1-2 Journal: Humans and Cybersecurity

Joshua Merren

Southern New Hampshire University

CYB-250-11621-M01 Cyber Defense

Professor Tchinda Mbuna

3 July 2024

Cybersecurity is not solely about protecting networks and digital infrastructures from malicious external attacks; it also critically involves managing the risk associated with human behaviors within an organization. Human factors are frequently identified as a significant vulnerability within cybersecurity frameworks, contributing significantly to breaches and security incidents. Gopikrishna Butaka's insights in the article "Is Cyberspace Secure From Humans?" reveal that humans cause a staggering 95% of cybersecurity breaches through errors such as mishandling data, misconfiguring servers, or falling for phishing attacks. This statistic underscores the complex and unpredictable nature of human behavior, which, despite the best technical defenses, can open doors to cyber threats. Laziness, fatigue, and ignorance are not just minor nuisances; they form the crux of many security lapses. For instance, a tired employee might reuse a simple password across multiple platforms or carelessly click on a malicious link, compromising organizational security. Furthermore, the pressure and stress of high-stakes IT environments can exacerbate human errors, leading to costly mistakes. Therefore, Organizations must look beyond technical solutions and address these human elements directly through continuous education and a strong culture of security awareness. This approach should include regular and engaging training sessions that not only cover the basics of cybersecurity but also highlight the latest threats and the personal responsibility of each team member in safeguarding the organization's digital assets. By integrating human-centric security practices, companies can significantly reduce the risk of breaches while fostering a proactive cybersecurity culture.

To mitigate the risks associated with human factors effectively, organizations should consider several strategic approaches, as discussed in both the textbook "Cryptography and Network Security" and the article by Butaka. First, implementing rigorous training programs that focus on the practical aspects of cybersecurity can help employees understand the consequences

of their actions. Such training should be continuously updated regularly to reflect the evolving nature of cyber threats. Automating specific processes can significantly reduce human errors. For example, automated systems can handle software updates and patch management, tasks that busy staff often overlook. Cryptographic measures and strict access controls are also essential, as they limit the potential for human error by restricting access to sensitive information based on roles and responsibilities. Techniques like multi-factor authentication and digital certificates enhance security by adding layers that compensate for potential human fallibility. Furthermore, encouraging a policy of 'least privilege' can ensure that employees access only the information necessary for their work, reducing the risk of insider threats. Regular audits and feedback mechanisms can also help identify potential areas of improvement in an organization's security practices. Finally, fostering a culture that values security as a fundamental aspect of every employee's role can lead to better compliance with established protocols and an overall safer organizational environment. These combined strategies address the technical aspects of security and the human elements, creating a comprehensive defense against a wide array of cybersecurity challenges.