A Cost-Effective Framework: Implementing Cybersecurity Practices for Biomedical Engineering Departments

Kamran Samanian[1], Qwynn Ferreira[1] and Adeel Alam[1]

[1] Sinai Health/Department of Biomedical Engineering, Toronto, Canada

Abstract— **An introduction to a step-by-step playbook for medical device security is presented through this paper. The research is on-going, however, this paper will introduce simple and cost-effective practices that users of biomedical engineering departments can implement to help mitigate the potential threats to medical devices. Utilizing the information provided in this paper, biomedical engineering departments will begin their journey in evaluating the potential threats of cybersecurity attacks on medical devices and implementing risk-based security practices.**

Keywords— **Biomedical Engineering Department, Medical Devices, Cost-Effective, Risks, Cybersecurity, Playbook**

I. Introduction

With the rapid advancement of medical technology comes new risks and unexplored areas for biomedical engineering departments to investigate. However, many departments are unaware of the potential cybersecurity threats associated with the increased complexity of medical devices. To better understand and mitigate these risks, biomedical engineering departments need to establish a cybersecurity protocol for inspecting and managing medical devices connected to the network.

As the complexity of cybersecurity threats continues to grow, it becomes increasingly important for biomedical departments to have measures in place to detect, manage, and protect patient information and medical device integrity. Unfortunately, many biomedical engineering departments tend to focus solely on the physical hardware of medical devices, neglecting the IT infrastructure that supports them, which can lead to a higher risk of cybersecurity breaches. To address this issue, biomedical engineering departments must bridge the gap between IT and biomedical engineering by creating policies and procedures to manage cybersecurity threats and improve their understanding of IT infrastructure. This will help to ensure the safety and security of both patients and medical devices. However, different challenges present themselves in cybersecurity for biomedical engineering departments.

When reviewing the topic of cybersecurity, it is a word used quite often, but with little depth behind what it really means and who really understands it. Biomedical departments today work with medical devices regularly, yet, most often than not, do not understand the concept of protecting medical devices from threats. When looking at the education of biomedical engineering technologists, they have a great understanding of electronic repair, preventive maintenance, and medical device management systems. However, concepts such as networking and IT infrastructure are introduced at a basic level in biomedical engineering technologist's education. Conversely, their IT technician counterparts have a deeper understanding of the hospital infrastructure and networking. The IT department's education encompasses network and server understanding, data security, operating systems and programming, and cloud computing which enables the IT departments to detect, protect, and prevent cybersecurity threats and vulnerabilities.

When searching for a software or tool that can protect a medical device from cybersecurity threats, it becomes clear that there is no one program that fits all. Thus, finding the right software is challenging due to the complexity of these devices, which have diverse operating systems, hardening tactics, and proprietary software. This complexity creates difficulties in choosing an appropriate cybersecurity software that meets the needs of biomedical engineering departments.

Biomedical engineering departments in healthcare face a major challenge in obtaining funding due to competition for funding sources, high cost of medical devices and economic factors. The challenge becomes even greater when it comes to purchasing medical technology such as cybersecurity programs, as they typically fall under IT. This process requires IT involvement as biomedical engineering staff have limited knowledge of IT concepts. Furthermore, the justification process for a cybersecurity software is intensive and requires consideration of factors such as cost, access, types of the medical device being scanned, and potential impact on the device. Having an understanding of these variables shows the difficulty in obtaining funding.

This paper considers roadblocks such as the elementary cybersecurity education of a biomedical engineering department, the broad variety of technologies available and the limited funding available for biomedical engineering departments. This paper will help to introduce practices that biomedical engineering departments can take to start their cybersecurity journey within their institutions, despite the challenges mentioned previously.

II. Methodology

The makeup of the playbook was an exercise that asked, “What is the best way a group of biomedical engineering technologists can implement and manage cybersecurity for medical devices?”

A. Training

Naturally, the first step was buy-in and increasing the cybersecurity appetite within the department. Thus, training was the first significant component and will continue to be an ongoing component in the department. We approached a cybersecurity professional to provide an overview of medical devices in the cybersecurity field and used resources from AAMI [1], NIST [2], MITRE [3] and the Canadian Center for Cybersecurity [4]. These resources helped generate the rest of the playbook.

