

# **A Multi-Motivational Approach to Influencing Cybersecurity Behavior**

**Early stage paper**

**Jake Mead**

The University of Tulsa  
School of Cyber Studies  
College of Engineering and Computer Science  
Jpm8609@utulsa.edu

**Stephen Flowerday**

The University of Tulsa  
School of Cyber Studies  
College of Engineering and Computer Science  
S.flowerday@utulsa.edu

## **ABSTRACT**

Malicious actors have effectively utilized the known tendencies in user behavior to exploit vulnerabilities and gain access to business networks as well as personal and organizational data. Researchers of cybersecurity behavior have long postulated the need for informed and tailored programs that meet the psychological profiles of its users, leveraging the known tendencies toward specific behaviors and perceived outcomes associated with biological and cultural traits. Protection motivation (fear) and self-determination theory (self-determined) provide the basis of motivational appeals, offering two competing but equally refined means of engaging the distinctive personality trait sensitivities. This study will administer motivational appeals in conjunction with cyber behavioral surveys and conduct PLS multivariate group analysis to determine the difference in effect sizes between single motivational and multi-motivational approaches. This exploratory paper employs carefully curated motivational appeals that speak most significantly to the traits and persuasions of the individual to establish a greater overall intention to engage in secure cyber behaviors when compared to single motivational strategies.

## ***Keywords***

Self-determination Theory, Protection Motivation Theory, Cybersecurity Behavior, Personality Traits

## **INTRODUCTION**

Individuals are often the primary target for attackers, homing in on subpar security behaviors to exploit vulnerabilities within information networks (Tolah et al., 2019). In this ever-transforming workspace, the threats and vulnerabilities faced by firms as a result of individuals working within organizational networks are higher than ever.

Organizations have attempted to smooth cyber learning curves and ensure their employees are at pace with emerging tools and threats through rigorous training initiatives and change management activities (Da Veiga, 2016). However, cybersecurity training and education has long been questioned for its effectiveness, often resulting in short term, diminishing returns (Cain et al., 2018). “Providing users with knowledge is the first step, but we need to determine how to improve users’ cyber hygiene attitudes and behaviors” (Cain et al., 2018). Motivation theories offer an additional perspective to consider within the conundrum of human cybersecurity behavior. Maintaining learning within complex domains requires effective motivation to promote quality learning and content engagement, individuals that are motivated to learn despite the challenges they will undoubtedly face along their journey (Kam et al., 2022). Despite numerous studies showcasing the influences of motivation-based strategies, results remain inconsistent and have failed to successfully translate into organizational cybersecurity strategies (Menard et al., 2017). One possible reason for the variance of results in cybersecurity and motivation research is how the population samples are perceived as being homogenous. Demographics representing cross-cultural

or cross-national differences are related to observed heterogeneity but have proven inconsistent in their impact on cyber behaviors (Cheah et al., 2023). Additional observed heterogeneous factors need to be applied within this specific context to aid in our interpretation of motivational research outputs. Research into personality traits would suggest that inherent characteristics of the population will predispose certain individuals to be more sensitive to certain appeals and ignorant of others. Given the known variances in the population, we propose that a multi-tool approach to motivating individuals to engage in secure cyber behavior may be more successful than a single motivational method. This leads to our research statement.

*Higher overall intentions to engage in secure cyber behaviors may be achieved by providing different motivational appeals to specific individuals within the same context.*

In this study, we examine the effects of different appeals, fear and self-determined, on personality traits. The appeals are developed in accordance with protection motivation theory (PMT) and self-determination theory (SDT). Both PMT and SDT have been comprehensively studied within IS literature and, in isolation, have been tested against personality traits. Studies of this nature have had varying results but often point to one or two personality traits resonating most significantly with a particular motivational theory in the given context. This is the first study, to our knowledge, that tests PMT and SDT through the lens of personality traits in a single study to determine the effectiveness of fundamentally different appeals in achieving a more effective overall intention to engage in secure cyber behavior. The objective being to create a catalogue of approaches to

motivating individuals that speaks to their individual nature, highlighting the aspects of cyber behavior that result in the greatest chance of continued secure behavior.

The prevalence of attacks targeted at poor user behavior was used as a measure to determine which behaviors are to be observed in this study. The behaviors studied include strong password creation and management, regular updates of software and the use of a VPN. The listed behaviors are desired as security measures for both personal and organizational data and engagement in which these behaviors significantly reduce the likelihood of falling victim to cybercrime (Wijayanto et al., 2020).

