Camrin Joyner

12/11/2024

Professor Hagh

CYSE 200T

Human Factor in Cyber Security Write Up

If I were a Chief Information Security Officer and had a small budget, I would use a risk based allocation plan to find the best balance between educating and cybersecurity technological advances. In this method, I would start by looking at the specific threats that the company faces and figuring out what its biggest weaknesses are. Based on this evaluation, I could put assets where they will most likely help lower the risk of big losses.

I would put more of the budget toward training if the company already has a pretty good cybersecurity infrastructure, with modern equipment and security practices in place. In this case, training would focus on making workers more aware of new threats like hacking, social engineering, and managing passwords. The goal is to get people to behave in ways that are safer and to make sure that workers protect the company from dangers that might get around technological defenses. Human mistake is the main reason for breaches, so focusing on training would help lower this risk without having to spend a lot of money on new tech.

But if the evaluation shows big holes in the current security system, like old software, bad monitoring systems, or not enough encryption, I would put more resources into improving and growing cybersecurity technology. Endpoint security, network security like firewalls and intrusion monitoring tools, and data encryption would all get more money. When workers have a solid technological base, they can focus on preventing threats and responding to them in the best way possible. This plan makes sure that the technological safeguards are solid while still putting a lot of stress on teaching the workers new skills.

Camrin Joyner

12/11/2024

Professor Hagh

CYSE 200T

In the end, this way hits a very good balance between how much training costs and how important it is to have strong cybersecurity in place. It helps me decide where to put my resources to have the most effect by carefully looking at the organization's specific weaknesses and threats. This method makes sure that spending on training focus on people, who tend to be the weakest link in security, and at the same time, technology changes fill in any technological holes in the infrastructure. Knowing exactly where the biggest risks are lets you focus where to put your money, making sure that your limited funds don't go to pointless efforts but instead get sent to the areas that need the most help.