Synergizing Human Behavior and Cybersecurity using Psychometric Behavioral Analysis

Final Year Project Report

Submitted by

Syeda Areej Asif (2276-2021)
Shahreen Sheikh (1771-2021)
Farees Fatima (1755-2021)

Supervisor

Dr. Khurram Iqbal

In partial fulfilment of the requirements for the degree of
Bachelor of Science in Software Engineering
2021-2025

Faculty of Engineering Sciences and Technology

Hamdard Institute of Engineering and Technology

Hamdard University, Main Campus, Karachi, Pakistan

Certificate of Approval

Faculty of Engineering Sciences and Technology

Hamdard Institute of Engineering and Technology
Hamdard University, Karachi, Pakistan

This project "_____" is presented by _____ under the supervision of their project advisor and approved by the project examination committee, and acknowledged by the Hamdard Institute of Engineering and Technology, in the fulfillment of the requirements for the Bachelor degree of _____.

_____
Dr. Khurram Iqbal
(Project Supervisor)

_____
In-charge FYP-Committee

_____
(Dean, FEST)

_____
Chairman
(Department of Computing)

Authors' Declaration

We declare that this project report was carried out in accordance with the rules and regulations of Hamdard University. The work is original except where indicated by special references in the text and no part of the report has been submitted for any other degree. The report has not been presented to any other University for examination.

Dated:

Authors Signatures:

_____
Syeda Areej Asif

_____
Shahreen Sheikh

_____
Farees Fatima

Plagiarism Undertaking

We, **Syeda Areej Asif**, **Shahreen Sheikh** and **Farees Fatima** solemnly declare that the work presented in the Final Year Project Report titled **"Synergizing Human Behavior and Cybersecurity using Psychometric Behavioral Analysis"** has been carried out solely by ourselves with no significant help from any other person except few of those which are duly acknowledged. We confirm that no portion of our report has been plagiarized and any material used in the report from other sources is properly referenced.

Dated:

Authors Signatures:

_____
Syeda Areej Asif

_____
Shahreen Sheikh

_____
Farees Fatima

Acknowledgments

"In the name of Allah, the most Beneficent, the most Merciful"

Firstly, we would like to extend our gratitude to Allah Almighty for enabling us to work on this project and in helping us to complete our tasks before the final evaluation. We feel privileged to express our deepest sense of gratitude and sincere thanks to our project advisor Dr. Khurram Iqbal for his guidance and valuable support. By replying to our inquiries and indicating our mistakes. His insightful feedback and constructive criticism have enriched our work, helping us overcome challenges and achieve meaningful outcomes. We are immensely grateful for the opportunity to learn from him and for the encouragement he has provided every step of the way.

We would like to extend our heartfelt and sincere gratitude to the Head of the Department Dr. Shahid Munir and Hamdard University for providing us with the opportunity to undertake this project. Your unwavering support, encouragement, and guidance have been instrumental in enabling us to explore and expand our knowledge in this field. This project has been an invaluable learning experience, and we are deeply grateful for the resources and platform extended to us. Your belief in our potential has inspired us to strive for excellence, and we hope to contribute meaningfully to our field as a result of this enriching experience. Thank you for your trust and support.

Document Information

Table 1: Document Information

Customer	Hamdard University
Project Title	Synergizing Human Behavior and Cybersecurity using Psychometric Scale
Document	Final Year Project Report
Document Version	1.0
Identifier	<FYP-038/ FL24>Final Report
Status	Final
Author(s)	Khurram Iqbal, Farhat M. Khan, Syeda Areej Asif, Shahreen Sheikh, Farees Fatima, Abdul Basit Abbasi, Farooq Iqbal
Approver(s)	Respective Project Supervisor(s)
Issue Date	

Definition of Terms, Acronyms, and Abbreviations

Table 2: Definition of Terms, Acronyms, and Abbreviations

HAIS-Q	Human Aspects of Information Security Questionnaire – A psychometric tool used to assess cybersecurity knowledge, attitudes, and practices.
CRPS	Cybersecurity Risk Perception Scale – A psychometric scale used to measure perceived cybersecurity risks and personal vulnerability.
SIEM	Security Information and Event Management – A system that collects and analyzes security-related data in real time.
IoT	Internet of Things – A network of physical devices connected to the internet.
AI	Artificial Intelligence – The simulation of human intelligence by computer systems.
Python	A high-level programming language used for statistical analysis and data processing in this project.
Cloud Storage	Online data storage services used to securely store project datasets and documents.

Abstract

The increasing complexity of cybersecurity threats requires organizations to adopt strategies that combine technological solutions with a deep understanding of human behavior. While cybersecurity systems continue to evolve, human error remains a critical vulnerability. Mistakes such as falling for phishing scams, using weak or repeated passwords, and disregarding security protocols are still common entry points for cyber attackers.

This literature review consolidates findings from multiple studies, with a particular focus on psychometric frameworks like the Human Aspects of Information Security Questionnaire (HAIS-Q) and the Cybersecurity Risk Perception Scale (CRPS). It also examines the growing importance of biometric tracking and real-time behavioral monitoring in analyzing how users interact with cybersecurity systems.

The review highlights that factors such as cognitive biases, individual risk perceptions, organizational culture, and the overall effectiveness of cybersecurity training programs play substantial roles in shaping user security behavior. Behavioral typologies introduced in recent studies categorize users into groups like “Naïve Greenhorns” and “Reliable Troupers,” which suggests the necessity of customized training programs instead of applying uniform security policies.

Despite significant progress, several gaps persist in current research. These include limited focus on Internet of Things (IoT) security behaviors, insufficient cross-cultural validation of psychometric tools, and a lack of dynamic, real-time systems that can adapt to rapidly changing cybersecurity landscapes. Additionally, most existing studies disproportionately focus on Western user populations, limiting their relevance to more diverse global environments.

Future research should emphasize the integration of real-time behavioral tracking, AI-powered data analytics, and culturally adaptive cybersecurity tools to build more comprehensive, human-centered security strategies. Shifting the industry’s perception from viewing users

as security liabilities to recognizing them as active defenders can lead to more resilient cybersecurity systems that effectively account for human behavior and its complexities.

Keywords

Cybersecurity, Human Behavior, Psychometric Assessment, Risk Perception, Security Awareness, Behavioral Profiling, HAIS-Q, CRPS, Cognitive Biases, Security Compliance, Personalized Security Training, Risk Tolerance, Security Self-Efficacy, Cybersecurity Risk Perception, Conscientiousness, Cybersecurity Culture, Behavioral Psychology, Protection Motivation Theory, Theory of Planned Behavior, Adaptive Security Controls.