## **LITERATURE REVIEW**

### **Personality Traits**

Factors such as age, gender and demographics have been well researched in terms of their impact on cybersecurity factors including awareness and training. Cain et al., (2018) found that there is no difference in cyber hygiene factors among age groups and while some consistencies emerged between gender groups, there was a lack of significant data to point toward conclusive findings. Personality traits, however, have found some prominence in cyber behavior research as significant and unique predictors of cyber behavior. The big 5 personality traits were established in Fiske's theory in 1949 and developed further by a host of researchers between 1967 and 1987 (Komarraju et al., 2011).

The big five personality traits are extraversion, agreeableness, openness, conscientiousness, and neuroticism (Church, 2016). Extraversion is characterized through assertiveness and emotional expressiveness (Terracciano et al., 2006). High levels of extraversion can be associated with

impulsive behaviors which may result in unnecessarily risky behaviors. Trusting, cooperative and empathetic individuals are associated with higher levels of agreeableness (Terracciano et al., 2006). Those that score low in agreeableness tend to display manipulative behavior, characterized by a lack of empathy and interest in the struggles of others (Church, 2016). Individuals who exhibit high openness are eager to experience new things and generally display more creativity and imagination when compared with the other personality traits. Conscientiousness is associated with impulse control, thoughtfulness, and goal-oriented behaviors. Individuals displaying higher levels of conscientiousness will be more analytical of their own behavior and enjoy working within structured environments. Finally, neurotic individuals are regarded as emotionally unstable, frequently experiencing irritability and anxiety through fluctuating moods (Terracciano et al., 2006). Neuroticism is a physical and emotional response to stress and perceived threats in someone's life (Frauenstein et al., 2023) as such individuals with lower levels of neuroticism tend to live 'in the moment' and are more resilient to stress and stressful situations.

Scholastic literature through the lens of personality traits has found some prominence across a diversity of fields. Originating in psychology, the big 5 personality traits have been used to evaluate and predict human behavior in nearly every field that requires the involvement of the human element. More specifically, within the IS field, personality traits have been used to shed light on predictable cyber behaviors. Gratian et al. (2018) undertook research aimed at explaining correlations between human characteristics and behavior intentions. The authors evaluated personality traits as unique indicators against four categories of user security behavior (device securement, password generation, proactive awareness and updating). Across the four security behaviors examined, extraversion was a significant unique predictor for device securement while

conscientiousness was the only significant unique predictor of secure password generation, proactive awareness and consistent updating (Gratian et al., 2018). In the context of regular updates of software for security patches, conscientiousness was the sole unique predictor of this behavior amongst the personality traits (Gratian et al., 2018). Gratian's study highlighted two key outcomes applicable to the current study. First, personality traits are significant differentiators when examining a variety of cybersecurity behaviors. Second, conscientiousness was a consistently significant indicator of the cyber behaviors observed, while it may be argued that the conscientious personality trait lends itself to more thoughtful and, in turn, secure behavior generally, this conclusion would shed a particularly dim light on the remaining personality traits and their tendency to engage in secure behaviors. We propose that all personality traits are capable of secure behaviors but the current methods of motivating users to engage in cyber behaviors are inflexible to different needs and perceptions of the cybersecurity landscape.

McBride (2012) proposed that personality traits are a significant indicator of cybersecurity policy violations and conducted an empirical validation of deterrence, protection motivation and personality factors on non-compliance within organizations. The results of their investigation were summarized in a few concise observations with regards to personality traits; 1, more open and neurotic individuals were observed to be less likely to violate cybersecurity policies and 2, more extraverted individuals were more likely to violate cybersecurity policies (Mcbride et al., 2012). McBride (2012) stated that personality traits were an indicator of varying reactions to the same situation and in this context, affected the way they approach compliance with cybersecurity policies. Frauenstein (2020) used the big five personality traits to determine whether individuals were predisposed to being more likely to fall victim to a phishing attack. In so doing, they proved

causation between personality traits and susceptibility to phishing on social network sites (Frauenstein et al., 2020). Frauenstein concluded that we can inform individuals and training programs better to target their own predisposed vulnerabilities and influence specific outcomes. These findings are aligned with the current research objective, which provides users with specific appeals that resonate most with their predisposed characteristics and in so doing, achieve a greater overall intention to engage in secure cyber behaviors.

