Discussion of Human Factors in Cybersecurity

            Recently, we have been given a limited budget for our training and use of cybersecurity technology. This has led to some setbacks in what we fully planned to teach our upcoming employees. However, writing this, I believe we will be able to allocate funding and achieve what we planned to do within our cybersecurity sector.

*What to Prioritize*

            According to Micke “Human error is the main cause of 95% of cybersecurity breaches” (Ahola,2022). This is a huge number that we feel could be shortened if most of our funding was allocated to human training. One of the biggest risks present within our field is the likelihood of an employee falling into a phishing attack. To mitigate this, we feel that instating a phishing simulation could help decrease the possibility of an employee falling for this attack. This could also improve our budget because instead of having to purchase better security systems we could instead focus on the training to prevent them from falling for this attack. Allocation of funding could also go to annual mandatory cybersecurity awareness training for all employees. If this was instated the cybersecurity team could hold a yearly review of attacks to look out for and what to do if they notice the possibility of an attack. This works for the future to as we would not have to be called in to repair a potential security breach due to a lack of knowledge of phishing attacks. Having these events would see a use of about 40% - 50% of our budget being provided.

*Deployment of basic but effective Cybersecurity Technology*

We already have effective security technology such as firewalls, endpoint protection, and intrusion detection systems (IDS). We find that many cost-effective technologies would be useful for extra security within the organization. VPNs are a semi-new technology that has been introduced to the world of technology. However, the ability of a VPN to not only change the location of a user but to also hide data and detect software misuse is a great technology we could implement. If we are worried about costs Curtis Franklin states, “at $82, this would be a near-perfect solution for field work, emergency operations, or other situations” (Franklin,2019). From this alone we find the budget would barely be dented leaving extra funding for more security technology. If our previous training above were to fail, we could use some funding to implement some critical technologies we find useful for user assistance. Technology such as email filtering and anti-phishing tools would be a useful and effective tool that could ensure a bit of cushion if an employee is worried an email received might be a potential attack. Lastly, we could segment our firewalls instead of keeping them in one big perimeter if we were to segment these technologies it would limit the movement of critical data in the event of a security breach. From this, we believe about 30% - 40% of the budget is being used which could be changed if needed.

*Budgeting of Risk Tolerance*

Using the remaining funding we believe a re-examination and possible update of our risk management would be a useful addition to this budget. This comes from the assumption that if our employees are well-trained within the cybersecurity field, we find it useful to shift the funding to be more focused on technological improvements. As stated previously while those ideas are good on our limited budget if we were able to increase it for technology, we could upgrade most of the weak points within our network security. While if training for employees outweighs upgrades in technology, we find it very important this training is performed. If 95% of breaches are caused by human error, we stress that training is needed and should be required by every employee present. This can be done in the hopes of our employees not falling for obvious attacks that could jeopardize the company. Looking at our current situation we find focusing on the employee training more important for the budget. Because, from our testing majority of our employees do not understand possible attacks, so moving forward with this training would be best

*Conclusion*

Overall, we find our planning of where the budget should go useful in what we plan to implement. Assuming our employees are not skilled in cybersecurity putting the majority into the training could help decrease human errors commonly made. Having this done could ensure the safety of the majority of the critical data within the organization in the future. On the other hand, if our employees are knowledgeable in cybersecurity putting more budget into technological upgrades would be useful as a backup in case the human factors were to fail. Understanding which one of these is needed more within the company will help us move forward with our budget allocation.

References

Ahola, M. (2022, June 17). The Role of Human Error in Successful Cyber Security Breaches. *The Role of Human Error inj Successful Cyber Security Breaches*. https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Franklin, C. (2019, March 15). *7 low-cost security tools*. 7 Low-Cost Security Tools. https://www.darkreading.com/iot/7-low-cost-security-tools