FYP

FYP-038/FL24

Synergizing Human Behavior and Cybersecurity using Psychometric Scale

AREEJ ASIF,SHAHREEN SHEIKH,FAREES FATIMA

SUPERVISOR NAME **KHURRAM IQBAL**

Department of Computing, FEST

Hamdard University

Summary

- Problem Statement
- Objective
- FYP Scope
- Our methodology
- FYP Deliverables
- Literature Review
- Demo of 100% of Work
- Experimental Evaluations & Results
- Test Plan & Test Cases
- References

Problem Statement

Cybersecurity today is not just a technological challenge but also a behavioral one. Although encryption, AI, and real-time threat detection systems have matured, human error remains the weakest link with studies indicating over 90% of successful cyberattacks stem from user mistakes rather than software flaws.

Common vulnerabilities include:

- Falling for phishing scams.
- Using weak or repeated passwords.
- Ignoring organizational security protocols.
- Modern cybersecurity demands an understanding of how individuals interact with systems, make decisions under pressure, and perceive risk. Tools like HAIS-Q and SeBIS offer a window into user behavior, but there's a growing need for adaptive, culturally-aware, real-time strategies that evolve with users and threats alike.

Objective

The project aimed to design a human-centered cybersecurity framework that merges technical tools with behavioral science. Specific objectives included:

- Integrate behavioral psychology (e.g., psychometric scales like HAIS-Q and CRPS) into cybersecurity practices.
- Identify and profile behavioral personas (e.g., "Naïve Greenhorns", "Reliable Troupers") for tailored security interventions.
- Develop personalized cybersecurity training using insights from psychometric analysis.
- Evaluate existing frameworks (like TAM and CVF) for strengths and gaps.
- Promote a cybersecurity culture led by leadership and reinforced through feedback loops.
- Build scalable, cost-effective tools usable across industries and organizations.

FYP Scope

Included in Scope:

- Analyzing human error in cybersecurity (e.g., phishing, weak passwords)
- Developing psychometric profiling using HAIS-Q and CRPS
- Behavioral interventions: nudging, gamification, feedback systems
- Cultural and leadership influence on cybersecurity behaviors
- Data collection from diverse roles and demographics
- Development of a modular, scalable analysis system using Python and Google Forms

Excluded from Scope:

- Creation of new technical security tools (e.g., antivirus software)
- Industry-specific case studies
- Longitudinal tracking (time-bound post-implementation changes)
- Real-time tracking (due to system and privacy constraints)

