Peer Response to Article One - **1886355595**

Thank you for a comprehensive and well-thought discussion. In the discussion, you emphasized the importance of considering the human factor in designing Cyber Security policies and programs. I agree with you that the impact of the human factor on cyber security is often overlooked. Nevertheless, human factors expose secure systems to cyber threats and attacks. Therefore, as cyber security technologies and tools improve and become more sophisticated, it is critical to elevate the technology users to the same level. As argued by Gonzalez and Sawicka (2002), cyber attackers are well aware that human factors such as fatigue, errors, and behavior present a weak link to the security of an IT infrastructure. This implies that having good cyber security policies and technologies is not enough. Khar (2017), in a 2017 survey, revealed that most of the common breaches in organizations were directly linked to human factors. The study found that attackers increasingly targeted employees using fraudulent emails, phishing, and ransomware. Therefore, it is evident from research that human factors play a critical role in enhancing cyber security (Hughes-Lartey et al., 2021; Khar, 2017; Schneier, 2009).

Queens Medical Center should address the human factor in its endeavor to secure ASIMIS. Since the staff have a higher authorization level, it is essential to consider factors influencing their behavior. As you have comprehensively argued in the article, human limitations and biases, risk perception, and stress pose a risk to the system’s security. Attackers that employ social engineering to attack organizations exploit human limitations such as curiosity, greed, and politeness. Also, work-related stress, such as burnout, impairs employees’ ability to make rational decisions, making them an easy target by attackers. As you have observed, in the wake of the Covid-19 pandemic, the healthcare system was overstretched, increasing stress and anxiety among healthcare workers. This can explain the spike in phishing and ransomware attacks during the era of Covid-19 (Alawida et al., 2022). Therefore, when developing cyber security policies and programs for the ASIMIS, it is essential to ensure vulnerabilities related to human factors are addressed.

**References**

Alawida, M, Omolara, A. E, Abiodun, O. I, & Al-Rajab, M 2022, ‘A deeper look into cybersecurity issues in the wake of Covid-19: a survey’, *Journal of King Saud University-Computer and Information Sciences*, https://doi.org/10.1016/j.jksuci.2022.08.003

Gonzalez, J. J, & Sawicka, A 2002, ‘A framework for human factors in information security’, In *Wseas international conference on information security, Rio de Janeiro*, pp. 448-187.

Hughes-Lartey, K, Li, M., Botchey, F. E, & Qin, Z 2021, ‘Human factor, a critical weak point in the information security of an organisation’s Internet of things’, *Heliyon*,  Vol. *7*, no. 3, e06522, https://doi.org/ 10.1016/j.heliyon.2021.e06522

Klahr, R 2017, ‘Cyber security breaches survey’, PhD diss.,University of Portsmouth.

Schneier, B 2009, *Schneier on security*, John Wiley & Sons.