Hannah Stivers

Professor Charlie Kirkpatrick

CYSE 200T – 33861

April 1, 2023

The human factor in cybersecurity

It is extremely important for our organization to put enough funding into properly training all employees on the basics of cybersecurity awareness rather than buying new hardware or software that will not create an impact on the human factor problems we face. A lot of the vulnerabilities we have within the organization start at the human level rather than the technical level. Throughout this write up I will be explaining what the human factor is, how to balance training and getting additional equipment, and how to allocate the funds.

What is the Human Factor in Cybersecurity?

The Human Factor is any instance where a person is connected to a device and can create a potential vulnerability. Usually, when people think of cybersecurity the first thing that comes to mind is the technology and software being used to secure a company, but how can that hardware a software protect against a malicious user within the organization or someone who has gained the credentials to have access to the organization's data. This is where the human factor comes into play. All employees need to be educated on proper cyber hygiene in order to help the cybersecurity department properly do their jobs. The most common and easiest way for a cybercriminal to gain access to an organization is through human error or unawareness. These problems can be fixed or managed by properly educating the employees on cyber hygiene (CYDEF, 2021).

How would you balance the tradeoff of training and additional cybersecurity technology?

If there is no training for all employees, then the company is potentially wasting money on this technology that cannot protect against the vulnerabilities caused by employees. Do we need to ensure our systems are up to date and patching any potential vulnerabilities within the hardware or software, yes but if we solely try to fix the problem from the technical point of view, we will not be a very secure company. One of the most common ways for malware to get onto the organization's network or systems is because an employee opened a link in a phishing email. With phishing emails, the most we can do from a technical standpoint is outing a filter on inboxes, but even that does not work one hundred percent of the time. But if we educate employees on what to look for and give them examples of what to look for then that reduces the risk of an attack. It is not so much that we are trading technology for training, but rather allowing the two to work together to benefit the company (CYDEF, 2021).

How would you allocate the funding?

I think when looking at the budget, roughly and quarter of it should be used towards ensuring everyone in the company has basic cybersecurity training. This training would go in-depth into proper cybersecurity hygiene and the rest of the budget would be used on the hardware and software that is also needed to ensure that the company is able to properly secure our data.

Conclusion

Ensuring employees are trained and the human factor is considered in the budget is just as important as it is when considering the hardware and software we need.

Works Cited

CYDEF. (2021, May 19). *The Human Factor: The Hidden Problem of Cybersecurity*. Retrieved from CYDEF Your Sentinel Inside: https://cydef.ca/blog/the-human-factor-the-hidden-problem-of-cybersecurity/