Disobedience and Deviance: An Empirical Categorization of Insider Cybersecurity Behaviors

by

Rachel Lee Whitman

A dissertation submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Auburn, Alabama
August 7, 2021

Keywords: Cybersecurity, Insider Behavior, Personality, Burnout, Profile Analysis

Approved by

Daniel Svyantek, Chair, Professor of Psychology
Jesse Michel, Associate Professor of Psychology
Alejandro Lazarte, Associate Professor of Psychology
Jinyan Fan, Professor of Psychology

Abstract

Employees pose a significant threat to organizational cybersecurity. Researchers have called for increased examination of the traits and antecedents related to poor cybersecurity compliance. The current study contributes to efforts to understand these cyberdeviant behaviors by presenting latent profile analytic evidence supporting the existence “types” or categories of various insider violations. In particular, four patterns of cybersecurity behaviors and five patterns of cyberloafing behaviors were observed. Covariate analyses were conducted in order to link behavioral profiles to both previously identified and unexamined personal and contextual antecedents, pointing to the influence of burnout and psychological contract violations upon employee willingness to adhere to recommended cybersecurity behaviors and engage in cyberloafing. Results from these analyses further enhance current theoretical understanding of the importance, thus facilitating the accumulation of cybersecurity research into impactful interventions for selection, deterrence, and education.

Acknowledgements

I would like to extend my deepest thanks to my major professor, committee members, and all the teachers and mentors that have equipped me with the know-how to complete a task of this magnitude. My eternal gratitude belongs to the administrative staff in the Psychology Department and Graduate School for being the most helpful, competent, accommodating, and kind people on the face of the planet. Thanks to all the mentors involved in the "Thor: The Dark World Ultimate Mentor Adventure," whose expertise led me to study psychology. To Dr. Gary Lautenschlager: you advised me that "*No matter how things work out, they do*." You were right.

I would also like to thank my parents, Dr. Michael Whitman and Dr. Rhonda Hake. Thank you for instilling a life-long love of reading, learning, storytelling, and teaching. Thank you for supporting me and encouraging me in equal measure. Additional thanks to my siblings—Alexander and Meghan—with whom I share many textbook dedications. This one's from me.

Nicole Shifrin and Taylor Willits—you are the best cohort anyone could ever ask for. From the late nights in stats lab to late nights trying to sort out our dissertation methodologies, you two have been the foundation of my time here. Whenever I hear mention of the Auburn Family, I think of you. Also, on our behalf: I would like to actively withhold thanks from that one conductor who drives the 4 am train route and blasts the horn all the way from Donahue to University. Grad school may have aged us, but you significantly contributed to the problem.

Finally, to my now-husband, Dr. Michael Rotch—thank you for being a colleague, a friend, a confidant, and a partner. For all that I like to think myself eloquent, I am struck dumb by the radiance of your presence in my life.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ISS	Information Systems Security (Also: InfoSec)
USD	United States Dollar
IT	Information Technology
ICT	Information Communications Technology
CWB	Counterproductive Workplace Behavior
ISP	Information Security Policy
COR	Conservation of Resources
TRA	Theory of Reasoned Action
TPB	Theory of Planned Behavior
TIB	Theory of Interpersonal Behavior
PMT	Protection Motivation Theory
HBM	Health Belief Model
NMSV	Non-Malicious Security Violation
PWU	Personal Web Use
NWRC	Non-Work-Related Computing
IAD	Internet Addiction Disorder
LPA	Latent Profile Analysis
E/CFA	Exploratory/Confirmatory Factor Analysis
HIT	Human Intelligence Task
MTurk	Amazon's Mechanical Turk
SFW	Safe-ish for Work
NSFW	Not Safe for Work

Disobedience and Deviance: An Empirical Categorization of Insider Cybersecurity Behaviors

"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it," –Stephane Nappo

The issue of Information Systems Security (ISS) poses a wide-ranging threat to our personal and professional lives. Information security issues consistently rank in lists of the top global threats to modern organizations (World Economic Forum, 2012). While mention of this danger conjures up the prototypical images of cybersecurity breaches caused by conniving hackers and dark-web fiends, the true threat to organizational security comes from a seemingly innocuous source: its own employees (Warkentin & Wilson, 2009). As such, good security protocols must incorporate some understanding of human behavior in order to fully account for the risks posed by employees.

Industrial-Organizational (I-O) Psychologists specialize in the study of human behavior within the demands of a work environment and are well-suited to contribute to this topic. As the current study examines, recent cybersecurity research cites commonly studied I-O topics and theories. Indeed, professionals in both fields recognize the potential for collaboration and call for more integrated research efforts (e.g., Dalal et al., 2021). The current study contributes to this effort through the examination of employee cybersecurity behavioral "types." That is, are there subgroups of employees demonstrating differing, distinct, and meaningful patterns of cybersecurity hygiene behaviors?

Cybersecurity: The Information War

Information is power, and its utility in modern society places data at a premium. At its core, Information Systems Security (also: InfoSec, cybersecurity, Management of Information

Security/MIS) is an attempt to balance the competing needs of availability and security of an organization's information resources. The need for security often expands to include the confidentiality, integrity, and availability of an organization's information systems, which must remain accessible in order to facilitate organizational operations while still protecting assets (Abouzakhar, 2013). Compromising any of these elements poses a severe risk to the organization's ability to function. The inclusion of information systems within this goal should be noted—an organization may still suffer even without a loss of data. This may occur when its cyber infrastructure is damaged in an incident (as in a DDOS: Distributed Denial-of-Service attack). As nearly every organization possess intellectual property and/or sensitive customer information, all companies are vulnerable to being targeted in a cyber incident (Posey et al., 2017).

Former FBI director Robert Mueller stated, "There are only two types of organizations: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again" (2012, pp. 6). From 2016 to 2019, the average number of cybersecurity incidents experienced *per company* tripled from 1 to 3.2, with the average cost for theft of credentials increasing from $493 thousand to $871 thousand USD (Ponemon, 2020). Reflecting the magnitude of this issue, the unemployment rate for cybersecurity professionals remains at 0%—with an estimated 3.5 million jobs to exist unfilled by the end of this year (Morgan, 2019).

A breach in the confidentiality, integrity, or decreased availability of an organization's data infrastructure incurs expenses beyond those needed to recover or restore the information. In addition to the increased operational costs from needing to implement additional security measures, organizations likely face income reduction via a loss of competitive advantage and reputation damage, as well as any fines or penalties levied by authorities should the company be deemed negligent (Couce-Viera et al., 2020). Merely two days following the announcement of a security breach, a firm can experience a 2.1% decrease in overall market value (Cavusoglu et al. 2004). The average cost of a malware attack was $2.4 million USD in 2019, with current trends showing a 27% increase in the number of large-scale breaches each year (Sobers, 2019).

These trends of increased cybersecurity costs and impacts preceded the COVID-19 pandemic. The lockdowns and their resulting transitions to working from home during the pandemic have accelerated the crisis. Cyber-related crime saw an increase of 300% from the beginning of the pandemic to May of 2020 (Walter, 2020), with the number of confirmed data breaches increasing by 58% in the healthcare industry alone (Verizon, 2021). Statistics also indicate that remote workers are particularly vulnerable—employees were responsible for breaches in 20% of surveyed organizations, with the cost of such breaches averaging $137,000 higher than externally-caused incidents (Sobers, 2021). Ultimately, the numbers indicate that the pandemic has amplified an already-pressing crisis.

The threat posed by cybersecurity breaches is one that has been acknowledged and discussed, but not slowed. While cybersecurity spending by companies has risen in recent decades, it remains an unfortunate myth that security may be bought. However, no significant correlation between spending on cybersecurity programs and their success in protecting information assets exists (Choi et al., 2019). The underlying assumption that advances in technology automatically equate to increased security—although laden with echoes of technological determinism (see Whitman, 2021)—is invalidated by the fact that firewalls and other prevention technologies offer limited protection when challenged by individuals with legitimate organizational access. Corporate insiders—be they employees, contractors, or executives—require access to information systems in order to successfully complete their job duties. It is this need for access that makes incidents originating from within the organization so devastating.

The Insider Threat

Devastating is not, in fact, an exaggeration. Though executives perceive organizational outsiders to be the only major risk to security, low-end estimates point to around 43% of all data breaches as being caused internally (Choi et al., 2019; Intel Security, 2015). As high as this percentage is, it likely still underrepresents the true frequency of these incidents. An organization may neglect to report an insider-driven breach out of ignorance, perceptions of the breach as insignificant, or a desire to avoid negative publicity (Sarkar, 2010; in Ophoff et al., 2014).

Even with likely-suppressed statistics, employees cause more information security breaches than outsiders (Baker et al., 2010; Richardson et al., 2011), thus representing the biggest, most challenging threat to security (Homoliak et al., 2019; Stanton et al., 2005; Warkentin & Wilson, 2009). Two major characteristics of insiders contribute to this threat.

First, employees possess increased knowledge of organizational assets, software, and defenses by nature of their employment within the organization (Warkentin & Willison, 2009). This knowledge derives from the legitimate access to information systems needed to perform their job tasks. Such exposure gives employees the potential to exploit organizational information while remaining unaffected by most technological defenses—which are commonly designed to keep systems secure from outsiders, not insiders (Homoliak et al., 2019). Second, employees are vulnerable to targeting from external hackers who might seek to trick an employee into divulging sensitive information, from which current technological defenses offer little protection.

For these reasons, cybersecurity professionals frequently identify employees as the weakest link in the chain of organizational security (Schneier, 2015; in Guo et al., 2011). What follows are three examples of breaches wherein insiders—accidental, negligent, and malicious in nature—contributed to a cyberincident with significant repercussions.

In July 2020, a chain of spear phishing attacks succeeded against a number of Twitter employees (Ekran, 2020). Spear phishing is a personalized scam involving a "bait" email that targets a specific individual or entity with the purpose of extracting personal login information or installing malware on the recipient's computer (Dalal et al., 2021). The tailored nature of spear phishing attacks makes them more difficult to detect, as the attacking party will often use social engineering tactics to make the bait email as compelling as possible (Whitman & Mattord, 2011). The hackers behind the 2020 Twitter breach identified vulnerable employees (those working from home), posed as Twitter IT administrators, and successfully convinced the employees to send in their credentials. Using these valid ID names and passwords, the hackers then accessed over 100 high-profile Twitter accounts—including the likes of Jeff Bezos, Barack Obama, and Uber—and promoted a "double your bitcoin" scam that generated $180,000 from tricked users before being halted by cryptocurrency platforms. While non-compromised Twitter users were able to draw attention to the incident, the attack significantly interfered with the functionality of the platform, leaving the National Weather Service in Lincoln, Illinois unable to tweet a tornado warning (Cappucci & Freedman, 2020). Twitter's stock price fell by 4% as a result of the breach, and the company immediately conducted security training for all employees.

American credit reporting agency Equifax suffered one of the largest information security breaches to date in 2017. This occurred when an employee neglected to install a recently released software update meant to patch a vulnerability within the company's enterprise management system (Fruhlinger, 2020). Hackers exploited the unpatched vulnerability and actively moved within Equifax's network undetected for 76 days, stealing the names, Social Security Numbers, credit card numbers, and more from over 40% of the US population. Routine security scans had not previously identified any of the multiple vulnerabilities within the system, and the security consulting firm that *did* draw attention to the numerous issues was ignored and released from contract. One of these issues concerned a security certificate that Equifax allowed to expire 10 months previously, meaning that internal network traffic—and the hackers—proceeded unmonitored and unaffected by any security protocols. The certificate was eventually renewed in July of 2017, at which time the breach was identified. Equifax officials delayed announcement of the breach for a month before acknowledging the issue. Even though zero cases of fraud or identity theft have been traced back to the Equifax breach, the company still incurred massive costs: their financial rating was downgraded, they spent $1.4 billion USD on updating information security systems, and a settled class action lawsuit required Equifax to commit at least $1.38 billion to resolving consumer claims (Fruhlinger, 2020).

Tesla, the American electric car manufacturing company, is a frequent target for cyberincidents. In 2018, an employee—reportedly angered over not receiving a promotion—deliberately and maliciously altered the code of the company's manufacturing operating system before stealing and sending proprietary information to an unknown external entity (Isidore & Horowitz, 2018; Kemp, 2018). The value of Tesla shares consequently dropped by 5% after announcement of the incident. A similar event occurred in October of 2020, where an ex-employee at the same manufacturing plant attempted to destroy a computer and then placed the blame on an innocent colleague (Osborne, 2020). Autumn of 2020 appeared to be a challenging time for Tesla employees, as another worker was offered $1 million USD by a Russian national to steal and send the attacker proprietary information—after which the attacker intended to ransom the information back to Tesla under threat of public release (Osborne, 2020). This conspiracy was discovered, however, and the economic impact minimal.[1]

Cyber CWBs

The above examples illustrate the variety of insider threats to cybersecurity. Both malicious and accidental actions possessed severe consequences for the victim organizations, with the malicious behaviors directed at Tesla strongly resembling counterproductive workplace behaviors (CWBs). CWBs are defined as "intentional employee behavior that is harmful to the legitimate interests of an organization" (Dalal, 2005; pp. 1241). This certainly describes the insider behavior detailed in the Tesla incidents. These similarities—observed in many cases of insider-caused cyberincidents—encouraged researchers to term such behavior as "cyber deviance" (also "cyberdeviance," "cyberdeviancy"). Defined as "voluntary behavior using information and communications systems which threatens or results in harm to an organization, its members, or stakeholders" (Weatherbee & Kelloway, 2006; pp. 39), some researchers have argued for its inclusion into the pantheon of counterproductive work behaviors (i.e., Weatherbee, 2010).

However, cyberdeviancy differs from other deviant or counterproductive behaviors (Mastrangelo et al., 2006). Consideration of cyberdeviance as a negatively directed form of contextual performance is not entirely accurate. Research indicates employees will intentionally fail to follow security guidelines in order to maximize task performance (Cram et al., 2019; Wall, 2013). Additionally, cyberdeviant behavior does not have to actively result in harm against the

[1] It should be noted that Tesla CEO Elon Musk intentionally and successfully devalued the company's stock in May of 2020 via a tweet stating, "Tesla stock price is too high imo" (Lopatto, 2020). However, the incidents discussed are unrelated to Mr. Musk's personal motivations, and corporate espionage remains undesirable for an organization.

organization—only threaten it or its constituencies. The behaviors also differ in target, with CWBs typically directed either at the organization (CWB-O) or other employees (CWB-I; Dalal, 2005). Insider cyberdeviance can be directed similarly but does not need to be consciously aimed since cyberdeviance is not always intentional or malicious in nature. For example, using a single password for multiple accounts weakens the security of said accounts, but the failure to maintain 20-something unique, complicated, and routinely updated passwords is not an act of malice, nor is it a behavior intentionally directed at the organization. Similarly, individuals who fall victim to a phishing attack do so accidentally, often because they do not know better.

As such, the definition of CWBs as "intentional" employee behavior excludes many cyber-related deviant behaviors, as not all insider-precipitated cyber incidents are brought about intentionally. Though the Tesla incidents were indeed malicious and intentional acts, many other security breaches result from the actions of non-malicious employees (Posey et al., 2014). The Equifax breach resulted largely from a lack of employee initiative, while the Twitter incident stemmed from employees falling victim to a cyber-mediated social engineering attack—hardly a demonstration of malevolence. However, even the above definitions of cyberdeviance neglect these aspects of insider cybersecurity behavior. The role of intentionality in describing and categorizing insider cybersecurity behaviors is a main subject of this study and is therefore fully addressed later in the document.

Antecedents

Organizations typically possess an Information Security Policy (ISP) establishing the rules and guidelines for proper employee use of information communication technologies (ICTs; Whitman et al., 2001). The ISP outlines acceptable use and handling of organizational technology, software, and data, and provides a practical metric for assessing "good" and "bad" employee computer use. Though deviance from this policy differs from other deviant or counterproductive work behaviors, it shares antecedents with these frequently studied I-O topics (Weatherbee, 2010).

Cybersecurity behaviors of employees are influenced by both intrinsic and extrinsic factors (Donalds & Osei-Bryson, 2020), complicating efforts to understand and predict when and if deviance will occur. It is also worth noting that characteristics ideal for work purposes can possess negative effects on compliance behaviors. Goal-oriented employees will violate the organization's security policy if such noncompliance facilitates the completion of their job tasks (Guo et al., 2011). Sometimes, individuals who are ethically inclined will violate ISPs with benevolent intentions, such as the time a hacker took control of aircraft systems in order to spy on passenger devices connected to the plane's Wi-Fi (Brewster, 2018; in Couce-Vieira et al., 2020).

The password paradox further emphasizes the complexity of employee compliance. An organization's implementation of additional cybersecurity training—combined with offering rewards for good security hygiene—saw an increase in employee password changing, with the new passwords possessing greater complexity (Stanton et al., 2005). However, employees who participated in the training and received incentives were also more likely to write down their new passwords and store them beside their computer, thus negating most of the additional protection gained from the more complex credentials (Stanton et al., 2005). While the implementation of evaluation, monitoring, and deterrence efforts from the organization may reduce these sorts of non-malicious ISS deviance (Ifinedo & Idemudia, 2017), monitoring fails to provide a viable solution: it is often perceived as a threat to employee privacy and is associated with decreases in employee satisfaction (Mastrangelo et al., 2006; Stanton & Lin, 2001). Additionally, monitoring is not effective against all types of cyberdeviance: it demonstrates no significant relationship with nonproductive computer use (Mastrangelo et al., 2006). As such, monitoring is less favored than more proactive interventions—with current researchers beginning to consider the role of personal characteristics of employees.

Individual Differences. Personal traits and characteristics are often favored by I-O psychologists in hiring situations due to their usefulness in selection, association with productivity, and decreased likelihood of inciting litigation. These individual differences also prove relevant to predicting cybersecurity compliance behavior. While self-control—a positively-viewed trait associated with higher levels of productivity—is negatively related to the ISP violation of cyberslacking (Kim & Byrne, 2011), self-efficacy is positively related to such behavior (Mercado et al., 2017). Of the "Big 5" personality traits, possessing high levels of openness to experience, agreeableness, or neuroticism are all associated with a decreased likelihood of violating cybersecurity policies, while more extroverted individuals indicated a higher likelihood of committing such violations (McBride et al., 2012). Another study found evidence for agreeableness and conscientiousness being strongly related to good cybersecurity habits (Hadlington & Murphy, 2018). The significance of conscientiousness is unsurprising, given the trait's typical association with dutifulness and attention to detail.

