Review of Cybersecurity in the Radiology Department

Leonardo Arthur Pangemanan

***Abstract*—Cybersecurity is an increasing concern for many healthcare organizations, information technology and medical cybersecurity professionals. As more computerized medical devices become connected to the network within and outside the facility increases, the risk of cyber attacks also increases. Moreover, the radiology departments have most of their devices connected to the network. Most radiologists are unaware of the vulnerability of their devices. This paper will review the cyber threat of modern medical devices within the radiology department to build more awareness to these vulnerabilities.**

***Index Terms*—Cyber-security, Security, Risk, Safety, Wireless, Medical devices.**

I. Introduction

THE medical industry has change ever since the first computer were introduced. The healthcare technologies have the potential to extend, save and enhance the live of patients. Furthermore, hospitals have witnessed a proliferation of networked medical equipment in the past decade. There is an emergent trend of connection medical equipment to the hospital network for easy accessibility and manageability. As healthcare devices continue to evolve, so does the inter-connectivity. For example, it provides efficiency, error reduction, automation, and remote monitoring. Interconnected technology allows health professionals to monitor and adjust devices without the need for hospital visit or invasive procedure [1]. With integration comes complexity and challenges in management and this protection [2]. However, interconnected technology introduces new cyber-security vulnerabilities in the same way other networked computing systems are vulnerable. Recently, securing medical devices against cyber-attacks or malware outbreaks and safeguarding protected health information (PHI) stored on devices or exchanged between a device and the provider's network is a growing challenge for clinical engineers and hospital information technology (IT) professional [3]. The number of high-profile public demonstrations of successful attacks on devices and medical networks have increased. This fact raises the concern that inter-connectivity will directly affect clinical care and patient safety.

Over the past few years, the question of inadequate clinical security has been gaining attention from both industry leaders and clinical practitioners. The integration of medical devices, networking, software, and operating systems means that the relative isolation and safety of medical devices are challenged [2]. These vulnerability is also due to many manufacturers focus their efforts on innovation and functionality, with little emphasis on the network security of this devices [4].

Designing a secure medical device is fundamentally different from any other devices that only focus on safety and efficacy. Safety design decisions are based on the assumption that hazardous condition or failure occur accidentally. However, the assumption that hazardous condition or failure occurs accidentally no longer holds true as malicious attackers try to trigger hazards in devices through intentional repeated attempts [5]. Thus manufacturer tends to not implement the necessary security check against these malicious attacks. This fact become more important as the radiology departments usually have the highest density of networked medical equipment in a hospital [4]. This paper will review the cyber threat of modern medical devices within the radiology department and implantable medical devices (IMDs).

II. Background

With the numerous data breaches in healthcare over the last several year, it seems to be unreasonable for patients having any expectation of privacy and security in their health information. In 2012, 780,000 patients records were stolen from the State of Utah Department of Health, Department of Technology server, by an Eastern European hacker. Another at Saint Joseph's Health System in California, approximately 31,800 patients' record was made potentially available through basic Internet search engines for about a year because security settings on the system were set incorrectly [6]. Increasingly, healthcare is a prime target for cyber attack with a recent SANS Institute report reporting that 94% of healthcare organization have been the victim of a cyber attack [2]. Table I shows the most common cyber attacks healthcare organizations is vulnerable to. The vulnerability of healthcare to cyber attack reflects a combination of factors, notably limited resources, fragmented governance, and cultural behavior. Most healthcare organization exist to provide cybersecurity within their devices. The industry more focuses on providing healthcare to the patients in need. Their revenue or reimbursement for healthcare is not tied to any cybersecurity effort. More importantly, there is a traditional believes that no one would be motivated to attack healthcare systems and protective measure were not necessary. As mentioned before, many of these healthcare organization ignore the potential danger of cyber attack and solely focus on giving patient care [1]. Moreover, the healthcare industry is one of the most targeted sectors globally; 81% of 223 organizations surveyed, and $>$110 million patients in the United States had their data compromised in 2015 [7]. Table I shows that the healthcare organization is not immune to these type of threats.

TABLE I
COMMON CYBER THREATS IN HEALTHCARE [7].

Data theft for financial gain	Stealing personal data for the purposes of monetary gain.
Data theft for impact	Theft and public release of sensitive medical information.
Ransomware	Using malware to block users from their data or systems or to delete data unless a fee is paid.
Data corruption	Deliberate corruptions of data, such as altering test results, for political or personal gain.
Denial of service attacks	Disruption of a network or system by flooding it with superfluous requestsn motivated by blackmail, revenge, or activism.
Business email compromise	Creating fake personal communications for financial gain.
The unwitting insider	Substantial disruption to systems or the loss of data owing to the unintentional actions of staff using outdated and at-risk systems.

A. Implantable Medical Devices

A typical IMDs monitor and treat physiological conditions within the body and improve patients' quality of life and help sustain their lives. These devices includes pacemakers, implantable cardiac defibrillators (ICDs), drug delivery systems, and neurostimulator. With these devices, health professional can treat abnormal physiological conditions within the body, such as cardiac arrhythmia, diabetes, and Parkinson's disease [8]. Some current-generation devices now have the ability to communicate wirelessly with external equipment from distances up to five meters away [9].

B. Radiology Devices

III. CYBERSECURITY IN RADIOLOGY DEPARTMENT

A. Types of Cyber Threats

IV. FUTURE SECURITY CHALLENGES

The medical industry face many challenges

V. CONCLUSION

The conclusion goes here.

REFERENCES

[1] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018.
[2] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices (Auckland, NZ)*, vol. 8, p. 305, 2015.
[3] A. Wirth, "Cybercrimes pose growing threat to medical devices," *Biomedical instrumentation & technology*, vol. 45, no. 1, pp. 26–34, 2011.
[4] V. Moses and I. Korah, "Lack of security of networked medical equipment in radiology," *American Journal of Roentgenology*, vol. 204, no. 2, pp. 343–353, 2015.
[5] A. Ray and R. Cleaveland, "An analysis method for medical device security," pp. 16:1–16:2, 2014. [Online]. Available: http://doi.acm.org/10.1145/2600176.2600192
[6] S. Murphy, "Is cybersecurity possible in healthcare," *National Cybersecurity Institute Journal*, vol. 1, no. 3, pp. 49–63, 2015.
[7] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: how safe are we?" *Bmj*, vol. 358, p. j3179, 2017.
[8] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE pervasive computing*, vol. 7, no. 1, pp. 30–39, 2008.
[9] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel, "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices," pp. 917–926, 2010.