Justin Deloatch

4/2/2023

Human Contribution in Cybersecurity

BLUF: In society Cyber has become a bigger industry that requires more people than it previously did due to the rapid advancements in technology. Although people would just think that it is just about computers and hacking is much more than that. In Cybersecurity there are humans that need to manually carry out some of the tasks. One of the main tasks being managing the budget that is needed for the technology, training, and other important aspects.

HYPOTHETICAL INFORMATION SECURITY OFFICER: Let's say hypothetically I was to become an Information Security Officer. That means that I have the role of trying to identify and prioritize the issues that will or could be present in the company. I would do this by having a budget and learning to spend it wisely on some of the necessities for the company to keep thriving. Some of the main necessities include training, and new technology.

BUDGET FOR TRAINING: If I was a Chief Information Security Officer and I had to allocate money to a budget for training and newer technology I would allocate roughly around 60% on training. Some might question that reasoning, but there are many factors that go into it. One of the main reasonings is because without good practices and protocol in the work environment no matter how much money you spend on new technology the company's proficiency will decline and steadily put you and your workers at risk of losing their job. Another reason so much is dedicated to learning and training is because as a company we have personal goals since we cannot fix everything so, if I were running a company, I would want to make sure we are very good at managing the main risks factors that we specialize in. To add on, I would allocate so much to ensure that the workers are comfortable and feel as if they want the best for the company, so that it minimizes the risk of them turning to other employers.

BUDGET FOR TECHNOLOGY: When it comes to spending money on new technology. I would spend the remaining 30% on newer technology. Some people may disagree with this, but there are a few reasons why. The first reason is that if we have newer technology without proper work training the use and need for the newer technology would be somewhat useless. To add on, newer technology typically comes out every couple of years, so if that is the case, we as a company could remain using the technology and upgrade as we get more clientele and notoriety. Also, to add on, with the additional 10% I would use to get maintenance and repairs on the system in the rare off chance that we needed them.

CONCLUSION: In conclusion, as a Chief Information Security Officer you have many responsibilities that are present. One of the main ones being allocating a budget for the company to spend on technology and the training of workers. If I had the chance to have a budget and spend it, I would spend roughly 60% on training, because without the proper training techniques and proper workforce training it minimizes the company's efficiency and productivity which could lead to reduced profit. Although 60% is being spent on training, I would spend around 30% on newer technology. I would spend 30% on technology, because if too much emphasis is given to technology, it would be pointless if we did not have people who are fit for the job. Lastly, the remaining 10% would be used for repairs on the off chance that the technology is unfit or malfunctions occur.