Table of Contents

5. **Implementation**
    5.1 Proposed System Architecture/Design
    5.2 Functional Specifications
    5.3 Non-Functional Specifications
    5.4 Testing
    5.4.1 Purpose of Testing
    5.4.2 Test Cases
6. **Experimental Evaluations & Results**
    6.1 Evaluation Testbed
    6.2 Results and Discussion
7. **Conclusion and Discussion**
    7.1 Strengths of the Project
    7.2 Limitations and Future Work
    7.3 Reasons for Failure – If Any
8. **References**

CHAPTER 1

INTRODUCTION

- **Motivation**

This initiative is driven by the urgent need to address cybersecurity's human weaknesses, which, in spite of technological developments, continue to be a major source of breaches. Strong technical systems continue to be undermined by human error, such as falling for phishing schemes, using weak passwords, and breaking policies. There is a vital chance to create creative, human-centered interventions that enhance technical solutions and drastically lower risks, especially in light of the financial and reputational harm that cyberattacks may bring.

By combining technical methods with behavioural insights, the study also aims to close current research gaps. Fewer studies examine the significance of organisational culture and human factors in cybersecurity, whereas the majority concentrate on technologies and systems. By closing this gap, the project hopes to provide a thorough and expandable framework that businesses from other sectors can use, making a theoretical and practical contribution to the subject.

Personally, I am passionate about using insights from behavioural sciences and cybersecurity to solve real-world challenges, and this project fits with that enthusiasm. By enabling people to actively participate in safeguarding sensitive data, it presents an opportunity to improve digital safety for both individuals and organisations. The project's ultimate goal is to promote a proactive security culture that will ensure resilience in a world that is becoming more and more digital.

- **Problem Statement**

Cybersecurity is no longer just about technology—it’s about people. While encryption, artificial intelligence (AI), and real-time threat detection have significantly improved security, human error remains one of the biggest weaknesses. Studies show that over 90% of successful cyberattacks exploit human mistakes rather than technical flaws.

Phishing scams, weak passwords, and social engineering attacks prove that even the most advanced security systems can be compromised if people aren't careful. This is why modern cybersecurity isn't just about firewalls and antivirus software—it's about understanding human behavior, decision-making, and the way people interact with technology.

To address this, researchers have developed tools like the Security Behavior Intentions Scale (SeBIS) and the Human Aspects of Information Security Questionnaire (HAIS-Q). These frameworks assess how users behave in security-sensitive situations, offering insights that help organizations improve security policies. However, as the digital landscape evolves—especially with interconnected systems like the Internet of Things (IoT)—new challenges arise, requiring cybersecurity strategies that adapt to both technological changes and human tendencies.

- **Goals and Objectives**

This project's main goal is to provide an all-encompassing framework that combines technical tactics with insights into human behaviour to improve cybersecurity. Despite technological developments, human errors—such as phishing vulnerability and non-compliance with security protocols—remain key weaknesses. This initiative intends to lower risks, enhance compliance, and promote a proactive security culture within organisations by tackling these human-centric issues and coordinating them with technology solutions.

In order to do this, the project has a number of important goals. Its first goal is to create a cohesive cybersecurity framework that combines organisational tactics, behavioural treatments, and technical solutions. Businesses of all sizes and sectors will be able to use this platform. In order to improve user engagement and awareness, the project also intends to address common human vulnerabilities using customised interventions, such as gamified training modules and real-world simulations.

Another goal is to strengthen cybersecurity culture by highlighting the part that leadership plays in encouraging communication and

compliance. The project also intends to assess current frameworks, such the Competing Values Framework (CVF) and the Technology Acceptance Model (TAM), finding weaknesses and suggesting enhancements. Additionally, it aims to offer widely applicable, scalable, and reasonably priced technologies that support both scholarly research and real-world cybersecurity applications.

- **Project Scope**

The primary goal of this research is to address the crucial nexus in cybersecurity between technical tactics and human behaviour. It seeks to investigate the ways in which human error—such as phishing, using weak passwords, and disregarding policies—contributes to security breaches and to create countermeasures. Designing customised training programs, putting behavioural interventions like nudging and feedback loops into practice, and examining how organisational culture and leadership contribute to the development of a security-first environment are important areas of study. The research also assesses how well technical tools, such AI-based threat detection and encryption systems, can be used to lower risks.

The scope does not include sector-specific research that is restricted to a single industry or solely technical solutions, such as the creation of new technologies. Additionally beyond the project's period are longitudinal studies, which call for monitoring the long-term effects of interventions. The project's emphasis on scalable and flexible solutions that work in a variety of industries guarantees a comprehensive approach to cybersecurity that closes the gap between technical and human-centric tactics.

CHAPTER 2

RELEVANT BACKGROUND & DEFINITIONS

2.1 Background

The field of cybersecurity has evolved rapidly over the past few decades, driven by the growing dependence on digital systems and the increasing sophistication of cyber threats. Despite significant advancements in technical solutions—such as encryption, firewalls, and AI-based threat detection—human factors remain a critical vulnerability. Studies estimate that over 90% of cybersecurity breaches are attributable to human errors, including falling for phishing attacks, using weak passwords, or neglecting organizational security policies.

The interplay between technical tools and human behavior has garnered attention in recent research, emphasizing the need for an integrated approach. Behavioral insights from psychology and organizational studies highlight the role of cognitive biases, stress, and leadership in influencing cybersecurity practices. At the same time, technical frameworks like the Technology Acceptance Model (TAM) and Competing Values Framework (CVF) provide valuable perspectives on user adoption and cultural dynamics in cybersecurity.

This project builds on these insights to address critical research gaps, including the lack of standardized methodologies for measuring cybersecurity culture, the limited integration of human behavior into technical strategies, and the insufficient exploration of scalable solutions that can be applied across industries.

2.2 Definitions

- **Cybersecurity**:
  The practice of protecting systems, networks, and data from unauthorized access, theft, and damage through a combination of technical, procedural, and human measures.

- **Human Factors in Cybersecurity:**
  The psychological, behavioral, and organizational elements that influence an individual's interaction with cybersecurity systems and policies, often contributing to errors and vulnerabilities.
- **Phishing:**
  A type of social engineering attack where individuals are tricked into providing sensitive information, such as login credentials, by fraudulent emails or websites.
- **Technology Acceptance Model (TAM):**
  A framework that examines how perceived usefulness and ease of use influence an individual's acceptance of technology.
- **Competing Values Framework (CVF):**
  An organizational culture model that evaluates values like innovation, control, and collaboration to understand cultural influences on behavior and policy compliance.
- **Cybersecurity Culture:**
  The shared attitudes, values, and practices within an organization that prioritize and promote secure behaviors and adherence to cybersecurity policies.
- **Behavioral Interventions:**
  Strategies aimed at influencing individual actions, such as nudging, gamified training, or real-time feedback, to reduce errors and improve compliance.

