International Journal of Innovations in Science & Technology

Synergizing Human Behavior and Cybersecurity using Psychometric Scale

Khurram Iqbal[1], Farhat M. Khan, Syeda Areej Asif[1], Shahreen Sheikh[1], Farees Fatima[1], Abdul Basit Abbasi[1], Farooq Iqbal[1]

[1]Hamdard University, Department of Computing, Faculty of Engineering Sciences and Technology, Karachi, Sindh, Pakistan

[2]Nazeer Hussain University,Karachi, Sindh, Pakistan

***Correspondence**: (KHURRAMIQBAL.NUST@GMAIL.COM)

Cybersecurity threats are increasingly shaped by human actions, making it crucial to comprehend the psychological elements that lead to vulnerabilities. This article examines the interplay between human behavior and cybersecurity through the use of psychometric scales to evaluate risk perception, decision-making, and adherence to security protocols. A quantitative research design was employed, using validated psychometric tools like the Human Aspects of Information Security Questionnaire (HAIS-Q) and the Cybersecurity Risk Perception Scale (CRPS). Data was gathered from 200 individuals in different organizational positions and examined using statistical techniques, such as correlation and regression analysis. Findings demonstrated a noteworthy association between psychological characteristics (e.g., risk tolerance, conscientiousness) and cybersecurity practices. People with a greater awareness of risks showed improved compliance with security policies, whereas individuals with lower levels of conscientiousness were more likely to engage in risky online activities. The results indicate that incorporating psychometric evaluations into cybersecurity training can improve threat management by customizing strategies according to personal behavior pat terns. This article adds to the expanding research on human-centered cybersecurity strategies, offering empirical data on the impact of psychometrics in enhancing security awareness and compliance. Future studies ought to investigate long-term impacts and cross- cultural assessments of psychometric scales within cybersecurity settings.

Keywords: Cybersecurity, Human actions, Psychometric assessment, Risk awareness, Adherence

Introduction:

Cybersecurity, previously largely technologically focused, has also experienced a paradigm revolution. While strong firewalls, advanced encryption, and intrusion detection systems are still crucial cornerstones of security, an uncomfortable reality has come to be understood: the most tenacious and most severe vulnerabilities quite often lie not in the code, but within the human operators themselves [1–5]. A great amount of research and incident reports repeatedly show that human error, misjudgment, and intentional insider actions account for an overwhelming majority of successful security breaches, from accidental clicks on phishing emails and password hygiene to the abuse of privileged access and no adherence to well-established protocols [1, 2]. This acknowledgment further emphasizes that cybersecurity is no longer merely a technical problem; it is, by nature and inescapably, a deeply human one. While there is ongoing and dazzling improvement in security technologies that are intended to counter evolving more sophisticated attacks from outside, the human factor is often the weakest link in the security chain [3, 4]. The reason is a multifaceted interplay of psychological, cognitive, and behavioral determinants. These can include poor security choices made because of a lack of knowledge about threats and best practice, cognitive biases (like optimism bias or underestimation of personal risk), misplaced confidence in systems or communications, levels of risk tolerance favouring convenience over security, resistance to altering habits, or even conscious neglect or bad faith [5, 6]. The implications go far beyond personal compromise, potentially to disastrous data breaches, substantial financial loss, disruption of operations, organizational reputational harm, and even national security threats. Helping to overcome this human weakness will involve transcending solely technical solutions and naively simplistic public awareness campaigns. A more profound, more systematic effort is needed—one rooted in the science of human behavior. Behavioral psychology provides valuable theories to explain the cognitive mechanisms, motivations, perceptions, and social factors that drive security choices and activity [6–9]. It is critical to understand why individuals make specific security decisions (or do not make secure decisions) in order to develop interventions that successfully alter behavior. Important psychological concepts become prime variables here: a person's innate risk tolerance or aversion (risk attitude), his/her security self-efficacy (security effectiveness belief in one's capability to carry out secure behavior), his/her faith in security technologies and security policies, his/her perceived threat susceptibility and severity, his/her intrinsic and extrinsic motivation to comply, and his/her social engineering susceptibility [7, 8]. In order to convert this psychological insight into practical recommendations and quantifiable results in the field of cybersecurity, tools that have been tested and validated are necessary. Here the psychometric scales offer a robust and systematic approach [10, 11]. Psychometrics, the discipline of theory and technique of psychological measurement, has rigorously constructed scales that can confidently measure attitudes, perceptions, beliefs, intentions to behave, and self-reported action on cybersecurity issues. These scales are more than mere tests of knowledge; they test the underlying psychological motivations.

