**BEHAVIORANCE-I**

Redefining Cybersecurity with Secure Sense Behavioral Compliance   
(Web Application Platform)

**Project Proposal**



**Supervisor**

Jibran Rasheed Khan

**Submitted by**

Farwah Butt

{1101-2021}

Emaan Nadeem

{2438-2021}

Hafsa Khalid

{2625-2021}

**Department of Computer Science,**

Hamdard University, Karachi.

[24/06/2024]

# Introduction

In an era where cyber threats are evolving at an unprecedented pace, the need for innovative cybersecurity solutions has never been more critical. Despite significant advancements in technology, many organizations continue to experience breaches and security incidents that can be traced back to human factors such as negligence, error, and non-compliance with established protocols. This ongoing challenge underscores the necessity of integrating behavioral compliance into cybersecurity frameworks to create a more resilient defense mechanism.

The current landscape reveals a substantial gap in the cybersecurity market: the lack of comprehensive solutions that effectively address the human element of security. Traditional cybersecurity measures, while robust, often neglect the behavioral aspects that can undermine even the most advanced technological defenses. This gap leaves organizations vulnerable to insider threats, phishing attacks, and other security breaches that exploit human weaknesses.

In response to this pressing need, Behaviorance introduces the Secure Sense Behavioral Compliance (SSBC) Platform, a groundbreaking software project designed to revolutionize cybersecurity. The SSBC Platform represents a significant innovation in the field, seamlessly integrating behavioral compliance into the core of cybersecurity strategies. By leveraging state-of-the-art technologies such as machine learning, real-time analytics, and advanced behavioral monitoring, the platform provides organizations with a dynamic tool to enhance their security posture.

The SSBC Platform's innovative approach focuses on real-time detection and mitigation of behavioral risks, ensuring that employees adhere to security protocols and reducing the likelihood of human error. This proactive stance not only strengthens an organization's defenses but also fosters a culture of security awareness and compliance.

This project delves into the intricacies of the Secure Sense Behavioral Compliance Platform, exploring its design, functionality, and the innovative technologies that underpin it. We will examine how this platform addresses the critical need for behavioral compliance in cybersecurity and the ways it can transform an organization's approach to managing security risks. Through this exploration, we aim to highlight the significant impact of integrating behavioral compliance into cybersecurity frameworks and demonstrate the potential of the SSBC Platform to redefine the future of digital security.

# Objective

# The project objective is to develop the smart human behavioral analysis based web application platform “Behaviorance-I”, with the predictive assessment to forecast human behavior and potential vulnerable actions.

# Problem Description

In the rapidly evolving digital landscape, organizations face increasingly sophisticated cyber threats that traditional security measures struggle to mitigate effectively. Despite significant investments in technology and personnel, many organizations continue to experience data breaches, cyber-attacks, and compliance failures. A critical gap exists in the integration of human behavior into cybersecurity protocols, leading to vulnerabilities that are often exploited by malicious actors.

The absence of robust behavioral compliance mechanisms means that even the most advanced technological defenses can be undermined by human error, negligence, or malicious intent. Current cybersecurity solutions often lack the ability to adapt to and predict human behavior, leaving organizations exposed to insider threats and non-compliance with regulatory standards.

This gap underscores the urgent need for an innovative solution that not only fortifies technical defenses but also integrates behavioral compliance to create a comprehensive cybersecurity posture. Addressing this need, Behaviorance introduces the Secure Sense Behavioral Compliance Platform, designed to seamlessly incorporate human behavior into the fabric of cybersecurity strategies, thus redefining the standards of digital protection.

# Project Scope

The scope of the project “Behaviorance” includes and limited to develop the Secure Sense Behavioral Compliance (SSBC) Platform, an innovative solution designed to enhance cybersecurity by integrating advanced technological measures with psychological insights. This project will focus on several key areas to achieve its objectives. Firstly, it will involve a thorough analysis of how human behavior impacts cybersecurity, identifying common vulnerabilities such as negligence, errors, and non-compliance with security protocols. Secondly, the project will create a comprehensive platform that integrates advanced cybersecurity measures with psychological factors, utilizing machine learning, real-time analytics, and behavioral monitoring to enhance security posture.

