# 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 cyberthreat 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. The interconnected technology introduces new cybersecurity 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 cybersecurity 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 1 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].

| Type of Threat | Description |
|---|---|
| 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 1 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.

## 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. Additionally, this improvement enables doctors extracting meaningful information from patients' digital records. It would permit doctors to detect and then treat a disease at its earliest stages. Increasing the quality of medical services [15]. Further, the radiology department have seen a more proliferation of networked equipment in the past decades. They also have the highest density of networked medical equipment. However, many manufacturers focus solely on innovation and functionality but little effort was put on the network security of this equipment. For example, radiologist uses a system called Picture Archiving and Communication System or Radiography Information System (PAC/RIS) [8]. It is a technology that provides doctors with economical storage and convenient access to image from multiple source machine types. PACS receive images from medical imaging devices through an acquisition gateway. From the acquisition gateway, the images is moved to the database system, where they are archived. This eliminates the need to manually file, retrieve, or transport film jackets, the folders used to store and protect X-Ray film. With the development of PACS/RIS, traditional diagnostic imaging system have been replaced to computer assisted ones. Further, the universal format for PACS is Digital Imaging and Communications in Medicine or DICOM [16]. DICOM is an international standard to transmit, store, retrieve, print, process, and display medical imaging information. This digital storage and transmission of images across the hospital network using PACS technology have become a well-established norm in most large radiology departments [4]. With this 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.

There is a common term used in medical device cybersecurity that is called CIA (or CIA triad), which stands for the categories confidentiality, integrity, an availability. Confidentiality refers to protecting patients' information and ensuring that data are always available to people with legitimate needs. Integrity means preventing malware from altering patients' medical information. Availability means the data, the device, the network, and the operations software are always accessible and available [17]. However, with all of these advancement of technology, 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]. Something have to be done to eliminate this security issue.

### A. Diagnostic Imaging System

Diagnostic imaging (DI) system is a technique that creates visual representation of the interior of a body for clinical analysis and medical intervention – for example magnetic resonance imaging (MRI), X-Ray, ultrasound, computed tomography (CT), and positron emission tomography (PET) [16]. Almost all of these devices uses PACS to store the data information and DICOM to transmit the data across the networked devices. All of these connection between the different diagnostic imaging system makes them more vulnerable to networked related cyberthreats. DI systems are used extensively all the time, and for various reasons such as supporting life-saving treatments. These devices are a critical resources because of the expensive cost to maintain one, thus, very few of them are held by hospitals. Therefore, failure of one device may sabotage entire hospital's operation [17]. This fact added with several motivations for malicious hackers to target medical imaging devices, can have a disastrous consequences that may cost millions of dollar to recover from.

TABLE II
Top 10 Countries with Open DICOM Servers [18].

| Absolute No. of Open DICOM Servers | | |
|---|---|---|
| **Rating** | **Country** | **No. Of Servers** |
| 1 | United States | 346 |
| 2 | Brazil | 51 |
| 3 | Turkey | 49 |
| 4 | Iran | 34 |
| 5 | India | 28 |
| 6 | South Korea | 15 |
| 7 | Taiwan | 14 |
| 8 | Mexico | 14 |
| 9 | Canada | 13 |
| 10 | Australia | 12 |

### B. Vulnerabilities Found in the Radiology Department

A recent worldwide security sweep of DICOM servers found more than 2700 networks that were not secured. A research was conducted by McAfee to find vulnerability on DICOM and PACS used by medical facilities of all sizes [19]. As mentioned above, PACS operates on acquisition gateway to receive images. This acquisition gateways usually are placed in the facility's computer network instead of being insulated from it. Although it is done to increase efficiency, this leaves the gateway vulnerable to attacks and potentially compromises patient confidentiality. PACS price ranges from free (open-source PACS)to exceedingly expensive. Many smaller facilities favor more towards free PACS to cut expenditure. The problem with free open-source PACS is that it runs on old software platform that contains multiple vulnerabilities. Many of these PACS system are based on Windows XP, even though Microsoft announced the end of support for Windows XP in 2014 [14]. Furthermore, the researchers found 1100 unprotected PACS servers that directly connected to the internet around the world. They also were able to obtain the server name and version number the PACS was built on.