The so-called "Dark Triad" traits of psychopathy, narcissism, and Machiavellianism all possess significant relationships with the intent to commit cyber revenge, while individuals with low Dark Triad scores appear to harbor less malevolent intentions (Maasberg et al., 2020). Recent research into the Dark Triad supports the inclusion of a fourth trait—sadism—to form a Dark Tetrad of related but distinct antisocial traits (Dinić et al., 2020; Neumann et al., 2021). Everyday sadism has been found to predict negative behaviors such as trolling on social networking sites (Cracker & March, 2016), but has not received the same attention as the other traits of the Dark Tetrad within cybersecurity research. Given the malicious nature of cyberincidents such as the Tesla espionage and sabotage, sadism may prove relevant to other cybersecurity behaviors. Though personality and psychological factors remain important antecedents that should be incorporated into the design of security systems (Greitzer et al., 2019, in Maasberg et al., 2020), employees do not behave in a vacuum. Behavior is a function of the individual and the environment (Bartunek & Woodman, 2015), and other contextual factors serve as important influences over employee cybersecurity behaviors.

Contextual Issues. Organizational culture is one such factor impacting employee cyberdeviance. Workgroup norms hold significant influence on both attitudes toward non-malicious security violations and intentions to engage in these behaviors (Guo et al., 2011). A similar relationship exists wherein organizational norms strongly and positively relate to cyberloafing: if it is common for employees to utilize the internet for personal reasons while at work, then individuals are more likely to use their information and communication technologies for such purposes (Mastrangelo et al., 2006). This finding echoes cybersecurity professional's calls for maintaining a strong organizational "Security Culture."

Employee's home lives are also suspected to play a role in less malevolent forms of insider behavior. Notably, researchers have proposed that the increasingly blurred boundaries between work life and home life—as exemplified in the expectation for employees to be reachable by email well past the close of business—may result in the intrusion of home duties into the workday via increased personal web use ("cyberslacking" or "cyberloafing"). As articulated by Kim and Byrne, "One can imagine that it is just as easy to slip into leisurely behaviors while one should be working as it is to slip into work behavior when one is not supposed to be working" (2011, pp. 2281). Meta-analytic examination of this relationship fails to identify any significant results, suggesting that unexamined moderators may be impacting how work-life balance and cyberloafing interact (Mercado et al., 2017). Additionally, the wide range of behaviors included under the label of "personal web use" may further confound results—a possibility discussed further in the current study. Still, this theoretical rationale offers a compelling explanation for how some cyberdeviant behavior might originate.

In a similar vein, a newer stream of research suggests employees are suffering under the cognitive load of cybersecurity-related demands. This avenue of investigation draws loosely from Conservation of Resources (COR) theory—in which the time, energy, money, and relationships possessed by individuals represent finite resources that people spend in order to meet the demands of their occupations and personal lives (Hobfoll et al., 2000). Under this perspective, stress results from an individual possessing insufficient resources to meet the full extent of their obligations or responsibilities.

The concept of decision fatigue echoes this conceptualization of psychological resources being diminished by demands, defining the concept as an "impairment of individual's self-control following the need to make too many deliberate, effortful decisions" (Baumeister, 2002; Cram et al., 2020 pp.4). Information overload may lead to such impairment. In such situations, individuals drain their psychological resources when they are forced to consciously and deliberately prioritize, balance, and heed as much of the presented information as possible. The deleterious effects of such overload are evidenced by the curvilinear relationship between decision accuracy and information load (Schroder et al., 1967).

Given that a primary strategy for promoting good security behaviors in employees entails regular education, training, and awareness efforts, Cram and colleagues hypothesized that employees might be similarly overwhelmed by the amount of security-related information routinely directed their way (2020). Terming the phenomenon information security fatigue, the same authors described it as a "socio-emotional state experienced by an individual who is tired and disillusioned with security policy requirements… employees who experience security fatigue and engage in non-compliant security behaviour for this reason are distinct from those employees who consistently ignore or refuse to comply with security policies" (Cram et al., 2020; pp.2).

Individuals are expected to suffer from security fatigue as a result of attempting to simultaneously meet the competing demands of prescribed security practices and their original job tasks, with the consequences of fatigue resulting in decreased self-control and ambivalence toward security practices (Cram et al., 2020). This fatigue may play into cognitive weariness—which, combined with physical fatigue and emotional exhaustion, form the negative experience of burnout (Shirom & Melamed, 2006). As such, it stands to reason that cybersecurity fatigue may contribute to the experience of burnout—though current research has not yet examined this connection. Repeated exposure to cybersecurity prompts and reminders also leads to habituation (Anderson et al., 2016; Dalal et al., 2021), with employees ignoring or disregarding warnings entirely if such a message interrupts other cognitive tasks (Jenkins et al., 2016). This stream of research represents a recent application of cognitive psychology to the understanding of employee cybersecurity reactions and behaviors—thus indicating a shift to a perspective of cybersecurity that accommodates human error.

Observing the substantive overlap in subject matter as described above, it is clear that I-O Psychology is well-situated to contribute to research on insider cybersecurity behaviors, offering a dual scientist-practitioner focus steeped in the study of human behavior. IT professionals possess higher openness to experience than employees in other fields, but also possess lower levels of conscientiousness on average, and largely indicate more interest in realistic and investigative vocational interests (Ash et al., 2006a, in Bashir et al., 2017). This is to say: the subject matter experts for organizational cybersecurity are not necessarily predisposed for the more social aspects of promoting good security habits to the organization at large.

Consequently, psychological factors of insider behavior have historically been deprioritized, representing only a recent addition to the scope of cybersecurity research. From the 1970's to the mid 2000's, only 5.8% of research in the Information Systems field considered the role of the workforce in ensuring organizational security (Zafar & Clark, 2009). Instead, the research focused nearly exclusively on the technological nuances of security frameworks, leading to a call for more holistic approaches to the problem (Dalal et al., 2021). Even with the recent rise in popularity of insider threat research, most articles from 1997 to 2013 addressed the application of theoretical perspectives or development of insider threat mitigation strategies: few examined insider threat behavior from a predominantly empirical perspective (Ophoff et al., 2014).

Current Theoretical Approaches

An additional fact supporting I-O psychology's entrance into this topic is that information security researchers already draw upon a number of interdisciplinary theories to explain insider behavior. Many of these theories possess relevance to traditional I-O topics of study—if they are not of psychological origin entirely. Detailed below is a brief overview of a selection of commonly cited theories. A summary of these theories may be found in Table 1.

Table 1: Summary of Commonly Utilized Theories

Theory	Authors	Characteristics	Predictions	Examples
Deterrence Theory	Akers, 1990	A theory explaining crime as occurring when individuals see payoffs for engaging in the behavior and deterred when costs of criminal behavior are perceived as significant.	Employees will violate the ISP depending on whether the perceived benefits of violation exceed any perceived costs (i.e., punishment for being caught).	Ifinedo & Idemudia, 2017: Increased certainty and severity of punishment associated with fewer non-malicious information systems security behaviors.
Theory of Reasoned Action (TRA)	Fishbein & Ajzen, 1975	Proposes that attitudes and subjective norms about a particular behavior influences an individual's intention to perform said behavior, which consequently predicts actual behavior.	Suggests that personal attitudes and workplace norms (i.e., "security culture") will influence an individual's cybersecurity intentions and behaviors.	Pahnila et al., 2007: Normative beliefs directly influenced intentions to comply with security behavior; ISP compliance intentions predict actual compliance behavior.
Theory of Planned Behavior (TPB)	Ajzen, 1991	An extension of TRA, this theory includes that perceived behavioral control will affect both intentions to perform a behavior and actual behavior.	Echoes TRA, but adds that individuals will perform positive cybersecurity behaviors when they possess high security self-efficacy.	Donalds & Osei-Bryson, 2020: Security self-efficacy predicted individual general security compliance, both predicted password compliance behaviors.
Theory of Interpersonal Behavior (TIB)	Triandis, 1977	Accounting for the influence of the attitudes, social norms, intentions, and efficacy described in TRA and TPB, this theory also posits that emotions and habits play a role in predicting behavior.	Echoes TPB, but adds that cybersecurity behaviors are indirectly influenced by an individual's affect, and directly affected by extraneous facilitating conditions and cybersecurity habits.	Moody & Siponen, 2013: Affect possessed a significant direct effect on intentions; habit moderated effect of intentions on behavior and also strongly predicted behavior
Protection Motivation Theory (PMT)	Rogers & Prentice-Dunn, 1997	A fear-driven model describing effects of threatening information on behaviors and attitudes. One's appraisal of the threat and their ability to cope influence their protection motivation (behavioral intentions).	Faced with information on cybersecurity, individuals will assess the magnitude of threat and the organization's ability to handle danger when choosing whether to perform various cybersecurity behaviors.	Li et al., 2017: Organizational policies and actions influenced employee's threat appraisals. Appraisals of organizational vulnerability to cyber incidents predicted more engagement in cybersecurity behaviors.

Health Belief Model (HBM)	Rosenstock, 1974	Based upon PMT, identifies four specific perceptions as influencing the seeking of medical care: perceived susceptibility, severity, benefits, and barriers.	Employees will violate or comply with an organization’s ISP according to the perceived susceptibility of the organization to cyberattack, severity of consequences, benefits of (non)compliance, and barriers to (non)compliance.	Dodel & Mesch, 2017: Perceived vulnerability to virus (susceptibility), awareness of severity, perceived benefits of antivirus, and willingness to put in effort for safe browsing (low barriers) all related to anti-virus preventative behavior.
Psychological Contract Theory	Rousseau, 1989	Using a “metaphor of the ledger,” describes unspoken but understood expectations about transactional/relational obligations owed by employee and employer to each other.	Posits that employees whose expectations are violated will not feel compelled to protect the organization with good security hygiene.	Han et al., 2017: For supervisors, perceived cost of compliance with an ISP was mitigated by the effects of a fulfilled psychological contract, which led to increased compliance intentions.

Models based upon Deterrence Theory (Akers, 1990) assume that individuals deliberate on the benefits and costs of violating security policies. Employees then make a rational choice to engage in or avoid ISP noncompliance based upon the likelihood of punishment weighed against the probable value of rewards (Straub, 1990). Undesirable behavior is said to be avoided when employees perceive punishments that are certain, swift, and severe (Akers, 1990; McBride et al., 2012). However, humans often make irrational decisions—and the theory does not consider accidental or unintentional forms of cybersecurity deviance. Deterrence Theory is also criticized for the fact that it primarily explains *when* an employee will violate or comply with an ISP, but not why (Guo et al., 2011). Additionally, not all components suggested by this theory prove significant in empirical research: while perceived severity of punishments reduces violation intentions, perceived certainty of punishment does not hold any significant effect (D'Arcy et al., 2009; in Guo et al., 2011).

Similarly, researchers draw upon the Theory of Reasoned Action (TRA; Fishbein & Ajzen, 1975), Theory of Planned Behavior (TPB; Ajzen, 1991), or both via the Theory of Interpersonal Behavior (TIB; Triandis 1977) to explain relationships between cybersecurity beliefs, attitudes, intentions, and subsequent behavior. Attributing intentions to commit ISP violation to personal attitudes and beliefs about cybersecurity, TRA identifies intentions to violate cybersecurity as the predominant contributor to actual actions of violations (McBride et al., 2012). Meta-analytic results confirm the importance of attitudes as antecedents of cybersecurity behaviors, identifying them as the second-most predictive characteristic (Cram et al., 2019).

Similarly, TPB posits that ISP compliance intentions are influenced by subjective norms, perceived behavioral norms, and compliance-directed attitudes—with empirical results supporting this assumption (Bulgurcu et al., 2010). TIB draws upon both TRA and TPB, but includes the addition of emotional factors, other exogenous influences, and habit (Moody & Siponen, 2013). Possessing a habit of personal web use strongly correlates to future intentionality and continued usage (Huma et al., 2017; Mercado et al., 2017; Moody & Siponen, 2013), thus indicating that employees may be asked about their “typical” or “habitual” computer use behaviors in order to gain an accurate idea of actual behaviors.

The Health Belief Model (HBM)—often examined in conjunction with Protection Motivation Theory (PMT; Rogers & Prentice-Dunn, 1997)—also holds relevance to framing the psychological considerations behind cybersecurity behaviors (Anwar et al., 2017; Rosenstock, 1974). In this approach, there are four main factors that interact with other organizational cues to influence employee compliance: perceived susceptibility of the organization to a cybersecurity incident, perceived severity of any incident likely to result from the employee’s behavior, perceived benefits of violating the ISP, and perceived barriers to complying with the ISP. Theoretically, the HBM and PMT explain why otherwise-diligent employees might choose to violate an ISP—for instance, in situations where complying with the ISP is perceived to have more barriers than benefits (Anwar et al, 2017). Researchers found that while no significant gender differences exist in the perceived severity, benefits, barriers, or susceptibility of organizations, male respondents reported more hygienic cybersecurity behaviors (Anwar et al., 2017). Prior exposure to cybersecurity best practices correlated with increases in perceptions of severity and vulnerability, with decreases in perceived barriers (Li et al., 2019). The same study found perceptions of severity and barriers predicted more and less protection behaviors, respectively.

Though less frequently cited by InfoSec professionals, Psychological Contract Theory (Rousseau, 1989) neatly complements other organizational justice theories in explaining more intentional forms of cyberdeviance (Leach, 2003). Encompassing both transactional and relational dimensions, the concept of the psychological contract describes the implicit understanding between a person and their employing organization that establishes the mutual obligations owed by and due to each party (Kofter, 1973; Morrison & Robinson, 1997). As such, any failure from an organization to preserve the terms of the working relationship may violate the psychological contract—leading to resentment and potential retaliatory behavior on the side of the employee. Perceived fulfillment of a psychological contract is consequently associated with higher ISP compliance intentions in both supervisors and supervisees, with the relationship stronger for supervisors (Han et al., 2017).

Several of the above theories place extrinsic factors as primary drivers or deterrents of behavior. The current paper does not pursue this perspective, as empirical research demonstrates the importance of intrinsic factors affecting compliance and deviance: a meta-analytic relative weights analysis identified personal norms and ethics to explain 21% of the variance in cybersecurity behavior, with attitudes, self-efficacy, and normative beliefs following behind as similarly influential (Cram et al., 2019). Dominant decision-making styles also influence an individual's general security orientation—which, combined with general security awareness and personal self-efficacy, significantly predicts compliance with recommended password hygiene (Donalds & Osei-Bryson, 2020).

Criterion Problems

Despite the wide variety of theoretical perspectives applied to cybersecurity behaviors, past and current research efforts have been hindered by a simple issue: which employee behaviors are included in the definition of cybersecurity deviance? This question prompted Warkentin and colleagues to name the biggest challenge for InfoSec research methodologies as properly measuring the dependent variable of cyberdeviance (2012; in Crossler et al., 2013). Dalal and colleagues reiterated this nine years later, likening the issue to I-O challenges with quantifying job performance by stating that "end-user cybersecurity performance has a 'criterion problem' (Austin & Villanova, 1992)" (2021; pp.7). This problem is exhibited in the breadth and variety of employee actions included within a single construct. Indeed, "cyberdeviance" may simultaneously refer to both an employee neglecting to routinely update their password and one actively tampering with security firmware. Even relatively minor behaviors such as scrolling through social media at work—an activity which falls under the sub-classification of cyberloafing—may be considered an act of cyberdeviance (Kim & Byrne, 2011).

This issue is far from one of semantics. Rather, the lack of specificity poses an empirical problem because many studies fail to differentiate among forms of cyberdeviance, thus potentially confounding or limiting the applicability of their results (Van Den Bergh & Njenga, 2016). Additionally, the directionality in which cyber behaviors are measured moderates the effect of behavioral antecedents: meta-analyses indicate that the impact of attitudes, cultural norms, and moral values depends on whether behaviors are measured as "compliance" or "deviance", pointing to the two operationalizations of behavior as separate but related constructs (Cram et al., 2019; Guo et al., 2011). A lack of compliance is not necessarily a presence of deviance—despite some studies finding support for common antecedents of the two—but typical operationalizations fail to account for this distinction (Sommestad et al., 2015). The average cost of security incidents varies dramatically depending on whether the involved employee is negligent or intentionally malicious, with the latter almost tripling the cost to redress the breach

(Ponemon, 2020). Therefore, establishing a classification system possesses practical implications in addition to promising theoretical clarity.

While compliance is a common concern of Information Security professionals, researching the specific nuances of deviant behavior may prove the more uniquely informative of the two (Warkentin & Willison, 2009). As individuals do not feel the need to explain or justify their behavior when complying with an ISP, deviant behaviors may be more informative in explaining why employees behave the way that they do since more cognitive processes are expected to be at play (Guo et al., 2011). For example, Siponen and Vance proposed a neutralization model of security violation, describing how employees use techniques such as defense of necessity in an attempt to rationalize ISP violations (Siponen & Vance, 2010). Guo and colleagues also argue that not all forms of security violations are the same (2011). Ethics and personal norms provide significant explanatory power for ISP compliance and general organizational deviant behavior (Cram et al., 2019; Hu et al., 2011; Myyry et al., 2011), but they are not relevant for predicting non-malicious forms of security violations since these behaviors are not necessarily unethical or illegal (Guo et al., 2011). Based on these considerations, the current study explores insider behaviors to identify whether reported behaviors support classifications among lines of compliance, deviance, or intentionality.

Summary

Threats posed by organizational employees are significant and explainable with a number of theories, as evidenced by the magnitude and variety of research efforts thussofar directed at the topic. However, this variety also confounds efforts to establish a strong common definition of cyber-related employee behaviors. Scholars reason that some practical differences exist between various types of cyberdeviance, but do not know for certain since little empirical research has been conducted to specifically examine how these behaviors should be categorized. Meta-analyses indicate that deviance and compliance are separate and related constructs, but questions remain as to the need to differentiate beyond the framing of cybersecurity behaviors.

The Cyberdeviance Spectrum

Acknowledging the need for classification, researchers have proposed various dimensions along which to differentiate cybersecurity-related employee behaviors. Judging insiders based on their levels of expertise (low or high) and motivation (malicious, neutral, or beneficial), Stanton et al. proposed six profiles of end users—though no manner of latent class cluster analyses were conducted (2005). Skill also played a role in Salem et al.'s categorization of malicious insiders as either less-knowledgeable masqueraders or highly-skilled traitors (2008).

