

Thomas Winterrowd

The Human Factor in Cybersecurity

Key Message

I would allocate funds by giving training and education 55% of the budget, while giving the technological side 45% of the budget. Training and education deserve more focus than technology because in most cases, humans are the weakest link in the chain. Human error and falling victim to social engineering schemes are often the cause of cybersecurity incidents, despite how well funded and secure the technology of an organization is. Well-funded training will ensure that employees are knowledgeable about the current threat landscape and can recognize errors and social engineering attempts.

The Human Factor

Humans are critical to the security and operation of an organization, which is why they deserve proper focus in budgeting. Spending a large portion of the budget on training is well justified because the cost of incidents that training could have prevented outweigh the cost of training by magnitudes. The “IBM Security Services 2014 Cyber Security Intelligence” report published by IBM found that 95% of security incidents had human error as a contributing factor: A single person could easily be the cause of a cybersecurity incident, and they could be the one who notices something off and prevents an incident. Employees for an organization need to be up to date with the current threat landscape: They must be aware of threats like phishing, pretexting, tailgating and more. Quality training and education will ensure that employees have the knowledge of what scams to look out for and what safety procedures to follow.

The budget for training needs to be spent on quality education over quantity to ensure that employees will take training seriously and retain information. Training routines should include examples and activities or simulations, increasing information retainment by having employees experience what they need to be careful of. Quality training can provide employees with better and more accurate information. Additionally, in choosing quality over quantity it is less likely for an employee to become overwhelmed by the amount of training they must go through and ignore all the information in the training.

The Technological Factor

The technological side of the budget deserves enough to thrive and be secure as possible. The human factor is still most important, but the technological factor is undeniably crucial to the success of an organization. The portion or amount of money dedicated to technology will be different for every organization, but it should not be underfunded. With an underfunded technology budget, there is less opportunity for taking options that increase safety and maintain operations, like building redundancy into an organization's systems. Making sure that the technological factor is well funded is important for avoiding mistakes like having outdated or unpatched software.

Conclusion

Training and education deserve a great portion of a business's budget because how costly human error can be. Technology will always be greatly important, but the risks of accidents and incidents caused by an employee's mistakes justifies the prioritization of education. The budget for training should be spent on quality, informative education over having large quantities of material for training. Despite the focus on training, it should be ensured that the technological

factor of an organization is funded well enough to maintain the consistency of operations and the security of a business.

Works Cited

T. Pham, T. (2014, June 19). *Human Error Accounts for Over 95 Percent of Security Incidents, Reports IBM*. Cisco Duo. <https://duo.com/blog/human-error-accounts-for-over-95-percent-of-security-incidents-reports-ibm>