Balancing the cost of Human Factors

Jadyn Richardson

Cybersecurity, Technology, and Society

11/28/2023

BLUF

The human factor in cybersecurity is a vital part of making a system secure. But companies do not have an unlimited budget and therefore must decide whether to spend more or less on securing the human factor of the business. In this paper, the act of balancing the cost of securing human factors in cyber security will be discussed.

What is the Human Factor, and why is it important?

The Human Factor in cyber security is a very important part of securing any organization. A lot of cyber security experts like to say that the people in the organization are the weakest part of any cyber security set ups. This is because of social engineering. Social engineering is a method used by malicious parties to trick a person into giving up critical information by psychologically manipulating them (Carnegie Mellon University). Examples of social engineering can be things like calls from people pretending to be your bank, or emails from people pretending to be your boss, and in those cyber-attacks, they will tell you to give up whatever information they are looking for or else there will be dire consequences such as the loss of money. These types of attacks have no need for the more technical aspects of a cyber-attack like getting remote access to their computer because the victim gives it to them willingly. In order to combat the weakness of the Human Factor, training and policy need to be followed.

Balancing the cost of Human Factors.

Implementing a policy and employee training is not free and can be costly. The price of maintaining training and enforcing policy is one that will persist as long as an organization is alive. But how one spreads their budget across the human factor and technical aspects of cybersecurity will vary depending on the size and type of an organization. An organization that does not employ many employees will spend significantly less money than an organization with hundreds of employees. This is because there are more people to train, and there will be more machines that have to be secured against potential vulnerabilities that people in the organization can make. An example could be that one employee can log into any computer that they want to because the proper policy has not been implemented or followed. That employee also uses the same password every time that they log in. Because the human factor of that employee has not been mitigated with proper training and policy management, an attacker can get access to all systems with just that person's password with a phishing attack. But an organization should not neglect all other aspects of security just because the human aspect is very important and should make sure to analyze risks and the potential costs of damages that may occur to those assets.

Conclusion

In conclusion, balancing the cost of human factors and other cybersecurity measures will vary based on the nature of the organization that needs to be secured. But neither the technical or human aspects of cybersecurity should be ignored. The budget for security should be carefully thought out based on a risk management analysis.

Sources

Social Engineering - Information Security Office - Computing Services - Carnegie Mellon University, Carnegie Mellon University, www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html#:~:text=Social%20engineering%20is%20the%20tactic,or%20giving%20away%20sensitive%20information. Accessed 28 Nov. 2023.