As with the above examples, many conceptualizations of insider behavior presume to organize such actions along lines of malice and intention to harm (Homoliak et al., 2019). Guo and colleague are attributed as the first researchers to consider *a lack of* malevolence when they presented their conceptualization of non-malicious security violations (NMSVs): "the behaviors engaged in by end users who knowingly violate organizational IS security policies without malicious intents to cause damage" (2011, pp. 205). These behaviors were characterized as being intentional and self-benefiting—insofar as to save employees time or effort—but performed without malice. Thus, while NMSVs could still pose a threat to the integrity of organizational information systems, they are not unethical or illegal behaviors in the same way as corporate espionage or hacking (Guo et al., 2011).

Other researchers soon followed suit, popularizing distinctions between intentional and unintentional insider deviant behavior. Clarifying intentional behaviors as deviance and unintentional ones as misbehavior, Crossler and colleagues noted "The mixing of these two categories of insiders can significantly limit the effectiveness and even applicability of some of the recommended remedies in [current] studies" (2013, pp. 92). Van Den Bergh and Njenga proposed three classes of insider deviance: misbehavior, non-malicious deviant behavior, and malicious deviant behavior (2016)—echoing Willison & Warkentin's 2013 dimensions of passive non-volitional, volitional non-malicious, and intentionally malicious insider behavior.

Addressing the components of intentionality and malice also brings up the question as to whether aggression should be considered as a factor, with researchers citing the emotion versus cognition driven aggression typology presented in Berkowitz, 1993 (Weatherbee, 2010). In accordance with this consideration, the current author presented a typology based upon both intentionality and neuropsychological manifestations of aggression, dividing cybersecurity behaviors into three main categories (Whitman, 2016). The first category, misbehavior, adhered to Crossler et al.'s definition of unintentional—and thus accidental—security violations, such as falling for a phishing attempt. Intentional behaviors were similarly labeled as deviant behavior and further split into "Hot Malcontents"—individuals committing neurologically "hot" or emotional acts of sabotage with intent to cause damage—and "Cold Opportunists," or those that commit fraud, espionage, or theft for the purpose of personal gain (Whitman, 2016). Should classifications based upon aggression prove accurate, then one would expect that everyday sadism could play a role in motivating various categories of cyberdeviance.

The above efforts at classification represent a relatively new branch of cybersecurity research, with many of the calls for clarity arising within the past decade. Historically, cybersecurity research tended to group cybersecurity violation behaviors performed by employees within a single category, leading current researchers to cite the need for more specific designations of employee cybersecurity violations. Additional taxonomies not discussed here similarly divided cybersecurity misbehaviors into various categories by means of their intentionality, malice, or technical impact. However, the actual underlying patterns of cybersecurity misbehavior that employees engage in remains unknown.

The introduction of cybersecurity violation behavior taxonomies has not been matched with a person-driven analysis of actual patterns of noncompliance. However, researchers have noted that it is theoretically unlikely that behaviors such as file theft would possess the same antecedents and correlates as cyberloafing or neglecting a password change (Crossler et al., 2013; Van Den Bergh & Njenga, 2016). Thus, attempts to discourage each type of behavior would need to differ in order to be effective. Conducting a latent profile cluster analysis would serve as a logical next step in this area of research by identifying common trends within employee behaviors and providing an empirical aspect to current taxonomic efforts.

The multitude of ways to categorize employee security behaviors ultimately poses more questions than answers—for they remain hypothetical delineations according to whatever rationale the researchers favored. Underlying all classification efforts, however, is an assumption that some insiders are inherently different from others. Whether by their malicious intentions or lack thereof, researchers and practitioners alike seem to agree that different types of insiders demonstrate different patterns of behavior. Therefore, examining actual behaviors may reveal more meaningful associations between actions than hypothetical categorizations. Drawing a taxonomy around empirically related behaviors may consequently enhance efforts to pinpoint antecedents of cyberdeviance without the need to moderate the analysis five ways to Sunday.

Identification of actual habits of computer-use CWBs would serve to better inform organizational interventions by enabling the targeting of specific patterns of misuse. Additionally, results may possess implications for the meaningfulness of current cybersecurity misbehavior taxonomies—thus contributing to the more accurate research and discussion of such behaviors. Examination of specific cybersecurity behaviors—rather than compliance or deviance from an information security policy or security norms—provides the most informative understanding of whether underlying insider "types" exist within observed cybersecurity behavior.

Research Question 1: How many latent profiles of employee cybersecurity behaviors can be identified, and what are their qualities?

Previously, this paper discussed the importance of personal characteristics and organizational context in predicting cyberdeviance. Namely, that several personality traits and the three Dark Triad characteristics demonstrated prior significance when predicting cybersecurity violations, with rationale for the inclusion of sadism and the Dark Tetrad. Models of decision fatigue implied that an individual's demands—and by extension, their degree of cognitive weariness, a facet of burnout—might lead to "cyber fatigue" and thus decreased cybersecurity compliance. Additionally, research identified the metaphor of the ledger as a means of explaining why employees willingly violate an organization's ISP, drawing attention to the relevance of the psychological contract. Given that these relationships proved significant even when aggregating cyberdeviant behaviors, examination of these traits as covariates is warranted.

Research Question 2a: Do any of the HEXACO or Dark Tetrad personality traits significantly vary with cyberdeviant profile membership?

Research Question 2b: Do levels of employee burnout or psychological contract fulfillment significantly vary according to cyberdeviant profile membership?

The Issue with Cyberloafing

Personal Web Use (PWU) poses an interesting challenge to cyberdeviance classification efforts insofar as it represents a continuum unto itself. A poster child for the jangle fallacy, PWU—or, more commonly, cyberloafing or cyberslacking—also appears within the literature as non-work-related computing (NWRC), cyberbludging, online loafing, internet deviance, problematic internet use, internet abuse, and ICT/IS/computer misuse, with more severe manifestations termed internet addiction, internet dependency, and internet addiction disorder (IAD; Kim & Byrne, 2011). Less commonly, personal internet use has been included under the umbrella of “work computer deviance” (Mastrangelo et al., 2006). The severity of cyberslacking-related behaviors therefore encompasses everything from emailing a joke to a co-worker to gambling and viewing pornography while at work (D’Arcy et al., 2009; in Guo et al., 2011).

Anandarajan and Simmers defined personal web use as the “voluntary act of using web access during work to surf non-work-related websites for non-work-related purposes” (2004; pp. 2), while Fox specified that such usage can include online shopping, job searching, video gaming, video streaming, and visiting news sites (2007). Meanwhile, Kim & Byrne defined cyberloafing as the “voluntary, aimless, and undirected way of using web access and engaging in non-work-related activities on a regular basis, partially due to a lack of self-control at work” (2011; pp .2272). Examination of these definitions leaves no confusion as to the near-identical nature of these differently-named variables.

Furthermore, researchers disagree as to whether all forms of cyberslacking are inherently detrimental to an organization. In addition to productivity losses, Chen and colleagues hypothesized that PWU might also lead to more serious concerns such as network congestion, legal liabilities, and vulnerability to malware attacks (2008). However, personal web use might also serve as a break from work, with potentially positive effects on employee satisfaction, productivity, and engagement (Kim & Byrne, 2011; Mastrangelo et al., 2006). Meta-analytic results do little to clarify this: while cyberloafing is related to overall CWBs at a correlation of +0.38, it is unrelated to job performance, and positively related with self-efficacy (Mercado et al., 2017). Though overall job satisfaction does not predict cyberloafing, satisfaction with *remote work* does, with dissatisfied employees more likely to cyberslack—potentially due to the limited organizational oversight offered by ecommuting (Mercado et al., 2017; O'Neill et al., 2014). This finding highlights the importance of examining these behaviors in the work-from-home culture of a post-COVID-19 society.

Even prior to the pandemic-induced transition to remote work, cyberloafing behaviors ran rampant through the workplace. Over 60% of employees spend some time on social networking sites, with 10% spending over a third of the workday or longer browsing the internet (Ethics Resource Center, 2012). The most commonly reported behaviors among cyberslackers were checking non-work emails, visiting news sites, and shopping online, while only half or fewer individuals reported booking vacations or job hunting (Blanchard & Henle, 2008). As pointed out by Mercado et al., the high frequency of personal web use might be attributed to the accessibility of cyberloafing, as employees need minimal technical skills to kill time on the internet (2017).

Several theories and classification efforts have been dedicated to the study of cyberloafing. The most comprehensive schema, presented by Kim & Byrne (2011), divides behaviors into three broad categories of personal web use: aimless PWU (cyberloafing/cyberslacking), strategic PWU (non-work-related computing), and problematic PWU (further separated by severity into internet abuse, internet addiction, and IAD). Other classifications of cyberloafing distinguish behaviors along lines of severity (Blanchard & Henle, 2008), its destructive or constructive effects (Warren, 2003), its nonproductive or counterproductive nature (Mastrangelo et al., 2006), email versus browsing behaviors (Lim & Teo, 2005), or along its intended purposes of commerce, research, and communication (Mahatanankoon et al., 2004). However, past research focused primarily on explaining employee motivations for engaging in cyberslacking, rather than theorizing as to its dimensions.

For example, Konig and De La Guardia drew upon Clark's 2000 work-family border theory to examine whether border strength between work and nonwork affected employee personal web use at the office (2014). The authors theorized that blurred boundaries between work and home might encourage employees to utilize ICT for personal reasons while at work. Results of a hierarchical regression found that while private demands and border strength significantly interacted when predicting PWU, the subsequent increase in R^2 due to this interaction failed to reach significance. They concluded that the observed relationship could not be interpreted, asserting that their results pointed to PWU as leading to more negative outcomes (Konig & De La Guardia, 2014). However, employees engaging in different types of personal internet use may have clouded these results: it stands to reason that employees with lower demands might perform more leisurely forms of PWU (such as streaming videos or browsing social media) than employees struggling with higher demands, for whom border strength might matter more and who would therefore be likely to engage in more purposeful, strategic PWUs (checking non-work emails, job searching).

Confusion as to the impact or severity of cyberslacking, combined with the vast array of behaviors labeled as such, leads to the question as to whether cyberslacking itself is also a construct with multiple patterns of engagement. As such, the existence of subgroups of cyberslacking "types" seems plausible and must be investigated prior to any inclusion of cyberslacking habits within a latent profile analysis of broader cybersecurity behaviors.

Research Question 3: Is there evidence to support the existence of distinct homogenous subgroups of cyberslacking behavior, and if so, what are their characteristics?

Proponents of the strength model of self-control (Muraven & Baumeister, 2000) consider the negative relationship between cyberloafing and self-control as a primary explanation for the prevalence of cyberslacking (Mercado et al., 2017). Echoing the Conservation of Resource (COR) theory (Hobfoll et al., 2000), the model states that individuals possess differing levels of self-control, which itself is a finite resource that is diminished throughout the day. Low levels of self-control are indeed linked to increased engagement in general workplace deviance (Restubog et al., 2010), and such a model would potentially explain the positive correlation between cyberslacking and general CWBs (Mercado et al., 2017). The personality trait conscientiousness is also positively associated with self-control and negatively related with cyberloafing, further supporting this theory.

Similar to findings on associations between personality and general cybersecurity behaviors, research found agreeableness and honesty to also predict cyberslacking—but no influence of neuroticism (O'Neill et al., 2014). Though Dark Triad traits are associated with intentions to violate cybersecurity policies, no previous research has specifically examined Narcissism, Machiavellianism, Psychopathy, or Sadism in conjunction with cyberslacking. The apparent relevance of the traits to the more severe forms of cyberloafing prompts the Dark Tetrad's inclusion in the research topic:

Research Question 4a: Do any of the HEXACO or Dark Tetrad personality traits vary according to cyberslacking profile membership?

Previous researchers suggested employees might engage in cyberslacking in order to "balance the books," thus compensating for work intruding upon family time (Kim & Byrne, 2011; Mercado et al., 2017). That is, since ICT enables organizations to reach employees while they are "off the clock," employees might find it justifiable or easy to use the internet for personal reasons while at work. Since high levels of reported boundary violations were associated with increased levels of burnout in a physician sample (Johnson et al., 2016), it stands to reason that burnout might also be related to increased cyberslacking—potentially as a method of emotion-focused coping. Indeed, Henle and Blanchard found evidence to support minor ICT misuse as just that, though they attributed it to role ambiguity and conflict (2008).

Previous discussions of boundary violations may also be interpreted under the lens of the psychological contract. This is appropriate due to the psychological contract's emphasis on mutual obligations and expectations that, when violated, cause distress and a loss of trust (Kofter, 1973). Han et al. (2017) found evidence for the influence of psychological contract fulfillment on general cybersecurity policy compliance, while Leach (2003) argued that a fulfilled psychological contract was one of three factors that could improve secure behavior. Meta-analysis also demonstrated a strong positive relationship between neutralization techniques and engagement in PWU, supporting the notion that employees rationalize perceived injustices inflicted by the organization as an excuse for their own wrongdoing (Mercado et al., 2017). Given that cyberslacking behaviors are also included in examinations of cybersecurity research, the above findings warrant examination of a potential relationship with the psychological contract.

Research Question 4b: Do burnout or psychological contract fulfillment vary according to cyberslacking profile membership?

LPA and Dimensionality

When attempting to discern the dimensionality of a construct, factor analyses are commonly used. Wielding a combined sequence of exploratory and confirmatory factor analysis, statisticians identify the number of latent variables that substantively and statistically explain variations in response (Kline, 2015). However, the current study utilizes latent profile analyses rather than factor analyses for multiple reasons.

Factor analysis is a process of identifying the underlying latent variables that compose the measurement model of observed indicators. Assuming indicators are independent from each other, factor-analytic methods partition total variance into common and unique variance (Bollen, 2002; Kline, 2015). Common variance shared among items is presumed to arise from a smaller number of underlying latent factors, while unique variance may be both specific (systematic but unexplained variance) and random measurement error (Kline, 2015). As such, exploratory (EFA) and confirmatory (CFA) factor analyses enable tests of unidimensional measurement by mapping simple indicators onto their respective latent factors.

EFA/CFA models therefore are a natural choice when testing questions about the dimensionality of a variable, such as addressing the number of facets composing a construct or examining whether two constructs statistically differ from each other. For example, Elhai and colleagues tested four theoretically supported models of depression using factor analysis, finding support for a two-factor model dividing symptoms according to somatic and non-somatic manifestations (2012). Additionally, researchers utilizing factor analyses discovered that negatively worded items on a commonly-used Organizational Citizenship Behavior (OCB) scale loaded on a separate latent factor when analyzed in conjunction with the full OCB scale, but loaded onto the latent CWB factor when included in analysis of a CWB scale—thus indicating that the original OCB measure incorrectly captured variance attributable to CWBs (Henderson et al., 2019).

As the driving question behind the current study concerns the need to identify meaningful dimensions of employee cybersecurity behaviors, one might consider factor analyses as appropriate for answering the question. However, the above examples describe how factor analysis may be used to inform researchers as to the underlying structure of a variable; the answer to the current research question lies not in *how cybersecurity items are related to each other*, but rather in *how employees engage in these behaviors*. This represents a person-centric research question, rather than one centered on latent variables.

Consider the following over-simplified metaphor: a restaurant's menu contains a number of salads, soups, pasta dishes, steaks, cakes, and pies for customers to order. Factor analysis—observing the commonalities shared between items—would inform the restaurant that soups and salads share variance explained by the latent variable *appetizers*, while pastas and steaks share variance with a different factor, *entrees*. This enlightens the restaurant as to which category each menu offering belongs to—just as in previous cyberloafing research, factor analysis supported the division of behaviors into email-related behaviors and browsing-related behaviors (Lim & Teo, 2005).

However, this particular restaurant is not interested in which menu items are most similar to each other—rather, it wants to know which items are commonly ordered together, just as the current research questions which behaviors are performed together. This represents a person-focused research question, in that the restaurant is asking what orders specific types of customers might make. A latent profile analysis would answer this question, perhaps reporting three profiles of restaurant customer: customers that order many appetizers and few entrees, customers that order few appetizers and some entrees, and customers that order both appetizers and desserts. Similarly, applying latent profile analysis to cybersecurity behaviors may inform researchers as to what types of insiders exist, and what sort of cybersecurity behaviors are performed by each type. Identifying these types of insiders provides a more comprehensive understanding of how cybersecurity and cyberslacking behaviors are related.

Cyberloafing

Several reasons prompt the separation of cyberloafing and general security behavior observed in this study. On its own, cyberloafing is a concept so broad as to be indiscriminate. The high base rates and correlation with engagement in other general CWBs initially differentiates it from other cyberdeviant behaviors. This combination of multidimensionality and frequency of occurrence means that examining cyberloafing independently can help maintain the maximum amount of variance in responses, thus providing a more informative understanding of any underlying profiles. If the current study were to utilize both cyberloafing and general cybersecurity behaviors as indicators within a single analysis, the former may overwhelm the latter and interfere with the interpretability of results.

The alternative would be to condense cyberloafing behaviors into a single indicator to be used in the profile analysis of general cyberdeviance. However, to do so would be to assume the relatedness of all cyberslacking behaviors. There are substantial theoretical reasons to believe that homogenous latent subgroups exist within the broader designation of cyberloafing behaviors—to ignore this possibility and proceed with a single larger analysis is to deliberately sabotage the investigation by potentially confounding what may be two separate patterns of behavior. Therefore, the current study examined cyberloafing independently from general cybersecurity behaviors.

Measurement Issues

The current study cites evidence of a criterion problem but does not distinguish between research examining cybersecurity behavioral intentions and research measuring actual behavior. However meta-analysis estimated the relationship between intentions to cyberloaf and actual cyberloafing behavior to correlate at +0.61—approaching the "rule of thumb" for collinearity (Mercado et al., 2017). Similarly, habitual cyberloafing relates to continued personal web use at +0.66, with habits of past cyberloafing behavior highly predictive of current and future cyberloafing (Huma et al., 2017; Soh & Yeik, 2018). Intentions to continue protective security behaviors positively related to actual continuance behaviors over time (Warkentin et al., 2016). Intended and actual compliance were also found to share seven out of eight examined antecedents in a meta-analysis of cybersecurity behavioral research (Cram et al., 2019). As such, the current author finds sufficient evidence supporting the use of self-reported insider security behavior as a proxy for other-rated reporting methods.

Exclusion of Contextual Factors. Behavior is a function of both the person and their environment, as reflected in the influence of organizational culture on insider cybersecurity attitudes (Guo et al., 2011). However, meta-analytic relative weights analysis identified employee's personal characteristics as the most influential upon their cybersecurity behavior (Cram et al., 2019). This is not to say that environmental factors—such as being passed over for promotion—cannot incite cyberdeviance, but such occurrences seem to be rare. Moody & Siponen found that one's past habit of personal web use was the strongest predictor of actual intentions and behavior, moreso than any facilitating environmental conditions (2013). Thus, with the exception of psychological contract fulfillment, the current study addresses only personal characteristics and individual differences, rather than attempting to assess extrinsic factors. Future I-O psychologists interested in organizational culture would be well-suited to contribute to the conversation on managing a company's security climate.