## **Protection Motivation Theory**

Protection motivation theory (PMT) was first developed by Rogers (1975) as a tool to explain the cognitive process people engage in to mediate behavior when facing public safety and health related threats or fear (Khan et al., 2023). PMT highlights the interaction between threat and coping appraisals and their impact on an individual's intent to protect themselves from the identified threat (Vrhovec et al., 2021). PMT posits that the appraisal process significantly affects an individual's intention to take some action leading to adaptive or maladaptive behaviors (Vrhovec et al., 2021). Coping mechanisms are representative of an individual's perception of response cost, self-efficacy and response-efficacy (Sharma et al., 2022). Sharma et al., provide a description of each of the constructs associated with threat and coping appraisals; response cost is the associated negative consequences, or sacrifices associated with taking protective action, the discomfort of wearing a seatbelt would be an example of response cost. Self-efficacy is the belief in one's ability to successfully execute a specific behavior required to achieve a desired outcome. Someone with high self-efficacy in quitting smoking has a high degree of confidence in their ability to resist cravings and cope with withdrawal symptoms. Response efficacy refers to the belief that the recommended action will effectively reduce or eliminate the threat. An example of response efficacy would be

the use of vaccines, users have high response efficacy regarding vaccines if they believe the vaccine will protect them against disease and the transmission of disease. Threat appraisals consist of the individual's perception of threat severity and threat vulnerability. Threat severity refers to the perceived seriousness or magnitude of the potential harm or negative consequence associated with a particular event, an example of threat severity is the degree to which individuals felt threatened by the Covid-19 outbreak and believed exposure could lead to illness and hospitalization or death. Threat vulnerability refers to the perceived likelihood or probability that an individual will be personally affected by the threat. To reuse our Covid-19 example, the elderly and immune-compromised were believed to be the most vulnerable to the threat of Covid and as such, even healthy individuals took protective measures to ensure they did not expose those more vulnerable than themselves.

PMT has been criticized for not truly encompassing a motivational construct and providing results that are inconsistent and at times contradictory (Menard et al., 2017). PMT originated in the health care sector and is based on the idea of personal threat. The theory was successfully translated into the cybersecurity domain due to the parallels of threat and solution that exist in both spaces. In the medical field, where PMT found significant application, threats (e.g. viruses, illnesses and injuries) have associated treatments (medication and operations). This relationship between threat and solution is often mirrored in cybersecurity where threats (e.g. malware and phishing attacks) have associated responses or protections (firewalls, network monitoring and training). However, factors such as psychological ownership of organizational assets have been suggested as one of several key factors that differentiate the healthcare and cybersecurity domain and subsequent applications of PMT (Menard et al., 2017).



Protection Motivation Theory (PMT) remains the most prevalent motivation theory used in cybersecurity literature and is particularly popular within the field of information security compliance (ISP) (Alassaf et al., 2021). Some examples of PMT being used in the cybersecurity field include; empirical investigations into factors affecting businesses decisions to adopt anti-malware software; analyzing the impact of individual characteristics such as psychological ownership of information within the context of cybersecurity behaviors; studies on the impact of cybersecurity awareness on desktop security behavior and identifying predictors that differentiate between users who secure their home wireless networks and those who do not (Alsharida et al., 2023). Research on PMT differs in terms of understanding whether people conduct appraisals in parallel or sequentially (Van Haastreht et al., 2021). A parallel processing of appraisals would suggest that the given constructs are evaluated independently. Sequential processes would suggest that individuals make a threat appraisal initially and only evaluate a subsequent cost appraisal where the initial threat appraisal deems a threat warrants a response. For the purposes of this study, threat and cost appraisals will be evaluated as parallel processes.

PMT has been chosen within this study due to the primal nature of its fear appeals on human psychology. The theory posits the response to a threat is driven by an interpretation of threat impact and the ability to respond effectively, this perception of cyber behavior is rooted in the lowest of Maslow's needs for safety and security. This type of appeal is the antithesis of appeals aimed at elevating the individual's consciousness of their environment, the threats encompassed within that environment and how the individual might mitigate, accept or avoid the associated risks through their own judgment and experience. This type of appeal is further referred to as self-determined appeals.

Both neurotic and conscientious individuals display traits that would suggest their sensitivity to fear appeals may be greater than self-determined appeals. Neurotic individuals are prone to greater worry, emotional instability and impulsiveness. Additionally, when coupled with low openness or conscientiousness, high levels of neuroticism led to decreases in decision performance and the ability to detect cyber-threats (Papatsaroucha et al., 2021). These results would suggest appeals emphasizing the severity and cost as well as the associated solution of an adverse event will result in a greater intention to behave securely (van der Schyff et al., 2020). Given the suspected susceptibility of individuals in these instances, the approach of clear risk and response incorporated into the PMT appeal will allow for lower cognitive load and easier decision making than the more contextual and more cognition heavy self-determined appeals. Conscientious individuals, characterized by their conformity, responsibility and tendency to follow norms are expected to be more responsive to the black and white nature of fear appeals that provide strict instruction as to the intended and desired behavior (Gratian et al., 2018). Employees displaying higher levels of conscientiousness tend to follow more systematic and rational approaches to the information processing activities associated with secure cyber behavior. As with the neurotic individual, but for different reasons, the association between risk and response creates strong systematic responses to certain threats which will result in more consistently secure behaviors (Papatsaroucha et al., 2021).

