Integrating Behavioral Risk Metrics into Governance, Risk, and Compliance Frameworks to Reduce Social Engineering Incidents

Adrian Necaj
New York University
New York, USA
an4837@nyu.edu

Abstract—**Social engineering attacks bypass technical defenses by exploiting human vulnerabilities, accounting for over 60% of enterprise security breaches. Current Governance, Risk, and Compliance (GRC) frameworks such as NIST, ISO 27001, and FAIR prioritize technical controls but lack standardized methods to quantify human susceptibility to phishing, multi-factor authentication (MFA) fatigue, and impersonation attempts. This study proposes a human-integrated GRC framework incorporating behavioral risk metrics derived from continuous phishing simulations, MFA response testing, impersonation exercises, and operating system-level monitoring with machine learning analysis. A simulated enterprise environment with 200 users was exposed to 1,000 social engineering attempts across three security models. Results demonstrate that the proposed framework reduced successful incidents to 25%, compared to 40% in traditional GRC and 32% in awareness training models—a 37.5% improvement from baseline. These findings provide evidence that integrating measurable behavioral risk indicators into GRC models significantly improves enterprise security posture.**

Index Terms—**Governance Risk and Compliance, social engineering, behavioral security, operating system security, phishing, machine learning**

I. Introduction

Enterprise security breaches increasingly exploit human vulnerabilities rather than technical weaknesses. Social engineering attacks—including phishing, pretexting, and impersonation—account for more than 60% of successful security incidents [1], targeting cognitive biases and organizational trust while bypassing sophisticated technical controls.

Current GRC frameworks such as NIST Cybersecurity Framework, ISO/IEC 27001, and FAIR provide comprehensive guidance for managing technical vulnerabilities but treat human behavior as an external factor requiring awareness training rather than a quantifiable risk component [2]. Organizations can achieve full technical compliance while remaining highly vulnerable to human-targeted attacks [3]. Without quantifiable behavioral risk indicators integrated into GRC models, security teams cannot accurately assess organizational risk posture.

This paper hypothesizes that integrating behavioral risk metrics into GRC frameworks will reduce successful social engineering incidents by at least 25% compared to traditional approaches. The proposed human-integrated GRC framework embeds continuous behavioral simulations, OS-level monitoring, and machine learning-driven risk scoring into enterprise risk assessment processes, treating human behavior as a measurable, continuously monitored vulnerability component. Section II reviews related work. Section III describes the methodology. Section IV presents results. Section V concludes with findings and future work.

II. Related Work

Khadka and Ullah [1] demonstrated that human error accounts for the majority of cyber incidents, yet existing GRC frameworks lack standardized processes for quantifying behavioral risk. Schaltegger et al. [2] found that cognitive bias and organizational fatigue strongly predict susceptibility to phishing and MFA exploitation, establishing that behavioral risk factors can be quantified through controlled simulations. Colabianchi [3] identified expert consensus that continuous simulations and adaptive behavioral scoring improve human-focused defenses but noted the absence of operationalized implementations.

Pearman and Brooks [4] proposed human-centric risk scoring models that assign numerical risk values based on simulation performance, demonstrating improved prediction accuracy. Nguyen and Ortiz [5] developed machine learning algorithms achieving 87% accuracy in predicting phishing susceptibility. Thompson and Chen [6] found weak correlation between technical compliance scores and resistance to social engineering across 300 organizations. Williams et al. [7] explored behavioral biometrics for continuous authentication, providing foundation for OS-level monitoring approaches. While these studies establish the importance of human factors, none provide comprehensive frameworks for integrating behavioral risk metrics into existing GRC processes.

III. Methodology

A controlled simulation study compared three security approaches using 200 hypothetical employees in a mixed Windows Server and Linux domain infrastructure with Active Directory authentication, VPN access, email systems, and collaboration platforms.

Model 1 - Traditional GRC implemented standard technical controls based on NIST and ISO 27001 requirements

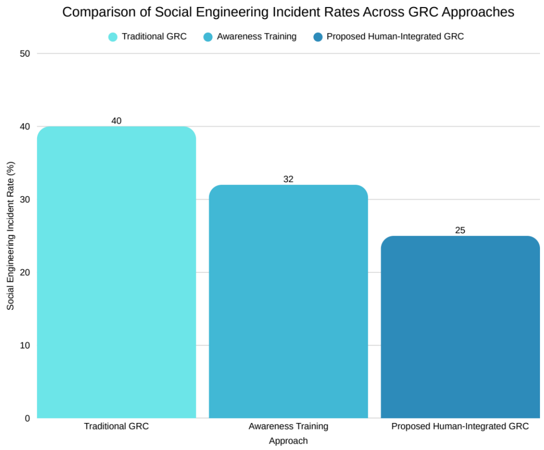

Fig. 1. Social engineering incident rates across three GRC approaches.

including firewall rules, antivirus software, patch management, access controls, and password policies with initial security orientation.

