Enhancing Cybersecurity Awareness Through Real-World Case Studies: A Data-Driven Evaluation of Training Effectiveness

Author: Fabian Eduardo Garcia Romero
Advisor: Alfredo Cruz, Ph.D.
Electric & Computer Engineering and Computer Science

Abstract

Social engineering attacks have emerged as a dominant threat vector, bypassing technical defenses by exploiting human behavior. The study evaluates the effectiveness of real-world case study integration in cybersecurity training to strengthen awareness and user response. A mixed-methods approach, incorporating data-driven and scenario-based methodologies, was employed to measure user engagement, knowledge retention, and behavior change. Findings indicate that real case presentations significantly outperform traditional training by fostering deeper engagement, improving long-term awareness, and strengthening the human element in cybersecurity defense. The study contributes an adaptive, scalable educational framework that leverages real-world cases, interactive methods, and forward-looking technologies such as AI-driven simulations and behavior monitoring tools. Additionally, the proposed model aligns with evolving workforce competencies sought by public and private sector employers, offering a relevant, industry-informed solution to cybersecurity education. Integrating behavioral insights, real-world dynamics, and emerging technologies provides an innovative approach to preparing users to confront increasingly intricate cyber threats.

Introduction

Social engineering is a significant cybersecurity vulnerability, ranking among the top threats according to the FBI IC3 2024 Report [1]. These attacks exploit psychological manipulation rather than technical flaws, targeting individual behavior to bypass advanced security systems. Despite significant investments in cybersecurity infrastructure, organizations continue to suffer breaches from phishing and impersonation tactics. Traditional training models, which are static, compliance-based, and theory-heavy, often fail to yield significant behavioral change or knowledge retention due to lack of interactivity, practical application, and contextual relevance. The FBI IC3 2024 Report documented over 4.2 million complaints and $50.5 billion in financial losses over the past five years, emphasizing the need for training that incorporates behavioral insights [1]. The study aims to evaluate the effectiveness of real-case cybersecurity training in enhancing threat recognition, knowledge retention, and behavioral resilience against social engineering attacks. The model seeks to conform to emerging workforce expectations, guaranteeing that cybersecurity awareness training is scalable and adaptable to changing threat environments.

Background

Despite existing technological defenses, research highlights persistent gaps in user awareness and readiness against phishing, vishing, and impersonation threats [2]. Frameworks such as the NIST Cybersecurity Framework [3] and Protection Motivation Theory (PMT) [4] underscore the importance of behavior-focused strategies to fortify the human element. Experiential methods like Kolb's learning model [5] and scenario-based learning have proven effective in enhancing retention, threat recognition, and proactive security behavior. Integrating real-world cases and adaptive simulations further improves emotional engagement, situational awareness, and critical thinking in combating social engineering. These insights support the development of the real-case training framework presented in this study.

Problem

Social engineering attacks pose a serious threat by targeting human behavior rather than technical systems, often bypassing even the most advanced defenses. Many individuals and organizations remain unprepared to recognize and respond to these tactics, which have become increasingly sophisticated and damaging. Traditional training methods often fall short by being too theoretical and not adapting to real-world threats. This project proposes using real-case scenarios to raise awareness and improve users' ability to detect and respond to social engineering, aiming to strengthen the human element in cybersecurity. The proposed framework integrates real-world case studies into cybersecurity training modules to address the gaps identified in traditional cybersecurity education. As illustrated in Figure 1, modern training strategies such as immersive case studies, simulations, role-playing, and gamification enhance knowledge retention, directly contributing to improved threat recognition, directly contributing to improved threat recognition and measurable behavioral change.

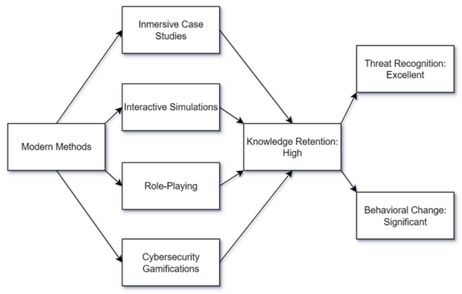

Figure 1

Modern Training Methods and Their Impact on Knowledge Retention

Methodology

The research uses a mixed-methods case study design to systematically evaluate how real-case presentations impact cybersecurity awareness. It combines quantitative data analysis of training outcomes with qualitative insights from real-world cases. Each cybersecurity incident or training activity is treated as an individual case for detailed comparison using Qualitative Comparative Analysis (QCA), which helps identify patterns of training practices and contextual factors linked to higher awareness. Data was gathered exclusively from secondary sources, including public cybersecurity datasets and academic literature. Quantitative metrics like phishing simulation success rates and post-training survey results were used alongside qualitative information about training types and outcomes. No direct interaction with participants occurred, so ethical approval was not required. Based on the findings, an educational framework was developed to enhance cybersecurity training. It integrates real-world incidents, interactive learning methods, reflection activities, and continuous evaluation tools. The framework is designed to be adaptable to various formats and organizational needs. The proposed framework offers a theoretical implementation of cybersecurity awareness training grounded in the analysis of existing datasets and prior research findings. It was developed in response to real-world cybersecurity incidents, using structured case studies to detail attacker tactics, breach impacts, and mitigation strategies. These authentic scenarios were chosen for their clarity, relevance, and alignment with learning objectives, promoting better engagement and knowledge retention compared to theoretical approaches. Each session incorporated contextual materials, visual aids, and open-ended questions to encourage critical thinking and personal reflection, using interactive storytelling techniques to reinforce risk awareness. Figure 2 illustrates the structure of this proposed framework, which emphasizes regular, engaging, and practical training to improve user awareness, retention, and behavior. It highlights the importance of immersive methods like simulations, despite their resource demands, for building a security-conscious culture and reducing human error.