*H1; Subjecting neurotic individuals to fear appeals will result in a greater intention to engage in secure cyber behaviors.*

*H2; Subjecting conscientious individuals to fear appeals will result in a greater intention to engage in secure cyber behaviors.*

## **Self-Determination Theory**

Self-Determination theory claims that the facilitation of basic psychological needs can give rise to intrinsic motivation and wellbeing (Poeller et al., 2022). Deci and Ryan (1985) proposed a discrete set of extrinsic motivation types and defined self-determination theory (SDT) as, “a quality of human functioning that involves the experience of choice. [It is] the capacity to choose and have those choices...be the determinants of one’s actions” (Gagné et al., 2014). Motivation has been widely generalized as either intrinsic or extrinsic, intrinsic motivation constituting the performance of “an activity for itself and the pleasure and satisfaction derived from participation” (Menard et al., 2017), extrinsic motivation inversely defined by “engaging in an activity as a means to an end and not for its own sake” (Menard et al., 2017). The discrete set of extrinsic motivation types suggest that extrinsic motivation is categorized by the degree to which an individual’s motivation is controlled by some external means (Gangire et al., 2020).

Chen (2010) provides a comprehensive breakdown of the motivational types described in SDT. Amotivation, the relative lack of motivation and intentionality, sits in between extrinsic and intrinsic motivation as an empty state. Intrinsic motivation within SDT is defined by high levels of personal interest, enjoyment, and inherent satisfaction. The intrinsically motivated individual requires no external means to regulate engagement and commitment to the respective activity. The subsequent 4 motivation types describe varying levels of extrinsic motivation influenced by

several constructs across research areas but fundamentally: competency, autonomy and relatedness. First, external regulation defines a compliant motivational state where the individual is heavily regulated by rewards (e.g. money, compensation) and sanctions (e.g. punishments). Second, introjected regulation occurs when an individual internalizes the reasons for their actions, suggesting the motivation is internal but not necessarily self-determined. Individuals are often motivated in this capacity by the desire to impress and receive affirmation from respected or senior individuals within our respective communities. Third, identified regulation is defined by a sense of personal importance and “synthesis with self”. Identified regulation occurs when a specific behavior is highly valued and judged as important upon identification (the behavior is a means to some, self-determined, end). Finally, integrated regulation describes an externally derived behavior that has been fully internalized by the individual. The individuals make a conscious choice to perform unpleasant but necessary behaviors that will enforce the individual’s own perceptions of themselves.

The self-determination theory further proposes that an individual is influenced by their perceptions of autonomy, competence, and relatedness of the given task to their personal goals and desires (Fatokun et al., 2020). Autonomy refers to an individual’s perception of whether the given behavior is one they may engage in of their own volition. Competence is one’s perception of the degree to which they feel they might interact effectively with their environment in the execution of a desired task or behavior. Finally, relatedness is defined as the degree to which an individual feels they have a connection with peers or colleagues.

Wall, Palvia and Lowry (2013), found that motivation had a significant effect on user compliance with security policies by highlighting the perceptions of how one's compliance would enhance cybersecurity within the organization. The competency and autonomy of users operating various security tasks was studied by Gangire et al., (2020) noting the influences of each construct on users' security motivation. In a series of papers, Menard et al., (2017) proposed understanding user's motivation as a tool to protect information assets and create a safer computing environment. Menard (2017) contrasted PMT and SDT to test whether the use of self-determined appeals would impact the user's perception of threat and cost appeals. Menard (2017) proved greater significance in the relationships between the constructs of self-determination and an intention engage in secure behavior when compared with the constructs of PMT. The conclusions reached would suggest that users are more sensitive to self-determined appeals overall. These findings imply that motivation is a significant indicator of intention to engage in secure behaviors and that for a user to feel engaged and motivated, careful consideration must be given to the relatedness of the task, the competency of the user in the given field and the autonomy to decide which behaviors they are to employ.

Self-determination theory has been applied within multiple domains, one of intrigue, game design and development. Game developers are forced to consider the motivations of their players to avoid attrition and keep gamers engaged (Tyack et al., 2020). Self-determination theory forms the foundation of how many game designers understand and seek to manipulate motivation, this has led to researchers in the game development field calling for a diversification of motivation tools to effectively engage a wide variety of gamers (Poeller et al., 2022). A sense of defaulting to the traditional approaches could be argued to plague cybersecurity initiatives trying to engage their

diverse cohort of users. Self-determination theory and personality traits have been studied with some regularity to shed light on personal factors that influence academic performance. Zhou (2015) explored the moderating effect of self-determination in the relationship between personality and academic performance. All personality traits, except neuroticism, were observed to have a significant and positive relationships with academic performance in English (Zhou, 2015). Openness and conscientiousness positively predicted English performance but only when the student's self-determined motivation was low. Zhou's research shed light on the importance of personality, self-determined motivation and academic achievement, particularly the need to monitor personality traits to help educators incorporate appropriate strategies into their existing curricula to enhance student learning experiences.

