Danielle Caplinger - November 17th, 2024

Human Factors in Addressing Cybersecurity

With a limited cybersecurity budget, we must invest a significant amount towards human-centered training in addition to technical cybersecurity defenses.

Overview

Cybersecurity is an issue affecting all industries across the globe. As attacks constantly evolve, it is important that our defenses also adapt. There must be a balance between human-centered training and technical cybersecurity defenses in order to be protected. According to Fujs, Vrhovec, and Vavpotic, “about 85% of data breaches involve a human element” meaning that we must devote a significant amount of our cybersecurity budget to addressing human error (Fujs et al. 2023). It is much easier for an attacker to infiltrate a system using one misguided user than it is to find an unpatched critical vulnerability. Since humans are cybersecurity’s weakest link, a majority of the budget should be spent on securing them first.

Cybersecurity Technologies

Essential cybersecurity technologies must be implemented, even with a limited budget. Basic infrastructure like firewalls, intrusion detection systems, and antivirus software must be used to keep our systems secure. Additionally, a strong patch and update policy is less expensive, but still necessary to keep vulnerabilities successfully mitigated. To address possible human errors, multi factor authentication, whitelist policies, and ad-blockers can also be used to keep the interaction between humans and technology safe. Although they would be a bit more expensive, we must also implement continuous monitoring logs as well as incident response plans in case a breach occurs. With a limited budget, all of these technologies are necessary to keep our networks safe and secure from unauthorized hackers.

Human-Centered Training

Since humans are more susceptible to cyber attacks than network infrastructure, a significant amount of our budget must be allocated to human-centered cybersecurity training. According to Ellucian, this will be most effective if the cybersecurity team works with communications and HR teams as well as make them mandatory on an annual or biannual basis (Ellucian, 2024). This training should cover phishing training, appropriate use of technology in the workplace, and how to report suspicious behavior if they suspect an incident is happening. Additionally, there should be some training on why technologies like MFA are important to decrease the likelihood of employees trying to bypass them. We should also allocate some of our budget towards tests of our cybersecurity posture including phishing tests, vulnerability scans, and penetration tests.

Budget Justification

With a limited cybersecurity budget, the necessities must be utilized while focusing on the humans that are most vulnerable to an incident. I propose that our budget consist of 40% for the necessary cybersecurity technologies, 30% dedicated to human-centered cybersecurity training, and 30% dedicated to continuous testing of our systems. Although there will always be costs in keeping systems secure, it will be cheaper in the long run. It is more financially responsible to focus on training and testing than to pay a major ransomware payment in a few years due to poor security.

Conclusion

The best cybersecurity departments must create a defense-in-depth strategy in order to keep their systems safe as attacks evolve. They must also address the weakest part of any cybersecurity system: humans. For this reason, employee training must be a top priority for cybersecurity teams when considering their budget. With this proposed budget, our systems will have a combination of training, testing, and basic cybersecurity technologies to keep them as secure as possible.

References

Fujs, Damjan, et al. (2023). Balancing software and training requirements for information security. *Computers and Security* 134. https://www.sciencedirect.com/science/article/pii/S0167404823003772?dgcid=rss_sd_all.

Solving cybersecurity's "people problem" (2024). *Ellucian.* https://www.ellucian.com/blog/cybersecurity-training-higher-education-8-tips-effective-strategy.