Chadwick Bennett

The Human Factor in Cybersecurity

April 15, 2026

CYSE 200T

Professor Duvall

Cyber Budget Allocations – Employee Training vs Cybersecurity Technology

BLUF (Bottom Line Up Front)

Human behavior remains the primary cause of cyber incidents. Even with advanced security tools, technology cannot compensate for poor user decisions, insider misuse, or errors. Therefore, with a limited budget, the organization should allocate more resources to employee training than to technology.

Introduction

Cybersecurity is often viewed as primarily technology-oriented, with technological problems requiring technological solutions. However, research shows that cybercrime is heavily influenced by human behavior and decision-making. Payne and Hadzhidimova (2018) explain that cybersecurity is an interdisciplinary issue. It extends into criminal justice and understanding why individuals commit cyber offenses. This is important because it helps organizations determine how to allocate limited resources between training employees and investing in cybersecurity technologies. That decision has direct and indirect impacts on the organization's information and security.

Employee Training vs. Technology Investments

As organizations struggle to manage limited budgets and resources, trade-offs between training employees and investing in technology must be made. Technology includes system hardware and software, including databases, networks, firewalls, intrusion detection, encryption, and authentication access. These technologies serve as barriers to protect system integrity and functionality. Payne and Hadzhidimova (2018) explain that cybercrime can still occur despite the technological safeguards that are in place, due to breaches by employees of security protocols, unintentional security bypasses, or providing system access to unauthorized individuals.

Employee training focuses on improving user awareness and behavior. This includes following security policies and procedures, understanding risks associated with daily activities, recognizing phishing attempts, and avoiding the unintentional granting of unauthorized access.

The Human Factor and White-Collar Cybercrime

Cybercrime is often driven by human reasoning and intent. White-collar cybercrime is the use of digital technology to commit financially motivated crimes, system interference, and non-violent crimes. Payne (2018) explains that white-collar cybercrime occurs when cybercrime overlaps with white-collar offenses. It is often committed by individuals within an organization who have authorization to the systems. Payne and Hadzhidimova (2018) describe how employees can abuse company resources, steal sensitive information, or engage in fraudulent activities, justifying it as their actions will not significantly harm the organization or that the organization deserves the loss. That justification is part of the broader behavior patterns that influence cyber offending.

This demonstrates the need to defend internally from within an organization equally as well as from external cyber-attacks. Since employees already have access to systems, organizations must address the human factor and behavior that contribute to system hacks that technology alone cannot prevent.

Why Prioritize Employee Training over Technology Investment

Both employee training and technology investments are crucial to establishing systems and digital security. Because human behavior directly causes a majority of cybersecurity breaches, organizations must prioritize employee training over technology investments. Second, as Payne (2018) explains, insider threats and cybercrime are closely related to white-collar offenses. This normally cannot be mitigated by just technology. Third, Payne and Hadzhidimova (2018) emphasize that the human element is a key component of cybersecurity, and its effectiveness depends on user behavior and how they use the system.

Recommended Allocation Strategy

Cybersecurity Awareness Training Model (CATRAM) has become more important as employees have been identified as the weakest link. Sabillion et al. (2019) argue that organizations need continuous, role-based, behavior-focused cybersecurity awareness training to address human vulnerability as a major cause of cyber risk. Hylender et al. (2025) *Verizon Data Breach Investigations Report* indicates that the human element was involved in about 60% of breaches. Given the high number of breaches attributed to humans, I believe the budget allocations to minimize cyber risk should be 60% employee training and 40% technology investments.

Conclusion

Cybersecurity has evolved from a technological issue to more of a human-based issue. Humans represent about 60% of the cause of cyber breaches. The readings indicate that cybercrime is an overlap of behavioral factors and white-collar crimes in the digital world. It is important to invest in technology to mitigate these crimes; however, research demonstrates that humans are the weakest link in cybersecurity due to poor decision-making, providing unintentional system access to unauthorized users, failure to follow security policies, and being victims of phishing attacks. Therefore, a more significant investment in providing employee training must be prioritized over technology investment. Current training benchmarks indicate 10-20% training in employees. CATRAM indicates the need for longer and better training to mitigate the cyber risk and human vulnerability. Hylender et al. (2025) indicated that 60% of cybersecurity breaches are attributable to the human element. Therefore, it is reasonable to recommend that organizations prioritize 60% of their budget to employee training and 40% of their budget to technological investments.

References

Hylender, C. D., Langlois, P., Pinto, A., & Widup, S. (2025). *2025 Data breach investigations report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Payne, B. K. (2018). *White-collar cybercrime: White-collar crime, cybercrime, or both?* Criminology, Criminal Justice, Law & Society, 19(3), 17.

Payne, B. K., & Hadzhidimova, L. (2018). *Cyber security and criminal justice programs in the United States: Exploring the intersections.* International Journal of Criminal Justice Sciences, 13(2), 385–404. https://doi.org/10.5281/zenodo.2657646

Sabillion, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. J. (2019). *An effective cybersecurity training model to support an organizational awareness program: The cybersecurity awareness training model (CATRAM): A case study in Canada*. *Journal of Cases on Information Technology, 21*(3), 26–39.