Interdisciplinary Research Paper

by

Galen Cole

A Research Paper

Submitted to IDS300W

Old Dominion University

Final Paper

February, 2024

Abstract: Cybersecurity threats continue to evolve, requiring organizations to implement proactive training and integrate security awareness into company culture. This paper explores how an interdisciplinary approach, drawing from computer science, education, and psychology, enhances cybersecurity training by fostering both technical competence and behavioral change. By synthesizing insights from these disciplines, this study demonstrates that a structured and adaptive training strategy significantly mitigates cyber risks and strengthens organizational security.

Keywords: cybersecurity, training, organizational culture, psychology, education, computer science, evolving, information technology

Introduction

Cybersecurity threats continue to evolve, necessitating proactive measures to safeguard sensitive information. Organizations must embed security awareness into their culture, ensuring employees not only possess technical knowledge but also develop long-term, security-conscious behaviors. The challenge lies not only in equipping employees with technical knowledge but also in ensuring behavioral adaptation and long-term compliance. By synthesizing insights from these fields, this study aims to demonstrate that a comprehensive and structured training strategy is crucial to mitigating cyber risks and fostering a resilient security culture.

Methodology

This research follows Repko and Szostak's interdisciplinary framework, integrating insights from multiple disciplines to form a comprehensive understanding of cybersecurity training. The study employs the 10-step interdisciplinary research process, beginning with defining the problem of cybersecurity training gaps and justifying an interdisciplinary approach. The methodology involves identifying relevant disciplines: computer science, education, and psychology, and conducting a literature review within each. Insights from these fields are analyzed to evaluate conflicting perspectives and establish common ground. By synthesizing technical, pedagogical, and psychological perspectives, this study develops a holistic training strategy that balances technical proficiency, engagement, and behavioral reinforcement. The approach ensures that organizations not only educate employees on cybersecurity but also foster long-term adherence to best practices.

Computer Science

Cybersecurity training must address evolving threats through scenario-based simulations, penetration testing, and real-time threat analysis (Chowdhury & Gkioulos, 2021). Research indicates that technical cybersecurity training should not be static but rather evolve alongside emerging cyber threats. Organizations must implement adaptive training programs incorporating artificial intelligence and machine learning to enhance real-time defense mechanisms. Automation in cybersecurity, such as AI-driven threat detection, supports human vigilance but requires ongoing training (Taherdoost, 2024). Hands-on training, such as simulated attacks, enhances readiness, while periodic assessments measure retention. A structured curriculum incorporating continuous updates ensures employees remain prepared for emerging threats. Furthermore, periodic cybersecurity drills and penetration tests provide employees with direct experience in mitigating potential threats. Effective cybersecurity programs also integrate modular learning paths, allowing employees to specialize in areas such as network security, social engineering defenses, and incident response. These measures ensure employees develop technical competency while maintaining agility in responding to cyber threats.

Cybersecurity training must cover threat landscapes, attack vectors, and mitigation techniques. Effective training incorporates interactive, scenario-based simulations to reinforce technical knowledge (Chowdhury & Gkioulos, 2021). E-learning platforms, penetration testing exercises, and real-time threat analysis tools enable employees to apply learned concepts in controlled environments. Furthermore, automation in cybersecurity, such as AI-driven threat detection and automated response systems, must be complemented by human vigilance (Taherdoost, 2024). Organizations must prioritize adaptive training methods that evolve alongside emerging threats and include periodic assessments to measure effectiveness.

Education

Effective cybersecurity education incorporates instructional design, gamification, and competency-based learning (Stănică, 2014). Gamification and role-playing exercises improve engagement and knowledge retention (Bognár & Bottyán, 2024). Regular training updates and assessments ensure employees stay informed. Leadership training models emphasize structured delivery and reinforcement mechanisms, essential for sustained learning outcomes.

Beyond engagement strategies, research suggests that cybersecurity education must be tailored to diverse organizational roles. Employees in administrative positions require different training than IT security teams, necessitating role-based learning paths. Cybersecurity training should also leverage microlearning techniques, short and focused training modules, to accommodate different learning paces and ensure accessibility. Additionally, incorporating interactive assessments and real-world case studies bridges the gap between theoretical knowledge and practical application. By aligning cybersecurity education with business operations, organizations can ensure that security practices become ingrained in employees' daily responsibilities.

Cybersecurity training must accommodate diverse learning styles. Effective programs incorporate instructional design principles, including scaffolding techniques and competency-based learning (Stănică, 2014). Research indicates that gamification, role-playing exercises, and periodic assessments enhance retention and engagement (Bognár & Bottyán, 2024). A structured approach to cybersecurity education includes continuous updates to training materials and integration into employee onboarding to ensure foundational security knowledge.

Psychology

Behavioral change is key to cybersecurity training success. Compliance programs influence employee attitudes, reducing cognitive biases like overconfidence in security knowledge (Deciu, 2020). Reinforcement strategies, such as structured feedback loops and incentives, improve adherence (Lacerenza et al., 2017). Organizations benefit from embedding security awareness into daily operations through sustained behavioral reinforcement.

The psychological impact of security training extends beyond compliance. Employees often exhibit resistance to security policies due to cognitive overload or lack of perceived relevance. Research suggests that organizations must frame security training in terms of personal responsibility and potential consequences. Psychological conditioning, such as reinforcement through simulated phishing attacks, helps employees develop instinctual responses to threats. Additionally, integrating positive reinforcement, such as rewards for consistent security compliance, fosters long-term behavioral change. By addressing human factors alongside technical measures, organizations can close the gap between awareness and action.