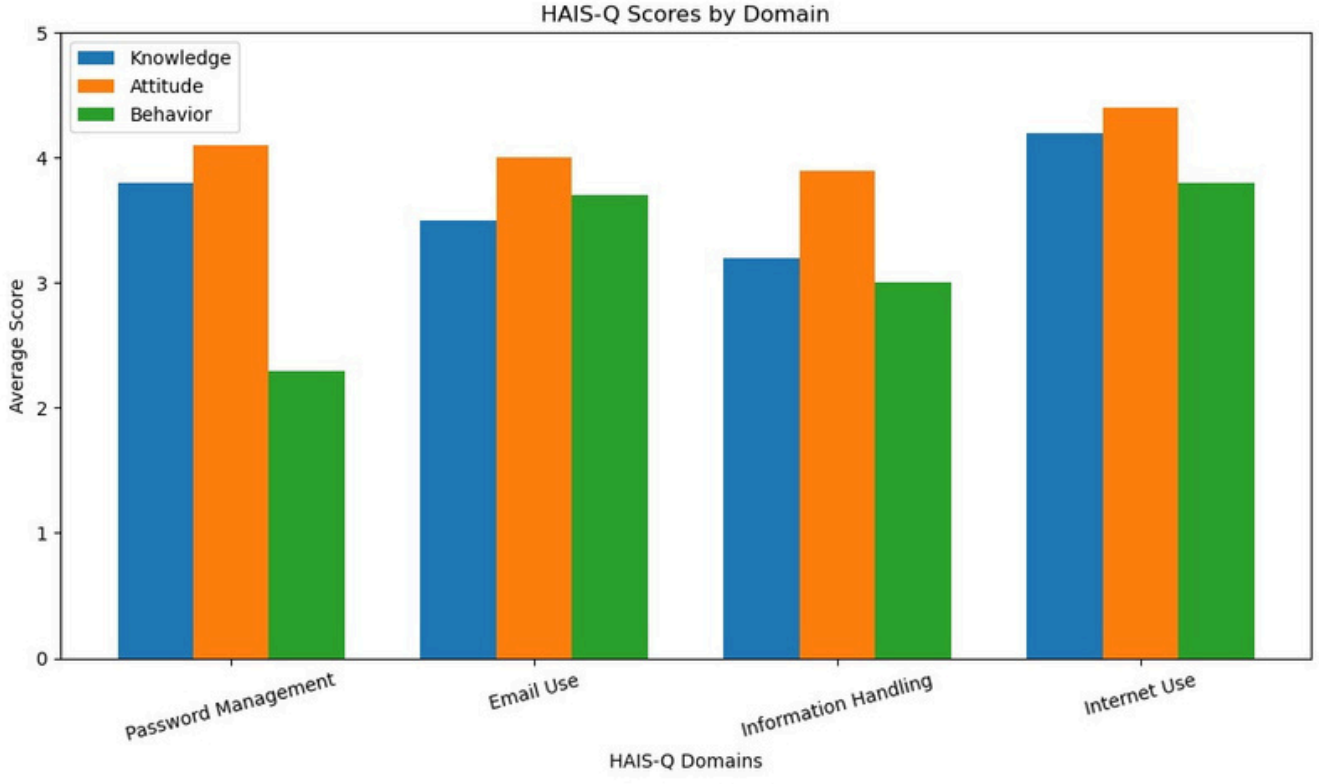
Our Methodology

We adopted a mixed-method, incremental development approach combining psychometric analysis and software engineering. Key components included:

- **Incremental Software Development Model:** Allowed for step-wise, flexible updates and feedback integration.
- **Participant Selection:** Diverse group from IT, admin, and non-tech roles.
- **Psychometric Tools:** HAIS-Q and CRPS were used to assess attitudes, knowledge, and behavior.
- **Data Collection:** Google Forms + Google Sheets for structured response logging.
- **Statistical Analysis:** Conducted in Python using pandas, matplotlib, and scipy.
- **Behavioral Profiling:** Created personas based on data patterns.
- **Customized Training Recommendations:** Based on risk type and psychometric scores.

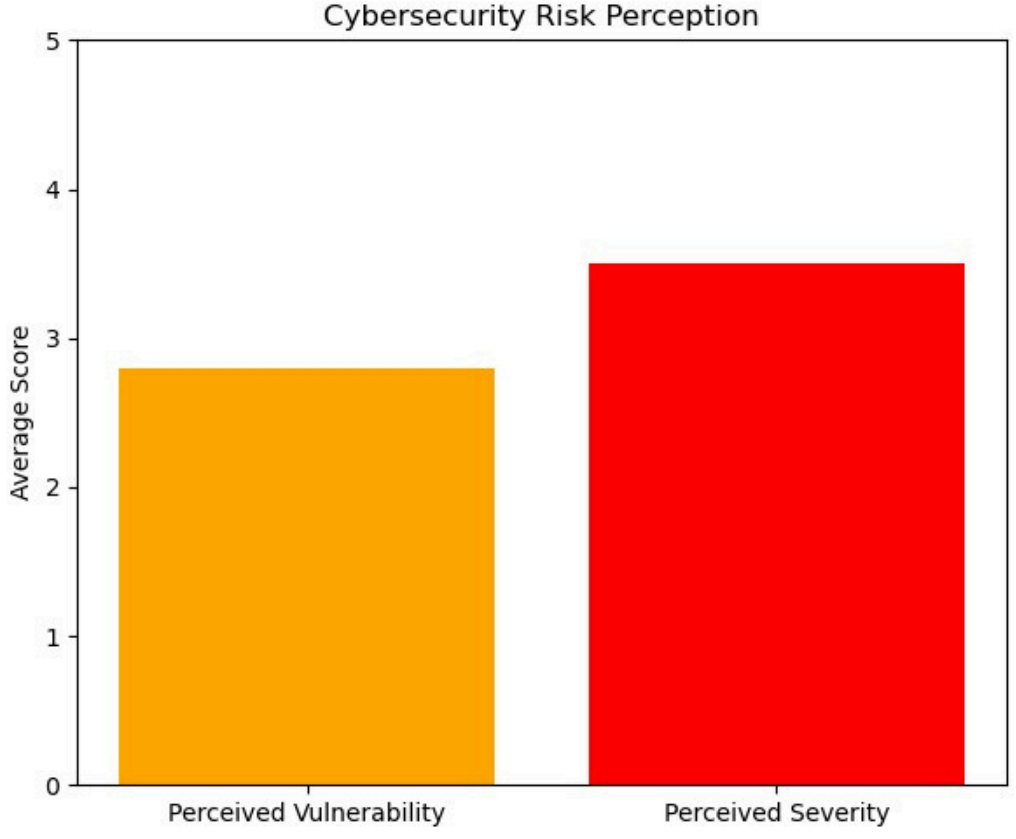
GRAPHS

Figure 1: Highlighted the variation in HAIS-Q scores across different cybersecurity domains, with Internet use scoring highest in knowledge but password management scoring lowest in behavior.