CHAPTER 3

LITERATURE REVIEW & RELATED WORK

- **Introduction**

Cybersecurity is no longer just about technology—it's about people. While encryption, artificial intelligence (AI), and real-time threat detection have significantly improved security, human error remains one of the biggest weaknesses. Studies show that over 90% of successful cyberattacks exploit human mistakes rather than technical flaws.

Phishing scams, weak passwords, and social engineering attacks prove that even the most advanced security systems can be compromised if people aren't careful. This is why modern cybersecurity isn't just about firewalls and antivirus software—it's about understanding human behavior, decision-making, and the way people interact with technology.

To address this, researchers have developed tools like the Security Behavior Intentions Scale (SeBIS) and the Human Aspects of Information Security Questionnaire (HAIS-Q). These frameworks assess how users behave in security-sensitive situations, offering insights that help organizations improve security policies. However, as the digital landscape evolves—especially with interconnected systems like the Internet of Things (IoT)—new challenges arise, requiring cybersecurity strategies that adapt to both technological changes and human tendencies.

- **Objectives**

This literature review focuses on understanding how human behavior influences cybersecurity and evaluating the effectiveness of existing

tools designed to measure security awareness and behavior. Specifically, it aims to:

Examine SeBIS, HAIS-Q, and other emerging frameworks to see how they assess security behavior.
Identify the strengths and limitations of these tools, especially in different organizational and cultural settings.
Explore gaps in real-time behavioral tracking and how AI-driven security systems can improve user safety.
Suggest future research directions, focusing on more adaptive cybersecurity strategies that integrate both human and technological factors.
By combining insights from psychology, data science, and cybersecurity, this review aims to help organizations develop smarter, more people-centered security strategies.

- **How This Paper is Structurere**

Introduction – Sets the stage for understanding the human side of cybersecurity.
Thematic Review – Traces how cybersecurity has evolved, discusses the latest research on security behavior, and explores tools used to measure user awareness.
Critical Analysis – Evaluates the strengths and weaknesses of existing tools, identifying key research gaps.
Future Directions – Proposes new approaches, such as AI-driven security assessments, real-time monitoring, and gamified cybersecurity training.
Conclusion – Summarizes key findings and provides recommendations for improving cybersecurity through a human-centered approach.

- **Thematic Review**

- **A Look Back: How Cybersecurity Evolved**

In the past, cybersecurity was all about technology—firewalls, antivirus software, and network security. But over time, major security breaches revealed a critical flaw: technology alone isn't enough.

A prime example is the 2013 Target data breach, where hackers gained access to sensitive customer information by exploiting weak security practices within a third-party vendor. The breach wasn't due to a failure in technology, but rather a human mistake—a lapse in password security and vendor oversight.

This incident, among others, forced organizations to rethink their approach. Instead of focusing only on technical solutions, they started incorporating human behavior research into their security strategies. This shift led to the development of SeBIS and HAIS-Q, which measure security awareness and behavioral tendencies, helping organizations understand and mitigate human-related risks.

- **Recent Developments: How Research is Evolving**

With cyber threats growing more sophisticated, researchers have expanded their focus beyond just user awareness. New studies have classified users into categories based on their security behavior. For example:

"Naïve Greenhorns" – Individuals with little to no security awareness, prone to falling for phishing scams.
"Reliable Troupers" – People with strong security habits who regularly update passwords and recognize threats.

By identifying these behavioral patterns, organizations can create customized security training programs instead of using a one-size-fits-all approach.

Another major advancement is the use of AI-driven tools for real-time security monitoring. Unlike traditional surveys, which only capture self-reported data, AI can track actual use

behavior—like how often someone clicks on suspicious links or how they respond to security warnings.

Other innovations include:

Biometric tracking – Using eye movement and stress detection to measure a user's response to cyber threats.
IoT security enhancements – Implementing machine learning models to detect anomalies in smart devices.
These advances show that cybersecurity is becoming more dynamic, moving beyond simple surveys to real-time, behavior-driven solutions.

- **How We Measure Cybersecurity Behavior**

Researchers use different methods to assess human behavior in cybersecurity:

Surveys & Questionnaires – Tools like SeBIS measure security habits, while HAIS-Q evaluates organizational awareness and compliance.
AI & Machine Learning – Algorithms analyze user activity, detect anomalies, and predict potential risks.
Simulated Attacks – Organizations conduct controlled phishing tests to measure how employees respond to security threats.
Biometric Tracking – Eye movement tracking during simulated attacks can reveal how quickly and accurately users identify phishing attempts.

Interviews & Observations – Researchers conduct ethnographic studies to understand the reasoning behind security decisions.
Each of these approaches provides valuable insights, but together, they create a more complete picture of how people engage with cybersecurity.

- **Challenges & Unsolved Problems**

Despite advancements, several challenges remain:

IoT security is still a major concern – Most cybersecurity frameworks weren't designed for smart home devices, industrial IoT, or connected cars, leaving gaps in how we protect these systems. Static approaches don't adapt to real-time risks – Surveys provide useful insights but don't capture live behavioral changes, making them less effective in dynamic environments.
Security strategies don't always account for cultural differences – A security policy that works well in the U.S. may not be as effective in Asia or Europe, highlighting the need for
cross-cultural validation.
As cyber threats evolve, researchers must focus on creating more adaptive security measures that integrate behavioral insights with real-time monitoring.Cross-Cultural Challenges and Biases

A major issue with current cybersecurity research is its narrow focus on Western contexts, which neglects the diverse cultural and organizational settings around the world. Cultural differences can significantly influence cybersecurity practices, yet many studies fail to address this, limiting the global applicability of their findings.

Another challenge lies in the reliance on self-reported data, which introduces biases. For example, people may overstate how compliant

they are with security practices or downplay risky behaviors. This creates a gap between reported and actual behaviors, leading to skewed results.

To address these issues, there's a growing need for adaptive tools that combine real-time monitoring with culturally inclusive designs. Incorporating AI-driven analytics can help provide more accurate insights and actionable data, reducing the impact of biases and improving the reliability of findings.

- **Critical Analysis**

- **Strengths and Weaknesses of Current Research**

Frameworks like SeBIS and HAIS-Q offer structured ways to evaluate cybersecurity behavior, providing useful insights into habits, compliance, and awareness. These tools have been instrumental in designing targeted security interventions.

However, their heavy reliance on static, self-reported data is a major limitation. Self-reports are often influenced by social desirability bias, where participants might exaggerate their adherence to security protocols or minimize risky actions. This can lead to unreliable results.

For instance, tools like PCSASS work well in academic environments but lack scalability for broader contexts, such as corporate settings or small and medium-sized enterprises (SMEs). Businesses often face unique challenges, like resource constraints and varying levels of technical expertise, which aren't adequately addressed by these frameworks.