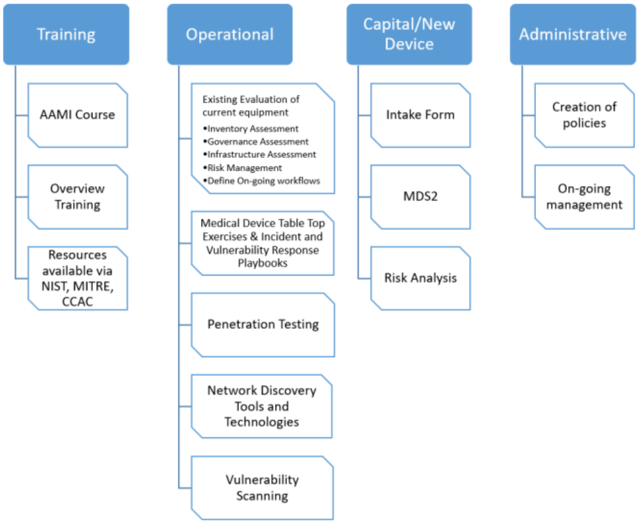

Training
AAMI Course
Overview Training
Resources available via NIST, MITRE, CCAC
Operational
Existing Evaluation of current equipment
•Inventory Assessment
•Governance Assessment
•Infrastructure Assessment
•Risk Management
•Define On-going workflows
Medical Device Table Top Exercises & Incident and Vulnerability Response Playbooks
Penetration Testing
Network Discovery Tools and Technologies
Vulnerability Scanning
Capital/New Device
Intake Form
MDS2
Risk Analysis
Administrative
Creation of policies
On-going management

Figure 1: Playbook Overview

B. Operational

The next step was looking at our operations and how we intend to manage this ever-growing risk. We needed to define the risk explicitly and learn more about our existing devices. We broke this into three categories: 1) Inventory assessment, 2) Governance Assessment and 3) Infrastructure Assessment. Once completed, these outputs all fed into our fourth category: Risk Management. The main output for this was how we are going to manage the risk (accept it, transfer it, avoid it, or mitigate it). This exercise will be completed for all of our medical device systems. The remaining portion of our operations looks at newer initiatives we are still working on defining. These include playbooks that explicitly list tasks for key stakeholders during a medical device security incident. We are also exploring penetration testing to ensure that all of our implemented controls are effective. We are exploring additional software tools like network discovery (where tools can identify computers on a network) and vulnerability scanning (where a tool scans a network for vulnerabilities).

C. Capital

As we transitioned from operations, we looked at our processes for our capital stream. Looking at existing resources, we heavily focused on the manufacturer MDS2 form along with vulnerability scanning. Furthermore, we are in the midst of generating an intake document, which derives from IEC 80001-2-8_2016. Together, the three documents formed the basis of our risk strategy for incoming equipment.

D. Administrative

The three major sections would then influence the administrative policies we aim to develop. These policies include how the biomedical engineering department manages the risk of new equipment. The second aim of the policy would be to manage the ongoing operational work required to upkeep and manage the cyber risk for medical devices at Sinai Health.

III. Work Done So Far

A. Training

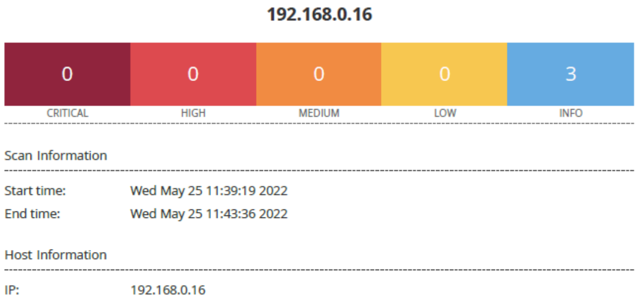
Our team contracted a cybersecurity expert from the Ministry of Ontario to provide an overview of the cybersecurity landscape and the real threat of medical devices getting attacked. The expert walked us through various use cases of cyber criminals' attacks to encrypt or destroy data, with the ultimate goal of soliciting payment via ransom. The expert spoke to us about the challenge with medical devices and how there have been real examples of medical devices getting hacked. This session intended to provide the biomedical engineering team with an appreciation of the threat at hand.

The biomedical engineering team members also attended the SecTor conference that occurs annually in October. The conference is a great opportunity to collaborate with mature and seasoned cybersecurity professionals and vendors. This information-gathering session gave our team a small glimpse into the intricacies and complexities of the cybersecurity space. Yet, it provided us with homework on the types of tools and technologies we need to look into as we mature our medical device cybersecurity program at Sinai Health.

In the future, we will continue to utilize conferences, vendor demos and sessions to increase our knowledge. For a long-term plan, we may look at having a team member attend formal training via our knowledge partners to enhance our skill set.

B. Operational

Our team set up vulnerability scanning as one of our first tasks. This task was essential to understand what devices on our network may already be susceptible to outside threats. After a market analysis, vendors such as Rapid7 and Tenable had vulnerability scanning products available. However, as we were starting, we were considering the option of free trials. Typically, these paid products sit on the network and continuously scan all network traffic. We found a free product Nessus Essentials, by Tenable, where it was restricted to 16 IP addresses concurrently. This suited our needs as we aimed to do vulnerability scanning one by one. Thus, we purchased a standalone laptop and an 8-port switch and router, allowing us to form a mini-network where medical devices can be connected wirelessly or wired. We conducted scans on various medical devices and found no high-risk or critical vulnerabilities. Any results we found were shared with the device manufacturer and added to our risk registry. Figures 2 and 3 shows the result summaries of these scans. The results could also be drilled down further to each individual alert. This provided us more information to further understand the alert and any remediation suggestions.



