Protecting Medical Devices & Systems from Cyber-attacks – Prevention is better than cure

Singapore Healthcare Management 2021

SingHealth
Defining Tomorrow's Medicine

Ma Guang Rui, OSS BME
Li Siying, OSS BME
Soh Wei Yan, OSS BME

INTRODUCTION

Internet of Medical Things (IoMT) is a connected infrastructure of medical devices and systems (MDS) that connects to electronic medical record systems via networking technology.

With the rise in the number of IoMT MDS in healthcare institutions, the sharing of patient medical records through cloud systems or local servers across healthcare institutions makes MDS a target for cyber-attacks. As such, it has become increasingly important to strengthen the security of such devices to prevent potential cyber-attacks that may put healthcare operations and patient lives at risk.

AIM

- Identify key areas concerning physical access control, where cybersecurity is lacking
- Set up proper guidelines for prevention of cyber-attacks on SingHealth MDS

METHODOLOGY

A gap analysis of current workflows were performed allowing us to identify the causes for potential cybersecurity breaches of MDS using the Fish Bone Diagram as shown in Figure 1.

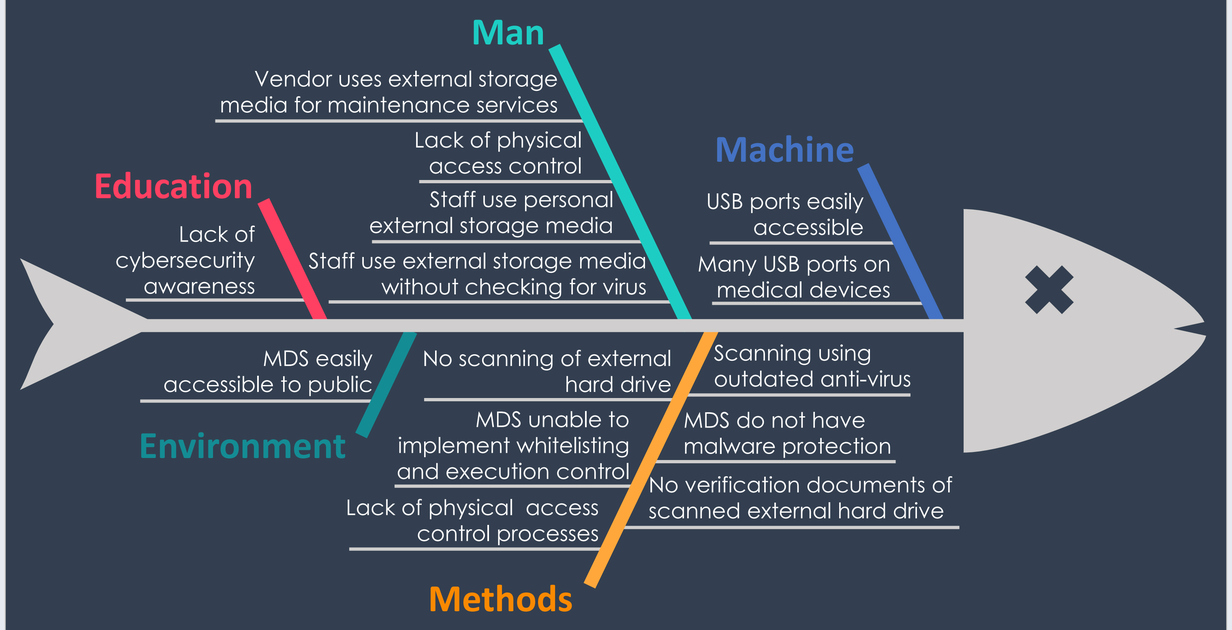

Figure 1: Fish Bone Diagram showing causes of potential cybersecurity breaches of MDS.

After determining the root causes, we performed a risk assessment, as shown in Table 1, on types of MDS in the clinical setting. We then calculated the overall risk, with reference to Table 2, to determine the priority of which we should implement our solution.

Threat Source	Equipment Type (example)	Severity	Likelihood	Overall Risk
• Internet capability, connected • Easily accessible	Physiologic Monitors	2	3	6
• Internet capability, connected • Not easily accessible	PACS connected medical systems	2	2	4
• Internet capability, Not connected • Easily accessible	Infusion pumps	3	2	6
• Internet capability, Not connected • Not easily accessible	EEG, EMG	1	1	1

Table 1: Risk Analysis of MDS vulnerability against cybersecurity breach

Severity \ Likelihood	Unlikely (1)	Likely (2)	Very Likely (3)
High (3)	3	6	9
Medium (2)	2	4	6
Low (1)	1	2	3

Table 2: Risk Assessment Table

- High Severity: Occurrence would lead to injury or loss of life
- Medium Severity: Occurrence would lead to misdiagnosis and/or mistreatment
- Low Severity: Occurrence would lead to loss of personally identifiable information

RESULT

Based on the Pareto Principle (Figure 2), we have identified that 80% of the risks of cyber-security breaches resulted from man and methods. By focusing on these two root causes, we determined that we would be able to effectively reduce the likelihood of cybersecurity breaches of MDS.