The fundamental standards running contemporary digital medicine, DICOM, were conceived and developed in the late

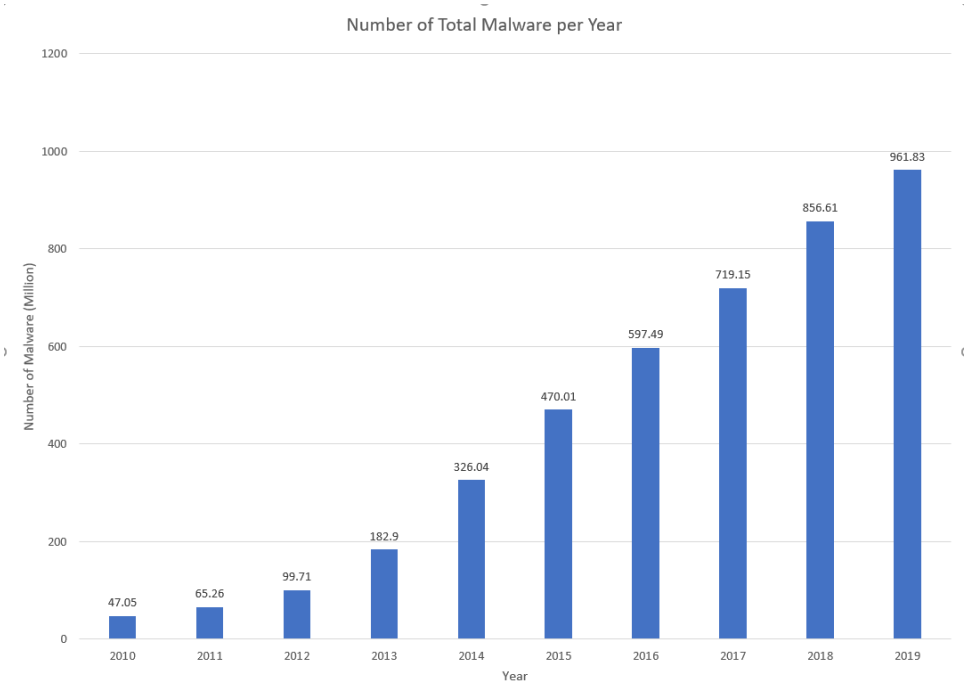


Fig. 1. A graph of total number of Malware per year, based on data from AV-TEST [13].

1980s. Despite being the standard for more than 20 years, the security part was nearly untouched. There was some later standard changes and legal reinforcements; However, the medical data security has never been soundly built into the clinical data or devices, and is still largely theoretical and does not exist in practice [8] [14] [18]. Furthermore, many researcher did a vulnerability scanning on the DICOM server worldwide. Table II shows the finding of Nmap scan result. Unfortunately, the country with the most prevalent DICOM rating also tend to lead in the most unsecured DICOM rating. In the United States, there is 346 number of servers that is open with no protection. This fact implies that patients in the United States have the highest risk of having their medical records stolen or compromised [18]. Then, Figure 2 gives a distribution of the heterogeneous composition of operating systems running on the radiology network. Most of the equipment used Microsoft Windows, and the next largest subnet running Unix or Linux. Among the equipment running on Windows, a significant portion ran Windows XP with Service Pack 2; Service Pack 3 and the security updates released subsequently had not been installed on these machines. The other equipment running different version of Windows is not been updated with the latest service pack or security update [4]. Additionally, another researcher, McAfee, discovered thousands of data available for download, many of them containing protected health information such as patients' names, ages, weight, facility, and city where the imaging study was done. They combined PACS and DICOM vulnerabilities to create a fictitious patient record, complete with a knee radiograph. They later penetrated the server again and changed all references in the record from the knee to elbow. The change was successful and saved in the fictitious patient's record [8]. In the end, this research was done with the intention to help. The McAfee researchers notifies all the vendors whose vulnerabilities they exploited from their finding and are working together to overcome these deficiencies [19]. On a side note, another big vulnerability of medical imaging devices is the reliance on portable storage media, such as universal serial bus, or USB, drives. Patients and care providers often bringing imaging scan results to the health delivery organization on portable media, which are not secure and can easily be infected with malware [8].

### C. Effort to Improve Cyberecurity

Many researcher and information technology professionals try to make a secure systems for the healthcare industry. For example, [20] made a threat modeling and mitigation of medical cyber physical systems. In December 2016, the FDA published nonbinding recommendations. the draft guidance intentionally does not prescribe any particular approach or technology but instead recommends that manufacturers to consider cybersecurity at the early phase of development of the medical device. The FDA recommends that manufacturers provide [21]:

- A specific list of all cybersecurity risk that were considered in the design process of a device.
- A specific list and justification for all cybersecurity controls.
- A traceability matrix that links actual cybersecurity risk.
- The systematic plan for providing validated updates and patches to operating systems or medical device software.
- Appropriate documentation to demonstrate that the device will be provided to purchasers and users free of malware.
- Device instructions for use and product specifications related to recommended antivirus software and/or firewall.