Hacking. Finally, the current study limits examination to only cybersecurity behaviors performed by typical employees. At the extreme end of destructive and counterproductive cyber behaviors lie "hackers"—individuals with the capability to delicately and deliberately gut the technological foundation of an organization's business operations. These individuals represent the epitome of the prototypical "dangerous insider," but the current study does not include measures of hacking-type behaviors for two reasons. Firstly, hacking is associated with higher self-efficacy and greater levels of self-control in the transgressing individual (Bashir et al., 2017). This suggests that hacking is dissimilar from other cyber-related deviant behaviors, particularly as the latter are related to negative self-control (Mercado et al., 2017).

The second reason for refraining from the analysis of hacking behavior is because these behaviors are already classified in InfoSec research and professional discourse: "black hat" hackers refer to insiders wreaking havoc with destructive or exploitative intent, "white hat" hackers refer to those who intrude upon information systems with the purpose of discovering and fixing weaknesses, and the label "grey hat" is reserved for hackers with mixed motives (Rogers, 2006). Given that the main goal of the current study is to address disagreement on the appropriate classification of insider behaviors, it does not make sense to include behaviors that are already well-distinguished from each other.

Summary

After considering disagreements within cybersecurity research, the current study highlights the needs to identify common patterns of employee security behaviors. This study argues there is evidence to support the existence of latent profiles of general cybersecurity behavior, with each profile depicting unique “types of insiders” according to the observed levels of each cybersecurity behavioral indicator. The current study notes that while cyberslacking is still considered a form of computer misuse, the breadth and variety of existing classifications—as well as differing theoretical backings—warrant analysis of profiles independent of general cyberdeviance. Suspecting the significance of personality, burnout, and psychological contract fulfillment in predicting various profiles of cyberslacking and cyberdeviance, the current study examines these variables as covariates.

Methods

In order to answer the research questions, the current study conducted latent profile clustering techniques in order to examine whether there are homogenous profiles of insider behavior. This study is the first to examine underlying subgroups of cybersecurity behaviors as a means of advising future classification efforts. Additionally, the current research examined several key covariates to determine if any variables relate to class membership in any particular profile. These efforts provide a more nuanced approach to examining the dimensionality of cybersecurity-related employee behaviors than previously attempted.

Participants and Procedures

Participants for the current study were recruited via Amazon’s Mechanical Turk (MTurk), following the recommendations of Peer et al. (2014). Namely, that participants possessed a minimum of 100 approved human intelligence tasks (HITs), with HIT approval ratings greater than or equal to 95%. Previous research identified MTurk participants to be more ethnically and socio-economically diverse than other typical sample methods (social media, undergraduate participant pool; Casler et al., 2013). Participants were limited to those who are 18 years of age or older, employed full-time, and resided in the United States.

Participants were paid $1.50 USD for completion of the survey measures and demographic information. Among other items assessing income, job sector, and work-from-home status, gender information was collected due to previous research found that women perform fewer cyberdeviant behaviors than their male counterparts (Anwar et al., 2017). Age was also be examined, though research on the relationship between age, tenure, and cybersecurity behaviors is mixed and varies according to whether technological expertise is controlled for (Dalal et al., 2021; Phillipps & Reddie, 2007).

The final sample consisted of 318 individuals who correctly answered all three instructed response items. Participants reported an average age of 42 (SD=10.82), with a fair balance between male and female respondents (42% female). The sample was largely white (71% Caucasian, 11% African American, <10% each Hispanic, Asian American, Native American), educated (82.4% possessing a bachelor's or higher degree), and married (72% married, 23% single). Two-thirds of respondents reported having at least one child.

Most participants (84%) indicated that they worked from home during the COVID-19 pandemic; only 20% of the total sample worked from home prior to lockdowns, and 16% remained in the workplace throughout. Only 17% of respondents occupied temporary positions within their organization, as corroborated by an average tenure of 10.16(SD=7.41) years. Unexpectedly, Information Technology was the most well-represented job sector, with 26% of respondents reporting employment within that field. Other prominent job sectors included Marketing/Sales (11%), Business Management, Education, Finance, and Manufacturing (around 8% each). While such a large representation of technologically literate respondents was not foreseen, the proportion of IT specialists is not unwelcome due to the relevance of the industry to the current study's focus.

Measures

Survey measures were hosted in Qualtrics. Measures for covariate variables were presented prior to the assessment of cybersecurity and cyberloafing behaviors. Measure details are as follows:

Cybersecurity Behaviors. General cybersecurity behaviors were measured with a modified version of the Self-Reported Cyber Security Behavior scale utilized by Anwar et al., (2017; Donalds & Osei-Bryson, 2020). Additionally, employees were asked to rate the cybersecurity behaviors of their peers using the Peer Behavior Scale from the same author (Anwar et al., 2017). Both measures are rated on a 7-point Likert type scale (1= "strongly disagree", 7 = "strongly agree"), with the final Self-Reported scale containing seven items and the Peer Behavior scale containing four. A sample item from the modified Self-Report scale is "I use different passwords for my different online accounts (e.g. online banking/shopping, Facebook, email)" (Donalds & Osei-Bryson, 2020). A sample item for the Peer Behavior scale is "My colleagues at work update their computers regularly." Though self-report measures rely on employees to honestly disclose their own habits, previous research found self- and coworker-reported cyberloafing behaviors to correlate at .64—nearing collinearity (Restubog et al., 2011). In the current study, peer behaviors are included for the purposes of assessing how employees perceive the cybersecurity environment in which they operate.

Cyberloafing. Cyberslacking was measured with Lim & Teo's Cyberloafing scale (2005). This measure is a 6-point Likert-type scale in which participants are asked to rate how often they perform specific behaviors while at work on a scale from 0 (never) to 5 (constantly). The scale consists of two dimensions: browsing activities ($\alpha = 0.85$) and emailing activities ($\alpha = 0.90$). Sample items include "shop online" and "send non-work-related email." An additional item, “browse social media websites” was added to account for the rise of platforms such as Twitter, Facebook, and Instagram (Greenwood et al., 2016). Often modified within cyberslacking research, this measure is one of the most commonly used scales for assessing personal web use (Mercado et al., 2017). Due to extremely high inter-item correlations, several items were averaged together for the sake of parsimony (e.g. “Check non-work related emails” and “Send non-work related emails”), or removed (“Browse sports-related websites”).

Personality. Previous research identified several intrinsic traits as significant predictors of cybersecurity behavior, with meta-analyses pointing to psychological factors as the most influential of all antecedents (Cram et al., 2019). In particular, personal ethics and morality are empirically associated with ISP compliance, but some researchers argue they are irrelevant to predicting non-intentional forms of cybersecurity violation. Therefore, personality traits were measured with the 60-item HEXACO PI-R (Lee & Ashton, 2020). This scale measures six facets of personality: Honesty-Humility (“I wouldn’t use flattery to get a raise or promotion at work, even if I thought I would succeed”), Emotionality (“I would feel afraid if I had to travel in bad weather conditions”), Extraversion (“I prefer jobs that involve active social interaction to those that involve working alone”), Agreeableness (“I rarely hold a grudge, even against people who have badly wronged me”), Conscientiousness (“I plan ahead and organize things, to avoid scrambling at the last minute”), and Openness (I’m interested in learning about the history and politics of other countries”). Participants are asked to rank statements to the extent that they agree with the statement on a scale from 1 (strongly disagree) to 5 (strongly agree).

The inclusion of the Honesty-Humility dimension in the HEXACO PI-R led to its selection over the commonly administered Big Five measure, as this dimension seems uniquely poised to capture variance due to both trait sincerity and morality. Previous research has not examined associations between this dimension and general cybersecurity behaviors—though it significantly predicted cyberloafing in previous studies (O'Neill et al., 2014). This warrants analysis of first-order correlations in addition to covariance with class membership of any profiles.

In order to measure "Dark" personality traits, the Short Dark Triad (SD3) scale developed by Jones & Paulhus (2014) were added to the survey battery, along with the shortened version of the Assessment of Sadistic Personality (ASP) designed by Plouffe and colleagues (2017). The SD3 consists of nine items for each of the three dimensions—Machiavellianism, Narcissism, and Psychopathy—with participants instructed to indicate how much they agree with each item on a scale from 1 (strongly disagree) to 5 (strongly agree). Sample items for the SD3 include "Most people can be manipulated" (Machiavellianism), "I know that I am special because everyone keeps telling me so" (Narcissism), and "Payback needs to be quick and nasty" (Psychopathy). Developed in conjunction with the SD3, the shortened version of the ASP contains nine items to measure Sadism, also on a 5-point Likert-type scale from *strongly disagree* to *strongly agree.* A sample item from the ASP is "Being mean to others can be exciting."

Burnout. Burnout was quantified by the Shirom-Melamed Burnout Measure (Shirom & Melamed, 2006). This measure assesses respondents' self-reported symptoms physical fatigue, cognitive weariness, and emotional exhaustion experienced while at work. The frequency of symptoms is recorded on a scale from 1 (never or almost never) to 7 (always or almost always). Sample items for physical fatigue, cognitive weariness, and emotional exhaustion are "I feel tired," "I have difficulty concentrating," and "I feel I am not capable of being sympathetic to co-workers and customers," respectively.

Psychological Contract. The Psychological Contract Transitions and Psychological Contract Fulfillment scales of the Rousseau's Psychological Contract Inventory (2008) were used to assess the extent to which employees feel that their organization's obligations have been fulfilled. In the Transitions subscale, participants are asked to rate the degree to which statements describe their employer's relationship to them on a scale from 1 (Not at all) to 5 (To a great extent). The three subscales examine an employer's violations of an employee's Trust (e.g. "Doesn't share important information with its workers"), the presence of Uncertainty ("Difficult to predict future directions of its relations with me"), and the Erosion of the employer-employee relationship ("Demand more from me while giving me less in return"). Participants are presented with short statements and are asked to rate how well their organizations have fulfilled these promises on a scale from 1 ("not at all fulfilled") to 5 ("very fulfilled"). The Psychological Contract Transitions Scale is worded such that high scores in each facet correspond to a worse psychological contract between employee and employer—a perspective that may also be interpreted as the existence of a more violated contract.

In contrast, the Psychological Contract Fulfillment Scale asks employees to rate how well they fulfill their commitment/promises to their employer on the same scale (1-5), and also how well their employer fulfilled their commitments to the employee. Employer fulfillment of the psychological contract was selected as a more general indicator of participant perceptions of the psychological contract for the current study and possessed small, negative relationships with each of the three Transitions facets.

Analyses

In addition to examination of descriptive statistics and first-order correlations, two latent profile analyses (LPA) were tested using cyberloafing and cybersecurity behavior scale items as indicators. Analyses proceeded with the tidyLPA and mclust packages in R (Rosenberg et al., 2018; Scrucca et al., 2016). Additional covariate analyses were conducted using mixed model analysis package in Mplus (Muthén & Muthén, 2021).

Latent profile analysis is a person-centric method for identifying underlying homogenous subgroups of a distribution that are otherwise obscured at the aggregate level of analysis (Pastor et al., 2007). Pointing out that a single normal or non-normal distribution may be composed of multiple combined sub-populations, researchers utilize LPA to investigate whether patterns of traits or behaviors exist as these sub-populations (Pastor et al., 2007). Model selection is not simply a matter of picking the solution with the best statistical estimates of fit; multiple sources of information must be jointly considered (Pastor et al., 2007). Latent profiles are analyzed for meaningfulness of membership (i.e., consisting of at least 10% of the total sample), distinction of profiles (i.e., all profiles able to be differentiated by at least one indicator), and interpretability of results (i.e., the profile is substantively meaningful). Indicators utilized within each profile analysis are located in Table 2.

Cyberloafing. Enumeration involved the sequential testing of one- to six-profile solutions, as well as four variance/covariance model structures. Fit statistics for candidate models may be found in Table 3. Ultimately, fit statistics for a class-invariant, unrestricted model—wherein variances between indicators were constrained across classes, and covariances between indicators were estimated and similarly constrained to equality—proved superior. Fit statistics for both of the class-varying specifications failed to converge beyond the first profile, and thus were not considered. Within the selected model, the Bayesian Information Criterion (BIC) and Corrected Akaike Information Criterion statistics both pointed to a five-profile solution. Latent class probabilities for most likely membership exceeded .89, indicating sufficient separation between profiles. The smallest class in the selected solution consisted of 13.5% of the total sample, with interpretation maintaining theoretical meaningfulness of each profile.

Table 2: Indicators for Cybersecurity and Cyberloafing Profiles

	Indicator	*Description*
Cybersecurity Behavioral Indicators	1 – Password Variation	*Uses different passwords for all online accounts.*
	2 – Password Freshness	*Regularly changes passwords every three months*
	3 – Setting Awareness	*Reviews security and privacy settings for online accounts*
	4 – Malware Awareness	*Monitors computer performance for changes; acts on malware alerts*
	5 – Phishing Checks	*Routinely double-checks emails before clicking attachments, avoids clicking unknown URLs*
	6 – Secure Transmission	*Avoids sending sensitive information over unsecure means, like text or email*
	7 – Backups	*Routinely backs up computer files*
Cyberloafing Behavioral Indicators	1 – Social Media	*Browses news websites or social media platforms (Twitter, Facebook, etc.)*
	2 – Online Shopping	*Shops online*
	3 – Gameplay	*Plays games online or in an app*
	4 – Seek Employment	*Looks for job postings, submits applications, etc.*
	5 – Adult Websites	*Visits sexually explicit websites*
	6 – Non-Work Email	*Checks and sends non-work/personal email*
	7 – Chatting	*Chats with family and friends via instant messaging or text*

General Cybersecurity Behaviors. Given the significance of cyberloafing profiles, only indicators included within the purview of general cybersecurity behaviors were included in the analysis. As with cyberloafing, enumeration proceeded with the comparison of candidate models across four variance/covariance model structures and from 1- to 6-class solutions (see Table 4). Fit statistics for the class-varying diagonal and class-varying unrestricted models failed to converge beyond a two-profile solution—with the response patterns in each profile ultimately lacking substantive meaning. Similarly, while the class-invariant and unrestricted model procured better numeric indications of fit, the BIC and CAIC values failed to converge on a model with substantial and meaningful latent profiles—membership proportions fell beneath the suggested 10% minimum with each additional class beyond two. Ultimately, a class-invariant and diagonal parameterization provided the most parsimonious and statistically supported model, with BIC and CAIC values supporting a 5-class solution. However, the AWE value supported a four-class solution. Given that the additional fifth class did not enhance interpretability of results—and class membership in the additional class failed to reach meaningful levels—the four-class solution was adopted.

Covariates. Following enumeration for both classes, additional covariate models with the identified variables was run using the mixed model analysis package in Mplus (Muthén & Muthén, 2021). Class memberships and covariate significance across profiles were examined. Namely, the HEXACO and Dark Tetrad personality traits, three facets of burnout, measures of psychological contract violation and fulfillment, and various demographic variables were studied to determine whether levels of any characteristic were associated with an increased likelihood of membership in any of the four cybersecurity profiles or five cyberloafing profiles.

Summary

The current study conducted two latent profile analyses in order to determine whether patterns of insider cybersecurity and cyberloafing habits support the existence of homogenous behavioral subgroups. Cyberloafing fit statistics pointed to a class-invariant unrestricted model with five profiles. For general cybersecurity behaviors, BIC and CAIC statistics were disregarded in favor of the AWE pointing to a 4-profile solution with a class-invariant specification with better interpretability and more meaningful profile membership. Following the selection of the final profile solutions, factors relating to personality, burnout, and psychological contract fulfillment were examined as covariates. This study represents the first effort made to examine cybersecurity behaviors using this person-centric analysis, as well as the first study to examine burnout in relation to personal web use.

Results

Correlations among key study variables are displayed in Table 5. Many of the covariate variables demonstrated surprisingly strong relationships, with some correlations approaching or exceeding the .70 threshold for collinearity. Most notably, sadism and psychopathy shared the most prominent association ($r = .90$, $p < .01$), though both facets also met the .70 threshold with Machiavellianism. All dark tetrad traits were significantly and negatively associated with the Honesty-Humility component of the HEXACO, with Narcissism's relationship being of moderate strength ($r = .45$, $p < .01$), and the rest demonstrating strong correlations.

Honesty-Humility also moderately and negatively correlated with all three facets of burnout, as well as moderately and negatively with the three psychological contract violations—individuals with a higher HH score were less likely to report experiencing a loss of trust, employer-induced uncertainty, and erosion of their employer-employee relationship. Similarly, individuals high in HH reported more positive views of their organization's fulfillment of its responsibilities ($r = .19$, $p < .01$). Conscientiousness displayed a strong relationship with Honesty-Humility ($r = .50$, $p < .01$), and correlated very strongly and negatively with psychopathy and sadism (r= -.71, -.74 *ps* < .01). These individuals also reported significantly fewer symptoms of burnout.

The three facets of burnout—cognitive weariness, emotional exhaustion, and physical fatigue—correlated with each other above the threshold for collinearity, indicating little differentiation between the facets. Burnout facets also strongly correlated with the similarly-intercorrelated psychological contract violation facets, such that individuals with more symptoms of burnout reported also feeling less trust, more uncertainty, and more erosion in their relationship with their organization. However, this relationship is not observed with the two-item measure of Employer Fulfillment, which significantly correlated with physical fatigue ($r = -.12$, $p < .05$), but neither of the other two burnout variables. Employer Fulfillment significantly and negatively related to the experience of Mistrust, Uncertainty, and Erosion. Interestingly, employees with high levels of extraversion and agreeableness were more likely to describe their employers as fulfilling their side of the psychological contract.

Respondents were asked to rate their perceptions of their peer's cybersecurity behaviors. Individuals who reported higher rates of peer cybersecurity behaviors also reported their organizations as more satisfactorily fulfilling their obligations ($r = .37$, $p < .01$), perhaps pointing to a sense of safety cultivated by the organization. Peer Cybersecurity behaviors also demonstrated small and positive correlations with participants' emotionality, extraversion, agreeableness, Machiavellianism, and narcissism.

Of the demographic variables, age significantly and positively related to the personality facets of honesty-humility and conscientiousness. Age also negatively correlated with all Dark Tetrad personality traits at a 99% significance level, though the effect size of these relationships remained small. Older individuals within this sample proved less likely to experience the physical fatigue, cognitive weariness, or emotional exhaustion aspects of burnout. Females in the sample demonstrated higher levels of emotionality, but lower levels of psychopathy and sadism than their male counterparts. No other significant correlations for gender were observed.