By systematically applying such psychometric tools, organizations can gain a number of key goals:

(i) **Objective Profiling:** Go beyond rumor or hunch and develop evidence-based profiles of the security stance of the workforce across key psychological axes (e.g., risk tolerance, security confidence, compliance motivation).

(ii) **Identification of High-Risk Groups:** Identify specific individuals or more typically categories of employees demonstrating psychological profiles strongly associated with insecure behavior (e.g., high risk tolerance in combination with low perceived threat).

(iii) **Root Cause Diagnosis:** Identify the exact psychological obstacles (e.g., low self-efficacy, high perceived burden of compliance) inhibiting secure behavior in various groups throughout the organization.

(iv) **Baseline Measurement:** Set an empirical benchmark against which the efficacy of training interventions and policy initiatives can be strictly tested longitudinally.

(v) **Personalization and Targeting:** Facilitate the creation and delivery of targeted, evidence-driven interventions that are specifically designed to counteract the particular psychological vulnerabilities detected across various groups of employees [10, 12]. This can vary from highly targeted training modules and subtle messaging campaigns to adaptive policy enforcement systems and focused support systems.

The possible dividends are considerable. Psychometric-guided interventions have the potential to be much more effective and have a greater return on investment than generic, one-size-fits-all solutions. They enable resources to be targeted where the risk is highest and the need is most pressing. In addition, this method brings about a deeper awareness of organizational security culture, showing underlying problems and allowing cultural changes towards increased collective security awareness [9, 13]. This article squarely addresses the essential disconnect between knowing human factors in cybersecurity and applying truly effective, psychology-based solutions. Our main goal is to fill the gap between behavioral psychology and applied cybersecurity by examining the predictive value and pragmatic applicability of psychometric testing [10–13]. We will look at the ways certain, quantifiable psychological variables, measured through validated instruments, correlate with and can predict measurable security-relevant behaviors in real or simulated settings. Most importantly, we will also look at how lessons learned from these evaluations can be turned into practical strategies for crafting interventions that help improve demonstrably the security compliance and resilience at individual and group levels. In creating this empirical connection between psychological measurement and behavioral consequences, this study aims to offer organizations a science-based approach to building a stronger human firewall – helping ultimately to create a more resilient and comprehensive cybersecurity stance at a time when the human element is a critical dimension.

Objectives:

This article is intended to fill the vital gap between behavioral psychology and effective cybersecurity by determining the empirical worth of psychometric testing for the control of human risk. Its overarching objective is to rigorously find, operationalize, and establish fundamental psychological constructs—like cybersecurity risk tolerance, security self-efficacy, perceived threat severity/susceptibility, security system trust, and security compliance motivation—that have proven impact on security decision-making and behavior. Based on this premise, the research endeavors to empirically validate these psychometric tests for their predictive utility through the strict examination of their correlation with empirically measurable, real-world (or realistically simulated) cybersecurity actions, thus allowing for the identification of high-risk psychological individuals or groups. In addition, the research directly responds to the call for improvement by converting psychometric findings into an actionable design framework for crafting customized interventions—such as customized training, focused communication, adaptive nudges, or refined enforcement of policy—specifically tailored to meet the unique vulnerabilities uncovered by the assessments. To test this strategy, the research will establish and demonstrate methods for leveraging psychometric baselines to measure the relative effectiveness of these psychology-based interventions against generic controls. In addition to individual prediction and intervention, the study will investigate how cumulative psychometric data can give a rich diagnostic of organizational security culture, unearthing systemic strengths and deficits in workforce attitudes and perception. Lastly, the goal is to leave practitioners with validated psychometric tests, unambiguous implementation instructions, and specific recommendations for incorporating these measures into comprehensive human risk management strategies, enabling organizations to transcend generic solutions and act proactively to enhance their human firewall using science-based targeted actions.