Self-determined appeals, aimed at elevating the individual's sense of competence, autonomy and relatedness to the given task or subject serve as the contrasting method for motivation in this study. The fear appeals associated with PMT seek to influence the individual's decision making toward a prescribed outcome (Alassaf et al., 2021). On the contrary, self-determination speaks to the freedom of choice, informed by engagement with the knowledge area. There is no 'prescribed' outcome or solution, and while there are perhaps best practices or preferred responses communicated within these appeals, the individual contextualizes the task within a broader area of knowledge and chooses freely their response to any given threat (Gangire et al., 2020).

Extraverted individuals are characterized by their sociable, energetic and assertive personalities (van der Schyff et al., 2020). They are also more likely to be sensation-seeking given their outgoing and adventurous persuasions, higher levels of sensation-seeking and general risk taking predict greater likelihood of engaging in risky cybersecurity behaviors (Kennison et al., 2020). Extraverts

are unlikely to respond favorably to direct instruction where their autonomy is compromised and their natural tendency to engage in chosen behaviors is met by an obstacle in the form of an instruction or company policy. Conversely, extraverted individuals are expected to respond well to self-determined appeals that emphasize their autonomy in selecting their best course of action and level of engagement, the relatedness of the task to their own self-determined goal, and their competency to effectively engage and execute the behaviors in line with their goals (Fatokun Faith et al., 2020). In this way, extraverts are equipped with a more comprehensive understanding of how their exploratory, risky behaviors impact not only them but also their environment and organization.

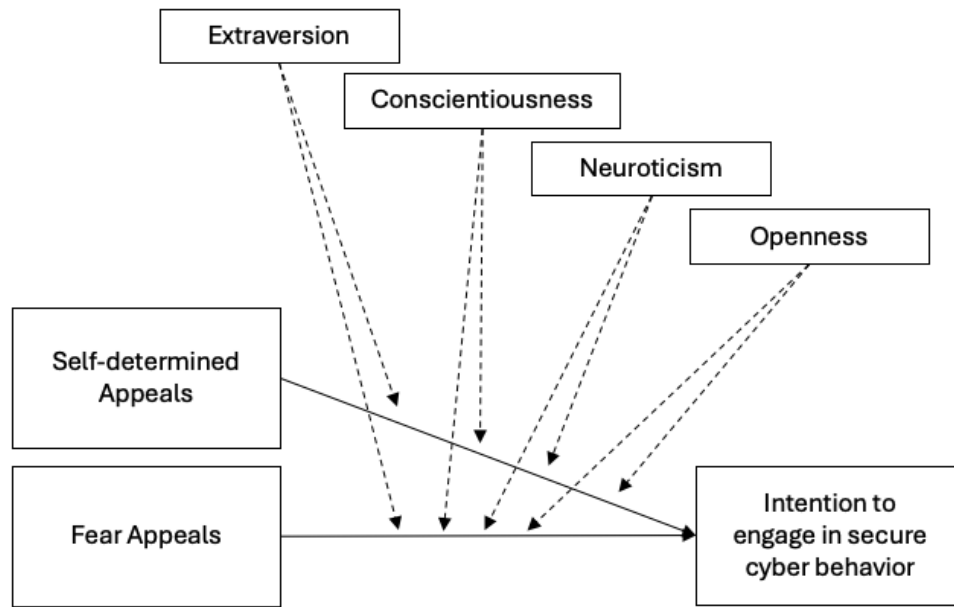
By exposing more open individuals to self-determined appeals, we might influence their intention to engage in specific and secure behaviors by appealing to their desire for exploration, new experiences, higher cognitive abilities and creativity (van der Schyff et al., 2020). Openness to experience was positively related with thinking, persisting, affiliating, desire for self-improvement and achievement. These characteristics are exemplified within the constructs of self-determination as the relatedness (affiliating), autonomy (thinking) and competency (desire for self-improvement and achievement) around a particular topic have been proven to enhance engagement with more open individuals (Komarraju et al., 2005). Attempting to box and over curate the behaviors of open individuals may result in the individual becoming demotivated and disengaged (Mcbride et al., 2012). Self-determined appeals that seek to engage the open user's sense of self-exploration and creativity in determining their own best course of action are expected to result in a greater intention to engage in secure cyber behaviors.