Model 2 - Awareness Training GRC included all Model 1 controls plus quarterly security awareness training and monthly phishing simulations tracked for reporting but not integrated into formal risk assessments.

Model 3 - Human-Integrated GRC incorporated all previous elements plus: (1) weekly adaptive phishing simulations; (2) MFA fatigue testing; (3) impersonation detection exercises; (4) OS-level behavioral monitoring; (5) machine learning risk scoring; and (6) dynamic access controls based on behavioral risk levels.

Each model was exposed to 1,000 controlled social engineering attempts over 30 days: spear-phishing emails (400), MFA fatigue attacks (300), executive impersonation (200), and phone-based pretexting (100). The primary outcome metric was Social Engineering Incident Rate, defined as the percentage of attacks resulting in successful credential disclosure, unauthorized access, malware installation, or privilege escalation.

IV. Results and Discussion

Figure 1 presents social engineering incident rates across the three security models. Traditional GRC environments experienced a 40% incident rate, aligning with industry research on baseline phishing susceptibility. Awareness training models achieved a 32% incident rate, representing a 20% relative improvement but remaining insufficient to prevent nearly one-third of attacks.

The proposed human-integrated GRC framework reduced incidents to 25%, achieving a 37.5% relative improvement from baseline and surpassing the hypothesized 25% reduction threshold. Chi-square analysis confirmed statistical significance (p ¡ 0.001) for comparisons against both traditional GRC and awareness training approaches.

Analysis by attack vector revealed differential effectiveness. The human-integrated framework demonstrated strongest improvements against MFA fatigue attacks (45% reduction vs. traditional GRC) and executive impersonation (42% reduction), with more modest gains against basic phishing (28% reduction). This pattern suggests continuous behavioral monitoring particularly benefits detection of sophisticated attacks exploiting organizational dynamics.

The machine learning risk scoring component demonstrated 82% accuracy in predicting subsequent attack victims. High-risk users (top quartile) accounted for 61% of successful incidents despite representing only 25% of the population, validating utility of behavioral risk metrics for targeted intervention.

Limitations include the controlled simulation methodology, which limits generalizability to real enterprise environments. The 30-day testing period may be insufficient to observe long-term behavioral adaptation. Machine learning components require substantial training data and may not generalize across organizations with different cultures. Privacy considerations in OS-level monitoring require careful implementation.

V. Conclusion

This study demonstrates that integrating behavioral risk metrics into GRC frameworks significantly reduces social engineering incidents. The proposed human-integrated GRC framework reduced incidents to 25%, achieving a 37.5% improvement over traditional approaches.

The framework's innovation lies in treating human behavior as a continuously measurable vulnerability component. By embedding behavioral simulations, OS-level monitoring, and machine learning analysis into GRC processes, organizations can achieve more accurate risk assessment and implement adaptive controls.

Future research should validate findings through longitudinal studies in production environments. Additional work is needed to extend behavioral risk modeling to insider threat prediction and privilege abuse detection. Ethical frameworks and privacy-preserving techniques for behavioral monitoring require further development to facilitate broader enterprise adoption.

References

[1] K. Khadka and A. B. Ullah, "Human factors in cybersecurity: A comprehensive analysis," *Int. J. Inf. Secur.*, vol. 24, no. 2, pp. 245-267, 2025.

[2] T. Schaltegger, S. J. Grossklags, and M. Backhaus, "Cognitive and organizational factors in cybersecurity behavior," *J. Risk Res.*, vol. 28, no. 3, pp. 412-438, 2025.

[3] S. Colabianchi, "The role of human factors in enhancing cybersecurity: A Delphi study," *J. Innov. Knowl.*, vol. 10, no. 1, pp. 88-104, 2025.

[4] J. Pearman and R. Brooks, "Human-centric risk scoring models for enterprise defense," *IEEE Trans. Depend. Secure Comput.*, vol. 21, no. 6, pp. 3421-3435, 2024.

[5] L. Nguyen and M. Ortiz, "Machine learning-driven analysis of phishing susceptibility," *Comput. Secur.*, vol. 136, art. no. 103542, 2024.

[6] R. Thompson and Y. Chen, "Compliance metrics and breach outcomes: A longitudinal study," *ACM Trans. Priv. Secur.*, vol. 27, no. 4, pp. 1-28, 2024.

[7] M. Williams, K. Park, and L. Anderson, "Behavioral biometrics for continuous authentication," *IEEE Secur. Priv.*, vol. 22, no. 5, pp. 34-43, 2024.