Despite these limitations, recent advancements in real-time behavioral monitoring and AI-driven tools offer promising solutions. Phishing simulations, for example, can dynamically adapt to user behavior, providing more precise and actionable feedback.

- **Contradictory Findings**

There's also inconsistency in how effective cybersecurity training programs are. Some studies show that training improves awareness and reduces risky behaviors, like falling for phishing scams or using weak passwords. However, these positive effects often fade over time, with users reverting to insecure practices after the training ends.

Targeted interventions—such as those tailored to specific user types, like "Naïve Greenhorns" or "Reliable Troupers"—show promise but face scalability issues. A program that works in one organization or culture may not be effective in another.

Traditional training models also tend to focus on delivering knowledge rather than fostering practical, long-term behavior changes. Research suggests that experiential and gamified training environments—which immerse users in real-world scenarios—are more likely to produce lasting results.

- **Research Gaps**

Several important gaps in cybersecurity research need to be addressed:

IoT-Specific Challenges: As IoT devices proliferate, they bring unique security risks that current tools like SeBIS and HAIS-Q aren't equipped

to handle. Issues such as device compatibility and rapidly changing threat landscapes require specialized frameworks.

Lack of Cross-Cultural Research: Most studies are based on Western populations, overlooking the cultural and organizational differences that influence cybersecurity behavior globally. This lack of diversity limits the development of universally applicable tools.

Static Assessments: Current tools fail to capture the dynamic nature of user behavior, especially in high-stress or rapidly evolving situations. Real-time monitoring systems powered by AI could fill this gap.

Leadership and Culture: The role of organizational leadership in fostering a culture of cybersecurity is underexplored. Top-down policies, leadership commitment, and workplace norms play a significant role in shaping user behavior.

- **Future Directions**

- **Emerging Trends in Cybersecurity**

Cybersecurity is evolving, with exciting new trends pointing the way forward.

IoT-Focused Frameworks: The rise of interconnected devices has created new vulnerabilities. Future tools need to address these risks with real-time monitoring and adaptive learning algorithms that can keep pace with evolving threats.

Gamified Training Programs: Introducing competition and rewards into training helps users stay engaged while practicing secure behaviors in

simulated real-world scenarios. These programs are gaining popularity for their effectiveness in retaining user attention.

Biometric Insights: Data such as gaze tracking, stress analysis, and voice recognition is providing deeper insights into how users make decisions under pressure. This information can help predict vulnerabilities before they're exploited.

Blockchain for Data Security: Blockchain technology is being explored to improve the transparency and integrity of cybersecurity data, ensuring that behavioral insights are securely handled.

- **Key Research Questions**

Future research should address the following questions:

- How can cybersecurity tools adapt to IoT environments to tackle the unique risks posed by interconnected devices?
- What methods can reduce biases in AI-driven security tools, ensuring they work effectively across different user demographics?
- How can gamified and scenario-based training models improve the long-term adoption of secure practices?
- What role can biometric data play in real-time monitoring and predicting cybersecurity risks?
- How can ethical AI frameworks be implemented in cybersecurity without compromising user privacy?
- What strategies can enhance the cross-cultural applicability of cybersecurity frameworks?
- How can leadership and organizational culture foster better cybersecurity practices?

- Can hybrid frameworks combining self-reported and real-time behavioral data improve the accuracy of risk assessments?

- **New Approaches and Methodologies**

To address these challenges, researchers are exploring innovative methods:

Blockchain for Secure Data Handling: This ensures transparency and protects the integrity of behavioral data collected for cybersecurity purposes.
Dynamic Behavioral Analytics: AI-driven models with real-time feedback capabilities can help organizations identify risks as they happen and adapt their defenses accordingly.
Hybrid Tools: Combining traditional self-reported surveys with real-time monitoring allows for a more comprehensive view of user behavior. Machine learning algorithms can analyze patterns and predict vulnerabilities, enabling proactive interventions.
By integrating these new approaches, organizations can build more robust and adaptive security systems that address both technological and human-centric challenges.

- **Conclusion**

- **Summary of Key Findings**

Human-centric approaches, such as psychometric assessments and factor analysis, are indispensable for robust cybersecurity strategies. Tools like SeBIS and HAIS-Q provide foundational insights into user behaviors and organizational practices. However, these tools must evolve to incorporate IoT-specific capabilities and account for cross-

cultural dimensions. Emerging methodologies, including AI-driven analytics and biometric data integration, promise to enhance cybersecurity frameworks by offering real-time adaptability and precision.

- **Unresolved Issues**

Despite advancements, several critical gaps remain unresolved. IoT-specific assessments require further development to address the unique challenges posed by interconnected devices. Cross-cultural validation of existing frameworks is limited, necessitating more inclusive research to improve global applicability. The role of organizational leadership and its influence on cybersecurity culture has also been underexplored, leaving opportunities for future studies.

Additionally, building trust in AI systems is vital for their effective adoption in cybersecurity practices. Addressing these issues is critical for advancing the field and fostering a resilient cybersecurity culture

Chapter 4

Project Discussion

4.1 Software Engineering Methodology

For this research project, the **Incremental Model** of software engineering was carefully selected as the primary methodology. The decision was driven by the model's inherent adaptability and its strength in supporting iterative, step-by-step improvements. In a project that relies heavily on evolving human behavior data, such flexibility was essential. Cybersecurity and human behavioral patterns are dynamic; thus, a rigid, linear development model would not have been suitable. The Incremental Model provided the ability to continuously refine each phase based on emerging data trends and fresh insights derived from ongoing psychometric assessments.

Each component of the project—whether it was the psychometric evaluation tool, the user engagement surveys, or the statistical analysis framework—was developed in manageable increments. This approach allowed the team to remain responsive to unforeseen challenges and behavioral findings that surfaced during the course of the study. The strength of the Incremental Model lies in its capacity for parallel development and integration, which proved invaluable in this project. Different teams could work on separate modules simultaneously, such as building the Google Forms interface, creating Python-based analysis scripts, and preparing survey distribution strategies.

The model also supported real-time updates and iterative validation. For example, as early results revealed certain user behavior gaps, the analysis tools were quickly refined to explore these findings in greater depth. This continuous improvement cycle was not only efficient but also enhanced the quality and relevance of the final behavioral profiles.

4.2 Project Methodology

The project methodology combined **quantitative research** with **psychometric behavioral analysis**, ensuring that the study was

grounded in statistically valid and behaviorally insightful techniques. The decision to use psychometric scales like the Human Aspects of Information Security Questionnaire (HAIS-Q) and the Cybersecurity Risk Perception Scale (CRPS) allowed the project to move beyond superficial observations and instead capture deep-seated attitudes, beliefs, and tendencies that drive cybersecurity behavior.