Literature Review:

The ubiquitous nature of human behavior as a key weakness in cybersecurity is no longer debatable due to the overwhelming empirical evidence. Major breach analyses consistently identify human behavior—ranging from unintentional mistakes such as clicking on offending links or misconfiguring systems, to conscious policy breaches or insider attacks—as the source in an estimated 74-95% of incidents based on reports such as the Verizon Data Breach Investigations Report (DBIR) and IBM Security reports [1, 2, 4, 5]. This harsh reality highlights a basic paradigm shift: powerful technical defenses, as they are required, are not adequate apart from a focus on the psychological and behavioral aspects of security.

Cognitive Biases and Weaknesses: Human vulnerability reaches well beyond mere ignorance. Considerable research, summarized by researchers such as Harlington [7, 14], explores the cognitive basis for incompetent security decisions. Central cognitive biases routinely skew rational threat analysis and reaction:

(i) Optimism Bias: Users always underestimate their individual risk of becoming a victim of cyberattacks ("It won't happen to me"), resulting in complacency and neglect of safeguards [7, 14].

(ii) Habituation and Normalization of Deviance: Constant exposure to security alerts without harm causes users to get into the habit of ignoring or skipping them ("alert fatigue") [7]. In addition, slight policy breaches that are not punished can be normalized, gradually building up tolerance for risk [15].

(iii) Instant Gratification Bias: Security interventions add friction (e.g., difficult passwords, multi-factor authentication). Users naturally prefer short-term convenience to long-term security and will choose weaker, more convenient options [16].

(iv) Authority Bias and Trust Heuristics: Offenders capitalize on the natural tendency to trust communications that seem to be from authority (e.g., CEO scams) or known brands (phishing) [17]. Users use simple heuristics (e.g., professional-looking email presentation) that are easily hacked.

These biases function largely out of awareness, and for this reason, orthodox awareness training, which usually aims at conscious knowledge, is less successful than methods based on behavioral science [6, 18].

Theoretical Underpinnings for the Explanation of Security Behavior: To explain security behaviors systematically and predict them, researchers have applied proven psychological theories:

(i) Protection Motivation Theory (PMT): This is still a bedrock framework. PMT supposes that protective behavior is caused by a threat appraisal (perceived seriousness of the threat and perceived vulnerability to it) and a coping appraisal (belief concerning the effectiveness of the response advocated, self-efficacy for executing it, and perceived response cost). When threat appraisal is high and coping appraisal suggests the response as effective, achievable, and low-cost, then people will be prompted to practice the protective behavior. Psychometric tools are essential to measure quantitatively these central PMT elements (severity, susceptibility, efficacy of response, self-efficacy, response costs) in the context of cybersecurity [8, 19, 20]. For example, perceived severity of threat scales in terms of data breaches or a belief in being able to detect phishing emails translate directly into PMT constructs.

(ii) Theory of Planned Behavior (TPB): TPB focuses on the fact that behavioral intentions, motivated by attitudes towards the behavior, perceived subjective norms (pressure from others), and perceived behavioral control (like self-efficacy), are the best predictors of actual behavior. Attitudes towards security compliance, peer/management expectations, and perceived control over secure actions can be psychometrically assessed.

(iii) General Deterrence Theory (GDT): Is concerned with the application of sanctions (certainty, severity, swiftness) in preventing unwanted behaviors (e.g., policy violations). Relevant but relying too heavily on deterrence risks engendering resentment and neglecting intrinsic motivation barriers. Perceived sanction certainty/severity and their effect on compliance motivation can be measured using psychometrics.

(iv) Protection Action Decision Model (PADM): Emphasizes the phases of information processing (exposure, attention, comprehension) and threat-related protective action decision-making, of use in understanding behavior during active attacks.

Individual Differences: Personality and Beyond: Experimental evidence repeatedly shows that security behavior is shaped by stable individual differences. The supplied strong evidence [8] implicating the Big Five personality traits in security compliance. Their evidence shows:

(i) Conscientiousness: Strongly linked to compliance with security policies, thoroughness, and responsible action. Very conscientious people tend to be more dependable security players.

(ii) Neuroticism: Correlated with greater anxiety and watchfulness, which occasionally can result in superior threat spotting but also possibly to freezing or wild reaction under pressure. The connection is multifaceted and situation-specific.

