**Name:** Marshall Brown

**Date:** 3/28/2023

# The Human Factor in Cybersecurity

*This essay outlines a Chief Information Security Officer's approach to balancing cybersecurity training and technology with a limited budget. The approach includes conducting a comprehensive risk assessment, investing in cybersecurity training, implementing necessary technology, regularly updating and patching software, and continuous monitoring. By following these steps, CISOs can enhance their organization's cybersecurity posture and protect their valuable information assets.*

## Introduction

As cyber threats continue to evolve, organizations are investing heavily in cybersecurity to protect their valuable information assets. However, with a limited budget, it can be challenging to balance the tradeoff between investing in cybersecurity training and additional technology. In this essay, we will discuss a Chief Information Security Officer's (CISO) approach to allocating funds effectively between cybersecurity training and technology to achieve the maximum protection of their organization's information assets.

## Conducting a Risk Assessment

The first step to allocate funds effectively between cybersecurity training and technology is to conduct a comprehensive risk assessment. A risk assessment helps to determine the organization's risk profile, identify areas that require attention, and prioritize the allocation of funds. Risk assessments are not only essential for allocating funds effectively but also for identifying and managing cybersecurity risks. Therefore, CISOs should make risk assessments a regular practice in their organization's cybersecurity program.

## Investing in Cybersecurity Training

Cybersecurity training is critical to mitigating human errors that can lead to cyberattacks. As the majority of cybersecurity attacks are caused by human errors such as phishing, it is essential to invest in cybersecurity training for employees. CISOs should allocate a significant portion of their budget to provide cybersecurity awareness training, phishing simulations, and cybersecurity incident response training to employees. Investing in cybersecurity training reduces the likelihood of employees falling victim to phishing emails or other social engineering tactics, which can lead to devastating cyberattacks.

## Implementing Necessary Technology

After identifying the most significant risks, CISOs should allocate funds to implement technology that can mitigate those risks. The specific technology solutions needed will vary depending on the organization's risk profile. For example, if the organization is at risk of malware attacks, CISOs should invest in anti-malware software and intrusion detection and prevention systems. In addition, organizations should implement multifactor authentication, firewalls, and data encryption to enhance their cybersecurity posture.

## Regularly Updating and Patching Software

Cyberattacks often occur due to unpatched software vulnerabilities. Therefore, it is crucial to allocate funds to ensure that software is regularly updated and patched to reduce the risk of cyberattacks. Regular software updates and patching enhance the security of systems and reduce the likelihood of cyberattacks caused by known vulnerabilities. CISOs should allocate a portion of their budget to regularly update and patch software to ensure the security of their organization's information assets.

## Continuous Monitoring

Continuous monitoring can help detect and prevent cyberattacks in real time. CISOs should allocate a portion of their budget to implement continuous monitoring systems such as security information and event management (SIEM) solutions. SIEM solutions collect and analyze security-related information from different sources in real time, providing valuable insights into potential threats. Investing in continuous monitoring enhances the organization's cybersecurity posture by reducing the time between threat detection and response, thus minimizing the impact of a cyberattack.

## Conclusion

In conclusion, a balanced approach is the most effective way to allocate funds between cybersecurity training and technology. The approach involves investing in both cybersecurity training and technology, but at different levels based on the organization's risk profile and budget. Conducting a comprehensive risk assessment, investing in cybersecurity training, implementing necessary technology, regularly updating and patching software, and continuous monitoring are all critical steps that CISOs should take to allocate their limited budget effectively. By implementing these steps, CISOs can enhance their organization's cybersecurity posture and protect their valuable information assets.

## References

"Cybersecurity Framework." National Institute of Standards and Technology, U.S. Department of Commerce, Apr. 2018, www.nist.gov/cyberframework.

SANS Institute. "SANS: Information Security Training." SANS Institute, 2023, www.sans.org/.

"Cybersecurity and Infrastructure Security Agency (CISA)." Department of Homeland Security, 2023, www.cisa.gov/.