Derrick Amissah

4/4/2025

Balancing Cybersecurity Training and Technology Investments: A CISO's Strategic Approach

When you are tight on money, invest in shaping people's behavior rather than in new technology. Allocate roughly 60% to teaching employees how to identify and prevent threats such as phishing. Spend the other 40% to enhance and fully utilize the tech you currently have. This not only closes the loophole in the biggest weakness human error but also ensures your defenses remain up to date.

Risk Assessment and Prioritization

Begin by checking where your greatest security threats are. According to human error statistics, approximately 82% of cyberattacks occur due to human mistakes (bcs365). This is why it is extremely important to train your team. Educate them to recognize phishing, create powerful passwords, and the appropriate use of devices. Invest in automatic threat discovery tools, such as smart monitoring systems. And plug any major gaps in your current systems. Use your budget on what really matters.

Why Training Deserves Greater Investment

So, get the maximum out of your existing tools by teaching employees how to use them correctly. Security tools will not serve much purpose if staff do not know how they function. Training maks your team utilize the tech in the right way. Not only does it save money (companies that do this are attacked less often) but educating people about what cybersecurity is

helps lot well. Training personnel is way cheaper than counteracting a major security violation. When everyone can recognize the threats, they become your defense. Having them updated on drills and new updates improves the organization as a whole.

Strategic Technology Investments

Utilize smart software to automate menial, huge elements of your business so employees have time to focus on bigger concerns. For example, auto-updates or security notifications save time and resolve issues faster. Use security patches on the most severe vulnerabilities first. For example, if your entire company works remotely, maybe a zero-trust architecture is the solution to maintain your network integrity. Also, don't forget about free solutions and some open-source options are just as effective. Therefore, you can be safe on a budget.

Conclusion

Budget-minded security is team training instead of purchasing options and increased use of what's already there. For instance, employee training where weaknesses and gaps exist is better than spending money on additional software. In addition, software that allows for the automation of small tasks that don't need to be done lets employees focus more on the bigger picture. Tackle the worst offenders first and ensure those who work from home have robust remote security in place. Don't overlook free applications; sometimes they work better than their paid versions. Support employees because a culture of security starts with what's in their best interest to be secure. The best security is an educated approach with ongoing process.

References

BCS365. (2024, February 16). The Human Factor: The Importance of Employee Training in Cybersecurity. BCS365. https://bcs365.com/insights/the_importance_of_employee_training_in_cybersecurity