192.168.0.16

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	3

Scan Information

Start time: Wed May 25 11:39:19 2022
End time: Wed May 25 11:43:36 2022

Host Information

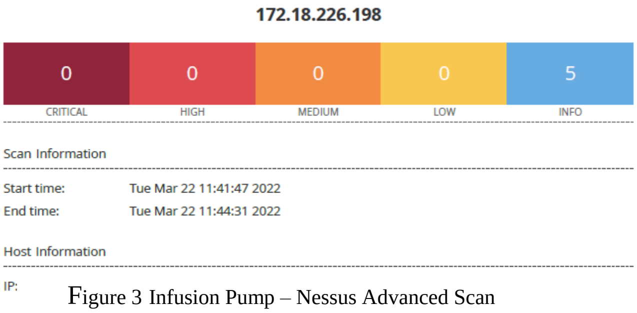
IP: 192.168.0.16

Figure 2 Vital Sign Monitor – Nessus Advanced Scan

Our next task was to go through the system-by-system evaluation. Our first system was our patient monitoring solution. The first task was to conduct an inventory analysis, ensuring all mac addresses, IP addresses, software revisions and locations were updated in our CMMS. We went through the additional step to gather all VLANs, switch port numbers and wall jack numbers.

We then reviewed the MDS2 of all products in our patient monitoring solution. This document, created by NEMA, "assists professionals responsible for security-risk assessment in the management of medical device security issues." [5]. This form provided the basis of how each component of the patient monitoring solution has been secured (or not secured) by the vendor. In going through this document, our team learned and evaluated different types of risks that our patient monitoring solution posed to our organization. These risks went into our risk register, which will be actioned at a later stage in our evaluation.

In going through the MDS2, a critical component is the patching strategy. Patches help to fix any security flaws or vulnerabilities that exist. Therefore, we established a patching strategy for our patient monitoring solution. The patching strategy considers two facets: 1) the windows OS updates which define and update security gaps that exist in a standard windows based OS, and 2) vendor-specific updates that address security gaps from the application perspective and add functionality. This strategy also considers multiple other factors:



172.18.226.198

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	5

Scan Information

Start time: Tue Mar 22 11:41:47 2022
End time: Tue Mar 22 11:44:31 2022

Host Information

IP:

Figure 3 Infusion Pump – Nessus Advanced Scan

1. The underlying architecture of our patient monitoring solution,
2. Our hardening measures and
3. Our appetite in accepting risk.

At this point, we had completed our inventory assessment and were now moving on to our governance assessment. One item under this bucket was access management. Here, we looked at how the patient monitoring solution can be accessed. We broke this down into three different categories:

1. *Physical Access*: refers to open access to any of our hardware systems deployed in the clinical space. We looked at locked cages for our PCs, different

types of USBs active on those PCs and how threat actors could potentially access them. These fed into our risk evaluation exercises, where we defined the potential risks.

2. *Location Access*: refers to access to sensitive locations. This includes Main Computer Rooms, network closets and specific departments.

3. *Login Access*: refers to known user logins, password and active directory accounts created for specific purposes.

Through this exercise, we discovered we had several "unknown" access accounts created over the years without knowledge of what they were created for and who has access to them. As such, we were able to disable those accounts. Furthermore, we also discovered several unknown individuals who had access to some of our sensitive areas. Again we were able to disable their access as well.

IV. Next Steps

In our cybersecurity journey, we will continue our governance and infrastructure management. The outcome of these exercises will flow into our risk registry. Our last step will be to concurrently evaluate all our risks and how each risk impacts the confidentiality, integrity and availability (CIA Triad) of the patient monitoring system and employ a known risk management technique.

The above steps will be repeated for all of our medical device systems that we support, such as defibrillators, infusion pumps, and other medical devices. Our longer-term goal is to procure software that manages, discovers and assesses medical device risk in real-time.

V. Conclusions

This paper provides guidance for biomedical engineering departments who are looking for a simple and cost-effective means in implementing a cybersecurity program. Our hope is that biomedical engineering departments across the country and elsewhere, can use this paper to start and build their medical device cybersecurity programs. This is an existential threat and there is no doubt that biomedical departments have to be the leaders in this space.

Acknowledgment

We would like to thank the department of Information Services and our CIO in allowing us the opportunity to take the lead on such an important initiative.

Conflict of Interest

The authors declare that they have no conflict of interest.

References

1. Association for the Advancement of Medical Instrumentation, *HTM Cybersecurity Resources Page,* Arlington, VA. Available: https://www.aami.org/HTM/htm-cybersecurity-page [Accessed: September 2022]
2. National Institute of Standards and Technology, *Cybersecurity Framework*, Gaithersburg, MD. Available: https://www.nist.gov/cyberframework [Accessed: September 2022]
3. Mitre, *Mitre Att&ck,* Available: https://attack.mitre.org/ [Accessed: September 2022]
4. Government of Canada, *Canadian Centre for Cyber Security,* Available: https://cyber.gc.ca/en [Accessed: October 2022]
5. American National Standards Institute, "Manufacturer Disclosure Statement for Medical Device Security," *National Electrical Manufacturers Association,* ANSI/NEMA HN 1-2019. [Online]. Available: https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security [Accessed: October.2022]