The methodological steps followed in this study were rigorously structured:

- **Participant Selection:** The project focused on employees from diverse organizational roles, intentionally including IT professionals, administrative staff, and employees from non-technical backgrounds. This diversity ensured a holistic understanding of cybersecurity behaviors across departments and knowledge levels.
- **Survey Administration:** Psychometric questionnaires were disseminated using digital tools to facilitate wide distribution and ease of access. Google Forms enabled participants to complete the surveys at their convenience, minimizing response barriers.
- **Data Collection:** Responses were systematically collected, carefully cleaned, and organized to prevent biases and inconsistencies from influencing the results.
- **Statistical Analysis:** Detailed statistical techniques using Python, including correlation and regression analysis, were applied to uncover patterns, relationships, and behavioral typologies.
- **Behavioral Profiling:** Participants were categorized into distinct security behavior archetypes, such as “Naïve Greenhorns” who exhibit risky habits and “Reliable Troupers” who consistently demonstrate secure practices. These profiles helped tailor intervention strategies.

This comprehensive methodology maintained a strict focus on **evidence-based analysis** and provided actionable insights throughout every phase.

4.3 Phases of Project

The project was executed in a sequence of **interconnected phases**, each designed to build upon the findings of the previous step.

- **Planning Phase:** This initial stage involved framing the research objectives, selecting psychometric tools (HAIS-Q and CRPS), and meticulously designing the questionnaires to ensure reliability and participant engagement.
- **Data Collection Phase:** The validated questionnaires were distributed to a diverse participant pool. Digital distribution via Google Forms enabled efficient data collection and broad accessibility.
- **Data Analysis Phase:** The collected data underwent rigorous Python-based statistical processing. Correlation and regression analyses were employed to reveal underlying patterns in security behaviors and psychological constructs.
- **Profiling Phase:** Based on the analysis, participants were assigned to behavioral categories. This phase was critical in identifying which user groups required targeted security interventions.
- **Intervention Phase:** Insights from the behavioral profiles were used to develop preliminary recommendations for **personalized cybersecurity training**. These tailored interventions have the potential to significantly improve security compliance by addressing the unique needs of each user group.

4.4 Software/Tools Used in Project

The following software and tools were integral to the project's success:

- **Python:** Used extensively for statistical analysis, data cleaning, behavioral profiling, and visual representation of results. Libraries like pandas, matplotlib, and scipy played a key role.
- **Microsoft Excel:** Served as a supportive tool for preliminary data organization, response tracking, and basic visual summaries.

- **Google Forms:** Enabled seamless distribution of psychometric questionnaires and efficient collection of participant responses.

The integration of these tools allowed for a comprehensive, reliable, and replicable data analysis workflow.

4.5 Hardware Used in Project

The project's hardware requirements were minimal, reinforcing its scalability and accessibility.

- **Standard Laptops/PCs:** Utilized for data processing, statistical analysis, and report generation. There was no need for high-performance computing resources.
- **Internet Connectivity:** Essential for distributing online surveys, managing cloud storage, and ensuring real-time access to data.
- **Cloud Storage Solutions:** Used to securely store survey responses, project documentation, and backup datasets. This ensured data safety, accessibility, and facilitated collaboration.

The modest hardware setup underscores the project's potential for replication in a variety of organizational settings without significant resource investment.

4.6 Psychometric Analysis

The core of this research centered around **psychometric analysis** as a scientifically validated method to measure and interpret human behavior in cybersecurity. Recognizing that most cybersecurity breaches are driven by human error rather than technical failure, this study adopted psychometric tools to capture the **psychological traits, attitudes, and decision-making patterns** that influence security behavior.

Purpose of the Psychometric Analysis

The psychometric analysis aimed to:

- Understand **why users behave insecurely** even when they are aware of cybersecurity threats.
- Measure psychological constructs such as **risk perception, self-efficacy, and security attitudes** that contribute to decision-making in cybersecurity contexts.
- Build **evidence-based profiles** that identify high-risk individuals or groups based on their psychological predispositions.
- Develop a foundation for **personalized security training** that directly addresses the unique vulnerabilities of different user profiles.

Psychometric Tools Used

Two validated psychometric scales were employed in this research:

1. **Human Aspects of Information Security Questionnaire (HAIS-Q)**
    a. Assesses user knowledge, attitudes, and behaviors across key cybersecurity domains like password management, internet use, and incident reporting.
    b. Provides a practical way to measure the gap between what users know and what they actually do.
2. **Cybersecurity Risk Perception Scale (CRPS)**
    a. Measures perceived severity of cybersecurity threats and personal vulnerability.
    b. Highlights the common psychological bias where users recognize the seriousness of cyberattacks but underestimate their own susceptibility.

Methodology

The psychometric questionnaires were distributed to a sample of **200 participants** from diverse organizational backgrounds, including IT professionals, administrative staff, and students. The data collected was analyzed using Python's statistical libraries, focusing on:

- **Descriptive analysis** to summarize overall knowledge, attitudes, and behaviors.
- **Correlation analysis** to explore the relationships between psychological traits and cybersecurity practices.
- **Regression analysis** to predict the impact of factors like risk perception and conscientiousness on security behaviors.

Key Findings from Psychometric Analysis

- **Knowledge-Behavior Gap:** While participants showed reasonable cybersecurity knowledge (e.g., internet use knowledge average 4.2/5), their actual secure behaviors, especially password management (average 2.3/5), were considerably weaker. This demonstrates that knowing about cybersecurity does not guarantee secure action.
- **Risk Perception Disconnect:** Participants generally understood the severity of cyber threats (average 3.5/5), but they consistently **underestimated their own vulnerability** (average 2.8/5). This "it won't happen to me" mindset increases risk exposure.
- **Correlation Trends:**
    - Higher cybersecurity knowledge correlated negatively with perceived vulnerability ($r = -0.4$), indicating that as knowledge increases, people may falsely believe they are less likely to be attacked.
    - Stronger cybersecurity behaviors correlated positively with perceived threat severity ($r = 0.3$), suggesting that individuals who follow security protocols tend to appreciate the potential consequences of security breaches.
- **Impact of Training:** Participants with formal cybersecurity training performed **15% better in secure behavior scores** than untrained participants, reinforcing the importance of structured cybersecurity education.
- **Demographic Insights:** Older participants (35+) perceived cyber threats as more severe compared to younger individuals (18-24). IT professionals consistently showed higher cybersecurity knowledge than non-IT participants.

Importance of Psychometric Profiling

The study demonstrated that **psychometric profiling can predict security behavior** and help organizations:

- Identify employees at higher risk due to psychological traits like low self-efficacy or high risk tolerance.
- Design targeted interventions rather than relying on generic, one-size-fits-all security awareness programs.
- Monitor psychological risk factors alongside technical vulnerabilities in real-time security management systems.
- Develop **adaptive security policies** that address both behavioral and technical weaknesses.

