Review of Cybersecurity in the Radiology Department

Leonardo Arthur Pangemanan
Southern Adventist University
lpangemanan@southern.edu

***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.**

I. Introduction

THE healthcare 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 connecting 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].

The rest of this paper first discusses the background of cyber security in II, and then describes my main topic in III. Lastly, IV presents the conclusions and describes future work.

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 [7]. 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. In May 2017, a ransomware called WannaCry infect more than 200,00 computers in 150 countries. One of the victim was the National Health Services (NHS) in the United Kingdom. Nearly 19,000 appointments had to be canceled, costing them and estimate £20 million. The NHS spent an additional £72 million to recover from the disaster and upgrade its systems [8]. The vulnerability of healthcare to cyber attack reflects a combination of factors, notably limited resources, fragmented governance, and cultural behavior.

In May 2017, The Ponemon Institute shared a survey that showed only 15% of healthcare delivery organization (HDOs) and 17% of medical device manufacturers (MDMs) were taking significant steps to prevent cyber attacks [9]. Figure 2 shows the total number of malware that is on the internet. With this many malware, there should be a protection against them. However, most healthcare organization exist to provide

TABLE I
COMMON CYBER THREATS IN HEALTHCARE [6].

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 requests 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.

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 [6]. Currently, there are many motivations for hackers to attack healthcare organizations and professional needs to increase the priority to enhance their cybersecurity.

A. Cybersecurity Terminology

Cybersecurity terms are unfamiliar to many people and can leads to misunderstanding by those who do not work in the cybersecurity or information technology professions. Here are some of the most common terms associated with cybersecurity based on [8]:

- **Distributed Denial of Service (DDoS)**: A cyber attack where the hacker use multiple device to send a request to a website or a network. If the number of requests is large enough, the website or network cannot handle the traffic and stop responding, therefore preventing legitimate users from accessing the network.
- **Malware**: Typically a software designed to interfere with the computer's normal function. This interference can take the form of destruction of data, inability to run the computer or certain programs, stealing personal information, or causing physical damages to the device. Figure 2 shows the yearly total number of Malware that has been developed in the past ten years. The different types of malware include:
  - *Ransomware* - Malware that encrypts all file on a device, making them unreadable and inaccessible.
  - *Virus* - Section of computer code that adds itself to files and spread in one computer and to other computers. Ransomware is a type of virus.
  - *Trojan* - A program that seems legitimate but are, in fact, malicious. Trojan allows hacker to access the infected device unnoticed and steal personal information or to steal passwords.
  - *Worm* - A standalone program that spreads among computers but does not infect individual files.
- **Phishing**: Emails that pretend to be from official entity. These emails usually contains a link or attachment that are malicious. The goal is steal sensitive information, such as financial institution login credential.
- **Virtual Private Network (VPN)**: A VPN allows users to connect to a private network securely, even when the connected network are not private (e.g., free internet connection at a coffee shop).
- **Vulnerability**: A weakness in software or hardware. When a vulnerability is discovered, manufacturer should release a patch or fix to eliminate the vulnerability.

B. Implantable Medical Devices

Implantable Medical Devices (IMDs) apply continuous monitoring and automatic therapies to the treatment of chronic medical disorders [10]. For example, 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. IMDs' pervasiveness continues with upward of 25 million United States citizens currently reliant on them for life-critical functions [11]. In the United States, over 100,00 patients a year receive implantable cardioverter defibrillators (ICDs), which detect dangerous heart rhythms and administer electric shocks to restore normal activity [10]. Some current-generation devices now have the ability to communicate wirelessly with external equipment from distances up to five meters away [12]. In fact, the latest IMDs is able to support remote monitoring over long-range, high-bandwidth wireless links, and emerging devices will communicate with other inter-operating IMDs.

Despite these advances in IMD technologies, they still can occasionally malfunction. Additionally, they are still behind in security and privacy. Many information technology professionals are still lacking in the understanding of how device security and privacy interact with and affect medical safety and treatment efficacy. Cybersecurity protection of these devices are not just a technical issue according to [2]. The foundational study of these devices demonstrated the vulnerability is detrimental to their safe operation, and the availability, confidentiality, and integrity ot the associated data. IMDs poses the challenge of having a balance of security and accessibility for medical professionals.

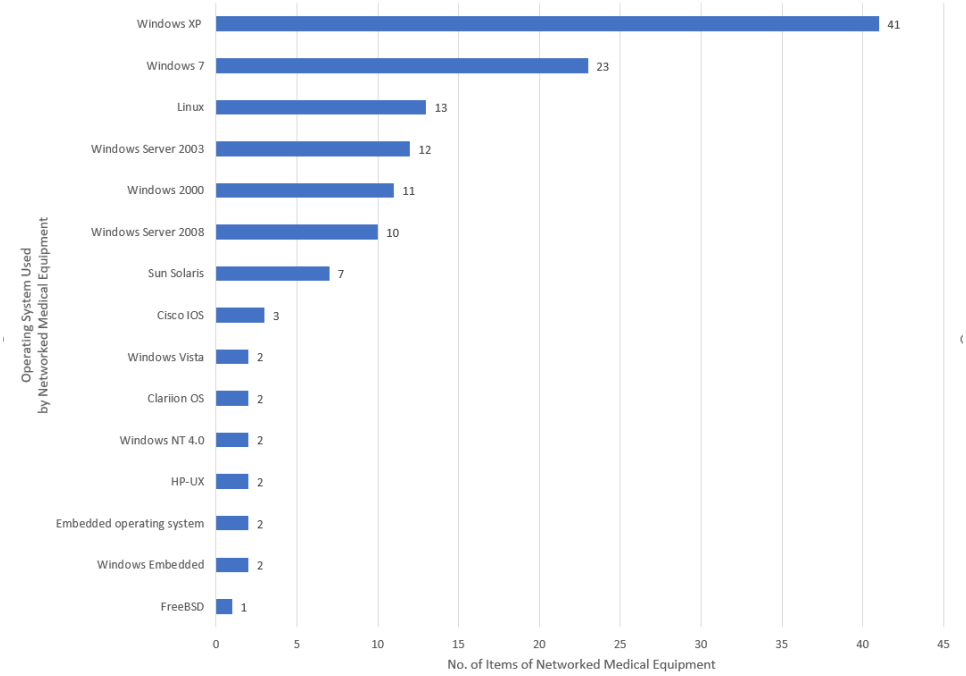

Fig. 1. The distribution of Operating System running on networked medical equipment in the radiology department [4].