*H3; Subjecting extraverted individuals to self-determined appeals will result in a greater intention to engage in secure cyber behaviors.*

*H4; Subjecting open individuals to self-determined appeals will result in a greater intention to engage in secure cyber behaviors.*

Finally, agreeable individuals, characterized by their influenceable, trusting and cooperative natures are likely to display an equal intention to engage in secure cyber behaviors based on fear or self-determined appeals alone. Research has frequently failed to identify the agreeable personality trait as one that resonates overly with either type of motivational theory (Zhou, 2015) (Komarraju et al., 2005), therefore the agreeable personality trait is descoped for the purposes of this study.





**Figure 1: Proposed Research Model**

## PROPOSED RESEARCH METHOD

### Sample Selection

We will employ cross-sectional surveys as the tool to collect primary data for this study. Candidates are to be recruited through a crowd sourcing platform, such as Prolific. The target population should engage in online activities befitting the highlighted behaviors and be representative of the population demographics including age, gender and education levels of people working in the United States of America that are between the ages of 22 and 65 years old.

## **Procedure**

The data collection procedure will be split into two parts. First, a survey encompassing questions relating to the sample demographics, cybersecurity behavior and personality traits will be administered. This survey will comprise questions relating to the observed behaviors in this study, namely secure password management, updating software and use of VPNs. A 44-item Big Five Inventory (BFI) personality assessment developed by John and Srivastava (1999) will be employed to evaluate the respondent's primary personality traits.

Once an initial survey has been conducted, data collected and initial results analyzed, the respondents will be requested to complete a subsequent survey. At the outset, respondents will be divided into two groups based on their dominant personality traits and provided either fear or self-determined appeal. The primary personality trait will be used to distribute respondents equally into groups receiving either fear or self-determined appeals, in this way we ensure equal representation of personality traits to each appeal. Finally, an assessment of intention will be conducted in respect of the behaviors questioned as part of the initial behavioral survey. We will aim to have approximately 400 completed and acceptable responses per group. To develop the respective surveys, multiple sources will be consulted, an approach common in both social psychology and behavioral technology research (van der Schyff et al., 2020).

## **Data Analysis**

To infer that a significant difference exists between the intention to behave securely by providing specific groups of people with different motivational appeals as opposed to a single type of appeal, we will conduct a PLS-based multigroup analysis (PLS-MGA) (Weston et al., 2006). Using this

technique, researchers can either explore their results for potential distortion by unobserved heterogeneity, or they can identify, thus far neglected, variables that describe the uncovered data segments (Sarstedt et al., 2011). In a similar fashion, this study aims to uncover the effect of two different motivational approaches on a heterogeneous sample defined by their personality traits. The multigroup approach followed in this study will provide observable and comparable statistical results that shed light on the effectiveness of one motivational appeal over another for a given personality trait as well as the collective groups. The multivariate groups will include equal representation of personality traits and be differentiated by the motivational appeal the group is exposed to. Sarstedt et al., (2011) provide an in-depth review of available multigroup analysis methods in PLS path modeling which allow for the testing of difference across more than two groups. Cheah et al., (2023) examined recent applications of multigroup analysis with more than two groups to provide guidelines and comprehensive recommendations for researchers applying PLS-MGA. The findings and recommendations included in these papers and others for PLS-MGA will be followed along with the use of PLS software, SmartPLS, for the purposes of data analysis.

## **CONTRIBUTION**

### **Contribution to theory**

Motivational theories and personality traits have been researched in many capacities but often focusing on a single theory of motivation or multiple theories without a view of the heterogeneity of the sample. This study aims to expand our understanding of how multiple motivation theories may be used to increase the overall intention of a sample. By targeting carefully curated motivational appeals to specific individuals that are most sensitive to the underlying constructs of

the appeal, we might achieve a greater net result compared to administering a single appeal. This study also expands on the use of personality traits within cybersecurity research through the confirmation of certain biases toward underlying constructs within the motivational theories. To our knowledge, no cybersecurity research currently exists that has compared PMT, SDT and personality traits within a single study.

## **Contribution to practice**

The contributions to cybersecurity practices are potentially significant. Unlike educational or medical contexts where the consequence of risky behavior contrary to industry standards or best practices is unlikely to impact anyone further than the individual, cybersecurity exposures are often carried out by exploiting the weakest link. Herein lies one of the greatest challenges to effective cybersecurity practices, achieving complete coverage is incredibly difficult but without complete coverage, or as close to, we remain vulnerable to any number of both sophisticated and simple cyberattacks. This research provides methods to achieve overall greater intentions to engage in secure cyber behaviors by homing in on individual tendencies and predispositions. This research focuses on the motivational approaches employed to encourage users to engage with cybersecurity concepts, tools and behaviors. Motivational appeals are a key step in the user's cybersecurity journey, contextualizing and grounding the reasons 'why' all individuals should take an active interest in the protection of data and devices. It could be argued that even marginal improvements in overall intentions found in this study are worthwhile for both organizations and individuals in the quest for complete coverage.

