The Human Factor: Balancing Training and Technology Updates

Prepared By: Ryan Stephens
Date: November 14th, 2025

Executive Summary:

To maximize business profits and increase operational resiliency, I recommend allocating 60% of the proposed budget towards employee training programs and using the remaining 40% for acquiring and maintaining equipment. The human element is often the weakest part of any organization and thus the most vulnerable, and by addressing this vulnerability with adequate employee training, the risk of cyberattacks is massively reduced, leading to cost-effective cyber strategies and increased Return on Investment.

Analyzing Phishing: Statistics and Types of Attacks

Statistics:

According to the *Phishing Trends Report* (Hoxhunt, 2025), the human element is involved in 68% of all cyber breaches, and 95% of these breaches are initiated through phishing attacks. Additionally, the *Phishing Trends Report* also states, "Employees can be trained to recognize and report social engineering attacks with a 6x improvement in 6 months, and reduce the number of phishing incidents per organization by 86%." The *Phishing Trends Report* further states that the estimated cost of a phishing breach is $4.8 million.

Types of Attacks:

Phishing attacks are becoming more frequent, complicated, and challenging to detect. Threat actors now employ a variety of attack types, including Business Email Compromise (BEC), Credential Phishing, HTTPS phishing, Voice Phishing, AI-driven attacks, QR Code Phishing, Government Agency Impersonation, and many others (Hoxhunt, 2025). These attacks are almost impossible to detect without cybersecurity experience. Even individuals in the cyber industry frequently fall victim to them. For example, threat actors can create fake replica websites that, upon visitation, force the client computer to download and run malicious files, highlighting the importance of basic cybersecurity knowledge that many individuals lack, which can result in significant financial losses for companies.

Importance of Employee Training:

Since phishing is the most common attack vector in the cybersecurity industry, it requires a significant and proactive approach to defend against it. The most effective and cost-effective way to do this is through employee training programs. These training programs would be tailored to each department in the corporate business structure (i.e., Human Resources, Operations, Finance, etc.). Departmentalized training programs make sense, as each department receives phishing

attacks that are tailored to its specific needs. For clarification, Human Resources is at a greater risk of receiving malicious/fraudulent job applications. At the same time, Operations is more likely to receive fraudulent emails regarding supply chain status, and the cycle continues. Trying to implement a “one-size-fits-all” employee training program might still be effective, but only to a certain degree, as employees might not realize just how in-depth these attacks are, especially with rising AI-driven phishing attacks, which are highly personalized and detailed, even more so if the attacker already has information about other employees through previous hacks or leaks. Regarding AI-driven phishing attacks, Mika Aalto, co-founder and CEO of Hoxhunt, stated, “In the near future, AI will power significantly more phishing attacks—everything from text-based impersonations to deepfake communications will become cheaper, more convincing, and more popular with threat actors” (Hoxhunt, 2025). Departmentalized training prepares employees to identify and act against the threats they are most likely to encounter in their daily operations. It will also help prevent future, more advanced AI-driven attacks.

Why Employee Training Takes Priority:

The primary goals of a business are to generate income, and while cybersecurity is a necessity, it can reduce profits if the budget is not managed correctly. Rather than spending most of the budget on expensive cybersecurity gadgets that will rarely be used, the most cost-effective measure is to focus on the attacks that are most likely to occur and invest heavily in preventing or mitigating them, while still having enough money left over to maintain the current systems and occasionally upgrading the software or hardware. Employee training programs make the most sense from both a cybersecurity and a business standpoint, which rarely align with each other.

Conclusion:

Most people assume that cybersecurity is strictly a technical issue. However, a lack of basic security knowledge is the primary driver of cybercrime. With each successful phishing attack costing millions of dollars, the most effective defensive measures lie in the hands of employees who are constantly under threat, whether they know it or not, of being hacked. Implementing mandatory departmentalized cybersecurity training is not only crucial to the longevity of the business, but it is also cost-effective, reduces risk, and allows for a security-conscious environment, which in today’s technology-driven landscape is increasingly more important.

References

"Phishing Trends Report (Updated for 2025)." *The Hoxhunt Human Risk Management Platform*, Hoxhunt, hoxhunt.com/guide/phishing-trends-report. Accessed 14 Nov. 2025.