Within the original article, “Compromising a Medical Mannequin”, several important threats that exist within the medical community were brought to light. In particular, there is a growing problem with cyber security and the lack of prevention. Training material such as mannequins was one such object that was tested in the article. The mannequin was identified to have two main vulnerabilities. Those are a weakness in the network security solution and the network protocol (Glisson, 2015). While the threats that exploit those weaknesses are brute force and denial of service attacks(DoS) (Glisson, 2015).

To protect against these threats, several security devices were suggested such as IP inspection and packet filtering (Mahjabin et al, 2017). As well, the use of a next-generation firewall(NGFW), was suggested to help protect the network that the mannequins are a part of. The built-in IPS and IDS, within NGFW, provide overall detection against threats (Thomason, 2012).

As for the contributions made by others, excellent points were brought up. In general, I agree that strict cyber security regulations for medical IoT devices will be very beneficial. As noted in the original article, there were no strong regulations or guidelines at the time of the testing. IoT devices are known for their weak security and vulnerabilities (Tawalbeh, 2020). It would make sense to begin securing the device from the start of the development while tailoring them to fit in a medical environment.

There are also great points brought up about Ip blocking not being a foolproof solution. Due to the ease with which individuals can access VPNs or even botnets. It makes sense to not rely on this solution. Instead, a more secure solution would be the previously suggested implementation of an NGFW. This would allow for IP packet inspection but in a more dynamic way, that can detect botnets. To provide another layer of security, it should be combined with the implementation of zero trust architecture. Zero trust is the idea that attackers are already within the network itself (Rose, 2020). Devices need to be constantly analyzed and evaluated to provide the most up to date security possible.

References:

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) [Compromising a Medical Mannequin**.**](https://aisel.aisnet.org/amcis2015/HealthIS/GeneralPresentations/5/) Healthcare Information Systems and Technology (Sighealth).

Mahjabin, T., Xiao, Y., Sun, G., Jian, W. (2017) A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks.* 13(12): 1-33. Available from:<https://journals.sagepub.com/doi/pdf/10.1177/1550147717741463>

Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020) *Zero Trust Architecture.* Available from:<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf> [Accessed 20 November 2021].

Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M.(2020) IoT Privacy and Security: Challenges and Solutions. *Journal of Applied Sciences* 10(12): 1-17. DOI: <https://doi.org/10.3390/app10124102>

Thomason, S. (2012) Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices. *Global Journal of Computer Science and Technology Network, Web & Security’.* 12(13): 1-5.Available from:<https://globaljournals.org/GJCST_Volume12/6-Improving-Network-Security-Next-Generation.pdf>