The results of this study are widely applicable to a variety of cybersecurity related initiatives. Training and awareness programs, incident response and recovery activities and change management of new and existing software and technologies are examples of where providing meaningful and sustained motivation can greatly enhance the chances of success. Incident awareness and communication as well as subsequent training and awareness programs are amongst the core activities of incident response management teams within a firm when attacked. This study proposes tools that would allow these efforts to be more targeted and impactful. The role of the individual within the firm, the situation within which a vulnerability was exploited, or a breach occurred and the tendencies of the individual to engage or ignore (as we have discussed here) are all factors that should be evaluated in conjunction when designing an effective response message. Change management activities, particularly those involving the implementation of new security software, protocols and processes can be enhanced through tailored communication on the purpose of the implemented tools. In so doing, we connect the user and the tool in a manner that ensures more effective and engaged use from day one.

## **CONCLUSION**

This exploratory study combines personality traits, protection motivation and self-determination theories in a manner consistent with the methods of extensive research in the field of cybersecurity. We hypothesize that using a multi-motivational approach, individuals and organizations might achieve a greater overall user intention to engage in secure cyber behaviors. Motivational appeals, specifically curated to emphasize the underlying constructs of each motivational theory, provide the lens through which different personalities will participate in cybersecurity initiatives and interact with various tools. To establish a clear difference in single and multi-motivational

approaches, we will administer cybersecurity behavioral, personality assessment and behavioral intention surveys coupled with carefully curated motivational appeals. PLS multivariate group analysis will provide the statistical underpinning of this research by comparing the effect sizes on intention to engage in secure cyber behaviors. We argue that the underlying heterogeneity of the population undermines single track solutions and initiatives, failing to truly engage the user base and shift behavior in the intended direction. By exploring the underlying nature of the intended audience and ensuring alignment of known differences with contrasting motivational theories, we might inch closer to a state of uniform engagement with and acceptance of cybersecurity initiatives, policies, tools and behaviors.

## **ACKNOWLEDGEMENTS**

We gratefully acknowledge funding and support from the TU Cyber Fellows initiative for this research.

## REFERENCES

- Alassaf, M., & Alkhalifah, A. (2021). Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review. In *IEEE Access* (Vol. 9, pp. 162687–162705). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ACCESS.2021.3132574>
- Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 73. <https://doi.org/10.1016/j.techsoc.2023.102258>
- Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42. <https://doi.org/10.1016/j.jisa.2018.08.002>
- Cheah, J. H., Amaro, S., & Roldán, J. L. (2023). Multigroup analysis of more than two groups in PLS-SEM: A review, illustration, and recommendations. *Journal of Business Research*, 156. <https://doi.org/10.1016/j.jbusres.2022.113539>
- Chen, K. C., & Jang, S. J. (2010). Motivation in online learning: Testing a model of self-determination theory. *Computers in Human Behavior*, 26(4), 741–752. <https://doi.org/10.1016/j.chb.2010.01.011>
- Church, A. T. (2016). Personality traits across cultures. In *Current Opinion in Psychology* (Vol. 8). <https://doi.org/10.1016/j.copsy.2015.09.014>
- Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *Proceedings of 2016 SAI Computing Conference, SAI 2016*. <https://doi.org/10.1109/SAI.2016.7556102>
- Fatokun Faith, B., Hamid, S., Norman, A., Fatokun Johnson, O., & Eke, C. I. (2020, March 1). Relating Factors of Tertiary Institution Students' Cybersecurity Behavior. *2020 International Conference in Mathematics, Computer Engineering and Computer Science, ICMCECS 2020*. <https://doi.org/10.1109/ICMCECS47690.2020.246990>
- Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers and Security*, 94. <https://doi.org/10.1016/j.cose.2020.101862>
- Frauenstein, E. D., Flowerday, S., Mishi, S., & Warkentin, M. (2023). Unraveling the behavioral influence of social media on phishing susceptibility: A Personality-Habit-Information Processing model. *Information and Management*, 60(7). <https://doi.org/10.1016/j.im.2023.103858>
- Gagné, M., & Deci, E. L. (2014). *The Beginnings The History of Self-Determination Theory in Psychology and Management* 1. <http://ebookcentral.proquest.com/lib/utulsa/detail.action?docID=1688432>.
- Gangire, Y., Da Veiga, A., & Herselman, M. (2020). *Information Security Behavior: Development of a Measurement Instrument Based on the Self-determination Theory*. 144–157. [https://doi.org/10.1007/978-3-030-57404-8\\_12i](https://doi.org/10.1007/978-3-030-57404-8_12i)
- Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers and Security*, 73, 345–358. <https://doi.org/10.1016/j.cose.2017.11.015>

