Elliot Mason

11/10/2024

CYSE200T

The Human Factor in Cybersecurity

As a Chief Information Security Officer, balancing funds between training and cybersecurity technology requires strategic decision making. Both training and cybersecurity technology are crucial in mitigating risks and lowering human risks. The main thing to do is to figure out what risk are higher and what training and technology can mitigate those risks. Prioritizing risks can be helpful with determining if it requires more technology or human assessment and training or an equal amount of both.

The most likely risk attacks are phishing, ransomware, malware, and insider threats. First thing it to assess which risks are higher especially those of human factor. Then looking at what technologies and systems are already in place to interfere upon human risks such as encryption, firewalls, access controls etc. Reviewing these existing systems means going over updates and possible augmentation needed to ensure these technologies are working properly to secure data and information. A portion of the budget should be allocated into doing so.

Technology can be strong and most of the time predictable to normal shutdowns and reboots. Humans, meaning employees, however, are unpredictable when it comes to cybersecurity. Human error is a huge risk in cybersecurity. A significant portion of funds should be allocated to human training to limit and mitigate human error and risk. These trainings should include training on the cybersecurity technology, training on how to control threats and how to recover from attacks if they so happen. One option is to create simulations to ensure every

employee knows their part in controlling an attack and recovery as well. Another is to constantly train employees on possible threats they may not see as threats, especially phishing.

Risk assessment should be continual, and training should be bi-annual, if an attack happens on another company that could be like ours, training will occur to see what we would do in that time. Technology changes very quickly, as it gets more advances, threats and attackers also get more advanced.

A smaller portion of funds should be allocated into a recovery plan. Backup systems, financial loss coverage, the ability to hire specialists and investigators if needed, etc. Due to attacks and human error being almost always non foreseeable, having a recovery plan is crucial. Recovery plans show where everyone needs to go, and what everyone's position and role is during an attack but also after the fact to ensure all systems can recover as quickly as possible.

The balance between technology and human training can be hard to find when allocating funds. I believe 50% should be allocated to training, 40% to technology and systems, and the last 10% to a recovery plan. Human risk and error are almost always the easiest to occur and extremely unpredictable. This is why a majority of the funds should be allocated to training. Errors and mistakes occur, but in cybersecurity it can create a larger issue than just a little mistake. Technology that can defeat and prevent outsider threats and keeping those systems updated are also crucial which is why a big portion of the funds should also go to that. Technology changes and requires updates to continue to function properly. The last 10% of funds should be allocated into that recovery plan, although attacks and error may not occur, it is crucial to have a plan in order to set roles and positions of every employee in order to recover quickly.