Table 3: Fit Statistics of Candidate Models for Cyberloafing Behaviors

Σ_k	# of classes, *k*	*LL*	npar	BIC	CAIC	AWE	BLRT, (*p*)
Class-invariant Σ_k	1	-4259	14	8598.2	8612.2	8718.9	---
	2	-3624	22	7374.4	7396.4	7565.2	1269.9 (<.01)
	3	-3440	30	7052.4	7082.4	7313.4	368.1 (<.01)
	4	-3347	38	6913.5	6951.5	**7244.6**	185.0 (<.01)
	5	-3299	46	**6863.0**	**6909.0**	7264.2	96.6 (<.01)
	6	**-3281**	54	6872.2	6926.2	7343.6	36.9 (<.01)
Class-varying, diagonal Σ_k	1	-4259	14	8598.2	8612.2	8718.9	---
	2	---	---	---	---	---	---
Class-invariant, unrestricted Σ_k	1	-3477	35	7154.8	7189.8	7459.5	---
	2	-3442	43	7132.6	7175.6	7507.6	68.4 (<.01)
	3	-3311	51	6915.0	6966.0	**7360.1**	263.7 (<.01)
	4	-3278	59	6895.7	6954.7	7410.8	65.4 (<.01)
	5	-3210	67	**6806.5**	**6873.5**	7391.7	135.3 (<.01)
	6	**-3197**	75	6826.9	6901.9	7482.3	25.7 (<.01)
Class-varying, unrestricted Σ_k	1	-3477	35	7154.8	7189.8	7459.5	---
	2	---	---	---	---	---	---

Table 4: Fit Statistics of Candidate Models for Cybersecurity Behaviors

Σ_k	# of classes, *k*	*LL*	npar	BIC	CAIC	AWE	BLRT, (*p*)
Class-invariant Σ_k	1	-3925	14	7930.2	7944.2	8050.9	---
	2	-3693	22	7512.6	7534.6	7703.7	463.8 (<.01)
	3	-3600	30	7373.7	7403.7	7634.9	185.0 (<.01)
	4	-3514	38	7247.7	7285.7	**7578.9**	172.1 (<.01)
	5	-3467	46	**7198.7**	**7244.7**	7600.0	**95.1 (<.01)**
	6	**-3461**	54	7232.3	7286.3	7703.9	12.5 (.34)
Class-varying, diagonal Σ_k	1	-3925	14	7930.2	7944.2	8050.9	---
	2	**-3571**	29	**7309.5**	**7338.5**	**7561.8**	707.2 (<.01)
	3	---	---	---	---	---	---
Class-invariant, unrestricted Σ_k	1	-3540	35	7280.9	7315.9	7585.5	---
	2	-3540	43	7327.5	7370.5	7703.9	-0.48 (>.99)
	3	-3455	51	7202.9	7253.9	**7648.0**	**170.7 (<.01)**
	4	-3455	59	7249.0	7308.0	7764.5	-0.03 (>.99)
	5	-3411	67	7207.6	7274.6	7793.1	87.5 (<.01)
	6	-3370	75	**7173.0**	**7248.0**	7828.4	80.7 (<.01)
Class-varying, unrestricted Σ_k	1	-3540	35	7280.9	7315.9	7585.5	---
	2	**-3303**	50	**7014.7**	**7085.7**	**6747.6**	473.6 (<.01)
	3	---	---	---	---	---	---

Table 5: Descriptive Statistics and Correlations Among Key Study Variables

	M(SD)	1	2	3	4	5	6	7	8	9	10	11	12	13
1.Age	41.8(*10.9*)	--												
2.Sex	42% Female	.08	--											
3.Income	~58k(*15k*)	.02	-.02	--										
4.Hours	39.6(*8.3*)	.09	-.01	.13*	--									
5.HonHu	3.26(*.73*)	.28**	.08	.11	.05	**.76**								
6.Emot	3.12(*.63*)	-.05	.33**	-.04	-.01	-.21**	**.73**							
7.Xtra	3.27(*.64*)	.03	.01	.12*	.01	.16**	-.20**	**.71**						
8.Agree	3.26(*.64*)	.01	-.01	.11*	-.05	.43**	-.09	.50**	**.73**					
9.Cons	3.58(*.72*)	.21**	.08	.15**	.19**	.50**	-.02	.24**	.25**	**.80**				
10.Open	3.49(*.67*)	.09	-.04	.04	.13*	.28**	-.09	.28**	.22**	.46**	**.77**			
11.Mach	3.28(*.83*)	-.16**	-.06	-.11	-.09	-.66**	.12*	-.16**	-.38**	-.51**	-.31**	**.89**		
12.Narc	2.88(*.76*)	-.22**	-.10	.01	-.16**	-.45**	-.14*	.43**	-.07	-.39**	-.09	.52**	**.81**	
13.Psyco	2.56(*.92*)	-.16**	-.20**	-.19**	-.13*	-.61**	-.05	-.19**	-.46**	-.71**	-.40**	.71**	.52**	**.87**
14.Sad	2.41(*1.14*)	-.23**	-.15**	-.20**	-.15**	-.63**	-.02	-.16**	-.40**	-.74**	-.42**	.70**	.55**	.90**
15.BrnPF	3.51(*1.64*)	-.11*	.07	-.17**	-.13*	-.42**	.31**	-.36**	-.33**	-.41**	-.29**	.48**	.16**	.48**
16.BrnCW	3.11(*1.73*)	-.14*	.01	-.17**	-.17**	-.46**	.24**	-.32**	-.28**	-.56**	-.36**	.53**	.25**	.59**
17.BrnEE	3.10(*1.82*)	-.16**	-.10	-.22**	-.14*	-.45**	.08	-.31**	-.33**	-.58**	-.38**	.53**	.26**	.66**
18.PC-Org	7.28(*2.18*)	.08	-.03	-.05	.03	.19**	-.08	.32**	.34**	.11	.03	-.02	.07	-.08
19.pcTrst	2.51(*1.23*)	-.01	-.04	-.22**	-.14*	-.41**	.10	-.28**	-.33**	-.45**	-.22**	.49**	.22**	.56**
20.pcUnct	2.49(*1.25*)	-.03	-.02	-.19**	-.18**	-.40**	.12*	-.30**	-.32**	-.47**	-.20**	.47**	.22**	.54**
21.pcEros	2.55(*1.24*)	-.05	.03	-.21**	-.16*	-.41**	.13*	-.22**	-.30**	-.40**	-.17**	.43**	.24**	.50**
22.PeerCy	5.07(*1.21*)	.06	.05	-.01	-.10	-.02	.23**	.20**	.30**	.03	.08	.14*	.12*	-.02

* = significant at α = .05; ** = significant at α = .01

Notes: N=318. Sex: 1=male, 2=female. HonHu=Honesty-Humility; Emot=Emotionality; Xtra=Extraversion; Agree=Agreeableness; Cons=Conscientiousness; Open=Openness to Experience. Mach=Machiavellianism; Narc=Narcissism; Psyco=Psychopathy; Sad=Sadism. BrnPF=Physical Fatigue [Burnout]; BrnCW=Cognitive Weariness [Burnout]; BrnEE=Emotional Exhaustion [Burnout]. PC-Org=Organization's fulfillment of psychological contract (higher score = more fulfillment). pcTrst=No Trust [Psychological Contract; higher score = more violation]; pcUnct=Uncertainty; pcEros=Erosion [Psychological Contract; higher score = more violation]. PeerCy=Peer Cybersecurity Behaviors.

Table 5 (continued): Descriptive Statistics and Correlations Among Key Study Variables

	14	15	16	17	18	19	20	21	22
14.Sad	**.94**								
15.BrnPF	$.48^{**}$	**.95**							
16.BrnCW	$.61^{**}$	$.87^{**}$	**.96**						
17.BrnEE	$.67^{**}$	$.76^{**}$	$.84^{**}$	**.93**					
18.PC-Org	-.07	$-.12^{*}$	-.01	-.06	**.88**				
19.pcTrst	$.57^{**}$	$.70^{**}$	$.67^{**}$	$.69^{**}$	$-.27^{**}$	**.93**			
20.pcUnct	$.55^{**}$	$.68^{**}$	$.66^{**}$	$.67^{**}$	$-.26^{**}$	$.89^{**}$	**.94**		
21.pcEros	$.53^{**}$	$.68^{**}$	$.65^{**}$	$.65^{**}$	$-.29^{**}$	$.82^{**}$	$.82^{**}$	**.91**	
22.PeerCy	.00	.02	.09	-.05	$.37^{**}$	-.04	-.06	-.03	**.84**

* = significant at α = .05; ** = significant at α = .01

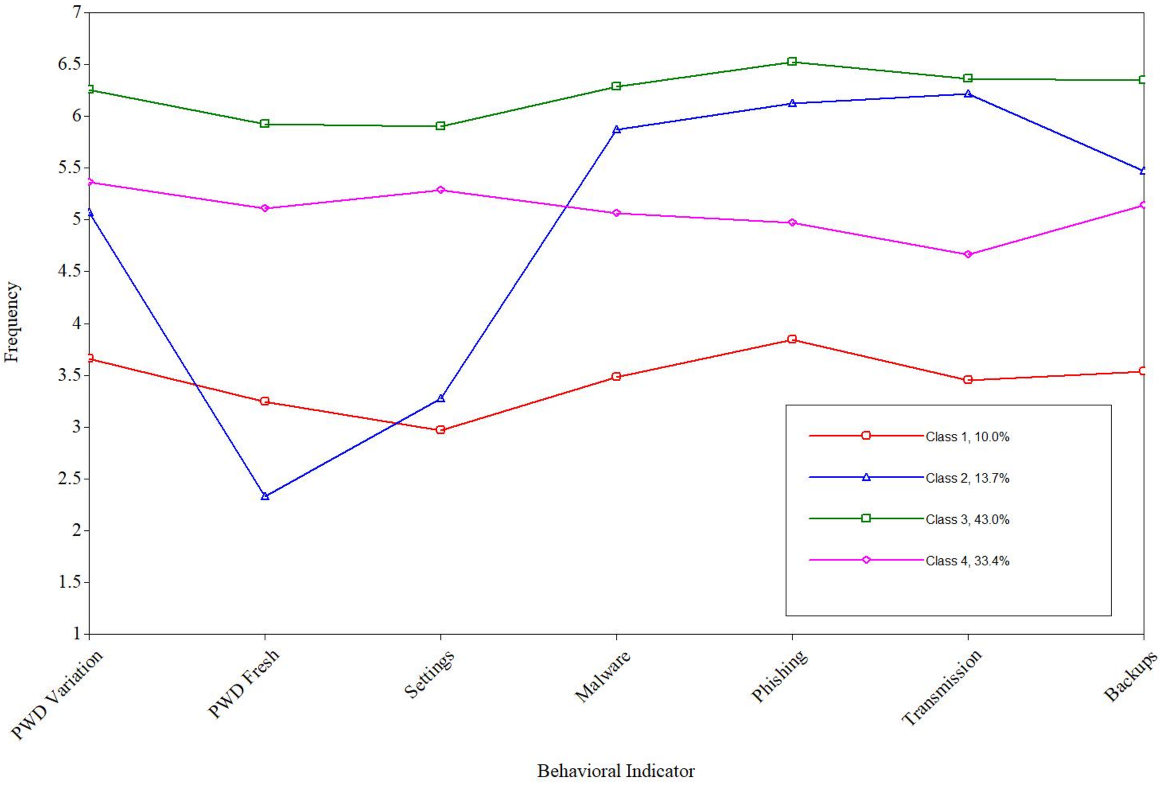
Notes: Sad=Sadism. BrnPF=Physical Fatigue [Burnout]; BrnCW=Cognitive Weariness [Burnout]; BrnEE=Emotional Exhaustion [Burnout]. PC-Org=Employer's fulfillment of psychological contract (higher score = more fulfillment). pcTrst=No Trust [Psychological Contract; higher score = more violation]; pcUnct=Uncertainty; pcEros=Erosion [Psychological Contract; higher score = more violation]. PeerCy=Peer Cybersecurity Behaviors.

Research Question 1

Fit statistics for candidate cybersecurity profile models are located in Table 4. When holistically considering the fit statistics, meaningfulness of membership, profile differentiation, and interpretability of candidate classes, the evidence suggests a 4-profile model wherein variances are constrained to equality across classes and covariances are fixed to zero. Class characteristics are displayed in Figure 1.

Profile 1. Representing the smallest profile in the solution with 10% of the sample, Class 1 is characterized by relatively low endorsement of all cybersecurity behaviors. Average levels of engagement in all behaviors remained close to the midpoint of the scale, indicating that while members of this class do not actively avoid these behaviors, they perform them with little frequency. Accordingly, members of this class are labeled as the Cyber Careless. Members of this class are differentiated from members of third and fourth classes by their comparatively worse password hygiene and disregard for security policies. Cyber Careless individuals differ from those in the second profile in that Careless respondents are much less attentive toward malware alerts, potential phishing attacks, safe transmission of sensitive information, and maintaining regular backups.

Figure 1: Final 4-Class Solution for Cybersecurity Behaviors



Profile 2. The second profile consisted of a slightly larger proportion of the overall sample with around 14% of respondents. Membership in this profile is characterized by inconsistent cybersecurity behaviors, earning this profile the label of Cyber Chaotic. These individuals utilize many unique passwords for their various accounts, yet do not change them regularly, and do not make a habit of checking the security policy of the online platforms they use—thus differentiating members from those in the third and fourth classes. However, Cyber Chaotics display extremely high awareness toward malware, routinely scrutinize potential

phishing links, and utilize secure transmission for sensitive information—behaviors that distinguish them from the Cyber Careless.

Profile 3. Class three proved to be the largest profile, consisting of 43% of the total sample. This profile's membership is typified by frequent performance of all seven cybersecurity behaviors, terming this profile the Cyber Champions. Cyber Champions differ from the Cyber Careless and Chaotic primarily due to their higher degree of password hygiene, though Cyber Chaotics are similarly concerned with scrutinizing emails/URLs and secure transmission of information. Cyber Champions differ from members of the fourth profile in their extremity of cybersecurity behaviors; these individuals also perform backups with the most regularity.

Profile 4. Members of the final profile—consisting of 33% of the sample—displayed a similar pattern of behavior as the Cyber Champions, but to a lesser degree. Accordingly, this profile was labeled as the Cyber Cautious. Members of this profile differ from the Champions in their lower endorsement of all cybersecurity behaviors but demonstrate higher frequency of behaviors than members in the Careless profile. Cyber Cautious members update their passwords more frequently and are more aware of their security settings than the Cyber Chaotics, but are less vigilant about secure transmission or monitoring the authenticity of links/emails. As such, the Cyber Cautious represent individuals who adhere to standard cybersecurity recommendations, but with a lesser degree of rigor.

Research Question 2A/B

Table 6 contains the results for all cybersecurity profiles covariate analyses. In order to answer Research Question 2A, HEXACO and Dark Tetrad personality traits were examined in relation to the selected profile solution. For these analyses, the high-security Champions class was selected as a reference class—therefore, the association of each covariate with the final profiles was examined in comparison to members of the Champion profile. This profile was selected in accordance with Blanton & Christie's (2003) assertion that studying deviance may prove more informative than examining compliance.

Table 6: Covariate Results for Cybersecurity Profiles

Variable	Profile			
	Careless	Chaotic	Champions	Cautious
HEXACO	B_E= -1.09(.39)** B_A= -1.69(.57)** B_C= -2.65(.86)**	B_X= -0.96(.48)* B_O= -0.79(.33)*	*Reference Class*	B_X= 2.64(1.2)* B_C= -3.49(1.3)**
Dark Tetrad	B_M= -1.43(.68)* B_S= 1.56(.63)*	B_{Tetrad}= *NS*	*Reference Class*	B_S= 1.34(.57)**
Burnout	B_{Tot}= -0.33(.13)*	B_{Tot}= -0.55(.13)**	B_{Tot}= -0.46(.17)**	*Reference Class – Total*
	B_{PF}= -0.62(.20)** B_{CW}= 0.75(.25)** B_{EE}= 0.32(.16)*	B_{EE}= 0.59(.21)**	*Reference Class - Facet*	B_{Facet}=*NS*
Psychological Contract	B_{Tot}= *NS* B_U= 0.97(.41)* B_{OrgFul}= -0.29(.13)*	B_{Tot}= -0.14(.07)* B_{Facet}= *NS* B_{OrgFul}= *NS*	*Reference Class*	B_{Tot}= 0.14(.05)** B_{Facet}= *NS* B_{OrgFul}= *NS*
Other	B_{Age}= -0.07(.03)** B_{Gender}= *NS* B_{IT}= -0.14(.07)* B_{Peer}= -1.25(.25)* *Reference Class - WFH*	B_{Age}= *NS* B_{Gender}= *NS* B_{IT}= *NS* B_{Peer}= -0.46(.22)* B_{WFH}= -1.63(.77)*	*Reference Class – all but WFH* B_{WFH}= *NS*	B_{Age}= -0.05(.02)* B_{Gender}= -0.70(.32)* B_{IT}= 0.70(.33)* B_{Peer}= -0.56(.17)** B_{WFH}= 25.5(.72)**
	——————— No effects for Tenure, Income ———————			

Notes: *NS* = not significant; * = significant at alpha = .05; ** = significant at alpha=.01

Compared to individuals with the highest levels of cybersecurity behaviors, members of the Careless profile possessed significantly lower levels of Emotionality, Agreeableness, and Conscientiousness, while lower levels of Extraversion and Openness were associated with membership in the Chaotic profile of cyberbehaviors. Cautious individuals, in comparison, possessed higher levels of extraversion but lower levels of conscientiousness compared to their more secure counterparts. Of the Dark Tetrad, membership in the Cautious and Careless profiles was associated with significantly higher levels of Sadism than in the Champion reference class, while Careless individuals were characterized by lower levels of Machiavellianism.

Burnout was examined at both the facet and general levels using the Cautious profile as a reference class. In comparison to this profile, membership in all other classes was associated with decreased levels of total burnout. Members of the Cautious profile demonstrated no facet level differences in Physical Fatigue, Cognitive Weariness, or Emotional Exhaustion when compared against the Champion profile as a reference. Chaotic individuals, however, demonstrated slightly higher levels of Emotional Exhaustion, whereas members of the Chaotic profile demonstrated lower Physical Fatigue and higher Cognitive Weariness and Emotional Exhaustion.