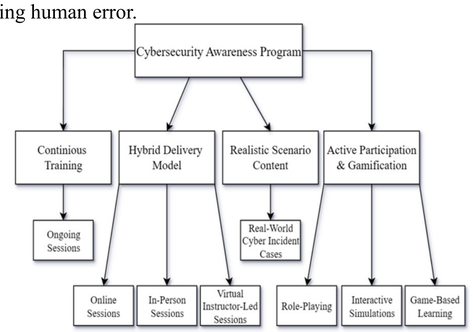

Figure 2

Cybersecurity Awareness Framework Diagram

The framework also aligns with the NIST Cybersecurity Framework, extending beyond the traditional "Protect" function to support the "Detect" and "Respond" capabilities through realistic training [3]. Some of the best practices were incorporated into the framework to enhance its effectiveness, including the need for relevance of content, personalization, and active engagement of learners. Some main strategies included frequent updating of training materials based on new events, personalizing modules for tackling industry-specific threats, and including interactive elements that allow reflection and discussions. The framework also suggested the development of a graded archive of case studies for flexible rollout of training. To facilitate learning and promote long-term behavior change, implementation included short, low-stakes tests, problem-solving activities with practical relevance, and periodic reinforcement sessions.

Results and Discussion

The real-world case-based training model evaluation used key performance indicators (KPIs) such as phishing detection, knowledge retention, behavioral change, and engagement. As shown in Figure 3, the model led to significant improvements across all metrics; phishing detection rose from 30% to 80%, knowledge retention from 20% to 75%, behavioral change from 30% to 80%, and engagement from 40% to 85%. Based on secondary data and past research, these gains validate the effectiveness of immersive, scenario-based cybersecurity education. The performance difference analysis highlights how modern training practices, embracing concepts like real-case integration, hybrid delivery, and interactive learning, strengthen awareness, engagement, and behavioral resilience. The findings validate a broader shift in cybersecurity training away from conventional, one-time yearly sessions and toward adaptive, ongoing programs. The discussion also confirms this trend, showing that regular training programs, particularly when reinforced by leadership buy-in and mixed delivery modalities, foster a more robust culture of cybersecurity. Blending practical content and gamification approaches promotes relevance and engagement, while enabling sustained behavior shifts. Additionally, incorporating artificial intelligence (AI) in awareness training presents new possibilities for customization and real-time adaptation. AI technologies like adaptive simulations, chatbots, and performance analytics allow content tailoring to individual learners, reducing training fatigue and improving effectiveness. In all, the study suggests an adaptive training model that is interactive, customized, and grounded in real-world threats to meet the demands of a growing, sophisticated cyber threat landscape.

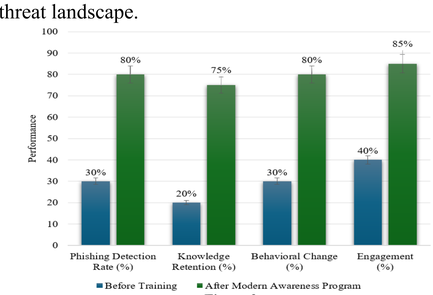

Figure 3

Impact of Real-Case Training on Cybersecurity Awareness Metrics

Conclusions

The project discovers that interactive and case-based training in realistic settings is far more effective than traditional theoretical approaches to boost cybersecurity awareness. These approaches improve retention, behavior, and threat detection by actively involving participants in realistic scenarios. Implementing realistic and engaging educational methods can foster a security-conscious workforce, reducing vulnerability to cyber threats and fostering a proactive cybersecurity culture.

Future Work

This project suggests that future research should address gaps by conducting longitudinal studies, determining the effectiveness of ongoing reinforcement, customizing training programs, comparing interactive formats, and exploring innovative approaches like virtual reality simulations, AI-driven trainings, and personalized learning to keep cybersecurity training dynamic, engaging, and aligned with evolving threat landscapes.

Acknowledgements

I am grateful for the support and assistance provided by the NSF CyberCorps SFS program and PUPR. Alfredo Cruz for his exceptional teaching methodologies and profound insights.

References

[1] Internet Crime Complaint Center (IC3), *2024 Internet Crime Report*, Federal Bureau of Investigation, Washington, D.C., Rep. Apr. 23, 2025. [Online]. Available: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[2] H. Aldawood and G. Skinner, "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues," *Future Internet*, vol. 11, no. 3, p. 73, Mar. 2019, doi: 10.3390/fi11030073.

[3] D. P. F. Möller, "NIST Cybersecurity Framework and MITRE Cybersecurity Criteria," in Advances in Information Security, 2023, pp. 231–271, doi: 10.1007/978-3-031-26845-8_5.

[4] S. Sutton, "Health Behavior: Psychosocial theories," in Elsevier eBooks, 2001, pp. 6499–6506, doi: 10.1016/b0-08-043076-7/03872-9.

[5] D. A. Kolb, *Experiential learning: Experience as the source of learning and development*. Prentice Hall, 1984. [Online]. Available: https://www.researchgate.net/publication/235701029_Experiential_Learning_Experience_As_The_Source_Of_Learning_And_Development