In discussing vulnerabilities of medical devices to cyber-attacks, it is observed that health care facilities have not shown enough preparation to deal with the security threats and issues that face medical devices. The increase in reliance on information technology in the medical sector requires heightened cyber security protection measures (Argaw et al 2020, pg. 2). However, the health sector has suffered from inadequate resources, thus failing to effectively secure their devices against cyber-attacks. The mannequins primarily susceptible to attacks are protocol and network security. In an article by (Glisson et al 2015, pg. 4), there is a case where the security of the medical devices was compromised through brute force attack on the router and denial of services attack on the network protocol. The training facility information was also attacked, posing a significant risk of the medics' incorrect analysis of patient data. This can have tragic effects such as death resulting from wrong diagnosis and treatment.

The outlined security threats and issues can be overcome by encrypting medical devices to improve their performance and longevity. This involves analysing encrypted traffic on medical devices to ensure the capability to identify attacks and imploring mitigation techniques (Baldini et al. 2020, pg. 1). Medical mannequins' attacks are preventable through various measures. First, regular updates of the antivirus software should be conducted to ensure its up-to-date and capable of identifying and preventing viruses and malware that may potentially attack the systems. Firewalls should be installed to obstruct attacks from Denial of Services. Another preventive measure from cyber-attacks is to employ virtual patching applications to identify any ill traffic before reaching the vulnerable devices. Lastly, there is a need to regularly conduct cybersecurity training among healthcare workers to ensure they remain vigilant and do not recklessly expose the medical devices to attacks.

**References List**

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O’Leary, C., Eshaya-Chauvin, B. and Flahault, A., 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*(1), pp.1-10.

Baldini, G., Hernandez-Ramos, J.L., Nowak, S., Neisse, R. and Nowak, M., 2020. Mitigation of privacy threats due to encrypted traffic analysis through a policy-based framework and MUD profiles. *Symmetry*, *12*(9), p.1576.

Glisson, W.B., Andel, T., McDonald, T., Jacobs, M., Campbell, M. and Mayr, J., 2015. Compromising a medical mannequin. *arXiv preprint arXiv:1509.00065*.