Conclusion on Psychometric Integration

The psychometric analysis in this research provides a **practical, science-based approach** for enhancing cybersecurity training and risk management. By leveraging psychometric assessments like HAIS-Q and CRPS, organizations can move beyond surface-level security awareness and start to address the psychological drivers that truly influence behavior. This human-centered strategy offers a proactive pathway to reducing security incidents and building a resilient cybersecurity culture.

4.7 Survey Questionnaire

The following questionnaire was developed to assess participants' cybersecurity knowledge, attitudes, and behaviors, as well as their risk perception and security practices. The survey items were designed to capture practical and psychological dimensions of cybersecurity behavior.

Demographic Information

1. Gender: _____
2. Educational Background: _____

3. Field of Study/Profession: _____
4. Current Occupation: _____
5. Have you received any formal training in cybersecurity?
   ☐ Yes ☐ No

Cybersecurity Knowledge and Practices

6. I know how to create a strong and secure password.
   ☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
7. I believe it is important to use different passwords for different accounts.
   ☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
8. I regularly update my passwords.
   ☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
9. I know how to identify suspicious emails or phishing attempts.
   ☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
10. I feel cautious when receiving emails from unknown senders.
    ☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
11. I avoid clicking on links or downloading attachments from unknown sources.
    ☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
12. I know how to securely store sensitive files.
    ☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree

13. I ensure sensitive information is encrypted when necessary.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
14. I understand the risks of accessing unsecured websites.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
15. I think using secure websites (HTTPS) is important.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
16. I avoid entering personal data on websites that are not secure.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree

Cybersecurity Risk Perception

17. I believe I am at risk of experiencing a cyberattack.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
18. I feel vulnerable to cybersecurity threats in my workplace.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
19. My online activities expose me to potential risks.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
20. A cybersecurity breach could severely impact my personal or professional life.
☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree
21. Cyber threats can cause significant financial and reputational damage.

☐ Strongly Disagree ☐ Disagree ☐ Neutral ☐ Agree ☐ Strongly Agree

Chapter 5

Implementation

5.1 Proposed System Architecture/Design

The system architecture designed for this project is **modular, layered, and scalable**, making it easy to expand in the future. The primary purpose of the system is to efficiently collect, process, and analyze psychometric data related to cybersecurity behavior.

- **User Interface Layer:** Google Forms was chosen as the front-end platform for its ease of use, data security, and compatibility with cloud-based workflows. It offered participants an intuitive way to engage with the questionnaires.
- **Data Storage Layer:** Collected data was automatically logged in Google Sheets, which was linked to cloud storage systems for regular backups. This setup ensured both data safety and convenient accessibility for analysis.
- **Processing Layer:** Data cleaning, processing, and statistical evaluation were executed using Python. The system's modular design allowed for the swift addition of new analytical functions or the integration of additional psychometric tools.
- **Reporting Layer:** The processed data was translated into detailed reports and visual summaries, which included behavioral profiles and security risk categorizations. These reports formed the basis for personalized security recommendations.

The system's **modularity ensures future flexibility**, allowing the potential integration of real-time tracking, machine learning algorithms, or additional security assessment layers.

5.2 Functional Specifications

The core functional requirements of the system were:

- **Secure User Data Collection:** Ensuring the integrity and privacy of psychometric survey responses during collection.
- **Organized Data Storage:** Structuring data in a retrievable, well-organized format while upholding strict data protection protocols.
- **Robust Data Processing:** Performing reliable and accurate statistical analyses to uncover meaningful patterns and correlations.
- **Behavioral Profiling:** Systematically categorizing users based on their cybersecurity attitudes and practices.
- **Comprehensive Report Generation:** Producing clear, actionable reports that could guide the development of tailored training programs.

5.3 Non-Functional Specifications

The system also had to satisfy several non-functional specifications:

- **Security:** User data privacy was a top priority, with access to raw datasets restricted to authorized personnel only.
- **Reliability:** The system needed to process large datasets without errors or data loss, ensuring the integrity of all outputs.
- **Usability:** Google Forms and related interfaces were designed to be user-friendly, reducing the likelihood of participant errors.
- **Scalability:** The system architecture was designed to easily accommodate larger datasets and participant pools in future applications.
- **Maintainability:** Flexibility to update psychometric scales or integrate new analysis tools without disrupting system operations.

5.4 Testing

Testing was an essential, multi-phase process aimed at verifying the system's functionality, reliability, and accuracy.

5.4.1 Purpose of Testing

The key testing objectives were to:

- Confirm accurate collection and storage of psychometric survey responses.
- Validate the reliability of data processing and behavioral profiling tools.
- Ensure consistent and accurate report generation.
- Assess the system's ability to handle multiple users and datasets without performance degradation.

5.4.2 Test Cases

Test Case ID	Description	Expected Result	Actual Result	Status
TC-01	Validate Google Form submission	Responses correctly stored in Google Sheets	Successful	Pass
TC-02	Verify cloud data upload	Data securely backed up without loss	Successful	Pass
TC-03	Test Python data analysis	Accurate statistical outputs generated	Successful	Pass
TC-04	Validate report generation	Comprehensive, user-specific reports created	Successful	Pass

All tests confirmed that the system was working as intended, delivering reliable performance across all components.

Chapter 6

Experimental Evaluations & Results

6.1 Evaluation Testbed

The evaluation environment for this project was carefully designed to provide a **controlled, yet practically relevant testbed**. The tools used for this purpose included **Google Forms** for survey administration, **Google Sheets** for initial data logging, and **cloud storage solutions** to ensure secure, redundant data backups. For data analysis, we utilized **Python** (with libraries such as pandas, matplotlib, scipy, and seaborn for visualization and statistical analysis).

The participant pool was carefully selected to ensure diversity and represent a broad spectrum of cybersecurity awareness levels. The **final sample consisted of approximately 200 individuals** from various professional backgrounds, including IT specialists, administrative personnel, and non-technical staff. This cross-functional participation was vital to understand how cybersecurity behaviors vary across roles, industries, and levels of technical expertise.

The participants were recruited through a mix of organizational partnerships, educational institutions, and professional networks. Most participants were **young adults between the ages of 18 and 24**, with a significant portion being university students and early-career professionals. Notably, over **90% of the participants had no formal cybersecurity education or training**, which provided valuable insight into natural cybersecurity behaviors in the absence of structured learning.

The **controlled evaluation environment** enabled the project team to track response patterns, ensure data accuracy, and maintain consistent testing protocols across all participants.