The Champion profile was retained as a reference class for examinations into Psychological Contract variables. Employee's Psychological Contract levels were examined in terms of facet violations (Uncertainty, Lack of Trust, Erosion), total violations, and perceived organizational fulfillment of obligations. Compared to the Champion profile, membership in the Chaotic and Cautious profiles was associated with greater and fewer total violations, respectively. Total violations for members in the Carelss profile did not significantly differ from those of the Champions, though Careless members reported higher levels of Uncertainty and lower levels of perceived organizational fulfillment. This general fulfillment did not covary according to the Chaotic or Cautious cybersecurity behavioral profiles.

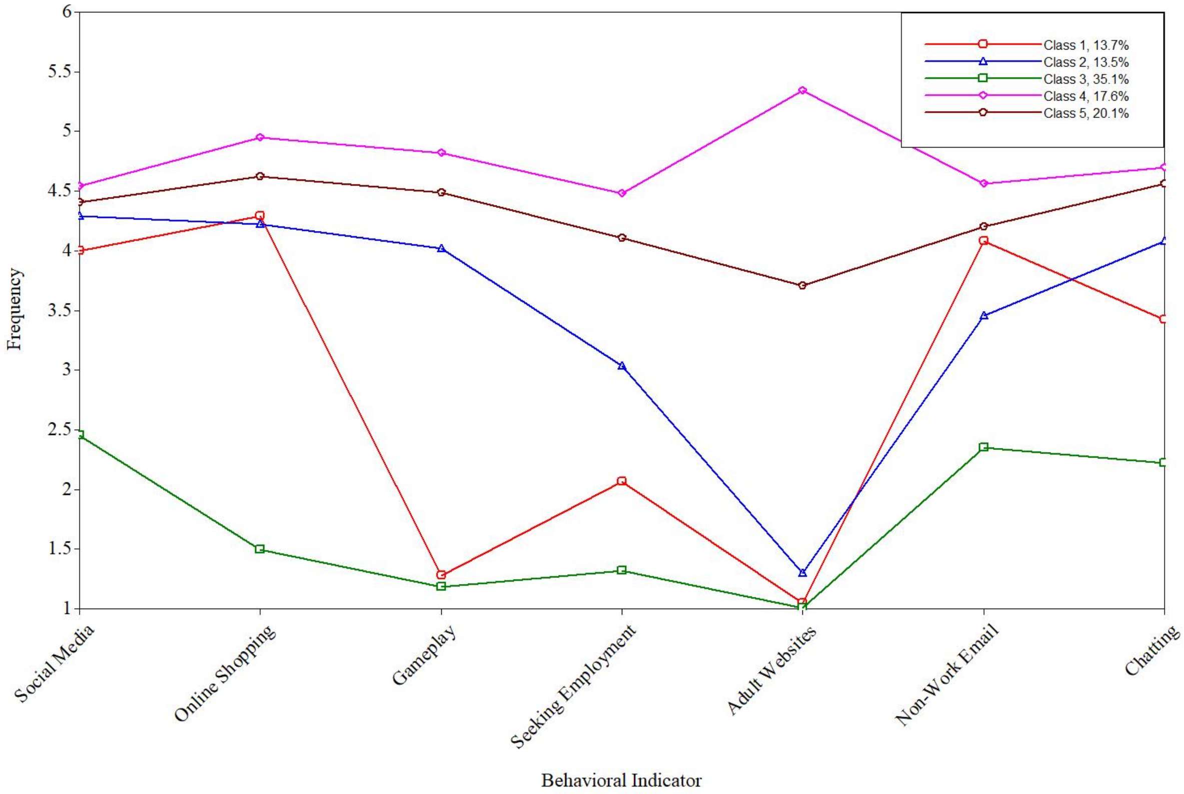
Additional variables such as age, gender, and peer cybersecurity behaviors were examined, again with Cyber Champions serving as a reference class. Working in the IT sector was positively associated with membership in the Cautious class, and negatively associated with membership in the Careless class. Both Careless and Cautious class membership significantly and negatively related to age—pointing to the Champion class as being slightly older. Gender effects were observed only insofar as being female was associated with a lower probability of membership within the Cautious class. All other classes reported lower levels of peer cybersecurity behaviors compared to members of the Champion profile. Finally, when compared to individuals in the Careless group, working from home negatively predicted membership in the Chaotic profile but positively predicted membership within the Cautious profile. No observed differences between the Careless and Champion groups were observed in work-from-home status.

Research Question 3

Statistics for candidate cyberloafing profiles may be found in Table 3. Ultimately, fit statistics and interpretability of results supported a class-invariant and unrestricted parameterization wherein item variances were constrained across profiles and covariances estimated, but also constrained to equality. While this represents a less-parsimonious model specification, it is particularly appropriate given the high correlations between cyberloafing behavioral indicators (see Appendix A). Within this model, a five-class solution presented the best combination of appropriateness of fit, profile interpretability, and distinction between classes. Figure 2 displays the characteristics and membership proportions of the final cyberloafing profiles.

Profile 1. Composing 14% of the sample, Class 1 was characterized by moderate frequency of social media use, online shopping, and checking/sending non-work email, but no gameplay of illicit website visiting. The occasional engagement in these behaviors earned members of this profile the label of Sometimes-Scrollers. Scrollers differed from members of Class 3 due to their more frequent use of social media and online shopping but differed from members of all other classes insofar as Scrollers did not report playing online or mobile games.

Figure 2: Final 5-Class Solution for Cyberloafing Behaviors



Profile 2. The second class also consisted of 14% of respondents. Membership in this class coincided with occasional social media use, shopping, gaming, and messaging friends or family, leading to the identification of this class as the Leisure Loafers. Leisure Loafers reported more frequent gaming and chatting than Sometimes-Scrollers or members of Class 3, but less frequent checking of email than the Scrollers. Membership in the Leisure Loafing profile differed from that of Classes 4 or 5 in that Leisure Loafers reported lower levels of gameplay, employment-seeking, explicit content viewership, and non-work email activities.

Profile 3. As the largest class with 35% of the sample, Class 3 demonstrated the lowest frequencies of all cyberloafing behaviors. As such, members in this profile are termed the Non-Loafers. Members of this class reported never playing games, seeking employment, or viewing explicit content, citing rare usage of social media, chat, and personal email.

Profile 4. Composed of 18% of respondents, Class 4 membership is characterized by the highest observed levels of all cyberloafing behaviors, with class means approaching or exceeding "very frequent" engagement in cyberslacking behaviors. Members in this class are differentiated from those in all other classes due to Class 4's reported rates of visiting adult (sexually-explicit) websites; this profile was accordingly labeled the Not Safe for Work (NSFW) Slackers.

Profile 5. With 20% of the sample, the final class resembled the NSFW Slackers in all indicators except viewership of adult content, to which respondents reported as viewing only "occasionally." This differentiates members from those of the NSFW slacking profile, but also from the Leisure, Scrolling, and Non-Loafing classes, who each reported "never" visiting such websites while on the job. As such, this profile was termed the Safe-ish for Work (SFW) Slackers to acknowledge the sporadic viewing of adult content.

Research Question 4A/B

Results from covariate analyses are located in Table 7. For examination of the personality covariates, the Non-Loafer profile was selected as the reference class. Compared to Non-Loafers, lower levels of Honesty-Humility significantly predicted membership in the Sometimes-Scroller, SFW Slacker, and NSFW Slacker profiles. Additionally, higher levels of Extraversion and lower levels of Conscientiousness were significantly associated with membership in the SFW/NSFW Slacking profiles. No significant associations between HEXACO traits and the Leisure Loafer profile were observed when utilizing Non-Loafers as a reference. Compared to Non-Loafers, SFW Slacker membership was significantly and positively associated with levels of Narcissism, Psychopathy, and Sadism. Sometimes-Scrollers demonstrated higher levels of Machiavellianism, while higher levels of Narcissism were associated with membership in the Leisure Loafer class. Finally, membership in the NSFW Slacker profile was positively associated with Sadism.

Only total burnout was examined across profiles, as facet-level results failed to converge upon a final solution. Leisure loafers were examined as the reference class, and displayed no significant differences from Sometimes-Scrollers. Comparatively, Non-Loafer membership was associated with lower levels of reported burnout symptoms. Both the NSFW and SFW slacker profiles were associated with higher levels of burnout.

NSFW Slackers were selected as the reference class for examining total psychological contract violations, reporting no significant differences from the SFW Slacker or Scroller profiles. Membership in both Leisure Loafer and Non-Loafer profiles corresponded to lower levels of total psychological contract violations. Facet-level analyses were conducted using the Non-Loafer profile as a reference. Only Uncertainty differentially predicted class membership, with positive associations for the Scroller and NSFW Slacker profiles. Employer psychological contract fulfillment remained unrelated to membership in any of the observed profiles.

Other covariate analyses indicated no effects for Peer Cybersecurity behaviors, gender, tenure, or income. When examining Non-Loafers as a reference, however, members of the Leisure, NSFW, and SFW profiles reported a higher incidence of working from home during the pandemic. Working from home did not significantly predict membership in the Scroller class when compared to Non-Loafing profile.

Table 7: Significant Covariate Results for Cyberloafing Profiles

Variable	Profile				
	Scrollers	Leisure Loafers	Non-Loafers	NSFW Slackers	SFW Slackers
HEXACO	B_{H}= -1.33(.64)*	B_{HEXACO}= *NS*	*Reference Class*	B_{H}= -2.67(.62)** B_{X}= 1.68(.77)* B_{C}= -3.76(.80)**	B_{H}= -1.73(.57)** B_{X}= 2.36(.63)** B_{C}= -3.67(.67)**
Dark Tetrad	B_{M}= 1.11(.41)**	B_{N}= 1.30(.48)**	*Reference Class*	B_{S}= 2.08(.70)**	B_{N}= 1.20(.42)** B_{P}= 1.85(.62)** B_{S}= 1.53(.52)**
Burnout	B_{Tot}= *NS*	*Reference Class*	B_{Tot}= -0.42(.13)**	B_{Tot}= 0.76(.18)**	B_{Tot}= 0.54(.14)**
Psychological Contract	B_{Tot}= *NS*	B_{Tot}= -0.41(.11)**	B_{Tot}= -0.73(.09)**	*Reference Class - Total*	B_{Tot}= *NS*
	B_{U}= 0.89(.40)*	B_{Facet}= *NS*	*Reference Class - Facet*	B_{U}= 0.69 (.34)*	B_{Facet}= *NS*
	———————— *No effects for Employer Psychological Contract Fulfillment*————————				
Other	B_{WFH}= *NS*	B_{WFH}= 26.2(.52)**	*Reference Class*	B_{WFH}= 36.3(.52)**	B_{WFH}= 26.2(.52)**
	———————— *No effects for Peer Cybersecurity Behaviors, Gender, Tenure, Income* ————————				

Note: *NS* = not significant; * = significant at alpha = .05; ** = significant at alpha=.01

Summary

Results pointed to the existence of four class-invariant latent profiles for cybersecurity behaviors: the Careless, Chaotic, Cautious, and Champions (RQ1). In response to RQ2a, differences in HEXACO and Dark Tetrad personality traits were observed between the Champion profile and all others. Differences in reported burnout symptoms and psychological contract fulfillment/violations were also identified and described (RQ2b). For cyberloafing behaviors, evidence supported the adoption of a 5-profile solution with a class-invariant and unrestricted parameterization (RQ3). Membership in the Non-Loafers, Sometimes-Scrollers, Leisure Loafers, Safe-ish for Work Slackers, and Not Safe for Work Slackers was examined in relation to HEXACO and Dark Tetrad traits (RQ4a). Significant associations with Burnout and Psychological Contract violations were also observed (RQ4b).

Discussion

The current study aimed to identify and describe underlying latent profiles of cybersecurity and cyberloafing behaviors. Through the association of personality traits and contextual employment factors with the observed behavioral profiles, the current study provides evidence for the need to adopt a more nuanced approach toward deterring insider cyberdeviant behavior and encouraging good cybersecurity habits. In particular, covariate relationships with cybersecurity and cyberloafing profiles highlight the complex relationships between employee characteristics, contextual factors, and cybersecurity behaviors.

As outline in the section above, the current investigation overturned a number of significant relationships between the study variables. Overall, respondents reported higher levels of cybersecurity behaviors than anticipated. Such a discovery bodes well for organizations and

MIS professionals alike, though replication of this study across multiple organizational levels would invoke greater confidence in the cybersecurity habits of employees observed here. Rates of membership in cyberloafing profiles resembled the 60% base rate presented in previous research (e.g., Ethics Resource Center, 2012), corroborating evidence for the widespread nature of these behaviors.

The strong correlations between each of the four Dark Tetrad traits initially led to doubt as to whether the constructs differed in any practical regard. In particular, the relationship between sadism and psychopathy (*r*= 0.90, *p*<.01) approached that of a perfect correlation, demonstrating the strongest relationship within the entire study. However, levels of sadism and psychopathy differentially predicted class membership across both cybersecurity and cyberloafing profiles, thus demonstrating some degree of empirical separation. It may be the case that the current sample consisted of individuals particularly high in multiple Dark traits, thus leading to the strong correlations observed herein. Alternatively, the predictive advantage of utilizing the Dark Tetrad over the Dark Triad may be overstated, if psychopathy and sadism are truly collinear.

Interestingly, individuals high in any of the Dark Tetrad also tended to possess higher levels of cognitive weariness, emotional exhaustion, or physical fatigue. These relationships between the Dark Tetrad and facets of burnout ranged from *r*=.16 to *r*=.67, with most of the bivariate correlations reaching the threshold for a strong effect size. Such associations are not entirely unprecedented, but the true relationship between the more popular Dark Triad traits and burnout remains confounded. One recent research study found moderate and high levels of narcissism to serve as a buffering effect between emotional labor and the experience of burnout

(Busuioc & Butucescu, 2020), while Prusik and Szulawski found Machiavellianism and psychopathy positively related to the burnout facets of disengagement and exhaustion (2019).

Still, the strength of the relationships observed within the current study remains unique. Though the present study cannot make any decisive claims as to the nature or origin of these relationships, the author wonders if individuals with Dark personality traits—typically viewed unfavorably by others—experience stronger burnout symptoms due to a lack of social resources. The negative correlations between extraversion and Machiavellianism, psychopathy, and sadism initially align with this supposition, but the moderate and positive correlation between extraversion and narcissism suggests otherwise. Future exploration into the intersection of these topics may prove illuminating.

Cybersecurity Behaviors

In order to address academic rhetoric about the presence of insider "types" within organizations, the current study investigated the existence of underlying profiles of employee cybersecurity behaviors. Among the observed behaviors, statistical and substantive evidence supported the existence of four classes of cybersecurity behavioral types. Reassuringly, good cybersecurity habits appeared to be the norm: membership in the least secure Careless class ranked the lowest, with only 10% of the total sample classified within the profile. Each of the other profiles reported extremely high levels of cybersecurity adherence (Champions), middling but consistent cyberbehaviors (Cautious), or a slight mix of poor and excellent security performance (Chaotic).

The high frequencies of reported cybersecurity behaviors should not be entirely attributed to the large proportion of IT specialists within the sample. Though employment within the IT sector was associated with decreased membership in the Careless class compared to the

Champion class, such employment was *positively* associated with membership in the Cautious profile. Therefore, while the IT specialists tended to report frequently engaging in good cybersecurity behaviors, they did not perform these behaviors at the highest observed rates within the sample. Rather, the most stringent cybersecurity adherence was observed among individuals who were more likely to be older, female, more conscientious, less burnt out, and less sadistic than those in the IT-dense Cautious class.

Members of the Champion profile seemed no more or less likely to work from home compared to Careless individuals, suggesting that desired cybersecurity behaviors cannot be cultivated simply through physical proximity. These employee behaviors may therefore be less likely to change based on an employee working within an office or home environment. Rather, membership in this Champion class coincided with higher peer cybersecurity behaviors than those of all other classes. The fact that profile members with the highest reported levels of cybersecurity behaviors perceived their peers as similarly diligent in their security efforts potentially supports the influence of an overarching cybersecurity culture within an organization.

This lies in seeming contrast with the suggestions of Protection Motivation Theory as applied by Li and colleagues, who concluded that an employee's appraisal of their organization as vulnerable to cyberattacks (such as due to the poor ISP adherence of one's coworkers) would result in increased motivation to perform good cybersecurity hygiene themselves (2017). Instead, peer cybersecurity behaviors appear to coincide with cybersecurity behavioral profiles, with Careless class membership related to lower levels of peer cybersecurity behaviors than all other classes when used as a reference. When referenced against each other, Cautious and Chaotic profiles demonstrated no significant differences in peer cybersecurity behaviors.

Of the four observed profiles, three appeared to stratify across general levels of cybersecurity behavioral performance. That is, the Careless, Cautious, and Champion profiles represented comparatively low, medium, and high adherence to recommended security behaviors, respectively. However, the final class of cyber Chaotic individuals displayed a unique pattern of cyberbehaviors, with individuals simultaneously displaying poor password hygiene but excellent skepticism and awareness toward potential phishing or malware attacks. Individuals in this Chaotic class represented the most unique insider "type," and were less extraverted and less open to experience than Champions, with fewer experienced psychological contract violations. These individuals also reported fewer peer cybersecurity behaviors than members of the Champion profile, but were less likely to work from home than their Careless counterparts.

Members of the Careless profile perceived lower employer fulfillment of obligations in comparison to those in the Champion profile, mirroring the relationship between organizational fulfillment and cybersecurity behaviors reported by Han and colleagues (2017). This connection between a lack of overall psychological contract fulfillment and fewer performed cybersecurity behaviors seems to coincide with the previously proposed metaphor of the ledger (Han et al., 2017). That is, employees who perceive their organization as failing to uphold their obligations may feel less beholden to compliance with requested cybersecurity behaviors. This may indicate that some employees view cybersecurity hygiene as an extra-role behavior to be performed as a favor to the organization. While individuals in the moderate-security Cautious class did not report significantly different perceptions of employer contractual fulfillment than their high-security Champion counterparts, Cautious membership was related to higher total levels of contract violations. In conjunction, these results support the conceptualization of cybersecurity behaviors within the psychological contract.

Cautious individuals also displayed a pattern of medium-to-high performance on all cybersecurity behaviors, with higher burnout in comparison to every other profile. The fact that both high levels of burnout and a high probability of working within the Information Technology domain coincide with membership in the Cautious profile provides initial empirical evidence for the existence of cybersecurity fatigue, albeit in a different manifestation than originally proposed. While researchers first presented information security fatigue as a consequence of attempting to balance job demands with recommended cybersecurity practices (Cram et al., 2020), the current study points to individuals with security or security-adjacent occupations as susceptible to a similar type of fatigue. Given that Cautious members also report lower levels of peer cybersecurity behaviors than those in the Champion profile, it may be the case that some degree of their burnout originates from exhaustion with attempting to enforce recommended cybersecurity behaviors. Future research would be appropriate to further examine whether these factors coincide with the qualitative descriptions of cybersecurity fatigue described by Cram and colleagues (2020).

