PEER-RESPONSE

The article Compromising a Medical Mannequin by Glisson et al. (2015) focuses on breaking production-deployed medial teaching mannequin. I agree with the research findings that the health care industry is unprepared for simple cyber intrusion attempts, which can have severe consequences for patients and medical services. With the industry's growing dependence on information technology (IT), cyber-criminals are increasingly targeting and profiting on hospital vulnerabilities (Muthuppalaniappan and Stevenson 2021, p.4). Consequently, healthcare professionals and organizations must demonstrate an awareness of cybersecurity and ensure they are protected and prepared to respond in case of any form of cyber-attack. Unfortunately, healthcare companies frequently lack the resources to defend themselves against cyber-attacks and can be severely impacted by the cost and long-term consequences of security breaches (Muthuppalaniappan and Stevenson 2021, p.5). In addition, several Internet of Things (IoT) equipment is susceptible to cyber-attacks mainly because healthcare gadgets are either inadequately protected against potential threats or not safeguarded (Yaacoub et al 2020, p. 581). Any cyber-attack might have disastrous implications thus endangering patients' lives and impeding the widespread use of these tools. In addition, cyber attacks may have consequences thus putting patients' lives at risk and limiting the use of these instruments.

Furthermore, the research highlights two principal vulnerabilities in a controlled environment, including Denial-of-Service attacks and brute force assaults. As such, organizations in the health care sector can employ threat intelligence technologies and artificial intelligence algorithms to mitigate these risks and boost security (Ranganayaki et al 2020, p.94). Additionally, Moudoud, Khoukhi, and Cherkaoui (2020, p.198) propose a cybersecurity system based on a Markov stochastic process used to watch each network device's behavior and employs a range-based behavior filtering strategy. Hospitals can employ this system to secure themselves against these attacks. Furthermore, hospitals can be secured against brute force attacks by establishing virtual patching applications to identify malicious traffic before it reaches the susceptible device. In addition, organizations can mitigate these risks by deactivating Internet control message protocol requests on edge nodes. The edge nodes might be set to block any IP address within the healthcare domain (Bradley, El-Tawab and Heydari 2018, p.150).

**References**

Bradley, C., El-Tawab, S. and Heydari, M.H., 2018, April. Security analysis of an IoT system used for indoor localization in healthcare facilities. In *2018 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 147-152). IEEE.

Moudoud, H., Khoukhi, L. and Cherkaoui, S., 2020. Prediction and detection of fdia and ddos attacks in 5g enabled iot. *IEEE Network*, *35*(2), pp.194-201.

Muthuppalaniappan, M. and Stevenson, K., 2021. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1), p.mzaa117.

Ranganayaki, R.S., Sreeja, B., Gandhari, S., Ranganath, P.T. and Kumar, S., 2021, December. Cyber Security in Smart Hospitals: A Investigational Case Study. In *2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART)* (pp. 92-98). IEEE.

Yaacoub, J.P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R. and Chehab, A., 2020. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Generation Computer Systems*, *105*, pp.581-606.