6.2 Results and Discussion

The results of this study offered **deep insights into human cybersecurity behavior and risk perception**.

Key Findings:

- **Awareness vs. Action Gap:** The analysis revealed a significant gap between what participants knew and how they behaved. For example, while participants demonstrated **high awareness scores in Internet use (average 4.2/5)** and displayed positive attitudes toward safe practices (average 4.4/5), their actual behavior, particularly in **password management (average 2.3/5)**, was considerably weaker. This pattern indicates that **knowledge does not automatically translate into secure actions**, a common challenge in cybersecurity education.
- **Perceived Risk Disconnect:** Participants consistently **acknowledged the severity of cyber threats** (average 3.5/5), but their perceived personal vulnerability remained low (average 2.8/5). Statements like "I perceive myself at risk of dangers at my job" scored particularly low (average 2.3/5). This mindset, often referred to as the **"it won't happen to me" bias**, was evident across most demographic groups.
- **Correlation Trends:** Correlation analysis using Python revealed:
    - A **negative correlation (-0.4)** between cybersecurity knowledge and perceived vulnerability. This suggests that as users gain knowledge, they may feel falsely secure and perceive themselves as less likely to be attacked.
    - A **positive correlation (0.3)** between cybersecurity behaviors and perceived severity, indicating that individuals who actively follow safe practices are more conscious of potential threats.
- **Impact of Training:** Participants with **formal cybersecurity education consistently outperformed** their untrained peers. Their cybersecurity behavior scores were approximately **15% higher**,

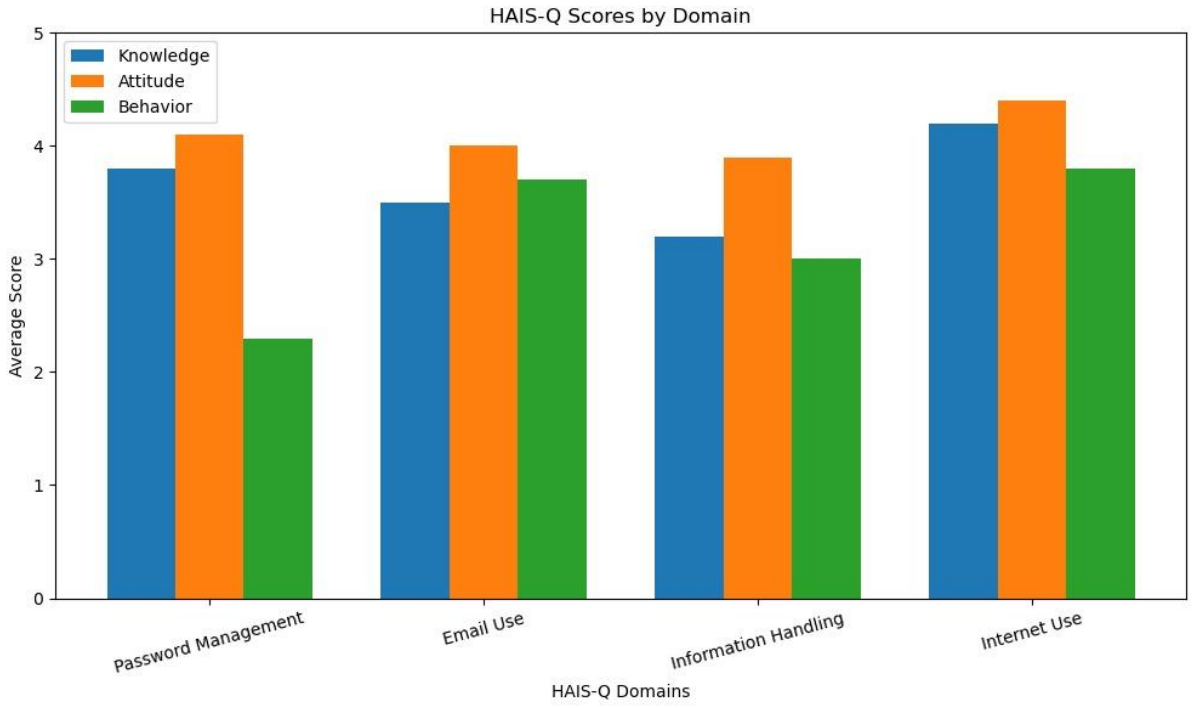
demonstrating that targeted training directly influences safer online habits.

- **Age-Based Differences:** Older participants (35 years and above) displayed a higher perception of threat severity (average 4.1/5) compared to younger participants (average 3.2/5). This suggests that **age and life experience may enhance risk sensitivity**.
- **Role-Based Insights:** As expected, IT professionals demonstrated superior cybersecurity knowledge (average 4.5/5) compared to non-technical participants (average 3.1/5). However, even among IT professionals, behavioral gaps persisted, especially in password updating and email vigilance.

