Review 1 - 1866175549

The author rightly points out habituation as one of the considerations for the human factor. According to Kim and Wogalter (2009), habituation is caused by three factors. First, the capacity of security warnings to inform users is lost. Second, because of the existing memory, users might respond less quickly in reaction to security warnings. The third reason is that the security alert repeatedly appears, making the user less responsive than it ought to be.

Another human factor the author correctly points out is Trust which leads to social engineering attacks. Curiosity, empathy, excitement, and fear contribute to social engineering attacks (Abraham and Chengalur-Smith, 2010). Social engineering attacks are both persistent and pervasive, and it is harmful to combine users' relative laziness toward security procedures with spammers' and hackers' aggressive nature. As pointed out by the author, frequent cybersecurity notifications might cause "alert fatigue," which makes personnel less responsive to alerts and increases the chance of missing or delayed alerts. The burnout that follows from tiredness can increase personnel turnover in the IT departments. The cycle restarts when replacement employees are employed (Segal, n.d). Overall, the author has captured quite well the implications of the human factor on ASMIS.

Review 2 – 1866016921

The author makes an astute observation about human error contributing to the human factor. According to IBM Cyber Security Intelligence Report, the most significant driver in 95% of cyber security breaches is human error. Additionally, according to IBM's Cost of a Data Breach Report 2020, human error-related cyber security breaches have an average cost of $3.33 million (Anon,2022). The author correctly identifies the different aspects leading to a skill-based error. Slips and lapses are minor mistakes when executing routine tasks and activities and constitute skill-based human error. The user may also showcase decision-based errors. The user may not have the required degree of understanding, not enough information about the particular situation, or may not even be aware that they are deciding on their inaction, leading to a decision-based error (Ahola, 2021).

One other human factor the author discusses is an insider with malicious intent. For an insider attack to occur, three key elements must exist: motive, ability and opportunity. Personality factors, current emotional state and predisposition contribute to an insider's motive, whereas opportunity is determined by the insider's roles in the system (Gheyas and Abdallah, 2016). Overall, the author did an excellent job of capturing the effects of the human factor on ASMIS.

References:

Amran, A., Zaaba, Z.F. and Mahinderjit Singh, M.K. (2018). Habituation effects in computer security warning. Information Security Journal: A Global Perspective, 27(4), pp.192–204. doi:10.1080/19393555.2018.1505008.

Abraham, S. and Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, [online] 32(3), pp.183–196. doi:10.1016/j.techsoc.2010.07.001.

Segal, E. (n.d.). 'Alert Fatigue' Can Lead To Missed Cyber Threats And Staff Retention/Recruitment Issues: Study. [online] Forbes. Available from: https://www.forbes.com/sites/edwardsegal/2021/11/08/alert-fatigue-can-lead-to-missed-cyber-threats-and-staff-retentionrecruitment-issues-study/?sh=5a26308a35c9 [Accessed 9 Jul. 2022].

Anon, (2022). Top 5 Cyber Attacks and Security Breaches Due to Human Error - Threatcop. [online] Available from: https://threatcop.com/blog/top-5-cyber-attacks-and-security-breaches-due-to-human-error/#:~:text=In%20fact%2C%20according%20to%20the [Accessed 11 Jul. 2022].

Ahola, M. (2021). The Role of Human Error in Successful Cyber Security Breaches. [online] blog.usecure.io. Available at: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches [Accessed 11 Jul. 2022].

Gheyas, I.A. and Abdallah, A.E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big Data Analytics, 1(1). doi:10.1186/s41044-016-0006-0.