Additionally, the project will develop and validate a comprehensive set of questionnaires aimed at assessing various psychological factors that influence security behavior, helping organizations identify and mitigate potential human-related risks. It will also integrate cybersecurity and psychological insights into a unified framework that considers both technological and human elements, providing a holistic approach to security. To ensure the platform's effectiveness, rigorous testing and validation will be conducted to empirically evaluate its impact on improving compliance and reducing security incidents. Furthermore, the project will develop and implement training programs based on the behavioral analysis to promote security awareness among employees, fostering a culture of compliance and proactive security practices within organizations.

However, the project scope does not include the development or implementation of any hardware solutions, nor does it extend to addressing purely technical cybersecurity issues that do not involve human factors. Additionally, physical security measures, such as access control systems or surveillance equipment, are not within the scope of this project. By focusing on these specific areas, the Behaviorance project aims to provide a comprehensive solution that addresses the critical role of human behavior in cybersecurity, ultimately enhancing the overall security posture of organizations.

# Literature Review

Traditionally, Computer Science (CS) researchers have focused on the technical aspects of cybersecurity (Kannelønning and Katsikas, 2023). However, the human aspect, though critically important, is often neglected (Rohan et al., 2023; Khan et al., 2022). This oversight is significant since the human element is considered the weakest link in the cybersecurity chain (Kannelønning and Katsikas, 2023; Almansoori, Al-Emran, and Shaalan, 2023; Rohan et al., 2023; Khan et al., 2022; Rohan et al., 2021; Rahman et al., 2021; Maalem et al., 2020). It is reported that 95% of security breaches are caused by human mistakes, underscoring the need for greater attention to human factors in cybersecurity (Kannelønning and Katsikas, 2023; Almansoori, Al-Emran, and Shaalan, 2023; Rohan et al., 2023; Rohan et al., 2021; Maalem et al., 2020).

Kannelønning and Katsikas (2023) provide a systematic review of how cybersecurity-related behavior has been assessed. They emphasize the diversity in methodologies and the challenges in standardizing measures. Their findings suggest that without considering human behaviors, technical countermeasures will remain ineffective. Given that 90% of cyberattacks involve human-based techniques (Rahman et al., 2021), it is crucial to develop consistent and reliable tools for evaluating cybersecurity behaviors. Almansoori, Al-Emran, and Shaalan (2023) delve into the theories and studies at the forefront of cybersecurity behavior. They highlight the significance of behavioral theories such as the Theory of Planned Behavior and Protection Motivation Theory in understanding the psychological and social factors influencing cybersecurity behaviors. Their review calls for integrating these theories into cybersecurity practices to enhance the effectiveness of interventions.

Rohan et al. (2023) examine the tools used to measure information security awareness. Their review reveals a variety of scales, each with different levels of validity and reliability. They stress the importance of developing comprehensive and universally accepted scales to accurately measure cybersecurity awareness. This aligns with the need to focus on social and behavioral issues to effectively deal with cybersecurity threats (Kannelønning and Katsikas, 2023; Almansoori, Al-Emran, and Shaalan, 2023; Rohan et al., 2023; Khan et al., 2022; Rohan et al., 2021; Rahman et al., 2021; Maalem et al., 2020).

Khan et al. (2022) provide a meta-perspective on cybersecurity behavioral research, identifying trends and suggesting future research directions. Their tertiary study complements Rohan et al.'s work by advocating for robust measurement tools and emphasizing the need for a holistic approach that includes human factors.

The human element in cybersecurity is a critical area of study. Rohan et al. (2021) discuss the role of user behavior in mitigating cyber threats. Their review identifies common human errors and proposes strategies to enhance user security behaviors through better design and education. They argue that without addressing human behaviors, technical measures will fall short. Rahman et al. (2021) conduct a scoping review on human factors in cybersecurity, highlighting the complexity of human behavior in this context. They call for a multidisciplinary approach, integrating insights from psychology, sociology, and computer science, to address the human aspects of cybersecurity effectively. Maalem et al. (2020) provide a comprehensive review of the behavioral aspects of cybersecurity. Their study offers insights into how individual behaviors impact cybersecurity and the factors influencing these behaviors. They propose a framework for understanding and enhancing cybersecurity behaviors, including educational initiatives and policy recommendations. Their work emphasizes that cyberspace has transcended technological artifacts, with increasing importance given to the behavioral aspect of cybersecurity.

