4-2022

Medical Devices and Cybersecurity

Hilary Finch
Old Dominion University

MEDICAL DEVICES & CYBERSECURITY

AUTHOR

Hilary Finch

AFFILIATIONS

Old Dominion University

This project will focus on how technology and medical devices interact with each other and how to safely transmit data.

INTRODUCTION

While the standardized use of newer technology was beneficial and necessary to keep up with ever-growing demand, the healthcare industry failed to place any kind of focus on the security of their Information Technology department. This shows a glaring oversight due to the amount of sensitive information contained in these servers. The connected medical device market is projected to grow substantially over the next few years. This poster focuses on the benefits of implementing the segmentation model within the Medical Technology field. Segmentation is a security technique that could be employed by dividing a hospital's network into smaller more easily managed networks, which are then routed through a firewall.

OBJECTIVE

The main objective of this project is to investigate the relationship between the increase in network-connectable medical devices and increased cybersecurity risks/threats. We will then explore segmentation as a tactic used to contain these threats and reduce the impact of a network security breaches.

RELATED LITERATURE

Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., Petrozzino, C., & Zuk, M. (2018). The evolving state of medical device cybersecurity. Biomedical Instrumentation and Technology, 52(2), 103–111. https://doi.org/10.2345/0899-8205-52.2.103

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1–10. https://doi.org/10.3233/THC-161263

McMahon, E., Williams, R., El, M., Samtani, S., Patton, M., & Chen, H. (2017). Assessing medical device vulnerabilities on the Internet of Things. 2017 IEEE International Conference on Intelligence and Security Informatics: Security and Big Data, ISI 2017, 176–178. https://doi.org/10.1109/ISI.2017.8004903

The State of Healthcare IoT Device Security 2022. (n.d.). Retrieved March 27, 2022, from https://www.cynerio.com/landing-pages/the-state-of-healthcare-iot-device-security-2022

METHODOLOGY

This experimental design was employed due to the growing amount of connected medical devices and cybersecurity risks. The occurrence of cyber attacks resulted in a slew of issues and increased workload. The main focus of this experiment was to understand medical device connectivity and cyber security. Survey data was collected from various publications. Informants were generally positive about segmentation technology to limit data virus infections and thus improve patient safety. Participants were vocal that segmentation would be useful for insider and outsider threats.

RESULTS/FINDINGS

-The results demonstrate a few things:
- Medical devices have the potential to cause significant harm.
- Users of medical devices need to understand how to stay secure.
- Cyber criminals can access and reprogram medical devices
- A way to reduce the risk of harm due to cybercriminals is by use of network segmentation.
The results highlight a high cost plan to maintain medical network security but would also force an understanding of the segmented network implementation. While few physicians would forgo the improved data-driven, networked, electronic health records, in fact- the AHA stated that medical devices that had internet capabilities increased customer care and efficiency (McMahon et al., 2017), many agree that the 2008 Health Information Technology for Economic and Clinical Health Act that expanded vulnerabilities without giving thought to cybersecurity.
A major source of limitation is due to lack of information on interconnected devices and their cybersecurity issues. In addition, several questions regarding the future of medical devices and cybersecurity remain unanswered.

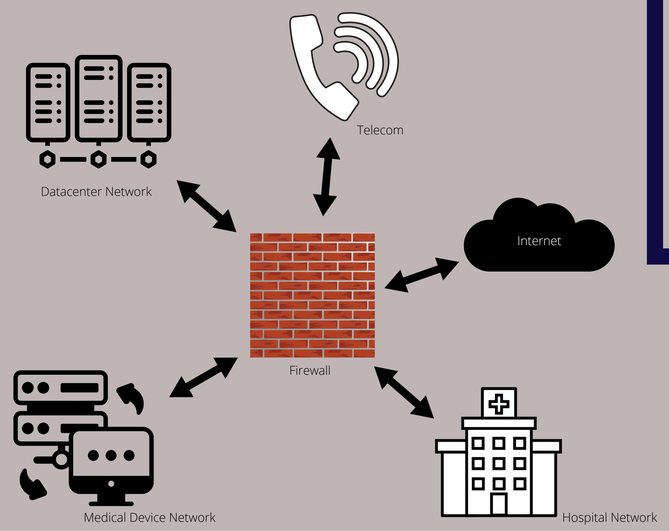
CONCLUSION

Networked medical equipment can inflict significant harm due to the fact that they have been developed without cybersecurity in mind. The interconnectivity of medical devices becomes increasingly problematic when bearing in mind that confidential data is worth a lot of money and is not protected due to outdated technology, budget limitations and resistance to change from stakeholders. Each interconnected medical device has its own unique security risks; there is not a one size fits all approach to medical device cybersecurity. This study of medical devices and segmentation provides insight into the complexity that is our healthcare network.

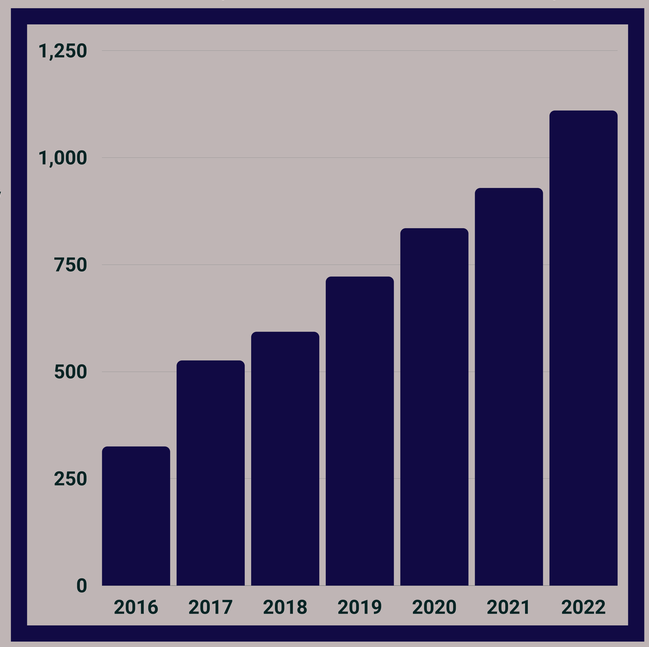
ANALYSIS

My data suggests that the implementation of segmentation would prove a need for more heightened security, budgeting toward costs, and administration. However, according to the data, not only would there be a cost for implementing, but there would also be a cost for administrative tasks and time. For the current work, it is sufficient to point out that there will be substantial growth in medical devices and their need for connectivity thereby increasing the need for cyber security.

Segmentation Example



Source: Cynerio The State of Healthcare IoT Device Security 2022



Number of connected wearable devices Worldwide, in millions