(iii) Agreeableness and Openness: Exemplify mixed or weaker correlations at times correlated with increased susceptibility to social engineering (agreeableness) or curiosity-related risky exploration (openness).

(iv) Extraversion: Frequently correlated with greater risk-taking tendency, possibly making people more vulnerable. Although personality traits can provide useful information, they are only one facet. Situational variables, organizational climate, knowledge of the situation, and transient states (workload, stress) also strongly influence behavior [8, 21- 23]. Both trait measures and state-specific and situation-sensitive constructs must be used in combination for an exhaustive assessment.

Psychometric Measurement in Cybersecurity: Current Tools and Applications: The awareness of human factors has fueled the creation of psychometric scales tailored specifically to cybersecurity:

(i) Human Aspects of Information Security Questionnaire (HAIS-Q): Published and well-validated, this widely used measure scores knowledge, attitudes, and practices for a variety of security topics (e.g., password handling, email use, reporting incidents). Its widespread deployment yields solid benchmarks and proves the practicability of secure psychometrics. It frequently uncovers disturbing discrepancies between safe attitudes and actual secure practices.

(ii) Security Behavior Intentions Scale (SeBIS): Explicitly measures intentions to carry out crucial security behaviors (password creation, device updates, active awareness, handling of information), showing good predictive validity for the actual behavior in certain situations.

(iii) Cybersecurity Attitudes Scale (CAS): Scales overall attitudes towards how important and responsible cybersecurity is.

(iv) Risk Propensity Scales (General & Domain-Specific): Measures individual differences in risk-taking willingness, which is strongly applicable to following security policies.

(v) Self-Efficacy Scales (e.g., Phishing Self-Efficacy): Assess confidence in undertaking particular security tasks, a powerful predictor of action in PMT and TPB. They have been found useful within research environments for user population profiling, determination of training requirements, and assessment of the effectiveness of security awareness programs [9, 10, 24, 25]. HAIS-Q studies, for example, have reliably found particular attitude-behavior gaps and demographic or role-based differences in security stance.

The Critical Gap: Proactive Integration into Organizational Risk Management: In spite of the tangible worth of having an understanding of the psychological drivers of security behavior and the existence of proven measurement instruments, there exists a wide gap between research and practice in organizations [12, 13, 29]:

(i) Reactive vs. Proactive Use: Psychometrics tend to be used reactively – after the breach for examination and ad hoc for training assessments. Their proactive, systematic adoption as part of regular human risk management practices is uncommon [13]. Companies do not have models for ongoing psychological risk scoring along with technical vulnerability scoring.

(ii) Lack of Predictive Targeting: Although measures such as HAIS-Q capture snapshots, they are rarely applied in predicting the levels of individuals or groups at risk before incidents and for dynamically tailoring interventions according to changing psychometric profiles [10, 12]. The capabilities for establishing "high-risk" psychological profiles (e.g., high risk tolerance + low self-efficacy + low perceived threat) remain operationally unused.

(iii) Integration with Technical & Process Controls: Psychometric information is isolated from Security Information and Event Management (SIEM) systems, access control decisions, and security operation centers (SOCs). There is little examination of how psychological risk indicators might drive adaptive security controls (e.g., increased monitoring for high-risk profiles, streamlined workflows for low self-efficacy users) [10].

(iv) Privacy and Ethical Issues: Organizations are reluctant because of perceived privacy invasions and ethical issues related to profiling psychological characteristics of employees without clear guidelines for ethical implementation [19].

(v) Transcending Compliance to Resilience: *Attention is usually paid to policy compliance. Psychometrics contain the promise to quantify and promote more profound security awareness, individual accountability, and adaptive resilience – attributes most important for addressing new risks – but this promise is underexploited [9].*

Research Design Method:

This research utilized a quantitative, cross-sectional survey approach to examine the link between psychometric con structs and cybersecurity actions. The design was chosen to (i) determine statistical connections between psychological characteristics and security measures,