# Methodology

Evolutionary Prototyping Development Methodology

WHY?

The evolutionary prototyping model combines incremental and extreme models. This model involves a series of prototyping refinements. The first assignment is to design and split the system into several independent modules. This model is used when the customers do not know the exact project requirements beforehand. The evolutionary model is suitable if trying to build a new product or technology that is not clearly understood at the moment.

## Project Planning

Establish a clear roadmap for the project, including timelines, resources, and milestones. Ensure alignment with stakeholder expectations and project goals.

**Activities:**

* Define the project scope, objectives, and deliverables in detail.
* Develop a comprehensive project plan, including timelines, resource allocation, and risk management strategies.
* Assemble the project team and assign roles and responsibilities.
* Conduct initial meetings with stakeholders to confirm requirements and expectations.
* Set up communication channels and project management tools to track progress and manage tasks.

## Literature Review

Gather relevant research and best practices in cybersecurity, behavioral compliance, and psychological factors. Establish a theoretical foundation for the project.

**Activities:**

* Conduct a comprehensive review of existing literature on cybersecurity measures, human behavior in cybersecurity, and psychological principles affecting security compliance.
* Identify gaps in current research and how the Behaviorance project can address them.
* Compile and analyze data from academic journals, industry reports, and case studies.
* Summarize findings and incorporate relevant theories and models into the project framework.

## Identifying Factors

Determine the key human and psychological factors that impact cybersecurity compliance and performance.

**Activities:**

* Collaborate with behavioral psychologists and cybersecurity experts to identify relevant factors.
* Review existing behavioral assessment tools and frameworks.
* Conduct interviews and surveys with stakeholders to gather insights on critical behavioral factors.
* Develop a comprehensive list of factors influencing cybersecurity behavior, such as motivation, awareness, training, and organizational culture.

## Design & Develop Platform

Develop a detailed design for the Secure Sense Behavioral Compliance (SSBC) Platform.

**Activities:**

* Create high-level system architecture, ensuring scalability, security, and interoperability.
* Design detailed components and modules, including machine learning algorithms, real-time analytics, behavioral monitoring, and user interfaces.
* Develop wireframes and prototypes for key features.
* Review design with stakeholders and refine based on feedback.

## Design Questionnaire

Develop a comprehensive set of questionnaires to assess psychological and behavioral factors influencing cybersecurity compliance.

**Activities:**

* Collaborate with behavioral psychologists to design valid and reliable questionnaires.
* Ensure questions cover all identified factors and are easy for participants to understand.
* Pilot test the questionnaires with a small group and refine based on feedback.
* Validate the questionnaires to ensure they accurately measure the intended factors.

## Integrate Cybersecurity and Psychological Principles

Create a unified framework that integrates cybersecurity measures with psychological principles.

**Activities:**

* Map cybersecurity strategies to relevant psychological factors identified earlier.
* Develop models that combine technical defenses with behavioral interventions.
* Create guidelines for applying psychological principles to enhance cybersecurity measures.
* Ensure the framework is adaptable to different organizational contexts and cybersecurity threats.

## Design Assessment Report

Develop a comprehensive reporting tool to evaluate and communicate the effectiveness of the SSBC Platform.

**Activities:**

* Define key metrics and indicators for assessing platform performance.
* Design report templates that provide clear and actionable insights.
* Develop automated reporting features within the platform to generate regular assessment reports.
* Ensure reports are customizable to meet different organizational needs.

## Evaluate Performance

Assess the performance and effectiveness of the SSBC Platform in real-world scenarios.

**Activities:**

* Deploy the platform in pilot organizations and monitor its impact on cybersecurity compliance and behavior.
* Collect and analyze data on key performance indicators (KPIs) to measure effectiveness.
* Gather feedback from users and stakeholders to identify areas for improvement.

## Documentation

Provide comprehensive documentation for all aspects of the project to ensure clarity and usability.

**Activities:**

* Document the system architecture, design specifications, and development processes.
* Create user manuals and training materials to guide platform users.
* Develop technical documentation for developers and IT staff.
* Compile all reports, findings, and insights from the project into a final project report.