GRAPHS

Figure 2: Illustrated the discrepancies between participants' perceived risk and actual cybersecurity practices, emphasizing the "false sense of security" trend.



GRAPHS

Figure 3: Compared behavior scores based on cybersecurity training, visually confirming the positive impact of formal education.

FYP Deliverables

Deliverable	Description
Questionnaire Design	Custom HAIS-Q and CRPS instruments
Data Collection Report	Responses from ~200 diverse participants
Python-Based Analysis Scripts	Scripts for correlation, regression, and profiling
Behavioral Personas	Categorized profiles like "Greenhorns" & "Troupers"
Personalized Recommendations	Tailored training guidelines based on behavior
Documentation	Complete project report + presentation
System Design	Modular pipeline from survey to analysis to reporting

Literature Review

- Cybersecurity evolved from tech-only focus to a human behavior concern.
- Frameworks like HAIS-Q and SeBIS help assess awareness and action.
- Human typologies (Greenhorns, Troupers) allow custom training.
- Challenges: self-reported bias, cultural blind spots, real-time data gaps.

Research gaps:

- Lack of IoT-specific human behavior studies.
- No cross-cultural validations.
- Few AI-based, adaptive training programs.
- Future direction includes gamification, biometric indicators, AI-enhanced psychometrics

Demo of 100% of Work

Modules Demonstrated:

- Google Form questionnaire capturing HAIS-Q and CRPS data.
- Automated logging to Google Sheets.
- **Python scripts showing:**

1. Statistical summaries
2. Correlation analysis (e.g., Knowledge vs. Vulnerability)
3. Behavioral profiling

- Visualizations: Risk disconnect graphs, score distributions, persona comparisons
- Final report generation and recommendation module.

All functionalities executed successfully during final demonstration.

Experimental Evaluations & Results

Testbed:

- ~200 participants (students, IT staff, admin personnel)
- Tools: Google Forms, Google Sheets, Python, Cloud Storage

Key Findings:

- **Knowledge-Behavior Gap:** Avg. internet knowledge = 4.2/5, but password behavior = 2.3/5
- **Risk Disconnect:** High threat awareness (3.5/5) but low perceived vulnerability (2.8/5)
- **Training Effect:** Trained users scored 15% better on secure behaviors

Demographics:

1. Older users perceived higher risk
2. IT professionals performed better but still had behavior gaps

Visualization Highlights:

- HAIS-Q domain scores
- Trained vs. untrained behavior bar chart
- Risk perception vs. actual behavior graph

Test Plan & Test Cases

Test Case ID Description Expected Result Status
TC-01 Validate Google Form submission Responses logged correctly ✅ Pass
TC-02 Test cloud storage backup Data securely stored ✅ Pass
TC-03 Python analysis accuracy Correct statistical outputs ✅ Pass
TC-04 Generate final report Personalized, correct profiles ✅ Pass
TC-05 Multi-user form response Handles concurrent inputs ✅ Pass

Reference

1. A.McCormac et al.,"Individual differences and information security awareness," Computers in Human Behavior, vol. 69, pp. 151–156, 2017.
2. J.Shropshire,M.Warkentin,andS.Sharma,"Personality,attitudes,andintentions:Predictinginitialadoptionof information security behavior," Computers & Security, vol. 49, pp. 177–191, 2015.
3. K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding no malicious security violations in the workplace:Acompositebehaviormodel,"JournalofManagementInformationSystems,vol.28,no.2,pp.203–236, 2011.
4. J.D'Arcy and T.Herath,"A reviewand analysisof deterrence theory in the ISsecurity literature:Making sense of the disparate findings," European Journal of Information Systems, vol. 20, no. 6, pp. 643–658, 2011.
5. T.HerathandH.R.Rao,"Protectionmotivationanddeterrence:Aframeworkforsecuritypolicycompliancein organizations," European Journal of Information Systems, vol. 18, no. 2, pp. 106–125, 2009.
6. M.Warkentin,A.C.Johnston,andJ.Shropshire,"Theinfluenceoftheinformalsociallearningenvironmenton informationprivacypolicycomplianceefficacyandintention,"EuropeanJournalofInformationSystems,vol.20,no. 3, pp. 267–284, 2011.
7. R.E.CrosslerandF.Bélanger,"Anextendedperspectiveonindividualsecuritybehaviors:Protectionmotivation theory and a unified security practices (USP) instrument," ACM SIGMIS Database, vol. 45, no. 4, pp. 51–71, 2014.
8. 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.
9. 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.

Reference

[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.