Singapore Healthcare Management 2023

EFFORTS TO MITIGATE RISKS IN Medical Devices and Systems (MDS) Security through People, Process and Technology

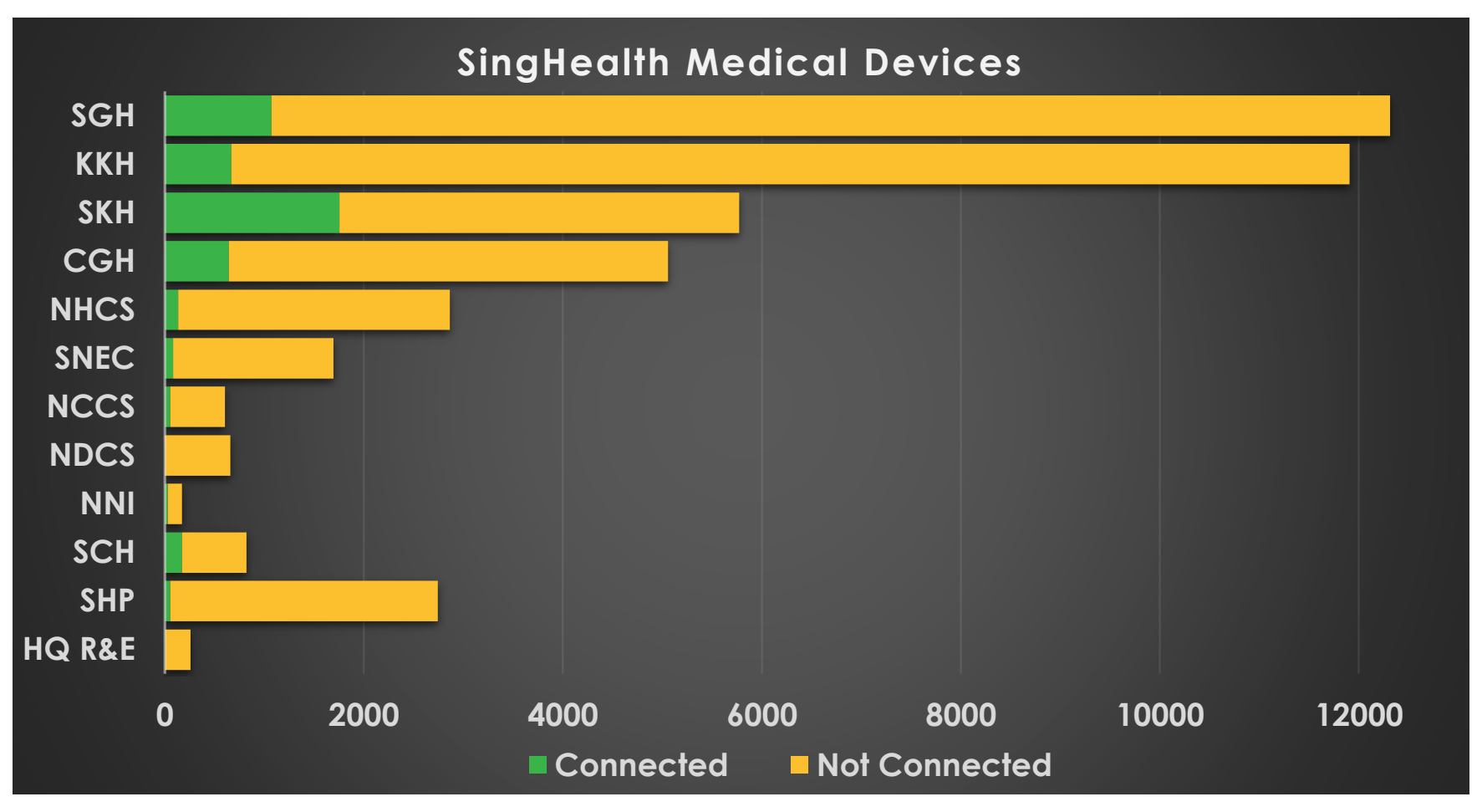
Singapore Health Services (SingHealth)
Billy Leung Zhen Kit, Medical Device Technology
Beatrice Eng Ai Lin, Medical Device Technology
Ma Guangrui, OSS Biomedical Engineering

SingHealth

INTRODUCTION

In November 2020, the **Medical Device Technology (MDT)** department, part of **Biomedical Engineering (BME)** Shared Services, was set up to provide oversight and management of Medical Devices & Systems (MDS). The team works closely with BME in identifying regulatory gaps and implemented security controls to improve the MDS security posture and achieve compliance to policies throughout its lifecycle.

