An Update on the Development of Cybersecurity Practices for Biomedical Engineering Departments

Adeel Alam[1]; Qwynn Ferreira[1]; Kamran Samanian[1]

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

Abstract— **Through the medical device framework, Sinai Health Biomedical Engineering team provides an update on the work they have done the previous year and provide an example of how this work has proactively reconciled a vulnerability in our medical device environment.**

Keywords— **Cybersecurity, framework, vulnerabilities, medical devices**

I. Introduction

At CMBEC45 in Vancouver, the Sinai Health Biomedical Engineering (BME) team introduced a framework (figure 1) on how biomedical engineering teams can start their cybersecurity journey in securing their medical devices. The framework was built on several assumptions:

1. This solution must be cognizant of the limited cybersecurity skillset that is available in biomedical engineering departments.
2. The framework must be cost-effective.
3. The framework must not heavily impact resources.

This paper provides a high-level update on the work the BME team has completed since CMBEC45.

II. Overview

A. Continuing the framework

The previous work ended off with a discussion on access management. This talks about how our patient monitoring system can be accessed by threat actors and how have we secured that.

Since then, we talked about change management for our patient monitoring solution. At first, we needed to define what a change refers to. Our group came up with the following specific events that refers to a change:

1. A software change: if a software upgrade/downgrade occurred
2. A configuration change: if a unit wanted to change their BP alarm limit
3. A hardware change: if the wireless adapter was upgrades on a module
4. A system level change: if the encryption standard was changed.
5. An access change: creating new credentials for accessing the system.

Our next step was to document these changes and disseminate this information to our team. To document, we created templates to ensure all the correct necessary information was captured and stored appropriately. We also needed to create a policy to define the work we are doing, which we are actively working on.

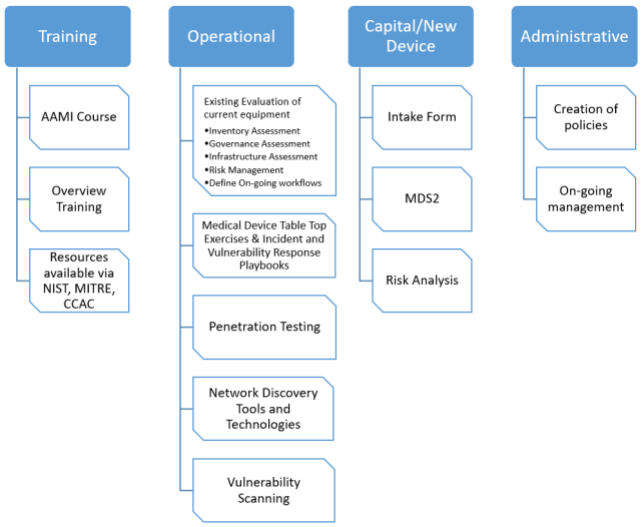

Figure 1: Cybersecurity Framework

B. Proactive Vulnerability Management

As part of our vulnerability management program, the team does bi-annual vulnerability scans. In a scan of an OR device, it came back with a high-risk vulnerability. The knowledge of this vulnerability triggered several actions:

1. Contact with the vendor: to inform them of the vulnerability and working with them to access what are some next steps we can take.

2. Contact with IT: to inform them of this flaw that exists.
3. Contact with the OR team: to inform them of any impact this vulnerability has to their workflow.

This led to several positive outcomes: a) the vendor was appreciative of our work and strengthened our relationship; b) the IT team further supported our work and helped us gain that credibility to show cybersecurity is a risk in the medical device space as well; and c) together, we were able to work collectively to mitigate any risk that this vulnerability posed.

C. Patch Management

The BME team also worked on its patch management strategy for the different medical device systems it supports. This strategy was based on several factors, 1) infrastructure: how the system is set up and the different nodes interact with each other and through what secure means; 2) resources: the cadence required for patching dependent on resources within the department and 3) method of patch retrieval: whether the biomed team has access to patches or whether they needed to be validated first. These factors helped to shape our patch management strategy.

D. Risk Register

Lastly, all the work mentioned previously started populating our risk register. The risk register's purpose is to have a consolidated document that outlines the medical device cybersecurity risks that our team has uncovered throughout our journey. It is then fed to the general cybersecurity risks in our organization and ultimately fed up to the enterprise risk. It is another active process we are engaged in to secure our medical devices.

III. Next Steps

Our next steps include continuing our framework and completing it for our patient monitoring solution. Then, as time permits, start our other systems in the hospital that the BME team supports (i.e. pumps, ECGs, defibrillators, etc.). We also will consider looking at a change advisory board (CAB) to monitor and approve any changes within our systems.

IV. Conclusion

Through the work the BME had done over the past year, we believe we are one step closer to the on-going battle of securing our medical devices. The intent is this knowledge transfer and the framework developed will assist biomed departments across the country to secure their medical devices; but also have secondary benefits; mainly related to gaining that credibility with the IT team on cybersecurity matters.

Conflict of Interest

The author declare that they have no conflict of interest.