(ii) gather snapshot data from various organizational roles, and (iii) facilitate comparative analysis among demographic subgroups. Data were collected from a sample of 200 individuals representing diverse organizational roles, including IT professionals, administrative staff, and management personnel. Participants were recruited through professional networks, online platforms, and partnerships with various organizations Participants were required to hold positions involving frequent use of digital systems. Analysis of survey responses from over 200 individuals revealed key insights into their cybersecurity knowledge and behaviors. The group was mainly comprised of young individuals (ages 18-24), mostly female, well-educated (largely holding Bachelor's degrees), and included students (in fields such as Computer Science, Engineering, Medical Sciences) as well as working professionals. Importantly, over 90% indicated they had no formal cybersecurity education. Two validated psychometric instruments were employed: (i) the Human Aspects of Information Security Questionnaire (HAIS-Q) and (ii) the Cybersecurity Risk Perception Scale (CRPS) The collected data were cleaned and analyzed using Python software. Descriptive statistics were first applied to summarize both demographic and psychometric information Subsequent inferential analyses were conducted, specifically (i) Pearson correlation analysis to investigate the connections between psychological characteristics and cybersecurity actions, and (ii) multiple regression analysis to assess the predictive strength of factors like risk perception and conscientiousness regarding adherence to cybersecurity protocols.

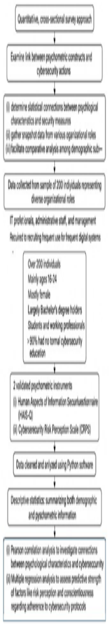
Quantitative, cross-sectional survey approach
Examine link between psychometric constructs and cybersecurity actions
(i) determine statistical connections between psychlogical characteristics and security measures
(ii) gather snapshot data from various oganizational roles
(iii) facilitate comparative analysis among demographic sub–
Data collected from sample of 200 indyiduals representing diverse organizational roles
IT profet ionals, administrative staff, and management
Reciured to recruiting frequent use for frequent digital systems
Over 200 individuals
Mainly ages 16-24
Mostly female
Largely Bachelor's degree holders
Students and working professionals
> 90% had no tormal cybersecurity education
2 validated psychometric instruments
(i) Human Aspects of Information Securiuestionnaire (HAIS-Q)
(ii) Cybersenecurity Risk Perception Scale (CRPS)
Data cleaned and anlyzed using Python software
Descriptive statistics: summarizing both demographic and pyschometric information
(i) Pearson correlation analysis to investigate connections between psychological characteristics and cybersecurity
(ii) Multiple regression analysis to assess predictive strength of factors like risk perception and conscientiousness regarding adherence to cybersecurity protocols

Figure 1 illustrates the fundamental connections between psychological factors and behaviors related to cybersecurity.

Correlation Analysis:

Correlation coefficient [22] measures linear association between two continuous variables: (i) X: HAIS-Q Knowledge score (scale: 1–5) and (ii) Y: CRPS Perceived Vulnerability score (scale: 1–5)

Psychological Attributes:

This includes personal traits such as risk tolerance, conscientiousness, and emissivity, which affect how individuals perceive and react to cybersecurity threats. Risk Perception & Decision-Making – These characteristics affect how people evaluate security threats, influencing their probability of adhering to security measures or participating in risky actions. Cybersecurity Practices. This denotes behaviors such as compliance with security protocols, handling of passwords, and vulnerability to phishing schemes, which diffuse to psychological inclinations.

Psychometric Scales (HAIS-Q & CRPS):

These validated tools evaluate the human dimensions of cybersecurity by measuring differences in individual risk awareness and compliance behaviors Statistical Analysis (Correlation & Regression) – This phase determines connections between psychological characteristics and cybersecurity actions, revealing trends that businesses can utilize for security education. Human-Focused Cyber security Method – This study advocates for customized measures, allowing organizations to modify their security training according to employees' psychological characteristics.

Results and Discussion:

Evaluation with the HAIS-Q tool revealed a continuous gap between knowledge and behavior across various areas. Although respondents showed fairly solid knowledge (e.g., Internet Use: 4.2/5) and favorable attitudes (e.g., Internet Use Attitude: 4.4/5), their behaviors were considerably less robust. The gap was most pronounced in Password Management (Behavior: 2.3/5), especially concerning frequent password updates. In comparison, acknowledgment of the significance of HTTPS (Internet Use Attitude) was the most robust aspect. An examination of Cybersecurity Risk Perception (CRPS) unveiled a troubling contradiction: participants recognized the significant seriousness of possible cyberattacks (avg. 3.5/5, for instance, "A violation could greatly affect my life"), while viewing their individual vulnerability as minimal (avg. 2.8/5, for example, "I perceive myself at risk of dangers at my job": 2.3/5). This indicates a common mindset of "it won't affect me." Correlation analysis was done in Python Jupyter Notebook [22]. Elevated HAIS-Q Knowledge scores showed a negative correlation with perceived vulnerability (r = -0.4), suggesting that greater knowledge might, counterintuitively, diminish feelings of personal risk. In contrast, elevated HAIS-Q