At the most basic level, implications of cybersecurity profiles point to the need to impose technological constraints on password age, as cyber Chaotics otherwise appear actively opposed to updating their login credentials. Otherwise, the current results provide evidence that no singular theory truly encapsulates the entire picture of employee cybersecurity behavior. Behavioral types coincide with different levels of personality, confounding efforts to apply a "one size fits all" solution to the problem of insider cyberdeviance.

Though unexpected, the picture painted of individuals in the moderately-secure Cautious profile is concerning. Cautious individuals appeared to report the worst contextual experiences: all other profiles reported lower total levels of burnout, and Cautious class membership positively related to higher levels of total psychological contract violations. The association between membership in this class and occupation within the Information Technology sector begs the question: *are the geeks okay?* These individuals are also the most likely to work from home, which may deprive these employees from the social support a workplace may otherwise offer. This is a potentially poor combination, given that high extraversion is associated with membership in this Cautious profile.

As mentioned, lower comparative levels of psychological contract fulfillment within the Careless class (compared to the Champion class) do seem to align with the metaphor of the ledger proposed by psychological contract theories. That is, individuals who feel their organization is fulfilling fewer of its promises are also the most likely to display lower engagement in recommended cybersecurity behaviors. Attempts to cultivate strong cybersecurity habits within an organization may therefore be wasted if the organization has not inspired a sense of trust, certainty, or security in its employees. These results further highlight the fact that cybersecurity cannot be bought when employee behavior is in question.

The observed covariate relationships between cybersecurity profiles and contextual factors of psychological contract fulfillment and burnout suggest that the typical approach to encouraging good cybersecurity habits may be misguided. Whereas employee failure to adhere to cybersecurity recommendations tend to be conceptualized as ignorance—with attempts to reduce the “weakest link” in security consisting largely of Security Education, Training, and Awareness interventions—the distribution of cyberbehaviors along the current profiles suggests otherwise. Indeed, the high proportion of IT professionals within the moderate-security, largely burnt-out Cautious class implies that some degree of fatigue or organizational disillusionment may prevent these individuals from higher performance of cybersecurity behaviors, as one would hope that IT education within the United States would not be completely deprived of basic Information Security training. More targeted research on this topic is clearly warranted.

Ultimately, the current results suggest consideration of a typology of insider behaviors aligned with convenience of cybersecurity adherence—thus coinciding with conceptualizations of misbehavior rather than deviance. The most unique pattern of employee cybersecurity behaviors was observed in the Chaotic profile, wherein individuals maintained unique passwords for all of their different accounts yet refused to change those passwords in a regular fashion. This behavioral pattern appears to reflect an attempted balance between convenience and security, with members unwilling to continuously re-learn new passwords. Beyond drawing attention to the importance of the psychological contract and IT burnout, no other cybersecurity profiles pointed to any particular insider typology.

Cyberloafing

Variation observed in the cyberloafing profiles support its conceptual and empirical distinction from other forms of computer-related deviance. This is emphasized in the fact that no significant associations between peer cybersecurity behaviors and cyberloafing profile membership were observed. Five distinct profiles of employee Personal Web Use were observed, each with unique defining characteristics. Covariate analyses also identified differences in profile associations with personality and contextual variables. In contrast to the occupational, gender, and age effects observed between certain cybersecurity profiles, none of the examined demographic variables differentially predicted membership in any cyberloafing class—a finding which emphasizes the universal nature of cyberloafing in the workplace.

However, the apparent universality of cyberloafing should not be mistaken for frequency of engagement: while employees of *every background* engage in personal web use, cyberloafing behaviors are not witnessed in *every employee*. Indeed, membership of the lowest-frequency Non-Loafer class consisted of 35% of the total sample—by far representing the largest profile of the observed classes. These individuals reported never or very rarely performing the selected cyberloafing behaviors, and also possessed the lowest levels of burnout of all profiles. Membership in the Non-Loafer class also was associated with fewer reported psychological contract violations than experienced by those in the more severe loafing profiles (SFW and NSFW Slackers).

The two smallest classes—Sometimes-Scrollers and Leisure Loafers—each consisted of about 14% of the total sample, still representing a significant portion of responses (Pastor et al., 2007). These profiles demonstrated the most unique behavioral patterns, with both Scrollers and Leisure Loafers frequently browsing social media, shopping online, and checking non-work email. Leisure class members spent more time playing online or mobile games. The behaviors and frequencies of the Scroller profile align with previous conceptualizations of Personal Web Use as a means of taking a break (Kim & Byrne, 2011; Mastrangelo et al., 2006). These individuals engage in the mildest levels of cyberloafing, but members did possess lower levels of Honesty-Humility and higher levels of Machiavellianism than Non-Loafers.

Even with potentially benign nature of cyberloafing observed in the Scroller profile, the current study does not intend to suggest that positive conceptualizations of cyberslacking be adopted. To the contrary: given that the three other profiles (composing 52% of the sample) display higher rates of more severe, security-risking loafing behaviors, the perspectives of loafing as more detrimental to an organization are preferred. In particular, the high rates of explicit website viewership among the NSFW/SFW Slacker profiles draws concerns about organizational security, given that these websites tend to be ridden with malware and may leave the organization vulnerable to cyberattack (Chen et al., 2008).

Class membership in these two cyberslacking-heavy classes was much higher than expected at a combined 38% of the total sample. The profile characteristics of personal web use in in the SFW and NSFW both resemble the problematic category of cyberloafing as presented in Kim and Byrne's taxonomy (2011). In particular, the NSFW class's extremely high frequency of explicit content viewership seems to adhere to descriptions of Internet Abuse or Internet Addiction Disorder (Kim & Byrne, 2011), though the current study does not presume to imply any psychological diagnosis. In comparison to the Non-Loafer profile, the higher levels of Narcissism, psychopathy, and sadism observed in Safe-ish for Work Slackers are interestingly not mirrored in the more-extreme NSFW Slacker profile. Rather, NSFW slacker membership was associated only with higher levels of sadism, indicating no notable pattern other than Non-Loafers possessing generally lower levels of most Dark Tetrad traits.

Additional covariate analyses revealed that levels of total burnout corresponded neatly to the severity of cyberloafing witnessed in each profile. That is, members of the SFW and NSFW Slackers were associated with the highest levels of burnout compared to all other classes, while Leisure Loafers and Sometimes-Scrollers only demonstrated higher levels of burnout than Non-Loafers. Burnout levels thus appeared stratified according to the frequency and severity of cyberloafing in each profile, supporting the notion of cyberloafing as a means of dealing with stress experienced at work. However, a similar relationship was not observed with employer fulfillment of the psychological contract, which demonstrated no differences across profiles. When lack of trust, uncertainty, and erosion were considered, however, lower levels of total contract violations predicted Non-Loafer and Leisure Loafer class membership in comparison to the NSFW Slacker profile. Therefore, the conceptualization of cyberloafing as a means of "righting the ledger" in response to an organization inappropriately demanding time from workers is somewhat supported.

Results of the present study partially support Kim & Byrne's (2011) typology of cyberloafing behaviors, insofar as individuals in the high-loafing SFW and NSFW Slacker profiles coincide with the author's category of "Problematic" forms of personal web use. Additionally, Leisure Loafers and Sometimes-Scrollers warrant classification as the less-negative "Aimless PWU"—thus representing the more benign slacking typically associated with the concept of cyberloafing. Correspondence of these profiles to this previously-proposed taxonomy does not diminish the uniqueness of these behavioral profiles, however. Indeed, sufficient meaningfulness, distinction, and interpretability of profiles were found in support of the five-profile solution presented herein. Covariate relationships with the observed profiles initially suggest that personal web use might serve as a coping mechanism for employees experiencing high levels of burnout or psychological contract violations. Thus, attempts to decrease cyberloafing behaviors may prove more complicated than initially conceptualized.

The current study previously drew attention to the potential to consider the current work-from-home culture of many organizations initiated by the effects of the COVID-19 pandemic. Results of the covariate analysis aligned with expectations: in reference to Non-Loafers, membership in the Leisure, NSFW, and SFW profiles all corresponded with an increased likelihood of working from home. Considering that these three profiles represented the most frequent cyberloafers of the sample, this suggests that lessened supervision or proximity to coworkers may serve as an enabling factor for these more severe forms of computer-assisted slacking (Mercado et al., 2017; O'Neill et al., 2014).

While an organization might initially consider the implementation of monitoring software as a means of combating this work-from-home slacking, such a reaction has two flaws. Firstly, the cyberslacking behaviors in the current study were reported as being performed on either a tablet, computer, or mobile device during work hours. Therefore, it is not certain to what extent employees engage in cyberloafing on corporate-owned technology—an unknown that may slightly reduce potential security issues, if not concerns about productivity losses. Additionally, if employees are engaging in nonproductive technology use on their personal devices, then an organization's ability to install any sort of monitoring program or lockdown browser would be limited. This is, of course, assuming that an organization would opt to ignore the evidence pointing to monitoring as an inefficient and demoralizing action to take against employees (Mastrangelo et al., 2006; Stanton & Lin, 2001). As such, further research is necessary prior to the establishment of any practical advice for mitigating cyberloafing.

Implications

The current study represents the first examination of cybersecurity and cyberloafing behaviors within the context of a person-centered latent class approach. Finding empirical support for the existence of underlying profiles, the current study identified characteristics and covariates of insider cybersecurity and cyberloafing "types." Such results legitimize previous articulations as to the need for distinction between insider behavioral patterns, laying an empirical foundation for future theoretical classification efforts.

Of the cybersecurity profiles, the characteristics of the Chaotic class possess the most meaningful implications for organizations. Due to the fact that this profile demonstrates significant awareness of hygienic cybersecurity habits—such as refusing to send sensitive information via insecure methods—these insiders seem to only neglect changing their password out of inconvenience. As such, implementing regular forced password changes at login would be likely to improve the security behaviors of this profile. No other complex patterns of behavior emerged from the cybersecurity profiles. However, results of the covariate analyses emphasize the need to support not only employees struggling to adhere to cybersecurity guidelines, but the professionals that are responsible for implementing them, as well.

Examinations into cyberloafing profiles illustrated more complex patterns of behavior, with results generally supporting Kim & Byrne's (2011) distinctions of PWU into aimless and problematic categories—though no particular profile seemed to coincide with their third category of "Strategic PWU." Covariate analyses suggested employees primarily engage in cyberloafing not a means of righting a wronged psychological contract, but as a means of coping, with cyberloafing frequencies covarying along with reported burnout levels. The association between cyberloafing and telecommuting also provides support for potential deterrence effects of an in-person mode of employment.

Also worth noting are the strong relationships between burnout facets and psychological contract transitions (referred to in the current study as contractual violations). Bivariate correlations between these variables approach collinearity, calling into question the true distinction between the scales. However, the differential association between these traits and both cybersecurity and cyberloafing profile membership points to some distinction between these concepts. Overall, the current study results suggest that the symptoms of burnout and the experience of psychological contract violations are intertwined to some degree, emphasizing the continued need for I-O researchers to consider the psychological contract in organizational research.

Limitations and Future Directions

Profiles of cyberloafing behavior were described in such a way as to suggest negative connotations for membership in profiles with higher frequency and severity of PWU. However, the true impact of profile membership on work outcomes remains unclear. Incorporating a measure of organizational performance may capture broad effects of greater cyberslacking on quality of job performance. Directly measuring the time spent completing various activities is necessary to provide a more direct estimate of productivity losses. Inclusion of additional direct quantitative measures would therefore enhance the precision of analyses and provide a more specific understanding of the cyberloafing profiles. However, with the aforementioned negative employee reactions to monitoring, such data would be difficult to capture without either deception or the potential for altered behavior. Previous research ultimately points to habitual cyberloafing as strongly correlated with observed PWU behaviors (Mercado et al., 2017), thereby supporting the trustworthiness of the current results.

Considering participant demographics, the current sample is largely white, educated, and employed. Incorporating more ethnically or occupationally diverse may improve confidence in the generalizability of results. In particular, consideration of individuals in part-time positions may reveal different patterns of cyberloafing. However, participation in the current study was limited to respondents engaged in full-time employment in order to capture the largest among of cybersecurity and cyberloafing behaviors. Indeed, more time spent on the job automatically corresponds to more *potential* time for cyberloafing. Given the significant results at the level of full-time employment, however, additional examination into other work structures may be warranted.

Specific multilevel examination of cybersecurity and cyberloafing behaviors within multiple departments of a single organization may prove illuminating. As evidenced by the current sample, MTurk workers tend to be fairly well-versed in appropriate cybersecurity behaviors and must possess a modicum of technological ability simply to utilize the MTurk platform. Employees in any given organization may not equally possess such expertise or technological familiarity. While the covariation of peer cybersecurity behaviors with high-security Champion profile membership seems to support that cybersecurity habits are shared to some degree between coworkers, it remains unclear as to what level this positive security contagion occurs. Is it at the organizational level, or confined solely to a single department? Future research into this topic may enhance the effectiveness of security interventions by informing the ideal scope for transmitting an organizational cybersecurity culture.

Finally, the analytic evidence cited during cybersecurity class enumeration proved relatively weaker than would be desired, potentially due to the comparatively smaller size of the final sample (N=318). However, guidelines outlined by Ferguson and colleagues (2020) identify this sample size as within the range of acceptable size, and enumeration was conducted according to the widely-cited recommendations of Pastor et al., (2007) to consider a holistic interpretation of profile results. Though lower membership in the profile with the most unique cybersecurity behavioral pattern questions the practical significance of distinguishing between the cybersecurity profiles described within the study, but membership levels in the Chaotic profile exceeded the 10% threshold for meaningfulness. Its inclusion within the final profile solution illustrates a relatable pattern of behavior with specific, actionable steps for organizations. Therefore, the current study remains confident in the appropriateness and meaningfulness of this profile.

Summary

The current study supports the need to consider the nuances of cybersecurity and cyberloafing behaviors. Not all employees are equally adherent to recommended cybersecurity behaviors, and not all forms of personal web use manifest similarly. The identified patterns of typical cybersecurity behaviors suggest that while many employees adhere to recommendations in a general fashion, a small portion of insiders do behave in a more chaotic way—emphasizing the need for technological controls of password changes. Additionally, the associations between levels of burnout and psychological contract fulfillment with cybersecurity profiles hints at deeper issues with cybersecurity adherence than simply a lack of security policy awareness. Within the observed classes of cyberloafing behaviors, stratification of burnout levels along lines of slacking severity and frequency implies similar nuances with regards to engagement in PWU as a potential coping mechanism. On the whole, evidence aligns with pre-existing classifications of cyberloafing behavior.

Conclusion

Information Security assurance remains a balancing act between technological and interpersonal factors. Previous sections in this study outlined decades of research surrounding the dire state of organizational cybersecurity, the role of insiders, and the undeniable fact that employee behavior must be understood and properly factored into a security plan. The natural overlap between cybersecurity and I-O Psychology is reflected in the current study, which heeds the call of Dalal and colleagues for more interdisciplinary research at this intersection (2021).

Cybersecurity research has historically been typified by the clash of competing theoretical approaches with concerns as to the appropriate typology of insider behaviors. The current study contributes to this research by laying an empirical foundation for a taxonomy of computer-related behaviors based upon actual reported patterns. Additionally, several avenues for future investigation into the nuances of cybersecurity, cyberloafing, and employee experiences of burnout and psychological contract fulfillment are highlighted. Though the observed cybersecurity profiles may be addressed primarily through forced password changes, the aimless and problematic patterns of Personal Web Use truly represent a problem of the disobedient and the deviant. Future investigations into these behaviors would be well-suited to consider such distinctions.

References

Abouzakhar, N. (2013). Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations. *Proceedings of the 12th European Conference on Information Warfare and Security,* 1-10.

Ajzen, I. (2005). *Attitudes, personality, and behavior*. McGraw-Hill Education (UK).

Akers, R. L. (1990). Rational choice, deterrence, and social learning theory in criminology: The path not taken. *J. Crim. L. & Criminology*, *81*, 653.

Anandarajan, M., Devine, P., & Simmers, C. A. (2004). A Multidimensional Sealing Approach to Personal Web Usage in the Workplace. In *Personal web usage in the workplace: A guide to effective human resources management* (pp. 61-79). IGI Global.

Anderson, B. B., Jenkins, J. L., Vance, A., Kirwan, C. B., & Eargle, D. (2016). Your memory is working against you: How eye tracking and memory explain habituation to security warnings. *Decision Support Systems, 92*, 3–13.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437-443.

Ash, R. A., Rosenbloom, J. L., Coder, L., & Dupont, B. (2006). Personality characteristics of established IT professionals I: Big Five personality characteristics. In *Encyclopedia of gender and information technology* (pp. 983-989). IGI Global.

Austin, J. T., & Villanova, P. (1992). The criterion problem: 1917–1992. *Journal of Applied Psychology*, *77*(6), 836.

Baker, W., Goudie, M., Hutton, A., Hylender, C., Niemantsverdriet, J., Novak, C., et al. (2010) Verizon 2010 data breach investigations report. Retrieved from:

https://www.wired.com/images_blogs/threatlevel/2010/07/2010-Verizon-Data-Breach-Investigations-Report.pdf

Bartunek, J. M., & Woodman, R. W. (2015). Beyond Lewin: Toward a Temporal Approximation of Organization Development and Change. *Annual Review of Organizational Psychology and Organizational Behavior*, *2*(1), 157-182.

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, *65*, 153-165.

Baumeister, R. F. (2002a). Ego depletion and self-control failure: An energy model of the self's executive function. Self and Identity, 1(2), 129–136.

Berkowitz, L. (1993). *Aggression: Its causes, consequences, and control*. Mcgraw-Hill Book Company.

Blanchard, A. L., & Henle, C. A. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in human behavior*, *24*(3), 1067-1084.

Blanton, H., & Christie, C. (2003). Deviance regulation: A theory of action and identity. *Review of General Psychology*, *7*(2), 115-149

Bollen, K. A. (2002). Latent variables in psychology and the social sciences. *Annual review of psychology*, *53*(1), 605-634.

Brewster T (2018) This guy hacked hundreds of planes from the ground. Forbes (August 9), https://www.forbes.com/sites/thomasbrewster/2018/08/09/this-guy-hacked-hundreds-of-planes-from-the-ground/#21804f4946f2

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.

