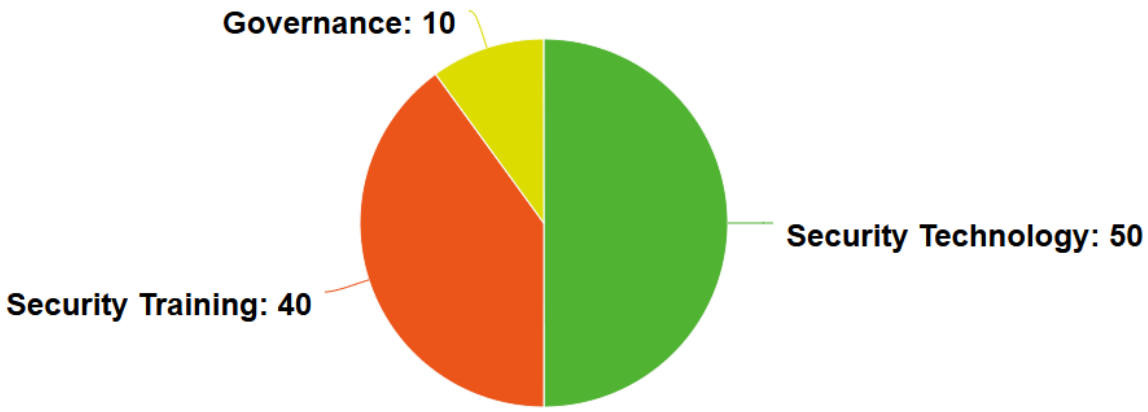
The Human Factor in Cybersecurity

By: Paul Cumiskey

If I were acting as a Chief Information Security Officer, I would prioritise security by providing security professionals with the proper tools and funding to maximise security. I would also focus on minimizing risk exposure. Human error is one of the leading causes of cybersecurity breaches, so it is extremely important to use a large portion of our budget to implement proper training. For this, I would suggest a broad budget breakdown as Security Technology(50%), Security Training(40%), and Governance(10%).



Security Technology (50%)

Technology is one of the most essential aspects of creating a secure network. It is extremely important for all aspects of Cybersecurity. Depending on the situation of the company, there are two options to manage security services: cloud or on-site. I would recommend using **cloud-based servers to reduce overhead and minimize the cost to maintain and operate**

the security services. It is also extremely important to use tools with great integration to **avoid issues with silos and other forms of inefficient operations.**

- Implementation of Security Technology
    - **Endpoint Detection and Response (EDR)**
    - **Firewalls**
    - **Multi-Factor Authentication (MFA)**

Security Training (40%)

One of the most overlooked aspects of cybersecurity is the human factor. Most cyber breaches have human error as one of the root causes. No matter how secure your network is, human error can always lead to a breach. Vulnerabilities caused by humans are usually ones such as susceptibility to **phishing attacks, bad password hygiene, and lack of security awareness**.

- Implementation of Security Training
    - Introduce a recurring required **security awareness program** that all employees must participate in. These programs will make employees aware of how to **identify many real-world threats and how to avoid them.**
    - **Train each role differently** depending on what their responsibilities are and what information they have access to
    - Implement metrics to **track employees' cyber hygiene.**

Governance (10%)

Governance is an extremely important aspect of creating a secure network. It is very important to create **transparent, enforceable policies and incident response strategies to**

ensure consistency and accountability. While governance is extremely important, it does not require as much funding as security training and technologies, and in many cases, only a few highly skilled employees are needed.

- Implementation of Governance
    - Create and update **incident response plans**
    - Make **policies that enforce and incentivize secure behavior**
    - Frequently run **risk assessments and internal audits**

Conclusion

Many human factors need to be kept in mind when creating a budget as a Chief Information Security Officer. While the three items on the budget are very broad, they do a good job of covering most of the bases that will be needed. The security technologies and training listed will certainly combat human error and do a great job of minimizing risk exposure.

Works Cited

NIST. “Cybersecurity Framework.” National Institute of Standards and Technology, 2024, www.nist.gov/cyberframework.