As technology advances in the MDS field, cyber threats are evolving and becoming more sophisticated. SingHealth has over 48,000 MDS, of which approximately 5,000 are connected to the corporate network. In 2022, MDS cyber-related incidents were primarily a result of improper usage of USB devices.



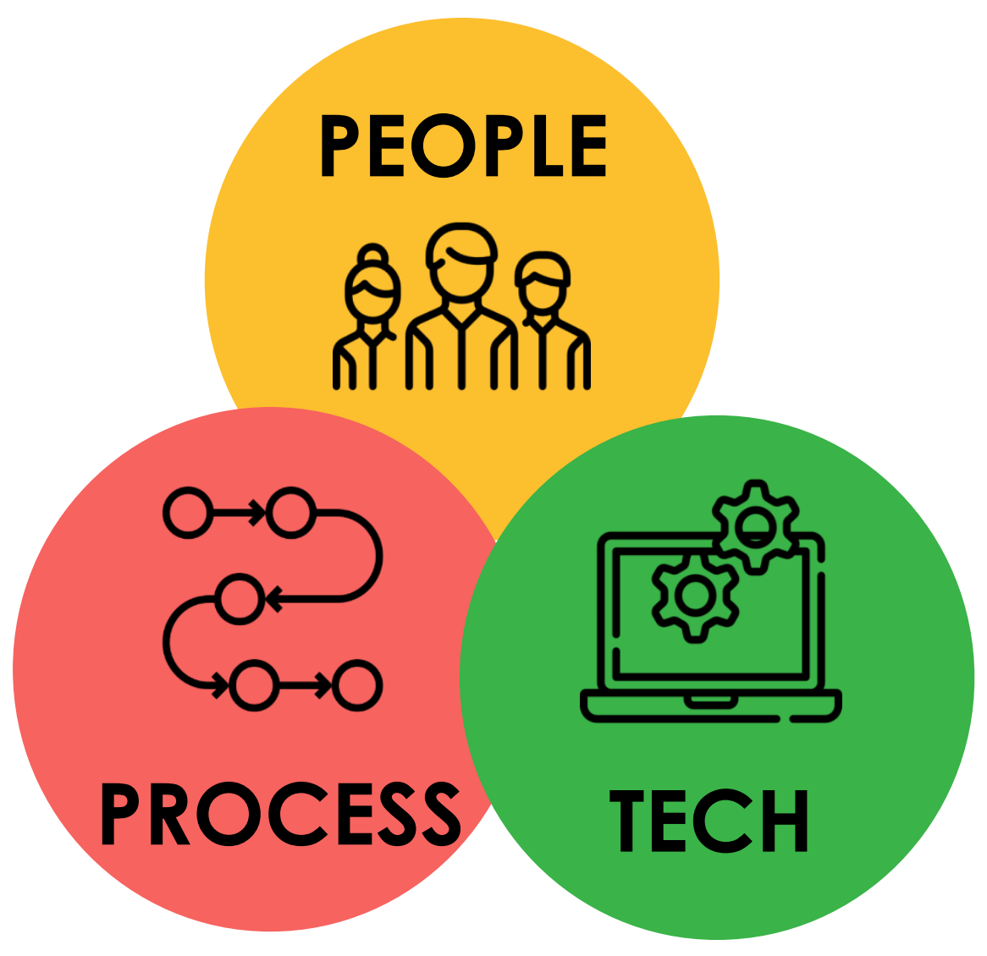
AIM

CREATE A MORE SECURE AND RESILIENT CULTURE

Better equipped against cyber threats, respond quickly and effectively to any MDS cybersecurity incidents.