# Feasibility Study

With the defined scope of the Behaviorance project, meeting the project schedule is achievable, provided that potential risks are effectively managed and the necessary resources are adequately allocated. Below are the key aspects to consider:

## Risks Involved

1. **Technical Risks**The integration of advanced technologies such as machine learning and real-time analytics can be complex and time-consuming.
2. **Behavioral Analysis Complexity**Accurately assessing and interpreting psychological factors influencing security behavior may be challenging.
3. **Compliance and Legal Risks:**Ensuring the platform meets all regulatory and compliance requirements across different regions.
4. **User Adoption Risks**Resistance from employees in adopting new security protocols and training programs.

## Resource Requirements

## Computing Resources:

* + High-performance servers and cloud infrastructure for running machine learning models and real-time analytics.
  + Secure databases for storing behavioral data and questionnaire responses.
  + Development environments and tools for software development, testing, and deployment.

## Human Resources:

* + Software developers with expertise in cybersecurity and machine learning.
  + Data scientists and analysts for developing and validating the behavioral assessment tools.
  + Behavioral psychologists for providing insights and guidance on psychological factors.
  + Project managers to oversee the development process and ensure adherence to the schedule.

## Other Resources:

* + Legal consultants to ensure compliance with cybersecurity and data protection regulations.
  + Training materials and resources for employee education and awareness programs.
  + Collaboration tools for efficient communication and project management among the team members.

By addressing above risks and ensuring the availability of required resources, the Behaviorance project is well-positioned to meet its project schedule. Continuous monitoring and adaptive planning will be essential to navigate any unforeseen challenges and ensure the successful delivery of the SSBC Platform.

# Application Areas

The project aims to provide tangible benefits that enhance the overall cybersecurity landscape, making organizations more resilient to the ever-evolving threats in the digital age. The following are the potential application area

* Government and Public Sector
* Education
* Corporate Sector
* Information Technology

# Tools/Technology

To ensure the successful execution and completion of the research project titled "Synergizing Human Behavior and Cybersecurity using Psychometric Behavioral Analysis," the following hardware and software requirements have been identified:

#### Hardware Requirements

#### **Computers/Laptops**

* Processor: Intel Core i5 or higher
* RAM: 8 GB or higher
* Storage: 256 GB SSD or higher
* Operating System: Windows 10, macOS, or Linux

**Purpose**: Essential for conducting literature reviews, developing the psychometric scale, designing surveys, analyzing data, and preparing reports.

#### **Stable Internet Connection**

Bandwidth: Minimum 4 Mbps download and 2 Mbps upload

Reliability: Consistent connectivity with minimal downtime

**Purpose**: Necessary for accessing online databases, administering online surveys, cloud-based analysis tools, and communication with team members and stakeholders.

#### **Printers and Scanners**

Printer: Laser with color printing capability

Scanner: High-resolution document scanner

**Purpose**: Useful for printing survey materials, reports, and other documentation; scanning completed paper surveys (if applicable).

#### **External Storage Devices**

External Hard Drive or SSD with at least 1 TB capacity

USB 3.0 or higher interface

**Purpose**: For backing up important project data and documents.

#### s

#### **Operating System**

* + **Specification**: Windows 10, macOS, or Linux
  + **Purpose**: Provides the primary platform for all software applications and tools.

#### **Office Suite**

* + **Specification**: Microsoft Office 365 or LibreOffice
  + **Purpose**: For creating and editing documents, spreadsheets, and presentations.

#### **Statistical Analysis Software**

* + **Specification**: SPSS, R, or Python (with relevant libraries such as pandas, numpy, scikit-learn)
  + **Purpose**: For analyzing survey data and performing statistical tests.

#### **Survey Design and Administration Tools**

* + **Specification**: SurveyMonkey, Google Forms, or Qualtrics
  + **Purpose**: For designing and administering online surveys to collect data on employee security behaviors and attitudes.

#### **Psychometric Analysis Tools**

* + **Specification**: Custom psychometric scale development software or statistical packages capable of psychometric analysis (such as R’s psych package)
  + **Purpose**: For developing and validating the psychometric scale.