- John, O., & Srivastava, S. (1999). The Big Five Taxonomy: History, Measurement and Theoretical Perspectives. In *Handbook of Personality: Theory and Research, second ed.* Guilford, New York.
- Kam, H. J., Ormond, D. K., Menard, P., & Crossler, R. E. (2022). That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal*, 32(4), 888–926. <https://doi.org/10.1111/isj.12374>
- Kennison, S. M., & Chan-Tin, E. (2020). Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. *Frontiers in Psychology*, 11. <https://doi.org/10.3389/fpsyg.2020.546546>
- Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers and Security*, 125. <https://doi.org/10.1016/j.cose.2022.103049>
- Komarraju, M., & Karau, S. J. (2005). The relationship between the big five personality traits and academic motivation. *Personality and Individual Differences*, 39(3), 557–567. <https://doi.org/10.1016/j.paid.2005.02.013>
- Komarraju, M., Karau, S. J., Schmeck, R. R., & Avdic, A. (2011). The Big Five personality traits, learning styles, and academic achievement. *Personality and Individual Differences*, 51(4). <https://doi.org/10.1016/j.paid.2011.04.019>
- Mcbride, M., Carter, L., & Warkentin, M. (2012). *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies*. [www.dhs.gov](http://www.dhs.gov)
- Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, 34(4), 1203–1230. <https://doi.org/10.1080/07421222.2017.1394083>
- Papatsaroucha, D., Nikoloudakis, Y., Kefaloukos, I., & Pallis, E. (2021). A Survey on Human and Personality Vulnerability Assessment in Cyber-security: Challenges, Approaches, and Open Issues. In *arXiv*. <https://datareportal.com/reports/digital-2021-global-overview-report>
- Poeller, S., & Phillips, C. J. (2022). Self-Determination Theory - I Choose You! The Limitations of Viewing Motivation in HCI Research Through the Lens of a Single Theory. *CHI PLAY 2022 - Extended Abstracts of the 2022 Annual Symposium on Computer-Human Interaction in Play*, 261–262. <https://doi.org/10.1145/3505270.3558361>
- Sarstedt, M., Henseler, J., & Ringle, C. M. (2011). Multigroup analysis in partial least squares (PLS) path modeling: Alternative methods and empirical results. *Advances in International Marketing*, 22, 195–218. [https://doi.org/10.1108/S1474-7979\(2011\)0000022012](https://doi.org/10.1108/S1474-7979(2011)0000022012)
- Sharma, S., & Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among IT employees. *Computers and Security*, 120. <https://doi.org/10.1016/j.cose.2022.102774>
- Terracciano, A., & McCrae, R. R. (2006). Cross-cultural studies of personality traits and their relevance to psychiatry. In *Epidemiologia e Psichiatria Sociale* (Vol. 15, Issue 3). <https://doi.org/10.1017/S1121189X00004425>
- Tolah, A., Furnell, S. M., & Papadaki, M. (2019). A Comprehensive Framework for Understanding Security Culture in Organizations. *IFIP Advances in Information and Communication Technology*, 557. [https://doi.org/10.1007/978-3-030-23451-5\\_11](https://doi.org/10.1007/978-3-030-23451-5_11)



- Tyack, A., & Mekler, E. D. (2020). Self-Determination Theory in HCI Games Research: Current Uses and Open Questions. *Conference on Human Factors in Computing Systems - Proceedings, 2020-January*. <https://doi.org/10.1145/3313831.3376723>
- van der Schyff, K., Flowerday, S., & Lowry, P. B. (2020). Information privacy behavior in the use of Facebook apps: A personality-based vulnerability assessment. *Heliyon*, 6(8). <https://doi.org/10.1016/j.heliyon.2020.e04714>
- Van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021, August 17). A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3465481.3469199>
- Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers and Security*, 106. <https://doi.org/10.1016/j.cose.2021.102309>
- Weston, R., & Gore, P. A. (2006). A Brief Guide to Structural Equation Modeling. *The Counseling Psychologist*, 34(5), 719–751. <https://doi.org/10.1177/0011000006286345>
- Wijayanto, H., & Prabowo, I. A. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, 9(3), 395–399. <https://doi.org/10.32736/sisfokom.v9i3.1021>
- Zhou, M. (2015). Moderating effect of self-determination in the relationship between Big Five personality and academic performance. *Personality and Individual Differences*, 86, 385–389. <https://doi.org/10.1016/j.paid.2015.07.005>