, Z., and Hu, Q. 2018. *The Role of Rational Calculus in Controlling Individual Propensity toward Information Security Policy Non-Compliance Behavior*, presented at the Hawaii International Conference on System Sciences. (http://hdl.handle.net/10125/50354).

Yar, M. 2005. "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory," *European Journal of Criminology* (2:4), pp. 407–427.

Yoo, C. W., and Rao, H. R. 2014. "Collective Security Efficacy and Group Security Compliance," in *Thirty Fifth International Conference on Information Systems, Auckland 2014*.

APPENDIX

Main Study Design

Method: Scenario-based Factorial Survey Approach

Manipulations: 6*2*2*1 (Self-regulated, Habitual)

Baseline scenario (Organizational setting)

Jay works as an investment strategist for a private equity firm. His role requires travel across the globe to understand suitable investment options. Jay is working at the airport using a public Wi-Fi network. [insert Threat Susceptibility statement here]. He is hoping to complete work before he boards the flight. [insert Type of Cyber hygiene statement here] [insert Type of Self Control statement here].

Sample Scenario

Jay works as an investment strategist for a private equity firm. His role requires travel across the globe to understand suitable investment options. Jay is working at the airport using a public Wi-Fi network. Jay believes that using the airport's public Wi-Fi network has High-security risks. He is hoping to complete work before he boards the flight. Before starting his work, Jay enables a firewall and also runs a virus scan to the external hard drive that he got from his clients. In this case, he deliberately performed this action.

Type of Cyber hygiene statements (Six Levels: Each one is exclusively present)

We consider that in a particular scenario only one of the cyber hygiene behaviors is present. This is a study limitation that excludes possible interaction or combination of two or more hygiene behaviors. However, it is realistic to believe that scenarios can have exclusive hygiene behaviors as the categories are derived from their operational definition (Vishwanath et al. 2020)

a) Storage and Device Hygiene: Before starting his work, Jay enables a firewall and also runs a virus scan to the external hard drive that he got from his clients.

b) Transmission Hygiene: Jay checks the URL address of the website that indicates “HTTPS” (where S indicates a secure connection) before making an online financial transaction.

c) Social media Hygiene: While preparing his work report, Jay is required to reference one of his close friends’ exact work designations. In order to obtain his friend’s work designation, he uses his personal mobile instead of the company’s laptop to access his social media account.

d) Authentication and credential hygiene: Jay is required to sign up on the start-up website he is looking to invest in, he creates and saves a unique password on the internet browser.

e) Email and messaging Hygiene: Browsing through his work emails, he finds an urgent authentication failure email from an unknown email address, he marks the email as spam.

f) Control group: Jay only follows all the compliances that are prompted to him by his company’s laptop.

Type of Self Control (Two Levels: Reflective vs Reflexive)

a) Reflective or Self-regulated control: He (deliberately/consciously) performed this action

b) Reflexive or Habitual or Impulsive control : He (always/automatically) performs this action.

Type of Attitudes (Two Levels but both levels exist together: Implicit and Explicit)

a) Explicit attitude: He always has a thoughtful mindset.

b) Implicit attitude: He always goes with the feeling of his situation.

Threat Susceptibility Level (Two Levels: Low/High)

a) Low: Jay believes that using airport’s public Wi-Fi network has low security risks.

b) High : Jay believes that using airport’s public Wi-Fi network has high security risks.

Perceived Target Suitability (DV)

a) Accessibility: In this scenario, do your think Jay’s action makes him less accessible to a likely perpetrator? (Strongly disagree-Strongly agree [1-7])

b) Visibility: In this scenario, do your think Jay’s action makes him less visible to a likely perpetrator? (Strongly disagree-Strongly agree [1-7])

c) Inertia: In this scenario, do your think Jay’s action creates barriers for a likely perpetrator? (Strongly disagree-Strongly agree [1-7])