VISHWAR: A Human-Centric Cybersecurity Training and Risk Measurement Platform

Mayukh Paul, M.S. in Cybersecurity

FACULTY MENTOR: Daniel Galeon, MBA

Katz School of Science and Health

Introduction

Human Cybersecurity Risk Costs Millions Annually

- 95% of breaches involve human error, including phishing and credential misuse.
- Social engineering—tricking users into revealing sensitive information—is a leading initial access vector.
- The average cost of a social engineering breach is $4.88 million.

Current Training Is Not Sufficient

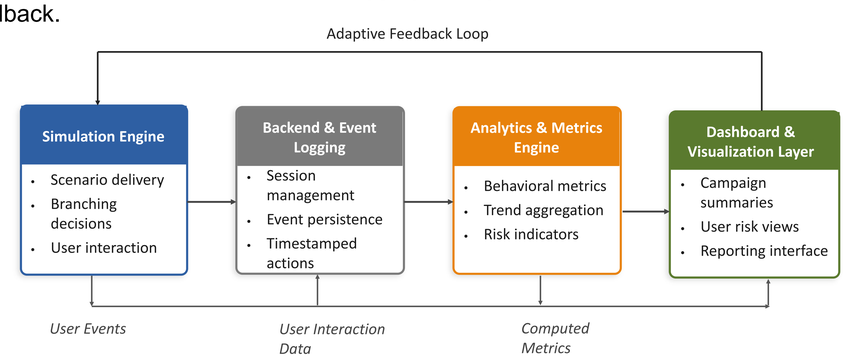
- Organizations rely on annual training, quizzes, and phishing tests
- Behavioral improvement only 2–19% and declines over time
- No continuous measurement of human risk

Project VISHWAR Introduces A Solution

- VISHWAR **(Virtually Interactive Simulation Hub For Warfare Against Ruses)** introduces a simulation-driven framework that treats human behavior as a measurable cybersecurity variable and enables continuous human risk management through simulation, feedback, and analytics.

Methodology

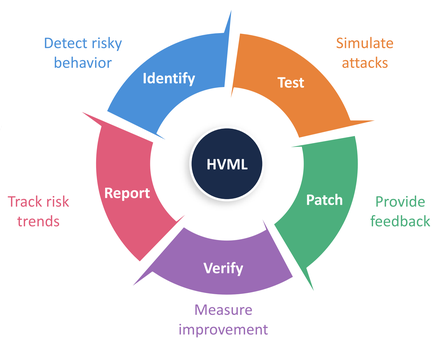
VISHWAR is a web-based platform that simulates real-world social engineering attacks and measures behavioral responses using quantitative security metrics. Platform components include behavioral data logging , analytics dashboard, and personalized feedback.



VISHWAR System Architecture

Human Vulnerability Management Lifecycle

The framework introduces a Human Vulnerability Management Lifecycle (HVML), which treats human susceptibility as a measurable security risk through five stages: identify, test, patch, verify, and report. This approach enables continuous measurement, improvement, and tracking of user behavior over time.



HVML Lifecycle

Results

- Evaluation conducted on a controlled group of users interacting with multiple simulation scenarios
- CTR decreased by 15–25% after feedback-driven interventions
- Time-to-Report improved significantly, with faster reporting in later simulations.
- Users showed high variability in risk across attack types, highlighting need for personalized training.
- Repeat risk events revealed behavioral patterns rather than one-time mistakes.
- Overall Human Risk Score showed downward trend across simulation cycles.

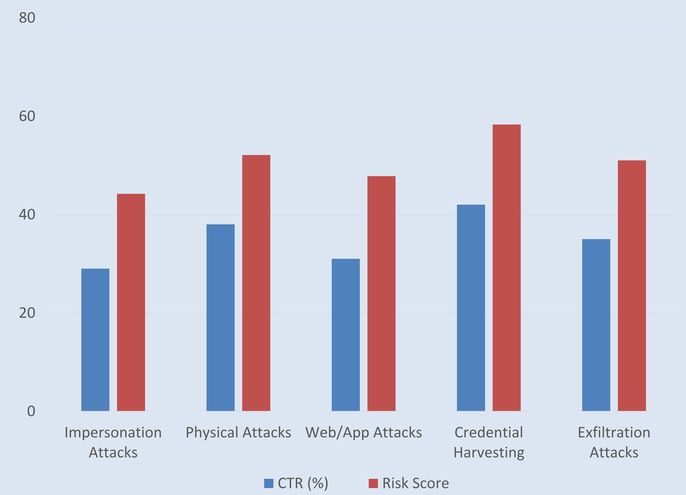
Behavioral risk scores across attack vectors | Score range: 0–60 | Green = Low Risk Red = High Risk

Risk Level: ◄ Low High ►

LEARNER	Email Phishing	Vishing	Pretexting	USB Baiting	Fake Website	Credential Stuffing	MFA Fatigue	QR Phishing	Risk Level
User A	45.2	58.3	36.2	52.7	46.0	49.5	37.9	50.8	High
User B	24.7	23.8	25.4	31.9	31.3	24.0	19.6	28.2	Low
User C	12.8	2.8	10.1	2.8	10.1	3.4	4.1	3.4	Very Low
User D	50.5	45.5	52.2	45.6	48.0	34.8	35.9	39.8	High
User E	48.0	46.7	39.4	37.9	36.4	36.0	38.1	35.3	High
User F	15.6	22.9	14.8	22.4	21.4	25.3	16.9	14.2	Low

Note: Scores represent simulated vulnerability percentage per attack vector. Higher scores indicate greater susceptibility.

Attack Type Vulnerability Heatmap



Behavioral Risk and Click-Through Rate Across Social Engineering Attack Modules

Behavioral Insights from Metrics

Metric	Key Finding
Click-Through Rate (CTR)	Higher CTR observed in phishing scenarios compared to impersonation attacks
Time-to-Report (TTR)	Reporting time improved across repeated simulations
Quiz Score	Increased after feedback-driven training cycles
Consistency Index	Users showed inconsistent behavior across attack types
Repeat Risk Events	Certain users repeatedly failed similar attack patterns
Human Risk Score	Overall risk decreased after exposure to simulations

Key Contributions

- Introduces Human Vulnerability Management Lifecycle
- Defines quantitative human risk metrics
- Implements simulation-based behavioral measurement
- Demonstrates prototype with real participants

Conclusions

- VISHWAR introduces a simulation-driven framework for measuring and improving human cybersecurity behavior.
- Realistic attack scenarios combined with behavioral analytics and feedback enable continuous human risk management using multi-dimensional metrics.
- The platform establishes a foundation for scalable deployment and future research in human-centric cybersecurity defense.

Acknowledgements

I would like to thank Professor Daniel Galeon for his guidance and support throughout the development of this project. Special thanks to my fellow students Benjamin Krev and Yash Dekate for their contributions to the design and development of simulation storylines used in the VISHWAR framework.

References