Nathan Jimenez

Professor Duvall

CYSE 200T

11/19/2025

Balancing People and Tools

BLUF

With a limited budget I would prioritize a 60/40 split in favor of people and processes which include training, governance, and incident response readiness. Technology is also essential, but most breaches still go back to human and process failures not tool shortages. So I fund baseline technical controls, invest in security awareness training, and strengthen policies. This combination would maximize risk reduction on a budget and build resilience.

Why training Matters as Much as Technology

A lot of industry reports show that human behavior is a leading factor in cyber incidents. Phishing and social engineering are one of the top attack vectors which often outpace technical exploits. A lot of studies and industry data (like Verizon DBIR and reports from ENISA and NIST) emphasize that human error is the key component to breaches. When organizations rely only on tools instead of training to try to improve behavior attackers go around the tools by targeting the individual instead. I think because of this investing in security awareness is not optional as it holds a big role in keeping the company safe. If the training is combined with realistic phishing simulations it can reduce the human error rates on malicious emails over a period of time which cause these breaches to occur.

Core Technical Controls I Would Fund First

As a CISO with a limited amount of funds I can't buy all the high end tools and everything so I would fund foundational controls before all the advanced ones. One of them I would get is IAM (Identity & Access Management) which contains MFA (Multifactor Authentication) for all remote access, accounts with clearance, and critical systems. It also comes with strong password policies and support for password managers. Another one I would get is logging, monitoring, and incident detection. This will give centralized logs for auth events, critical apps, and network devices. It will also alert on high risk events such as an admin failing to login, an anonymous user logging in, or large data transfers. This will create a minimum security baseline so once I get these settled in place I can consider once my budget improves to more specialized technologies.

How I Would Allocate the Budget

With a limited budget I would mostly split it off to 40% on technology and tools like EDR/AV, MFA, SIEM/logging, backup solutions, email security, essential licenses, minimal automation, and integration work. Another 40% would go to people, training, and processes as this is the most important part. So this would include security awareness training and phishing simulations, role based training for developers and admins, testing of incident response plans, and policy development. The last 20% would go on governance, risk management, and improvement. This would be regular risk assessments, third party assessments/penetration tests, and reporting dashboards. I think this approach will show that you can't just tool yourself out of human risk and putting forth a lot of the budget on training will make sure people know what to look for and what to do, avoiding these incidents later on.

Reasoning: Risk Based Not Tool Based

A risk based approach is the strongest reasoning for balancing training and technology under a small budget. As a CISO I think my goal is to not buy the most tools possible but to reduce the real world exposure to cyber threats. Most of the most successful cyber attacks come from human error or credential compromise which means that the training and awareness was lacking and should be improved. At the same time, foundational technical controls reduce the impact if an attack does occur. By focusing on the highest likelihood and highest impact risks will create a layered security as people learn to avoid threats, tools to detect and block malicious activity, and strong processes to ensure that the organization can respond quickly if something does get by.

Conclusion

With limited funds, a CISO has to resist not buying all the new top tier security products and instead build a balanced risk based program. I would allocate most of my budget to ensure strong baseline technical controls while equally investing in training, culture, and incident response readiness. Technology alone cannot solve all the human errors that can occur and these tools without training on how to use them will leave the employees unsupported and confused. By combining both I can achieve the best reduced risk for the organization and create a security that is resilient, adaptable, and sustainable over a period of time.

References

ENISA. (2025). ENISA Threat Landscape 2025. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025#contentList

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce. https://www.nist.gov/cyberframework

Proofpoint. (2023). State of the phish 2023. Proofpoint, Inc. https://www.proofpoint.com

Verizon Business. (2025). 2025 Data Breach Investigations Report (DBIR). Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

IBM Security & Ponemon Institute. (2025). Cost of a Data Breach Report 2025. https://www.ibm.com/reports/data-breach

SANS Institute. (2025). 2025 Security Awareness Report: Embedding a Strong Security Culture. https://www.sans.org/for-organizations/workforce/resources/security-awareness-report