Behavior scores showed a positive correlation with perceived severity (r = 0.3), suggesting that individuals who engage in safer behaviors have a better comprehension of the possible outcomes. Comparing groups provided useful insights. Individuals with formal cybersecurity education exhibited notably enhanced security habits (15% higher HAIS-Q Behavior scores) compared to their untrained counterparts, emphasizing the real-world effect of training. Participants aged 35 and older viewed the severity of attacks more intensely (4.1 compared to 3.2 for those aged 18-24), while IT experts, as expected, demonstrated greater knowledge (4.5 versus 3.1 for non-IT individuals).

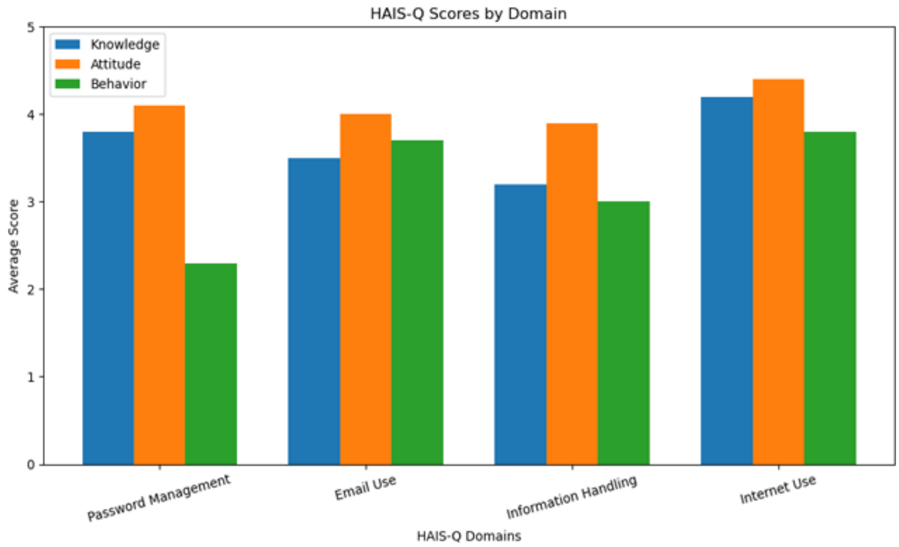

Figure 2: HAIS-Q scores by Domains

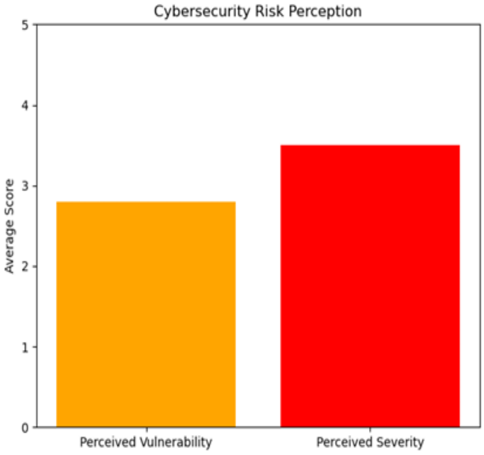

Figure 3: Cybersecurity Risk Perception

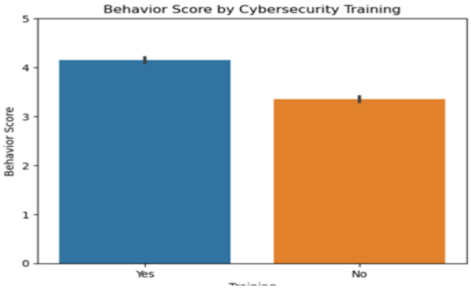

Figure 4: Behavior Score by Cybersecurity Training

Conclusion:

This research reveals a significant gap between cybersecurity awareness, risk assessment, and safety practices in a largely youthful, inexperienced group. The minimal perceived risk despite acknowledged seriousness, along with the significant knowledge-behavior disparity (particularly in password handling), underscores a major security weakness. The significant positive effect of formal training offers clear proof for specific educational measures to close this gap and enhance cyber hygiene. This research demonstrates that psychometric scales can efficiently evaluate and forecast cybersecurity behaviors. Organizations ought to incorporate psychological evaluations into security training to mitigate behavioral weaknesses. Future studies should investigate AI-based psychometric instruments for immediate threat reduction.

