Name: John Ryan

Date: April 3, 2023

The Human Factor in Cybersecurity

Employees are the weakest link in cybersecurity. Training is critical to mitigate this and should always be accounted for in the budget, even if this allows for fewer technical defenses.

Onboarding and Acceptable Use Policies

Before a new hire touches an IT asset, they should have completed cybersecurity training. This should be a part of the onboarding process, similar to how new employees have to sit for other HR-centric courses. Humans are the weakest link in any cyber defense and this training can do much for preventing incidents. Additionally, when an adverse event happens that exposes customer data, runs afoul of regulators, etc., the company can potentially limit liability by showing records that 100% of employees received this training.

Acceptable use policies serve as a contract of sorts between the organization and the end user. This may be a signed document in an employee's training jacket or a click-through acknowledgement on an IT asset at logon. These policies should be updated and acknowledged regularly and remind employees that there may be consequences for failing to act responsibly while using company assets. These policies should be explicit regarding remote work, as cybercriminals see this trend as an opportunity to prey on workers away from the office (Habert, 2021).

Training Refreshers and Drills

It is insufficient to train employees only during onboarding. Memory fades with time. Recurrent training for incumbents also reinforces the culture of the company as one that cares about cybersecurity. Finally, threats are constantly changing, and it is important employees be made aware of the latest actors and attack methods.

How can leadership measure the efficacy of training? Tests may be conducted months after training but may be met with resistance. Gamification of testing during company events can be a less stressful, more engaging method. According to Habert (2008), one company runs a virtual escape room where “employees work in teams, finding and piecing together security-related tips to build a key that enables them to unlock the door and free themselves. For example, they may call out a password left on a note or a sensitive document left open on a monitor.” The best indicator of retention, however, is to conduct a real-life scenario by sending out phishing simulation emails or dropping a thumb drive in the employee parking lot.

Technical Solutions

Training should be coupled with technical solutions where possible. Capone (2018) argues that “while people are certainly an important aspect of data security and serve as critical administrators, they cannot serve as the be-all-end-all. Human behavior has proven that we choose to take the easy road, cut corners and make mistakes.” Technical solutions can do things that humans cannot, like aggregate and inspect millions of logs or inspect every packet leaving the network.

Modern technical solutions are powerful, but the initial cost of purchase represents a fraction of the total cost of use. Every security appliance must have support from the vendor, be

maintained within a broader lifecycle management program (that is, retired when vendor support ends), be maintained and administered by company IT personnel, and have outputs reviewed by company cybersecurity personnel. For example, an intrusion detection and prevention system (IDPS) may cost $10,000 to purchase. If installed with professional services, this price will increase. Support will be required to maintain access to new threat signatures and keep up with upgrades to the device itself and can run into thousands of dollars per year. An administrator will need to ensure uptime and device patching. Even if applying only a percentage of their salary to any one device, one could add thousands of dollars more for administration. Finally, the review of events by a cyber professional may make up most of their job, adding tens of thousands of dollars more in overhead.

The above example is only one product among many. There can be endpoint security system software, firewalls, SIEMs, email gateways, data loss prevention systems, and file integrity monitors, all in the same enclave. Each product has an initial cost, support costs, administrative costs, and the cost of reviewing findings. It is easy to see how the total cost of technical solutions is likely to exceed that of training efforts. There may be temptation to buy one more product to secure the network from a different angle and forgo employee training and engagement. This would be a mistake.

Stating a specific percentage of a budget that should be reserved for training is not possible given the differences in each organization’s size and industry. In smaller companies, there may be limited funds for expensive technical solutions and training may be the only means available to reduce risk. Certain industries may favor more technical solutions because they are already populated by technically savvy employees (e.g. cloud provider organizations) or due to regulatory demands. However, it can be stated with conviction that the cyber training budget must not fall below a sustainable level and that it represents the highest ROI of any

cybersecurity effort. People may be the weakest link, but they can become the strongest weapon to thwart cyber events when properly motivated and trained.

Conclusion

Technical solutions remain a powerful tool for protecting organizations. The cost associated with deploying them will almost certainly exceed any cost associated with training. This cost should not be allowed to consume the entirety of the budget, thereby restricting the ability to train, a much more cost-effective solution. In no cases, given how frequently humans ignore existing controls and allow cyber incidents to occur, should organizations neglect to thoroughly train on cybersecurity best practices.

References

Capone, J. (2018, May 25). *The impact of human behavior on security*. CSO. https://www.csoonline.com/article/3275930/the-impact-of-human-behavior-on-security.html

Harbert, T. (2021, October 23). *The Weakest Link in Cybersecurity.* Society for Human Resource Management. https://www.shrm.org/hr-today/news/all-things-work/pages/the-weakest-link-in-cybersecurity.aspx