#### **Data Visualization Software**

* + **Specification**: Tableau, Power BI, or Python libraries (such as matplotlib, seaborn)
  + **Purpose**: For creating visual representations of data analysis results.

#### **Reference Management Software**

* + **Specification**: EndNote, Mendeley, or Zotero
  + **Purpose**: For managing references and citations during the literature review and report writing.

#### **Collaboration and Communication Tools**

* + **Specification**: Microsoft Teams, Slack, or Zoom
  + **Purpose**: For team collaboration, communication, and virtual meetings.

#### **Project Management Software**

* + **Specification**: Asana, Trello, or Microsoft Project
  + **Purpose**: For tracking project progress, managing tasks, and ensuring adherence to timelines.

#### **Cloud Storage Services**

* + **Specification**: Google Drive, Dropbox, or OneDrive
  + **Purpose**: For storing and sharing project files and documents securely.

By ensuring the availability and proper configuration of the specified hardware and software, the research team can efficiently conduct the study, analyze the data, and produce high-quality reports, ultimately contributing to the successful completion of the project.

# Responsibilities of the Team Members

| **Task/Activity** | **Farwah** | **Emaan** | **Hafsa** | **Mr.Jibran** |
| --- | --- | --- | --- | --- |
| **Project Planning** | R,A | R | R | C,I |
| **Literature Review** | R,A | R | R | C,I |
| **Identifying Factors** | R,A | I | R | C,I |
| **Design Platform** | I | R,A | R,A | C,I |
| **Design Questionnaire** | R,A | R,A | R | C,I |
| **Integrate CybPsy Principals** | R,A | C.I | I | C,I |
| **Predicting Human Behavior** | R,A | R,A | R | C,I |
| **Design Assessment Report** | R,A | R,A | R | C,I |
| **Evaluate Performance** | R,A | I | R | C,I |
| **Documentation** | A,I | R | R,A | C,I |

# Planning

| **Task/Activity** | **Duration** |
| --- | --- |
| **Project Planning** | 2 weeks |
| **Literature Review/Competitive Analysis** | 4 weeks |
| **Identifying Factors** | 2 weeks |
| **Design Questionnaire Database** | 6 weeks |
| **Design & Development Platform** | 8 weeks |
| **Integrate CybPsy Principals** | 8 weeks |
| **Predicting Human Behaviour** | 4 weeks |
| **Design Assessment Report** | 6 weeks |
| **Evaluate Performance** | 4 weeks |
| **Documentation** | 8 weeks |
| **Total Estimated Duration** | **52 weeks** |

**12.References**

1. Kannelønning, K. and Katsikas, S.K. (2023) ‘A systematic literature review of how cybersecurity-related behavior has been assessed’, *Information & Computer Security*, 31(4), pp. 463–477. Available at: https://doi.org/10.1108/ICS-08-2022-0139.
2. Almansoori, A., Al-Emran, M. and Shaalan, K. (2023) ‘Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories’, *Applied Sciences*, 13(9), p. 5700. Available at: https://doi.org/10.3390/app13095700.
3. Rohan, R. *et al.* (2023) ‘A systematic literature review of cybersecurity scales assessing information security awareness’, *Heliyon*, 9(3). Available at: https://doi.org/10.1016/j.heliyon.2023.e14234.
4. Khan, N.F. *et al.* (2022) ‘The cybersecurity behavioral research: A tertiary study’, *Computers & Security*, 120, p. 102826. Available at: https://doi.org/10.1016/j.cose.2022.102826.
5. Rohan, R. *et al.* (2021) ‘Understanding of Human Factors in Cybersecurity: A Systematic Literature Review’, in *2021 International Conference on Computational Performance Evaluation (ComPE)*. IEEE, pp. 133–140. Available at: https://doi.org/10.1109/ComPE53109.2021.9752358.
6. Rahman, T. *et al.* (2021) ‘Human Factors in Cybersecurity: A Scoping Review’, *ACM International Conference Proceeding Series* [Preprint]. Available at: https://doi.org/10.1145/3468784.3468789.
7. Maalem, A. *et al.* (2020) ‘Review and insight on the behavioral aspects of cybersecurity’, *Cybersecurity*, 3(1), p. 10. Available at: https://doi.org/10.1186/s42400-020-00050-w.