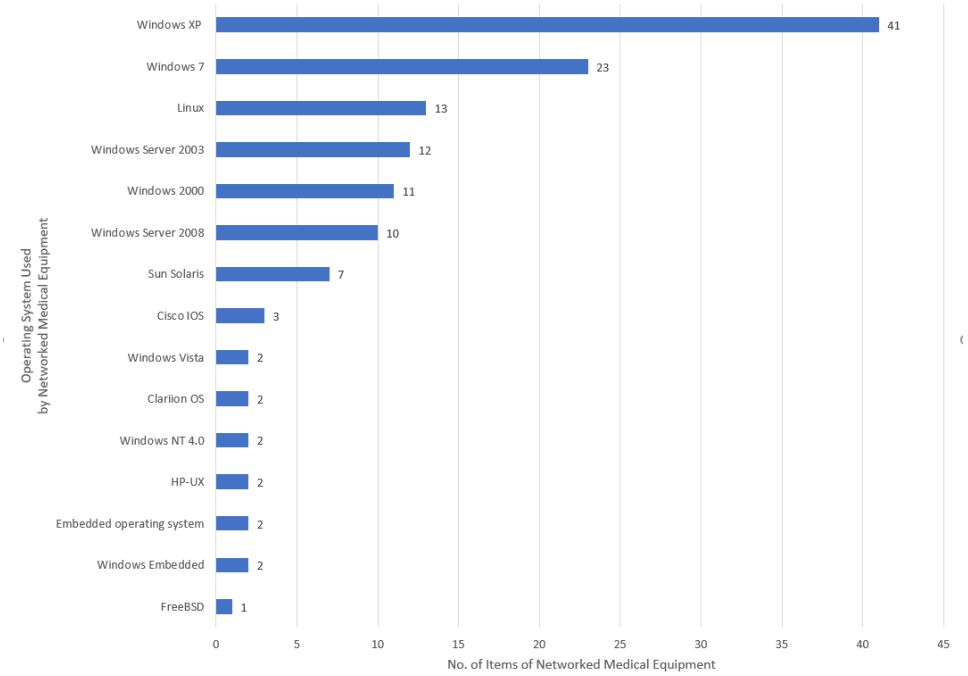


Fig. 2. The distribution of Operating System running on networked medical equipment in the radiology department [4].

Although the FDA acknowledges the need to consider cybersecurity throughout the life cycle of a medical device, these guidance documents are not enforceable by law. This recommendation to manufacturers is not enough to keep the radiology department cybersafe. Cybersecurity training should be mandatory for all employees of a health delivery organization, regardless of their role in the organization [8]. Lastly, there should be a matching between the lifecycles of underlying software to the production lifecycles of the medical device. For example, if a component is known to have a limited lifetime, then the medical devices using that component run the risk of inheriting the limited lifetime [21].

## IV. Conclusion

Modern healthcare delivery is depended on medical device software to help patients lead more normal and healthy life. The cybersecurity issue with medical devices is real, but the focus on solving the issue is still lags behind. As a consequence, many medical devices is highly vulnerable at a time when it is increasingly becoming a high value target for malicious hackers. Furthermore, network breaches and vulnerability findings should be the driving force to increase the protection of medical devices. Patients should not worry about their medical records being compromised. Health professionals should be trained regularly about the importance of cybersecurity.

In summary, the technological shift in medical device manufacturers and health delivery organizations is required to better deter and prevent cyber attacks on medical devices. More collaboration between the two is needed to established a foundation where many medical devices can operation without being compromised and enables efficient, high-quality patient care.

## 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] M. Marwan, A. Kartit, and H. Ouahmane, "Design a secure framework for cloud-based medical image storage," pp. 7:1–7:6, 2017. [Online]. Available: http://doi.acm.org/10.1145/3090354.3090361

[16] Z. Wang, P. Ma, Y. Chi, and J. Zhang, "Medical devices are at risk: Information security on diagnostic imaging system," pp. 2309–2311, 2018. [Online]. Available: http://doi.acm.org/10.1145/3243734.3278513

[17] T. Mahler, N. Nissim, E. Shalom, I. Goldenberg, G. Hassman, A. Makori, I. Kochav, Y. Elovici, and Y. Shahar, "Know your enemy: Characteristics of cyber-attacks on medical imaging devices," *arXiv preprint arXiv:1801.05583*, 2018.

[18] M. Stites and O. S. Pianykh, "How secure is your radiology department? mapping digital radiology adoption and security worldwide," *American Journal of Roentgenology*, vol. 206, no. 4, pp. 797–804, 2016.

[19] C. Beek, "Mcafee researchers find poor security exposes medical data to cybercriminals," Mar. 2018. [Online]. Available: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-researchers-find-poor-security-exposes-medical-data-to-cybercriminals/

[20] 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

[21] K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," *Biomedical instrumentation & technology*, vol. 48, no. s1, pp. 38–41, 2014.