Acknowledgement:

The authors sincerely appreciate the Department of Computing, Faculty of Engineering Sciences and Technology, Hamdard University, Pakistan for their technical assistance with this research project.

References:

[1] C. Faklaris, L. Dabbish, and J. I. Hong, "Do they accept or resist cybersecurity measures? Development and vali dation of the 13-item Security Attitude Inventory (SA-13)," arXiv preprint arXiv:2204.03114, 2022.

[2] D. J. Howard, "Development of the Cybersecurity Attitudes Scale and modeling cybersecurity behavior and its antecedents," M.S. thesis, University of South Florida, 2018. [Online]. Available: https://digitalcommons.usf.edu/etd/7306

[3] H.-Y. Huang et al., "Smartphone Security Behavioral Scale: A new psychometric measurement for smartphone security," arXiv preprint arXiv:2007.01721, 2020.

[4] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," Computers & Security, vol. 42, pp. 165–176, 2014.

[5] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors," Heliyon, vol. 3, no. 7, e00346, 2017.

[6] M. Gratian, S. Bandi, M. Cukier, A. Ginther, and B. Olson, "Correlating human traits and cybersecurity behavior intentions," Computers & Security, vol. 73, pp. 345–358, 2018.

[7] B.-Y. Ng, A. Kankanhalli, and Y. C. Xu, "Studying users' computer security behavior: A health belief perspective," Decision Support Systems, vol. 46, no. 4, pp. 815–825, 2009.

[8] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," Computers in Human Behavior, vol. 24, no. 6, pp. 2799–2816, 2008.

[9] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," Computers & Security, vol. 31, no. 1, pp. 83–95, 2012.

[10] C. Posey, T. L. Roberts, and P. B. Lowry, "The impact of organizational commitment on insiders' motivation to protect organizational information assets," Journal of Management Information Systems, vol. 32, no. 4, pp. 179–214, 2015.

[11] A. McCormac et al., "Individual differences and information security awareness," Computers in Human Behavior, vol. 69, pp. 151–156, 2017.

[12] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," Computers & Security, vol. 49, pp. 177–191, 2015.

[13] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding no malicious security violations in the workplace: A composite behavior model," Journal of Management Information Systems, vol. 28, no. 2, pp. 203–236, 2011.

[14] J. D'Arcy and T. Herath, "A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings," European Journal of Information Systems, vol. 20, no. 6, pp. 643–658, 2011.

[15] T. Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organizations," European Journal of Information Systems, vol. 18, no. 2, pp. 106–125, 2009.

[16] M. Warkentin, A. C. Johnston, and J. Shropshire, "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," European Journal of Information Systems, vol. 20, no. 3, pp. 267–284, 2011.

[17] R. E. Crossler and F. Bélanger, "An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument," ACM SIGMIS Database, vol. 45, no. 4, pp. 51–71, 2014.

[18] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," MIS Quarterly, vol. 34, no. 3, pp. 523–548, 2010.

[19] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from habit and protection motivation theory," Information & Management, vol. 49, no. 3–4, pp. 190–198, 2012.

[20] R. B. Cialdini, "Crafting normative messages to protect the environment," Current Directions in Psychological Science, vol. 12, no. 4, pp. 105–109, 2003.

[21] AlHogail, A. (2015). Design and validation of information security culture framework. Computers in Human Behavior, 49, 567–575.

[22] Hadlington, L., & Parsons, K. (2017). Can education and training really help improve cybersecurity? A psychological perspective. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 11(4), Article 5.

[23] Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. Decision Support Systems, 51(3), 434–445.

[24] Alqahtani, H. A., & Thurasamy, R. (2021). Information security awareness: Literature review and integrative framework for future research. Telematics and Informatics, 58, 101537.

[25] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—A human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122–131.