Balancing the Cybersecurity Equation: Prioritizing the Human Factor in Capital Expenditure

By: Alexander fotakis

In this scenario, as a CISO with a budget of 100,000 dollars and I will be splitting the budget 60% (60,000) to human training and 40% (40,000) to cybersecurity technology. The reason behind 60% of human training is that cybersecurity technology is only useful if there is a human behind it to do upkeep and stop the attackers, instead of just detecting them. While the 40% technology is for the basics of cybersecurity technology and not the bleeding-edge, so that we do not become reliant on technology, so that when it goes down, we can pick up the slack.

Human training

Directing more of the budget towards Human Training would allow for proper training of employees and a better ROI (return on investment) because. The only certain in the cybersecurity field is that technology fails, so having proper training for when technology fails ensures that the company's integrity is maintained and damages to customers' confidentiality are minimized. Micke Ahola's blog has a prime statistic from IBM showing this: 'According to a study by IBM, human error is the main cause of 95% of cyber security breaches.' Using Micke's logic and previous knowledge of technology and the very common occurrence of it going out or not working, makes human training Vital for a cybersecurity department.

Cybersecurity technology

According to Danny Murphy's blog, most security breaches are misuse of privileged access. which can be mitigated by simple tech the rest of the reasons are a part of social engineering and out of date software, so having most of our budget dependent on

technology and not on the people behind the technology leaves the company open to phishing attacks, misused access, and any other social engineered attack. But if we give proper training to all employees, from manager to customer service agent, it eliminates the biggest issue most companies deal with.

Summary

As the CISO with a $100,000 budget, I preferred training people to buy expensive technology that would eventually become obsolete. This strategy is based on the idea that technology will fail at some point and that 95% of breaches are caused by human error (according to studies cited by IBM). The goal of the training is to ensure sure that every employee can be an important "firewall" to protect the business's integrity. The small technology budget is enough for the basic tools needed to fix basic security holes, which stops people from relying too much on technology.