METHODOLOGY

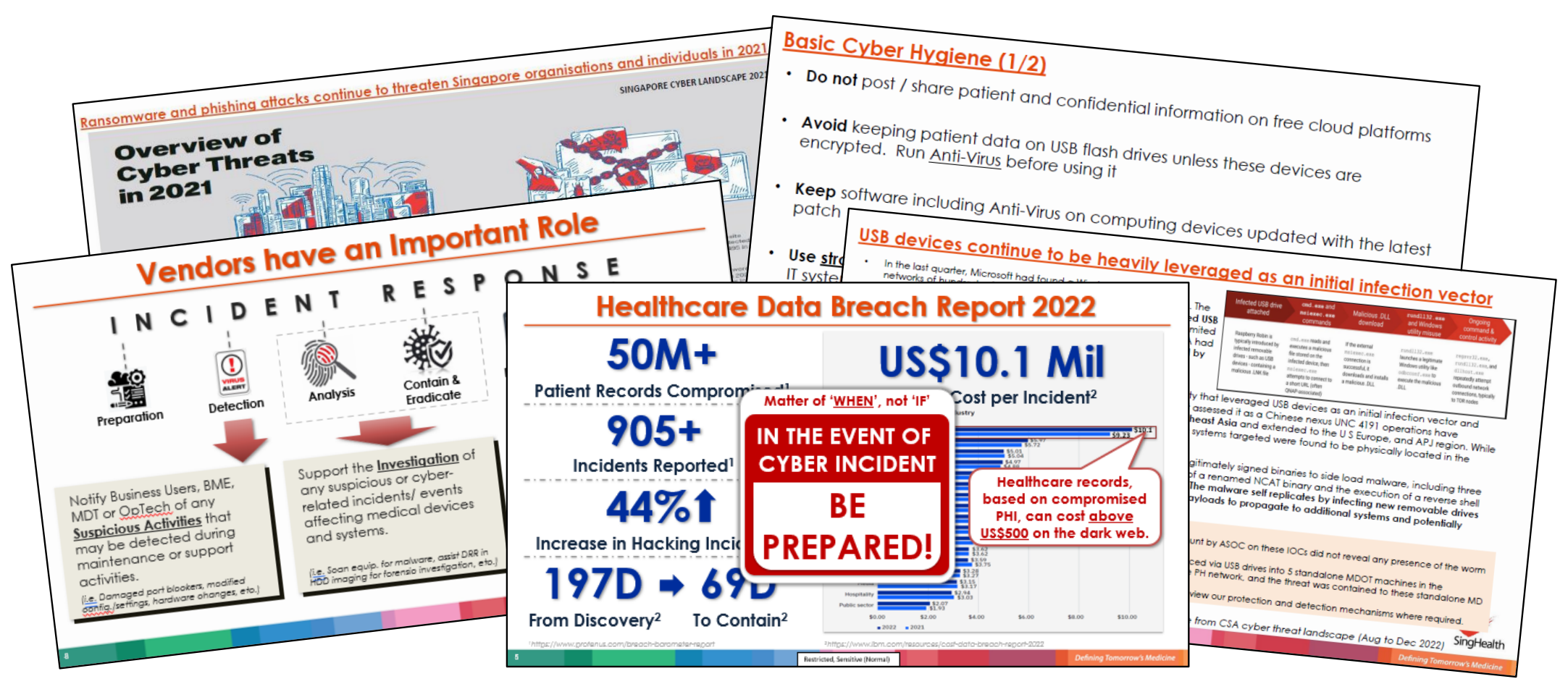
The **People, Process, Technology (PPT)** Framework was used to identify cybersecurity gaps, root causes of cybersecurity breaches to improve our ability to protect against cyber-threats and reduce the likelihood of cybersecurity breaches on MDS.



PPT Framework

PEOPLE refers to stakeholders with access to MDS, network, and data. Without the necessary training, knowledge, and awareness, even the most advanced security technology remains vulnerable.

- ✓ Regular briefings to stakeholders were conducted to emphasise the importance of safeguarding sensitive data, reporting cybersecurity incidents, and following established protocols. In 2022, over 350 medical device vendors as well as staffs across SingHealth institutions participated in our briefings.
- ✓ Having established MOU partnerships with local universities, cybersecurity trainings were part of our staffs' competency framework.
- ✓ Annual Table-Top Exercises conducted with key stakeholders.

