Braden Gilbert

CYSE 200T

Professor Lida Hagh

10 November 2024

The Human Factor in Cybersecurity

Balancing the allocation of a limited budget between training and technology is crucial since both are essential to effective cybersecurity strategies. It would be important to first evaluate the existing technologies within a company to see if they need any priority. If there is already a decent set of cybersecurity tools like firewalls, intrusion detection or prevention systems are all systems are properly configured and maintained then any additional investments into additional technologies would not provide any significant returns.

It is also important to know if human error is a major contributor to security incidents within the organization. To minimize the risk of breaches caused by human error, it is important to not only use cybersecurity solutions but also provide training for their employees (Yamada, 2024). A significant portion of a budget should go toward security awareness training for employees. There are many cyberattacks that rely on human error such as malware, password attacks, phishing, and mis-delivery of information (The Biggest Cyber Threat to Your Disaster Recovery Plan Is Human Error). Even with robust technologies for defense, employees can be the weakest link in security. Employees should be taught the best practices and also recognize threats. They should be able to recognize phishing emails, create strong passwords, know safe browsing practices, and be able to report any suspicious activities.

An organization should also have a strong core for cybersecurity technology. These technologies would have the best return on investment. There should be an endpoint detection and response which is an essential tool to help detect, investigate and respond to potential threats on endpoints (Aarness, 2023). Firewalls are also important since they provide protection against outside cyber attackers. They can shield computers or networks from malicious or unnecessary network traffic and also prevent malicious software from accessing computers or networks from the internet (Understanding firewalls for home and small office use, 2024). Threat Intelligence Platforms can help analyze data on new threats which can help stay ahead of attacks by using up-to-date information. The choice of specific tools will depend on the organization's risk profile and security goals.

It is important to remember that human error remains the weakest link in cybersecurity. Even if an organization uses the best technologies for cybersecurity, it can easily be undermined by a lack of training of employees. This is why both training and core security technologies should be almost equally invested in for a limited budget.

References

Aarness, A. (2023, October 26). *What is EDR? Endpoint Detection & Response defined*. CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

The Biggest Cyber Threat to Your Disaster Recovery Plan Is Human Error. OVHcloud. (n.d.). https://us.ovhcloud.com/resources/blog/cyber-threat-human-error/

Understanding firewalls for home and small office use: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024, October 2). https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use/

Yamada, Y. (2024, November 8). *How to prevent human error in cybersecurity*. Keeper Security Blog - Cybersecurity News & Product Updates. https://www.keepersecurity.com/blog/2024/05/08/how-can-companies-reduce-human-error-in-cybersecurity/