For my article, I chose an article from the "Cybersecurity" journal entitled, "Review and Insight on the Behavioral Aspects of Cybersecurity." (Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. et al. (2020, April 21st). Review and Insight on the Behavioral Aspects of Cybersecurity. Cybersecurity 3(1), https://doi.org/10.1186/s42400-020-00050-w) The authors of this article address the growing concern of a lack of behavioral science and human consideration in cybersecurity.

Behavioral Science & Cybersecurity

Most of the time, cybersecurity efforts mostly focus on the technical aspects of the problem. However, this article describes how including human behavior into cyber security technology and decisions can be much more effective. One of the ways that this can be accomplished is by expanding the dynamic of a cybersecurity team. Instead of relying solely on individuals with a technical background, it is argued that those with criminology, psychology and human factors background should also be employed.

They also argue for enterprises to work to account for human error vulnerabilities when designing systems. "Avoiding a vulnerability altogether is a much more reliable option than trying to patch it." Some of the vulnerabilities in behavioral psychology are exploited by hackers. For example, password attacks like dictionary attacks take advantage of users not being able to remember complex passwords. Another example is phishing, which is an attack that takes advantage of a user's psychology through several forms of manipulation.

Another behavioral insight explored is that of insider threats. Insider threats are hackers that are inside of an organization; they use their access privileges and or status to take down the company from the inside. A couple explanations are explored, such as frustration, lack of job satisfaction, and irrational behavior. It is recommended that when building an enterprise, automatic detection of behaviors such as unauthorized use of privileges should be implemented. An alert system that monitors how admin credentials are being utilized could be an example of this.

Principles of Social Science

There are three principles of social science that can relate to this article, they are: Determinism, Relativism and Parsimony. In the theories section of this article, both the "Social Learning Theory" and the principle of determinism are described. As stated by Hardy et al., "Learning happens in a social context with reciprocal determinism." (Hardy et. al, 1980) Relativism is addressed by understanding that several factors can contribute to a cybercriminal's mentality.

Some theories that address this are the theory of self-control, social cognition theory, social learning theory and more. Other related factors among cybercriminals are that they tend to have weak social bonds, a high level of agreeableness, and an early exposure to crime. Finally, parsimony is used in this study by effectively explaining human behavior. This article effectively explains several complicated theories, including the theory of self-control, theory of normative behavior and social cognition theory through use of diagrams and several easy-to-understand examples.

Questions & Hypotheses

One of the questions is, "What are the deficiencies in current research and what areas need immediate attention or improvement?" After reviewing this article, I believe that some of the biggest deficiencies come from the lack of behavioral science research in cyber security. There are also few studies on how human error heavily affects an enterprise and how they can be best mitigated. Another question is, "What are acceptable and unacceptable behaviors among users?" The article addresses this by verifying that acceptable behaviors include effectively completing user training, opening an authorized file, safely starting an authorized application, and more. A few examples of unacceptable user behavior include opening an unauthorized file, visiting a website that is on a block list, browsing unsafe websites, or sending a bulk of pages to a printer.

Research Methods and Data

This article utilizes literature review, surveys and several theories to describe their findings. For example, the theory of planned behavior is used here for insider threats: it argues that an individual's behavioral intention is close to their actual behavior. An insider threat's intention could be to exact revenge on the company by leaking trade secrets. Their intentions line up with their actions, thus confirming the theory of planned behavior. Another theory is neutralization theory, as several deviant employees try to justify their bad behavior by seeking justification. They are also hardly worried about the punishment for their insider crimes, rather they are simply worried about getting caught. According to the authors in Payne and Hadzhidimova (2018), "The most popular criminological explanations of cyber crime include learning theory, self-control theory, neutralization theory, and routine activities theory."

Surveys are used in this article for data, such as Halevi et al.'s survey of different demographics susceptibility to phishing. (Halevi et al., 2013) Along with this, diagrams are also

used. For example, there is a comparison for the Social Cognition theory. They compare personal cognitive factors, environmental factors, and behavioral factors together to fully address the theory.

Concepts From Class & Marginalized Groups

Several concepts from class are addressed in this article, they include human factors , psychology, several theories such as self-control theory, behavioral theory, the theory of planned behavior and neutralization theory, hacker motivations, human error, and victimization indicators like agreeableness and extraversion. This article relates to two marginalized groups; women and adolescents. According the the authors in Halevi et al., "women are more vulnerable to prize phishing attacks than men, and a high correlation between neurosis and responsiveness to phishing attacks was discovered." This was determined in a survey study. Data such as this addresses how training can be catered effectively to each group affected by phishing. This article also discusses how adolescents can be affected by malicious behavior or actors. This group may not have enough supervision or knowledge about the internet to refrain them from encountering cyberbullies. Hacker's manipulation tactics are especially dangerous to adolescents who are not able to understand the danger they are in, and when someone is fooling them.

Contributions

This article works to contribute to the growing argument that cybersecurity issues are not just technical, but they are also behavioral based. It helps to inform readers how to take into account the many aspects of cognition, personality, and bias that affect one's behavior in the digital world.

Human error is thoroughly explained in this article, as it is described in three categories here; unintentional, intentional, and malicious. Unintentional user error can mean a lack of knowledge, intentional human error by one who misuses assets despite being educated about them, and malicious as some intentional deals damage to a company by exacerbating an "error". This contributes to a more in-depth explanation of this common phenomena rather than a "one-size fits all" approach to human error.