Brandon Creech

Professor Kirkpatrick

CYSE 200T

31 March 2023

The Human Factor in Cybersecurity

How would you allocate the funds of being a Chief Information Security Officer (CISO) between the training and additional cybersecurity technology with a limited budget?

Importance of Training

Training is important for employees because it teaches the vital defensive measures to protecting valued data and keeping the company's infrastructure secure. Employees' themselves serve as a defense against crucial infrastructure in which they are expected to be able to execute actions that quarantine the imminent threat online. They are expected to learn case-by-case scenarios in which they are to act quickly without hesitation through which training teaches them. They are also supposed to monitor the company network for malicious activity if the technology itself isn't able to detect it (Rijmenam 2022). This is why training is important because it helps employees gain insight into hackers because they have to be able to keep up with the knowledge them.

Importance of Improving Cybersecurity Technology

In addition to educating employees through training, **improving the technology within the company plays an important role in cyber defense because it is the first line of defense that detects against malicious activity before the employee.** Improving technology involves ensuring all security systems have up-to-date hardware and software that will mitigate the chance of a cyberattack from happening. If a cyberattack does happen, having an up-to-date security system will be able to respond quicker to the threat and quarantine it. AI is also becoming a more growing trend in society so it could become incorporated into security systems to do the tasks of both technology and employees (Rijmenam 2022).

Allocating funds as CISO

Considering the factors in the importance of training and cybersecurity technology to protecting the company and its infrastructure, **being the CISO involves making the tough decision on what areas of infrastructure security should be prioritized in optimizing against a limited budget.** Whether that be physically through educating employees or cyber through improving the technology, allocating funds becomes a challenge against the ultimate objective of preventing cyberattacks.

If I was CISO, I would prioritize more of my funds towards additional cybersecurity technology rather than training. The main reason for this is because algorithms and tasks can be incorporated into the technology so it can match the skills of the employees and the training they receive. A CISO's landscape is constantly evolving with advancements in technology that I have to be able to match the sophisticated efforts of cyber criminals (Hay 2023). Giving Take AI

for example, it is becoming so advanced that it could be the main driving line of companies, not employees. AI the knowledge of employees and their training balances out the tradeoff of having lesser funds in training the employees. Now before incorporating AI into being part of the defense system, I would test its mechanisms through means of monitoring or activity from white hats. This is how I could see the weaknesses the AI present and how I can actively improve on it before it's implemented. AI still isn't perfect so employees will still be able to play a contribution in protecting infrastructure against cyber threats until it has mitigated its issues. It's a foreseeable future that in some minds might be unnerving, but in others it's the realistic way of life for companies who seek to perform at a higher level with more profits.

In conclusion, both training and additional cybersecurity technology are vital components to making a secure defense system against cybercrime. Training helps educate employees on being more aware of malicious activity and helps them understand how to act in certain scenarios. Improving and adding cybersecurity technology is also important because having up-to-date hardware and software helps the security system as a whole to respond quicker to incoming threats. With advancements in technology, AI is also an option to be able to incorporate into company infrastructures. Becoming CISO carries a big responsibility of monitoring over all operations with managing a budget that crucially adheres to the company's framework. Everyone, including the CISO, ultimately share the same objective which is to protect their company's important data.

Works Cited

Dr Mark van Rijmenam, C. S. P. (2022, August 25). *How Cybersecurity is Changing Technology Today*. Dr Mark van Rijmenam, CSP | Strategic Futurist Speaker. Retrieved March 31, 2023, from https://www.thedigitalspeaker.com/cybersecurity-changing-technology/

Hay, A. (2023, January 5). *The Evolving Role of the CISO in 2023*. Forbes. Retrieved March 31, 2023, from https://www.forbes.com/sites/andrewhayeurope/2023/01/04/the-evolving-role-of-the-ciso-in-2023/?sh=13123c76663f