Camryn Patillo

Old Dominion University

10.08.23

Human Factors in Cybersecurity

Introduction

To have a well-working system for cybersecurity, you will always need to ensure that your technology and your employees are working efficiently. These two factors are important in the working process of securing your systems. However, it is not as easy to keep your employees up to date on policies as it is with your technology. In fact, it is said that 88% of data breaches are caused by human error (CYDEF, 1).

Social Science Principles

This article used a few social science principles to explain the Human Factor issue in cybersecurity. Some examples are Relativism, Parsimony, Empiricism, and Determinism.

Relativism: The article recognizes behavior issues depending on the employee's age. The article explains that employees from ages 31-40 who grew up with the internet were more likely to fall for phishing emails compared to employees ages 51 and older (CYDEF, 14).

Parsimony: The explanation of the human factor in cybersecurity in the article is straightforward and concise and does not show any complexities within the article.

Empiricism: Survey results are listed throughout the article to give further insights on human behavior.

Determinism: The article discusses the factors that could cause human error in cybersecurity. It stated that 57% of employees claimed they are more distracted while working in an environment

that requires more productivity and attention (CYDEF, 9). The stress and lack of energy causes more human errors to occur.

Research Question/Hypothesis

A good research question for this article would be "How do factors such as age and workplace conditions affect the human behaviors that enable employees to fall for phishing attacks?"

Some Hypothesis that could go with this research question would be,

Age: younger employees are more susceptible to phishing attacks compared to older employees

Workplace Conditions: Employees under harsh working conditions are more likely to commit human error due to increasing distractions.

Types of Research Methods/Data & Analysis

The research method used the most in the article was quantitative data and the use of numbers, percentages, and data to give further information on the factors of human error. The type of data used in this article are surveys and questionnaires for the quantitative data and comparative data (used to explain factors such as age and workplace conditions to explain the causes of human error).

Challenges, Concerns, and Contributions of Marginalized Groups

- Although employees who are older are more likely to get phishing attacks, employees who are younger are more likely to click on them.
- Employees who are not as exposed to threats and face educational setbacks are more likely to commit more human errors and fall for phishing attacks.

Conclusion

As technology advances, Cyber-threats will grow along with it. The field of cybersecurity is to make sure these technologies are safe for individual and business use. The benefits are well-functioning organizations and the safety of society as a whole. So it is extremely important to make sure cybersecurity employees are above the threats that come with advanced technology. Falling for phishing threats is a microcosm of bigger things that could happen to society if human errors are not regulated. To prevent such things from happening, it is important for organizations to make sure their employees are properly trained and are up to date on any cybersecurity policies.

References

CYDEF. (2021, May 19). The Human Factor: The Hidden Problem of Cybersecurity. Retrieved from https://cydef.ca/blog/the-human-factor-the-hidden-problem-of-cybersecurity/