me: Justin Graham

Date: 11/20/2022

CS Training Programs

BLUF

Are cybersecurity training programs beneficial to companies and organizations? There are many benefits to training programs, but they come at a cost. This article helps analyze whether a company should create a program and under what conditions it can succeed.

Benefits of Training

Some of the benefits of having cyber security training include preventing the risks of incidents through the education of employees, better responses to incidents that do occur, and providing a higher profit for the company. The question posed from the journal was to determine the cost benefit of whether training or using funds elsewhere was better in the long run. Zhang describes three main components of having training programs as “Development costs, Direct loss of productivity, and Loss of reputation”. A company should consider these three components before deciding whether or not to implement a training program.

Costs Benefit Analysis

The journal from Zhang explains that the other main concerns a company should consider when they decide to implement a training program are the company’s current level of security, the anticipated cost of implementing the training, and the cost of a failure or attack. Generally speaking, if the cost of the training is well within a budget and the potential profits from the training can overtake some of the initial investment then it would be a good decision to start a training program. Zhang created four categories that a training program could be classified in with the benefit to the company. These were “Negligible, Consistent, Increasing, and Diminishing” (Zhang). The first represents a situation where the failure cost is the same as before the training, consistent with a situation where the cost is reduced with better security, increasing has the best cost efficiency at the highest degree of security, and diminishing has reduced benefits with higher levels of security. Should the company’s increased level of security reduce enough of the potential costs of an attack, then the training program would be a success. In those situations, I think the training programs make sense. For smaller companies or ones where

having cyber security specialists do not have much influence, I think investing in technological solutions would be the better option.

Conclusion

Most companies have to deal with cybersecurity risks with the new age of technology and the waves of users that followed. Almost all companies around the world have some sort of online technology whether it is the internet in their stores, databases, online shopping, or other companies that specialize in technology. As a result, companies should be willing to invest in training programs or better security devices. After reading the journal article, I believe that if the company is willing to allocate some of its resources to training that it will benefit the company. The ability to help prevent cyber attacks by educating its employees is crucial in negating losses. Whether it is opening a phishing attack via email, participating in risky online behaviors and social media, or preventing data from being thrown out onto the internet by accident, they all have benefits. If the company does not have enough resources or employees to make a significant change, then allocating whatever resources it can into technological solutions would be the better option.

References

Zhang, Zuopeng (Justin), et al. "Cybersecurity Awareness Training Programs: A COST–Benefit Analysis Framework." Industrial Management & Data Systems, vol. 121, no. 3, 2021, pp. 613–636., https://doi.org/10.1108/imds-08-2020-0462.