The success of cybersecurity training hinges on behavioral change and risk perception. Compliance programs influence employees' attitudes toward security practices (Deciu, 2020). Cognitive biases, such as optimism bias and overconfidence, often lead employees to underestimate security risks. Training should emphasize real-world consequences and reinforce security-first mindsets. Structured reinforcement mechanisms, such as feedback loops and periodic security assessments, enhance long-term compliance (Lacerenza et al., 2017).

Applications & Synthesis

Cybersecurity training programs are most effective when they incorporate interactive and structured learning techniques. Integrating insights from computer science, education, and psychology, organizations can develop holistic cybersecurity training programs that provide technical skills and foster behavioral change. Research by Chowdhury and Gkioulos (2021) and Taherdoost (2024) suggests that hands-on, scenario-based cybersecurity in critical infrastructure training, arguing that practical exposure enhances skill retention and engagement. Educational research by Stănică (2014) and Bognár & Bottyán (2024) emphasizes structured learning methodologies, ensuring training effectiveness across diverse employees. Although Deciu (2020) primarily examines compliance programs, the study suggests that training must align with organizational culture to increase effectiveness and engagement. Similarly, Lacerenza et al. (2017) emphasize structured training design in leadership development, reinforcing the need for well-organized cybersecurity training programs. Together, these findings suggest that cybersecurity education should move beyond passive learning and adopt a more interactive, psychologically informed, and assessment-driven approach to ensure long-term effectiveness. By fostering a cybersecurity-centric culture through well-designed training programs, organizations can significantly reduce human-related cyber incidents. Psychological insights refine training effectiveness by addressing behavioral biases (Deciu, 2020; Lacerenza et al., 2017). Organizations can apply these principles through periodic security assessments, feedback loops, and behavioral reinforcement strategies.

To implement an interdisciplinary cybersecurity training model, organizations must align training programs with both organizational objectives and employee roles. A successful model integrates technical simulations with adaptive learning frameworks, ensuring employees not only

understand threats but can respond effectively. Organizations should leverage behavioral psychology techniques, such as social proof and behavioral nudging, to reinforce security awareness continuously. Additionally, leadership engagement plays a crucial role in embedding security culture, with management demonstrating security best practices and fostering an environment of continuous improvement. By merging technical expertise, educational methodologies, and behavioral science, organizations can create a cybersecurity training framework that is both comprehensive and adaptable to evolving threats.

Conclusion

Effective cybersecurity requires integrating technical training, structured learning, and behavioral reinforcement. Research from computer science, education, and psychology highlights that hands-on simulations, adaptive learning, and compliance strategies improve security awareness. Leadership support and continuous reinforcement embed security into company culture, ensuring long-term adherence. Organizations must prioritize interdisciplinary training models to mitigate cyber threats. A proactive security culture strengthens resilience and reduces vulnerabilities. Enhancing cybersecurity across organizations requires robust training programs addressing both technical competencies and behavioral factors. Integrating interdisciplinary perspectives ensures that cybersecurity training is effective and sustainable. Research highlights that hands-on training, structured learning methodologies, and behavioral reinforcement are critical to internalizing cybersecurity best practices. Leadership engagement and continuous reinforcement solidify security awareness within an organization. Ultimately, fostering a proactive security culture reduces vulnerabilities and enhances resilience against evolving cyber threats.

References

Bognár, L., & Bottyán, L. (2024). Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. *Education Sciences*, *14*(6), 588. https://doi-org.proxy.lib.odu.edu/10.3390/educsci14060588.

Chowdhury, N., Gkioulos V. (2021). Cyber security training for critical infrastructure protection: A literature review. Computer Science Review Vol. 40. https://doi.org/10.1016/j.cosrev.2021.100361.

Deciu, V., (December, 2020). Impact of Compliance Programs on Organizational Psychology. Psychology No. 11-12. https://doi.org/10.4236/psych.2020.1112118.

Stănică, O. (2014). E-Learning for the Development New Skills in Security of Information Field : E-Cyber Security Competence. ELearning & Software for Education, 2, 478–485. https://doi-org.proxy.lib.odu.edu/10.12753/2066-026X-14-129.

Taherdoost, H., (2024). A Critical Review on Cybersecurity Awareness Frameworks and Training Models. Procedia Computer Science Vol. 235. https://doi.org/10.1016/j.procs.2024.04.156.

Lacerenza, C. N., Reyes, D. L., Marlow, S. L., Joseph, D. L., & Salas, E. (2017). Leadership training design, delivery, and implementation: A meta-analysis. *Journal of Applied Psychology*, *102*(12), 1686–1718. https://doi.org/10.1037/apl0000241.

Appendix: Extra Credit

Initially, I would outline potential disciplines, evaluating them through a pros and cons list or conducting a simple review of relevant articles to assess their value to my topic. After selecting the appropriate disciplines, I utilized resources like ODU LibGuide, and EBSCO, rather than relying on third-party databases like Google Scholar. Meeting with the ODU resource librarian confirmed some of my assumptions, though it was less helpful than anticipated. Next time, I plan to be more strategic by not only providing an overview of my paper but also preparing specific questions and related topics to discuss. This insight highlighted an aspect I was theoretically aware of but hadn't personally experienced: the rigorous preliminary work required before starting on a paper. By treating each discipline as a supporting element of the central thesis, my revision process has become more structured and effective, ultimately enhancing the depth and coherence of my work.

I enjoyed putting everything together, especially since a cybersecurity topic necessitates an interdisciplinary approach. I learned to identify various disciplines and their sub-disciplines, understanding how each overlaps. This knowledge will assist me in both writing my paper and more easily identifying sources in the future. For revisions, I've developed an effective process by considering each discipline as a component that supports the central ideas throughout the paper.