Data Summary Table

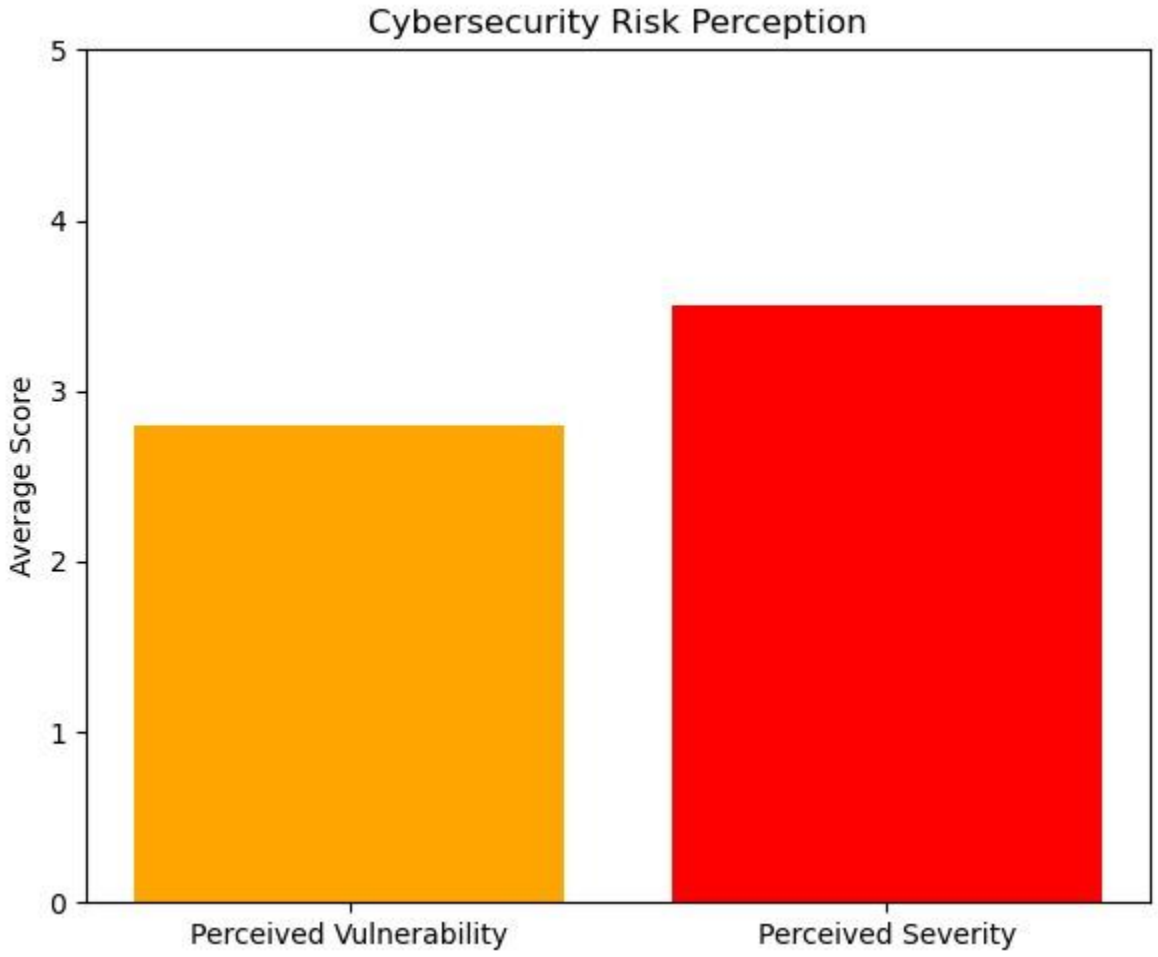
Metric	Score (out of 5)
Internet Use - Knowledge	4.2
Internet Use - Behavior	3.2
Password Management - Knowledge	3.8
Password Management - Behavior	2.3
Email Use - Knowledge	4.1
Email Use - Behavior	2.9
Perceived Severity	3.5
Perceived Vulnerability	2.8
Behavior Score (Trained)	3.6
Behavior Score (Untrained)	3.1

Visual Summaries:



- **Figure 2:** 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.



- **Figure 3:** Illustrated the discrepancies between participants' perceived risk and actual cybersecurity practices, emphasizing

the"false sense of security" trend.

- **Figure 4:** Compared behavior scores based on cybersecurity training, visually confirming the positive impact of formal education.

Practical Implications:

The findings validate that **psychometric assessments can successfully predict cybersecurity behaviors**. More importantly, these results reinforce the need for **personalized, behaviorally informed interventions** rather than generic training modules. Cybersecurity strategies should focus on bridging the knowledge-behavior gap by incorporating psychological factors such as risk perception, self-efficacy, and motivational triggers.

Chapter 7

Conclusion and Discussion

7.1 Strengths of this Project

This project has made a significant contribution to the growing body of **human-centered cybersecurity research** by systematically integrating psychometric tools with security behavior analysis. The major strengths of this project include:

- **Behavioral Focus:** Unlike many cybersecurity studies that focus purely on technical vulnerabilities, this project placed human behavior at the core, acknowledging that the human element is often the weakest link.
- **Validated Psychometric Tools:** By utilizing the HAIS-Q and CRPS, the study was able to capture both knowledge and psychological drivers of cybersecurity behavior with a high degree of reliability.
- **Practical Applicability:** The modular system architecture, minimal hardware requirements, and scalable design make this model easily adaptable for organizations of varying sizes. Companies can now employ this framework to conduct their own psychometric assessments and develop **targeted security awareness programs**.
- **Customized Interventions:** The ability to profile participants into distinct behavioral categories paves the way for personalized cybersecurity training, which is significantly more effective than generic awareness campaigns.
- **Evidence-Based Approach:** The integration of quantitative research, statistical analysis, and psychometric profiling created a data-driven methodology that strengthens the practical value of the findings.

7.2 Limitations and Future Work

While the project achieved its primary objectives, several limitations should be acknowledged:

- **Sample Size and Diversity:** The sample was limited to approximately 200 participants, predominantly from a younger age group and within a specific geographic region. To increase generalizability, future studies should involve **larger, more diverse, and international participant pools.**
- **Self-Reported Data:** The reliance on self-reported behaviors can introduce **response bias**, as participants may have unintentionally or intentionally provided inaccurate answers. Incorporating **behavioral tracking systems or observational studies** could provide more objective data.
- **Lack of Real-Time Data:** The project did not include real-time monitoring tools, which could have offered insights into immediate decision-making and security responses.
- **Cross-Sectional Design:** Since the study captured participant responses at a single point in time, it does not provide information on how cybersecurity behaviors may evolve over time. Longitudinal studies could address this gap.
- **Cultural Context:** The study was conducted within a specific cultural and organizational context. Future research should explore **cross-cultural comparisons** to determine whether the psychometric patterns hold true in different regions and organizational cultures.

Future Recommendations:

- Incorporate **AI-driven adaptive systems** that can dynamically adjust training materials based on individual psychometric profiles.
- Develop **gamified training interventions** that directly address the psychological factors identified through psychometric profiling.
- Expand research to explore **IoT security behaviors**, as connected devices introduce new types of risks.

- Study the **long-term effectiveness** of personalized training programs developed using psychometric baselines.

7.3 Reasons for Failure – If Any

The project successfully completed all planned phases without major failures. However, **minor challenges** did arise, particularly in participant recruitment and ensuring high response accuracy. Some participants initially demonstrated survey fatigue, which was mitigated through follow-up reminders and the inclusion of attention-check questions.

Additionally, there were minor technical delays in data synchronization between Google Sheets and Python, which were quickly resolved by enhancing the data cleaning process.

Despite these small setbacks, the project met its objectives and delivered **reliable, actionable results.**

References

1. C. Faklaris, L. Dabbish, and J. I. Hong, "Do they accept or resist cybersecurity measures? Development and validation 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:
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. A. AlHogail, "Design and validation of information security culture framework," *Computers in Human Behavior*, vol. 49, pp. 567–575, 2015.
22. L. Hadlington and K. Parsons, "Can education and training really help improve cybersecurity? A psychological perspective," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 11, no. 4, Article 5, 2017.
23. H. Li, R. Sarathy, and H. Xu, "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors," *Decision Support Systems*, vol. 51, no. 3, pp. 434–445, 2011.
24. H. A. Alqahtani and R. Thurasamy, "Information security awareness: Literature review and integrative framework for future research," *Telematics and Informatics*, vol. 58, 101537, 2021.
25. M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link'—A human/computer interaction approach to usable and effective security," *BT Technology Journal*, vol. 19, no. 3, pp. 122–131, 2001.