David Kyle

Wearing the CISO Hat

If I were the Chief Information Security Officer with a limited budget, I would spend roughly 55% on people and training (security awareness, role-based upskilling, phishing sims, and measurements) and 45% on technology (basic detection/prevention, identity protection, patching, and automation). This mix prioritizes fixing the human weak link while investing in the minimum effective tech stack and automation to scale limited staff. My reasoning and sources are below.

Simultaneously, technology is essential: fundamental protective measures such as multi-factor authentication (MFA), timely updates, endpoint detection and response (EDR), and dependable backups can prevent numerous attacks or mitigate their effects if an employee makes an error. NIST recommendations underline the importance of awareness and training as a key component of a security strategy, while also highlighting the necessity of technical controls and documented procedures within a layered defense approach. An effective CISO understands that training without technological safeguards is overly optimistic, while technology without properly trained personnel is ineffective. These two concepts—educating individuals AND reinforcing systems—aren't opposing objectives; they are supportive layers of security that, when combined, provide optimal risk reduction for the investment. NIST Computer Security Resource Center+1

Considering the tradeoff, here is the budget allocation I would suggest: approximately 35% dedicated to an ongoing security awareness and role-specific training initiative; 40% for crucial security technologies (including MFA, patch management, EDR, and logging); 10% for identity and access management along with least-privilege efforts; 10% allocated for incident response, backups, and tabletop simulations; and 5% set aside for metrics, measurement, and engagement from leadership. I selected 35% for training because instilling behavior change requires multiple, well-structured interventions rather than a single presentation. Studies and industry professionals indicate that awareness programs help lower "phish-prone" rates and are most effective when they have backing from leadership, which is why I also allocate funds for metrics and executive updates to maintain the program's funding and visibility. At the same time, a slightly larger share for essential technology (40%) guarantees that there are effective, automated safeguards in place to minimize consequences when human errors occur. SANS Institute+1

Investing in training involves more than just quarterly compliance modules. I would allocate resources for a curriculum that features monthly brief micro-lessons, realistic phishing simulations with tailored remediation, secure coding or privileged user training aimed at technical personnel, and onboarding modules that establish expectations from the very start. The objective is to achieve measurable changes in behavior: reduced click rates on simulated phishing attempts, quicker reporting of suspicious emails, and a decrease in high-risk privilege escalations. Research from academia and industry regarding program metrics highlights the importance of measurable results to demonstrate to leadership where risk is being mitigated; that is why I reserve a small yet vital part of the budget for analytics and reporting. Effective metrics enable the CISO to demonstrate ROI and reallocate funds gradually from costly last-resort technologies to preventive measures if the data indicates it is justified. (OUP Academic+1)

When it comes to technology expenditures, I would focus on controls that provide substantial risk reduction for the investment. Multi-factor authentication (MFA) and centralized patch management are straightforward measures that prevent many typical attacks and should be widely implemented. Integrating endpoint detection with logging and automated containment reduces the time threats linger and lessens the impact of incidents. Having reliable, tested backups along with a well-rehearsed incident response plan makes dealing with ransomware feasible and helps prevent significant losses when preventive measures fail. According to Gartner's analyses of the market and spending, organizations keep investing in essential controls and resilience, and a savvy CISO utilizes those investments to minimize the time taken to detect and respond to incidents.(Gartner+1)

Ultimately, the cultural aspect is crucial. When leadership and managers actively support security through the inclusion of security objectives in performance evaluations, anticipating immediate reporting of errors, and rewarding positive actions, training proves to be much more effective, and technology is utilized appropriately. SANS and various professionals stress the importance of leadership commitment and ongoing programs instead of one-time training sessions because culture is what ensures policies and tools function effectively in reality. This is why I allocate funds for executive briefings, assessments of program effectiveness, and communications that integrate security into everyone’s role rather than being solely an IT responsibility. In summary, the financial priorities are to invest in individuals to mitigate prevalent human-driven risks and to fund essential technology that prevents and addresses attacks that people may not always evade. Collectively, these investments enhance organizational resilience, allow for measurement, and provide rationale to leadership. (SANS Institute+1)

Works Cited

NIST. Building an Information Technology Security Awareness and Training Program, Special Publication 800-50. National Institute of Standards and Technology, 2003, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf. NIST Publications

NIST. Security and Privacy Controls for Information Systems and Organizations (SP 800-53) and related guidance on training and awareness. National Institute of Standards and Technology, https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter13.html. NIST Computer Security Resource Center

Verizon Business. 2024 Data Breach Investigations Report. Verizon, May 2024, https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf. Verizon

Spitzner, Lance. "Securing Leadership Buy-In: The Key to Scaling Your Security Awareness Program." SANS Institute Blog, 17 Feb. 2025, https://www.sans.org/blog/securing-leadership-buy-in-the-key-to-scaling-your-security-awareness-program. SANS Institute

Gartner, "Gartner Forecasts Global Information Security Spending to Grow," 28 Aug. 2024, https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025. Gartner

Chaudhary, S., et al. "Developing metrics to assess the effectiveness of security awareness programs." Cybersecurity (Oxford Academic), 2022. OUP Academic