Radoslav Yanev

Oct 26th, 2025

The human Factory in Cybersecurity

The resource allocation in the cybersecurity branch in our company is of the biggest challenges we face. Prioritizing what is important and focusing our efforts on it would be crucial to navigate during times when cyberattacks happen almost daily. My solution is pretty simple but effective.

Prioritizing training.

Our number one focus would be training so I am suggesting allocating 50% of the budget to it. Human error plays one of the biggest roles in breaches and it is often due to the limited and ineffective training. “By understanding how people interact with security systems, what affects their decision-making processes, and what cognitive biases or stress can trigger errors, organizations can develop more effective ways to reduce vulnerabilities that people bring to the fore Ensures that employees are prepared to make appropriate decisions that enhance rather than decrease safety” (Tambe-Jagtap, 2023). Training would include month classes about new types of cyber threats and after each session there will be a test. Training will be interactive and would include games. Employees who fail the test would need to retake it and show improvement, otherwise fines and writeups would be issued. I cannot emphasize more how important this is. According to James Coker (2025), Human error contributed 95% of the breaches in 2024, driven by insider threats, credential misuse and user-driven errors.

Foundational Technology and Advanced/Specific Technology

Foundational Technology would take the other priority with 40% of the budged while the Advanced/Specific Technology would pick up the rest. We all know that Automation is essential. High repetitive processes and task, such as filtering network traffic, patching systems and detecting know malware can be managed with automation. Our baseline protection- Firewall, EDR/Anti-Malware, Multi-Factor Authentication and Backup and recovery would be covered under those 40% of the budget. The other 10% would be distributed to those high-impact tools to supplement whatever the training program lacks. Log Management and Monitoring would help us figure out who clicks on those phishing attacks and how effective the training process is. Vulnerability scanning would also be useful – this is a tool that identifies and remediate configuration errors that training cannot fix.

Conclusion

“All studies show that human-center approach to cybersecurity reduces the impact of human error on cyber incidents” (Tambe-Jagtap,2023). Focusing on efficient training would be a priority with Foundational Technology right behind it. Limited budged is not ideal but following my strategy we should be able to minimize the risk.

References

View of Human-Centric Cybersecurity: Understanding and Mitigating the Role of Human Error in Cyber Incidents. (2025). Peninsula-Press.ae. https://peninsula-press.ae/Journals/index.php/SHIFRA/article/view/31/350

Coker, J. (2025, March 11). *95% of Data Breaches Tied to Human Error in 2024*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/data-breaches-human-error/