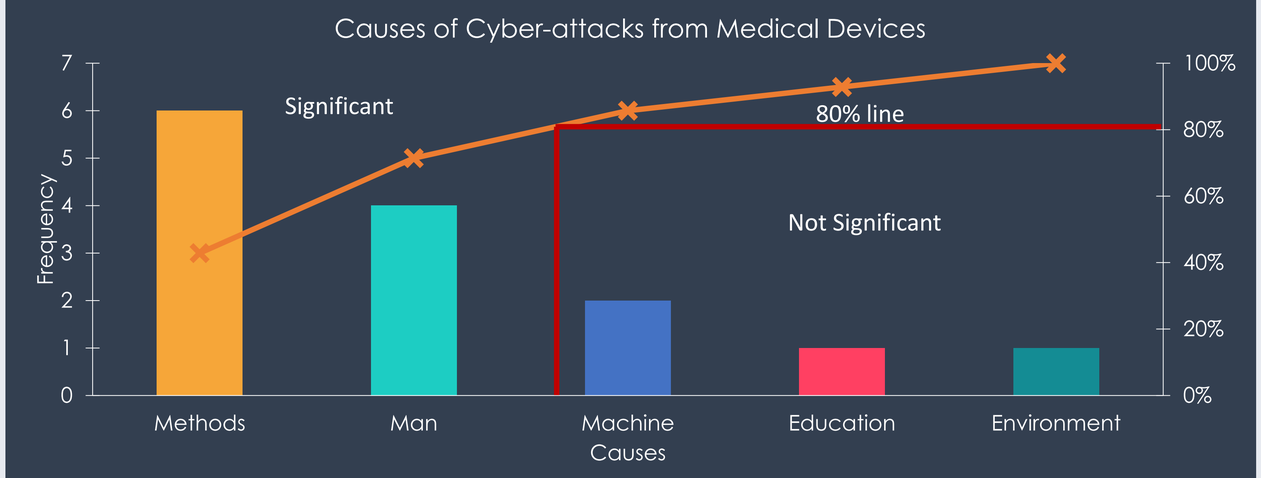

Figure 2: Pareto chart showing relative frequency of causes for potential cybersecurity breaches of MDS

We therefore implemented the following solutions at all SingHealth institutions:

1. Lockdown of all USB ports on MDS using USB port blockers
2. Policy of scanning all external storage media before use on MDS
3. Vendor self-declaration form for scanning of external storage media

Based on the overall risk calculated in Table 1, we prioritised network-connected MDS which were easily accessible during our USB port lockdown exercise. To date, we had locked down over 96% of MDS in all SingHealth institutions.

The policy of external storage media scanning was also shared across all SingHealth institutions on July 2020 along with the vendor self-declaration form that needs to be endorsed before use of external storage media on MDS.

Looking at the causal loop diagram in Figure 3, the reinforcing loops reflect that as the number of MDS in healthcare institutions increases, so does the risk of cybersecurity breaches. With the implementation of our solutions, a resulting positive change can be clearly seen in Figure 4, whereby the loops have become balanced. Thus reflecting an overall reduction of risk of cybersecurity breaches.

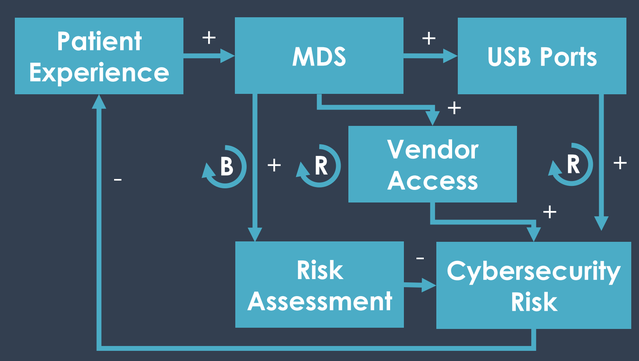

Figure 3: Causal Loop Diagram before implementation of solutions

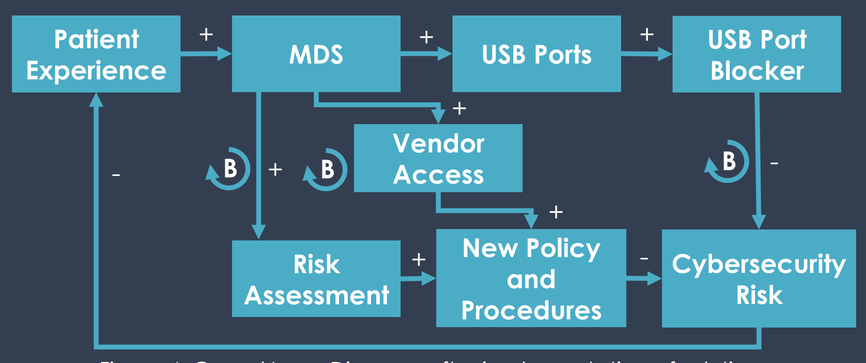

Figure 4: Causal Loop Diagram after implementation of solutions

CONCLUSION

As medical technology advances, we would expect a continual increase in the number of IoMT devices. With the implementation of USB port blockers and policy of scanning all external storage media throughout all SingHealth institutions, we had successfully achieved our goal of reducing the risk of cyber-attacks on MDS.

More importantly, with the introduction of the policy to staff, users, and vendors, we have also raised awareness on cybersecurity for MDS.