The Evolving State of Cybersecurity in Medical Devices

Chelsey Luc

California State Polytechnic University, Pomona

Presented By: Chelsey Luc, 19

INTRODUCTION

The healthcare industry has rapidly adopted digitally connected outpatient medical devices to improve patient monitoring and reduce hospital visits. Devices such as insulin pumps, pacemakers, and imaging systems are now integrated into hospitals and even patient homes, forming part of the Internet of Medical Things. However, this increased connectivity poses significant cybersecurity risks. Vulnerabilities such as outdated operating systems, a lack of encryption, and unclear protocols expose medical devices to cybersecurity attacks (Williams & Woodward, 2015).

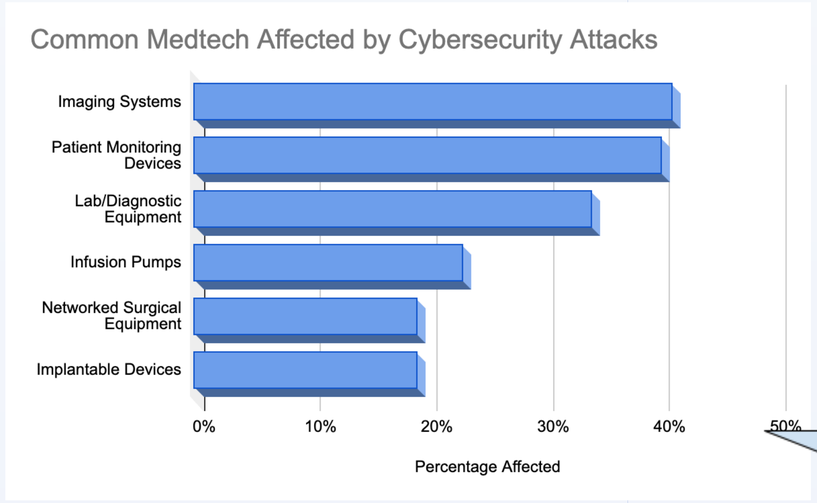
OBJECTIVES

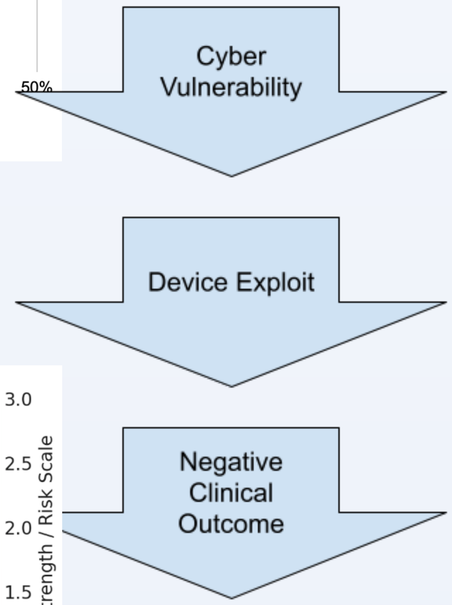
1. Identify recurring cybersecurity vulnerabilities in medical devices
2. Examine patient safety risks associated with device insecurity
3. Evaluate the impact of cybersecurity training for healthcare professionals
4. Propose strategies for cybersecurity improvement

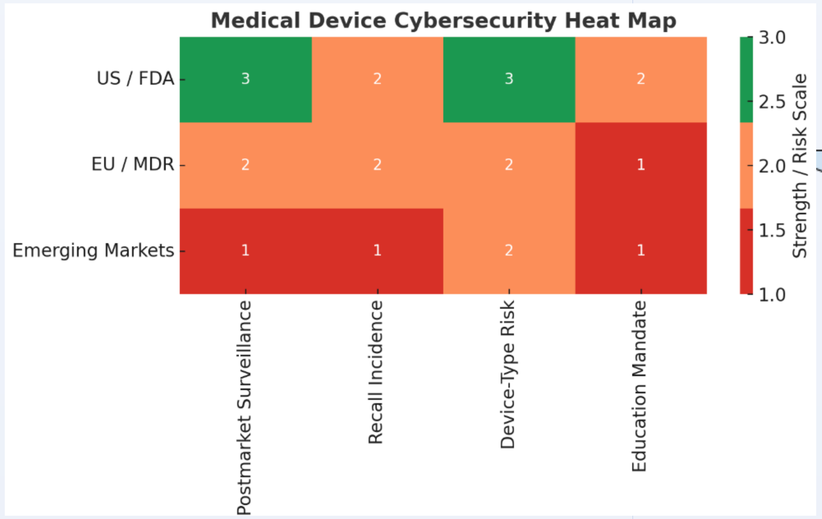
METHODS

Literature review from peer-reviewed journals and dissertations focusing on the cybersecurity of medical devices was cross-analyzed to expose technical flaws, policy gaps, and human factors.

RESULTS







CONCLUSION

Cybersecurity in medical devices is a multifaceted challenge that involves technology, education, and regulation. Addressing these risks requires a change to a standardized regulation regime in which government and international bodies ensure consistency among manufacturers and cybersecurity literacy to prepare clinicians to evaluate device risks. If these problems are ignored, healthcare systems risk economic losses and patient safety.

REFERENCES

Fomanka, E. M. (2025). Cybersecurity Threats to Medical Devices: An Exploratory Study on Implications for Clinical Outcomes (Order No. 32122487). Available from Publicly Available Content Database. (3230011137). http://proxy.library.cpp.edu/login?url=https://www.proquest.com/dissertations-theses/cybersecurity-threats-medical-devices-exploratory/docview/3230011137/se-2

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 & Technology, 52(2), 103-111. http://proxy.library.cpp.edu/login?url=https://www.proquest.com/scholarly-journals/evolving-state-medical-device-cybersecurity/docview/2018965228/se-2

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Medical Devices : Evidence and Research, 8, 305-316. doi:https://doi.org/10.2147/MDER.S50048

Eskelsen, E. (2024). Cybersecurity education of medical device prescribers and medical professionals (Order No. 31300707). Available from ProQuest Dissertations & Theses Global: The Humanities and Social Sciences Collection. (3064896256). Retrieved from http://proxy.library.cpp.edu/login?url=https://www.proquest.com/dissertations-theses/cybersecurity-education-medical-device/docview/3064896256/se-2

ACKNOWLEDGEMENTS

I would like to acknowledge my professor, Dr. Indira R. Guzman, for informing me of this opportunity.