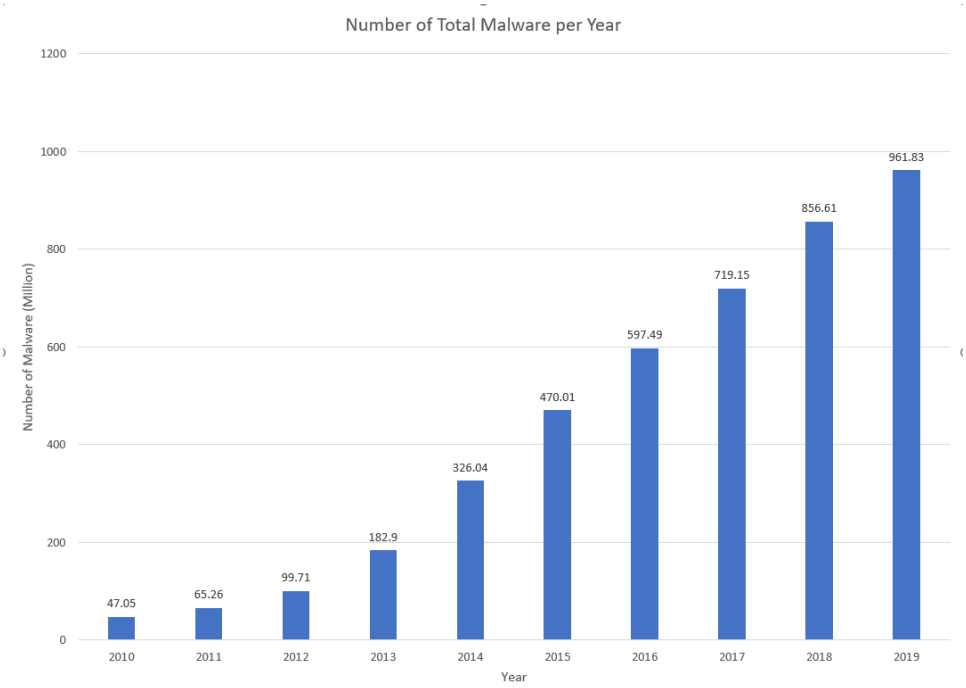

Fig. 2. A graph of total number of Malware per year, based on data from AV-TEST [13].

III. Cybersecurity in Radiology Department

Healthcare today increasingly depends on computers, networking, and information system. Due to the need of digital healthcare, most diagnostic imaging systems are connected to the Internet/LAN (Local Area Network) [14]. Furthermore, this connectivity enables computer enhanced medical imaging capabilities, that allows for early discovery of diseases, research new diseases, and better treatment of medical condition. The radiology department specifically, have seen a more proliferation of networked equipment in the past decades. They also have the highest density of networked medical equipment. Many manufacturers focus solely on innovation and functionality but little effort was put on the network security of this equipment. Also, digital storage and transmission of images across the hospital network using PACS have become a well-established norm in most large radiology departments [4]. With the increase of connectivity imaging devices, the issue of cybersecurity is now involves more than just the security and integrity of patient data and machine operation. In current clinical environment, a breach of security on one computer can bring down the entire hospital's network, compromising patient care and putting patients at risk of harm, threatening their confidentiality, safety, and well-being [8]. The number of medical imaging devices has increased tremendously in the United States since their introduction

A. Types of Vulnerability

B. Security Challenges

The medical industry face many challenges

IV. Conclusion And Future Work

Many researcher try to make a secure systems for the healthcare industry. For example, [15] made a threat modeling and mitigation of medical cyber physical systems.

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] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: how safe are we?" *Bmj*, vol. 358, p. j3179, 2017.

[7] S. Murphy, "Is cybersecurity possible in healthcare," *National Cybersecurity Institute Journal*, vol. 1, no. 3, pp. 49–63, 2015.

[8] A. Ferrara, "Cybersecurity in medical imaging," *Radiologic technology*, vol. 90, no. 6, pp. 563–575, 2019.

[9] M. Busdicker and P. Upendra, "The role of healthcare technology management in facilitating medical device cybersecurity," *Biomedical instrumentation & technology*, vol. 51, no. s6, pp. 19–25, 2017.

[10] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (h2h): authentication for implanted medical devices," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 1099–1112. [Online]. Available: http://doi.acm.org/10.1145/2508859.2516658

[11] 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.

[12] 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.

[13] AV-TEST, "Malware statistics and trends report," 2019. [Online]. Available: https://www.av-test.org/en/statistics/malware/

[14] P. Ma, Z. Wang, X. Zou, J. Zhang, Q. Liu, X. Lyu, and W. Wang, "Medical imaging device security: An exploratory study," *arXiv preprint arXiv:1904.00224*, 2019.

[15] H. Almohri, L. Cheng, D. D. Yao, and H. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in *Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies*, ser. CHASE '17. Piscataway, NJ, USA: IEEE Press, 2017, pp. 114–119. [Online]. Available: https://doi.org/10.1109/CHASE.2017.69