Busuioc, A., & Butucescu, A. (2020). The role of Dark Triad on the link between Emotional Labor and Core Burnout. *Psihologia Resurselor Umane*, *18*(1), 51-64.

Cappucci, M., & Freedman, A. (2020, July 16). *Twitter outage affected National Weather Service office during a tornado warning*. The Washington Post. https://www.washingtonpost.com/weather/2020/07/16/twitter-outage-affected-national-weather-service-office-during-tornado-warning/.

Casler, K., Bickel, L., & Hackett, E. (2013). Separate but equal? A comparison of participants and data gathered via Amazon’s MTurk, social media, and face-to-face behavioral testing. *Computers in human behavior*, *29*(6), 2156-2160.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70-104.

Chen, J. V., Chen, C. C., & Yang, H. H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *Industrial Management and Data Systems*, *108*(1), 87-106.

Choi, J., Kaplan, J., Krishnamurthy, C., & Lung, H. (2019). *Hit or myth? Understanding the true costs and impact of cybersecurity programs.* McKinsey. https://www.mckinsey.de/~/media/McKinsey/Industries/Public%20and%20Social%20Sector/Our%20Insights/Hit%20or%20myth%20Understanding%20the%20true%20costs%2

0and%20impact%20of%20cybersecurity%20programs/Hit-or-myth-Understanding-the-true-costs-and-impact-of-cybersecurity-programs.pdf

Clark, S. C. (2000). Work/family border theory: A new theory of work/family balance. *Human relations*, *53*(6), 747-770.

Couce-Vieira, A., Insua, D. R., & Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. *Decision Analysis*, *17*(4), 356-374.

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. *MIS Quarterly*, *43*(2), 525-554.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, *1-29.*

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.

Dalal, R. S. (2005). A meta-analysis of the relationship between organizational citizenship behavior and counterproductive work behavior. *Journal of applied psychology*, *90*(6), 1241-1255.

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: abundant opportunities for research at the interface. *Journal of Business and Psychology*, 1-29.

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.

Dinić, B. M., Sadiković, S., & Wertag, A. (2020). Factor Mixture Analysis of the Dark Triad and Dark Tetrad: Could Sadism Make a Difference? *Journal of Individual Differences*, *1*(1), 1-10.

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human behavior*, *68*, 359-367.

Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, *51*, 102056.

Ekran, (2020, November 18). *5 Real-life examples of breaches caused by insider threats*. Ekran System. https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches

Elhai, J. D., Contractor, A. A., Tamburrino, M., Fine, T. H., Prescott, M. R., Shirley, E., ... & Calabrese, J. R. (2012). The factor structure of major depression symptoms: a test of four competing models using the Patient Health Questionnaire-9. *Psychiatry Research*, *199*(3), 169-173.

Ethics Resource Center, (2012). *National business ethics survey of social networkers: New risks and opportunities at work*. Ethics Resource Center. https://s3.amazonaws.com/berkley-center/120101NationalBusinessEthicsSurveyFortune500Employees.pdf

Ferguson, S. L., G. Moore, E. W., & Hull, D. M. (2020). Finding latent groups in observed data: A primer on latent profile analysis in Mplus for applied researchers. *International Journal of Behavioral Development*, *44*(5), 458-468.

Fishbein, M. & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley.

Fox, A. (2007). Caught in the Web: Internet surfing takes on addictive qualities for some employees who may be hiding their abuse at work-at a cost to both themselves and their employers. *HR MAGAZINE*, *52*(12), 34.

Fruhlinger, J. (2020, February 12). *Equifax data breach FAQ: What happened, who was affected, what was the impact?* CSO Online. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

Greenwood, S., Perrin, A., & Duggan, M. (2016). Social media update 2016. *Pew Research Center*, *11*(2), 1-18.

Greitzer, F.L., Purl, J., Becker, D.E., Stitcha, P.J. and Leong, Y.M. (2019) Modeling expert judgments of insider threat using ontology structure: Effects of individual indicator threat value and class membership. In *Proceedings of the 52nd Hawaii Intern. Conf. System Sciences* (Maui, HI, USA), 3202–3211.

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.

Hadlington, L., & Murphy, K. (2018). Is media multitasking good for cybersecurity? Exploring the relationship between media multitasking and everyday cognitive failures on self-reported risky cybersecurity behaviors. *Cyberpsychology, Behavior, and Social Networking*, *21*(3), 168-172.

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, *66*, 52-65.

Henderson, A. A., Foster, G. C., Matthews, R. A., & Zickar, M. J. (2020). A psychometric assessment of OCB: Clarifying the distinction between OCB and CWB and developing a revised OCB measure. *Journal of Business and Psychology*, *35*(6), 697-712.

Hobfoll, S. E., Shirom, A., & Golembiewski, R. (2000). Conservation of resources theory. *Handbook of organizational behavior*, 57-81.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*, *52*(2), 1-40.

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.

Huma, Z., Hussain, S., Thurasamy, R., & Imran Malik, M. (2017). Determinants of cyberloafing: a comparative study of a public and private sector organization. *Emerald Insight*, *27*(1), 97–117.

Ifinedo, P., & Idemudia, E. C. (2017). Factors Influencing Employees' Participation in Non-Malicious, Information Systems Security Deviant Behavior: Focus on Formal Control Mechanisms and Sanctions.*Twenty-third Americas Conference on Information Systems,* Boston, MA.

Intel Security (2015). Grand Theft Data. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-data-exfiltration.pdf

Isidore, C., & Horowitz, J. (2018, June 20). *Elon Musk: Tesla worker admitted to sabotage*. CNNMoney. https://money.cnn.com/2018/06/19/technology/tesla-fire-musk-note/index.html.

Jenkins, J. L., Anderson, B. B., Vance, A., Kirwan, C. B., & Eargle, D. (2016). More harm than good? How messages that interrupt can make us vulnerable. *Information Systems Research, 27*(4), 880–896.

Johnson, H., Worthington, R., Gredecki, N., & Wilks-Riley, F. R. (2016). The relationship between trust in work colleagues, impact of boundary violations and burnout among staff within a forensic psychiatric service. *Journal of Forensic Practice*, *18*(1), 64-75.

Jones, D. N., & Paulhus, D. L. (2014). Introducing the short dark triad (SD3) a brief measure of dark personality traits. *Assessment*, *21*(1), 28-41.

Kemp, T. (2018, October 1). *Council Post: What Tesla's Spygate Teaches Us About Insider Threats*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2018/07/19/what-teslas-spygate-teaches-us-about-insider-threats/.

Kickul, J., & Lester, S. W. (2001). Broken promises: Equity sensitivity as a moderator between psychological contract breach and employee attitudes and behavior. *Journal of business and psychology*, *16*(2), 191-217.

Kim, S. J., & Byrne, S. (2011). Conceptualizing personal web usage in work contexts: A preliminary framework. *Computers in Human Behavior*, *27*(6), 2271-2283.

Kline, R. B. (2015). *Principles and practice of structural equation modeling*. Guilford publications.

Koay, K. Y. (2018). Assessing Cyberloafing Behaviour among University Students: A Validation of the Cyberloafing Scale. *Pertanika Journal of Social Sciences & Humanities*, *26*(1).

König, C. J., & De La Guardia, M. E. C. (2014). Exploring the positive side of personal internet use at work: Does it help in managing the border between work and nonwork?. *Computers in Human Behavior*, *30*, 355-360.

Kotter, J. P. (1973). The psychological contract: Managing the joining-up process. *California management review*, *15*(3), 91-99.

Leach, J. (2003). Improving user security behaviour. *Computers and Security, 22*(8), 685–692.

Lee, K., & Ashton, M. C. (2020). HEXACO Model of Personality. *The Wiley Encyclopedia of Personality and Individual Differences: Models and Theories*, 249-256.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24.

Lim, V. K., & Teo, T. S. (2005). Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. *Information & Management*, *42*(8), 1081-1093.

Lopatto, E. (2020, May 1). *Was Elon's Tesla Twitter meltdown illegal? An investigation*. The Verge. https://www.theverge.com/2020/5/1/21244747/elon-musk-tesla-tweets-shares-sec-settlement-stock.

Maasberg, M., Van Slyke, C., Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. *Communications of the ACM*, *63*(12), 64-80.

Mahatanankoon, P., Anandarajan, M. and Igbaria, M. (2004), "Development of a measure of personal web usage in the workplace," *CyberPsychology & Behavior, 7*(1), 93-104.

Mastrangelo, P. M., Everton, W., & Jolton, J. A. (2006). Personal use of work computers: Distraction versus destruction. *CyberPsychology & Behavior*, *9*(6), 730-741.

McBride, M., Carter, L., & Warkentin, M. (2012). The role of situational factors and personality on cybersecurity policy violation. *Institute for Homeland Security Solutions*.

Mercado, B. K., Giordano, C., & Dilchert, S. (2017). A meta-analytic investigation of cyberloafing Brittany K. Mercado, Casey Giordano, Stephan Dilchert. *Career Development International*, *22*(5), 546-564.

Moody, G. D., & Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information & Management*, *50*(6), 322-335.

Morgan, S. (2020, August 4). *Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021*. Cybercrime Magazine. https://cybersecurityventures.com/jobs/.

Morrison, E. W., & Robinson, S. L. (1997). When employees feel betrayed: A model of how psychological contract violation develops. *Academy of management Review*, *22*(1), 226-256.

Mueller, R. S. (2012, March 1). *Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies*. Federal Bureau of Investigation. https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

Muraven, M., & Baumeister, R. F. (2000). Self-regulation and depletion of limited resources: Does self-control resemble a muscle?. *Psychological bulletin*, *126*(2), 247.

Muthén, L. K., & Muthén, B. O. (1998-2021). Mplus User's Guide. Sixth Edition. Los Angeles, CA: Muthén & Muthén.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139.

Neumann, C. S., Jones, D. N., & Paulhus, D. L. (2021). Examining the Short Dark Tetrad (SD4) Across Models, Correlates, and Gender. *Assessment*. Advance Online Publication.

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. *Predicting Health Behaviour*, *81*, 126.

O'Neill, T. A., Hambley, L. A., & Bercovich, A. (2014). Prediction of cyberslacking when employees are working away from the office. *Computers in Human Behavior*, *34*, 291-298.

Ophoff, J., Jensen, A., Sanderson-Smith, J., Porter, M., & Johnston, K. (2014). A descriptive literature review and classification of insider threat research. In *Proceedings of Informing Science & IT Education Conference (InSITE)* (pp. 211-23).

Osborne, C. (2020, October 8). *Tesla accuses employee of Californian factory sabotage*. ZDNet. https://www.zdnet.com/article/tesla-accuses-employee-of-californian-factory-sabotage/.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Which factors explain employees' adherence to information security policies? An empirical study. *Pacis 2007 Proceedings*, 73.

Pastor, D. A., Barron, K. E., Miller, B. J., & Davis, S. L. (2007). A latent profile analysis of college students' achievement goal orientation. *Contemporary educational psychology*, *32*(1), 8-47.

Peer, E., Vosgerau, J., & Acquisti, A. (2014). Reputation as a sufficient condition for data quality on Amazon Mechanical Turk. *Behavior research methods*, *46*(4), 1023-1031.

Philipps, J. G., & Reddie, L. (2007). Decision style and self-reported Email use in the workplace. *Computers in Human Behavior, 23*, 2414–2428.

Plouffe, R. A., Saklofske, D. H., & Smith, M. M. (2017). The assessment of sadistic personality: Preliminary psychometric evidence for a new measure. *Personality and individual differences*, *104*, 166-171.

Ponemon, (2020). 2020 Cost of Data Breach Report. Retrieved from: https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542

Posey, C., Raja, U., Crossler, R. E., & Burns, A. J. (2017). Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA. *European Journal of Information Systems*, *26*(6), 585-604.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51*(5), 551–567.

Prusik, M., & Szulawski, M. (2019). The relationship between the Dark Triad personality traits, motivation at work, and burnout among HR recruitment workers. *Frontiers in psychology*, *10*, 1290.

Restubog, S. L. D., Garcia, P. R. J. M., Toledano, L. S., Amarnani, R. K., Tolentino, L. R., & Tang, R. L. (2011). Yielding to (cyber)-temptation: Exploring the buffering role of self-control in the relationship between organizational justice and cyberloafing behavior in the workplace. *Journal of Research in Personality*, *45*(2), 247-251.

Restubog, S. L. D., Garcia, P. R. J. M., Wang, L., & Cheng, D. (2010). It's all about control: The role of self-control in buffering the effects of negative reciprocity beliefs and trait anger on workplace deviance. *Journal of Research in Personality*, *44*(5), 655-660.

Richardson, (2011). 2010/2011 CSI computer crime and security survey. Retrieved from: https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital investigation*, *3*(2), 97-102.

Rogers, R. W., & Prentice-Dunn, S. (1997). *Protection motivation theory.* In D. S. Gochman (Ed.), *Handbook of health behavior research 1: Personal and social determinants* (p. 113–132). Plenum Press.

Rosenberg, J. M., Beymer, P. N., Anderson, D. J., & Schmidt, J. A. (2018). tidyLPA: An R Package to Easily Carry Out Latent Profile Analysis (LPA) Using Open-Source or Commercial Software. *The Journal of Open Source Software*, *3*, 978.

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health education monographs*, *2*(4), 328-335.

Rousseau, D. M. (2008). Psychological contract inventory: Employee and employer obligations. *The Heinz School-Carnegie Mellon University, USA*.

Rousseau, D. M. (1989). Psychological and implied contracts in organizations. *Employee Responsibilities and Rights Journal, 2*(2), 121-139. https://doi.org/10.1007/bf01384942

Salem, M. B., Hershkop, S., & Stolfo, S. J. (2008). A Survey of Insider Attack Detection Research. *Insider Attack and Cyber Security, 39*, 69-90.

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *information security technical report*, *15*(3), 112-133.

Schneier, B. (2015). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

Schroder, H. M., Driver, M. J., & Streufert, S. (1967). Human information processing—Individuals and groups functioning in complex social situations, New York: Holt, Rinehart, & Winston.

Scrucca, L., Fop, M., Murphy, T. B., & Raftery, A. E. (2016). mclust 5: clustering, classification and density estimation using Gaussian finite mixture models. *The R journal*, *8*(1), 289.

Shirom, A., & Melamed, S. (2006). A comparison of the construct validity of two burnout measures in two groups of professionals. *International journal of stress management*, *13*(2), 176.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Sobers, R. (2019). *60 Must-Know Cybersecurity Statistics for 2019*. Retrieved from: https://adaptus.com/60-must-know-cybersecurity-statistics-for-2019/

Sobers, R. (2021). 134 Cybersecurity statistics and trends for 2021. Retrieved from: https://www.varonis.com/blog/cybersecurity-statistics/

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*, *23*(2), 200.

Stanton, J. M., & Lin, L. F. (2001). Electronic monitoring, privacy, and organizational attraction: A field experiment. In *Sixteenth Annual Conference of the Society for Industrial and Organizational Psychology, San Diego, CA*.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security*, *24*(2), 124-133.

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

Triandis, H. C. (1977). *Interpersonal behavior*. Brooks/Cole Publishing Company.

Van Den Bergh, M., & Njenga, K. (2016). Information security policy violation: The triad of internal threat agent behaviors. In *Proceedings of the 1st International Conference on the Internet, Cyber Security, and Information Systems (ICICIS)* (pp. 1-12).

Verizon, (2021). 2020 Data Breach Investigation Report. Retrieved from: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security journal*, *26*(2), 107-124.

Walter, J. (2020, May 2). *COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes*. IMC Grupo. https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101-105.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, 25-35.

Warkentin, M., Straub, D., & Malimage, K. (2012, June). Featured talk: Measuring secure behavior: A research commentary. In *Annual Symposium of Information Assurance & Secure Knowledge Management, Albany, NY*.

Warren, D. (2003). Constructive and Destructive Deviance in Organizations. Academy of Management Review, 28(4), 622−632.

Weatherbee, T. G. (2010). Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. *Human Resource Management Review*, *20*(1), 35-44.

Weatherbee, T. G., & Kelloway, E. K. (2006). A Case of Cyberdeviancy: CyberAggression in the Workplace. In E. K. Kelloway, J. Barling, & J. J. Hurrell (Eds.), Handbook of Workplace Violence. (pp. 445−487). Thousand Oaks, CA: Sage Publications, Inc.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information systems security and the need for policy. In *Information security management: Global challenges in the new millennium* (pp. 9-18). IGI Global.

Whitman, R. L. (2016). Brain Betrayal: A Neuropsychological Categorization of Insider Attacks. In *Proceedings of the 2016 Conference on Cybersecurity Education, Research and Practice* (Vol. 2016, No. 1).

Whitman, R. L. (2021). Armed, Not Ready: Technological Determinism, Discourse, and the Blitzkrieg of Today. In D. J. Svyantek (Ed.), *Organizations Behaving Badly: Destructive Behavior and Corrective Responses*, (pp. 89-109).

World Economic Forum, (2012). Global Risks 2012, Seventh Edition. Retrieved from: http://reports.weforum.org/global-risks-2012/#

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, *24*(1), 34.

Appendix A: Supplemental Tables

Cybersecurity Behavior Inter-Indicator Correlations

	M(SD)	1	2	3	4	5	6
1 – Password Variation	5.54(1.43)						
2 – Password Freshness	4.89(1.66)	.44**					
3 – Setting Awareness	5.04(1.63)	.33**	.56**				
4 – Malware Awareness	5.54(1.19)	.51**	.34**	.39**			
5 – Phishing Checks	5.68(1.15)	.40**	.27**	.30**	.64**		
6 – Secure Transmission	5.49(1.50)	.30**	.20**	.22**	.47**	.63**	
7 – Backups	5.54(1.41)	.36**	.31**	.35**	.53**	.45**	.38**

Note: ** - Correlation is significant at the 0.01 level (two-tailed).

Cyberloafing Inter-Indicator Correlations

	M(SD)	1	2	3	4	5	6
1 – Social Media	3.67(1.43)						
2 – Online Shopping	3.48(1.73)	.71**					
3 – Gameplay	2.38(1.81)	.58**	.69**				
4 – Seek Employment	2.77(1.69)	.57**	.66**	.78**			
5 – Adult Websites	2.36(1.76)	.45**	.58**	.76**	.70**		
6 – Non-Work Email	3.50(1.48)	.64**	.62**	.50**	.51**	.47**	
7 – Chatting	3.54(1.64)	.67**	.63**	.63**	.59**	.52**	.67**

Note: ** - Correlation is significant at the 0.01 level (two-tailed).