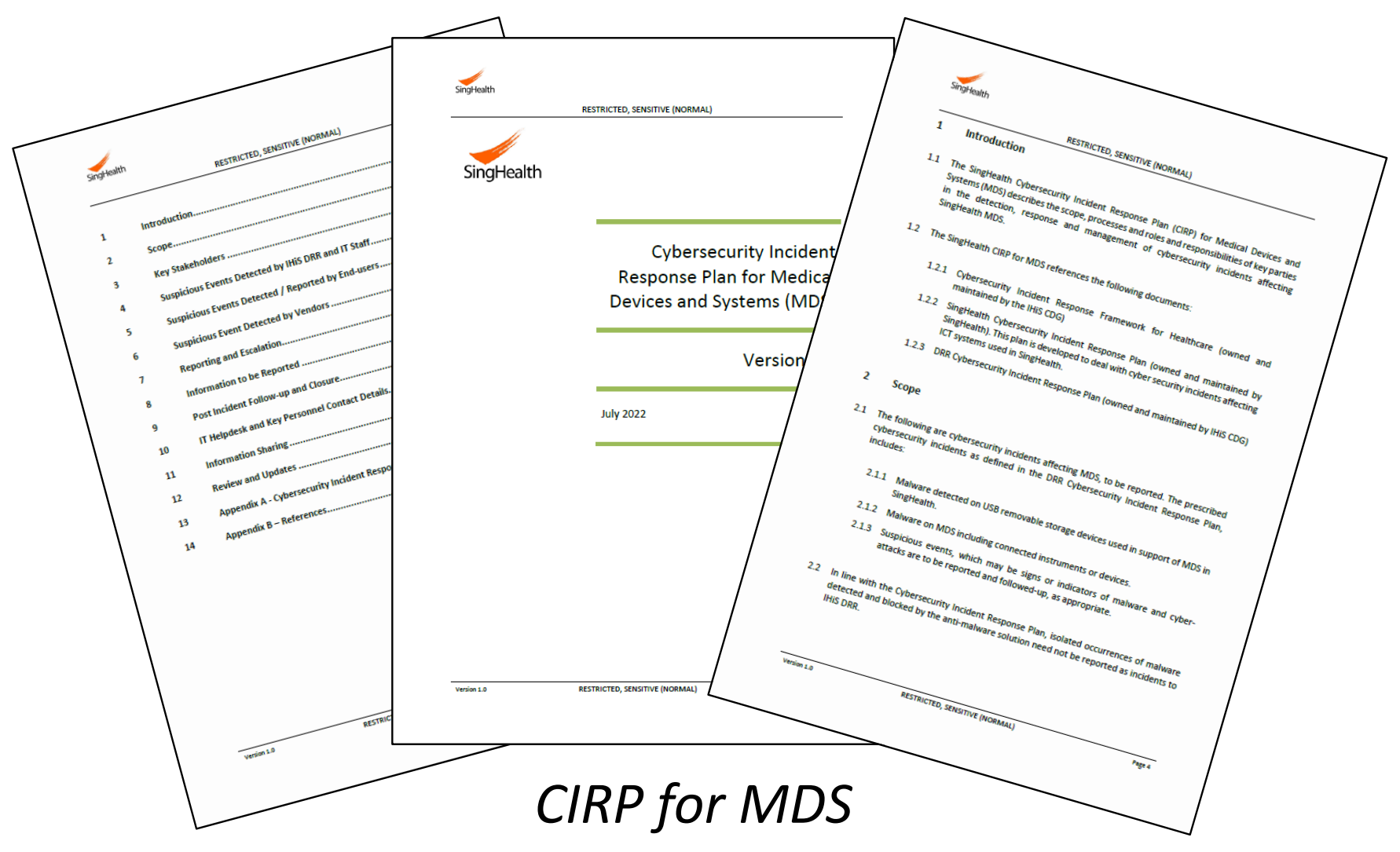

Overview of Cyber Threats in 2021
Vendors have an Important Role
INCIDENT RESPONSE
Basic Cyber Hygiene (1/2)
Healthcare Data Breach Report 2022
50M+
US$10.1 Mil
905+
44%
197D → 69D
IN THE EVENT OF CYBER INCIDENT
BE PREPARED!

Regular briefing for stakeholders

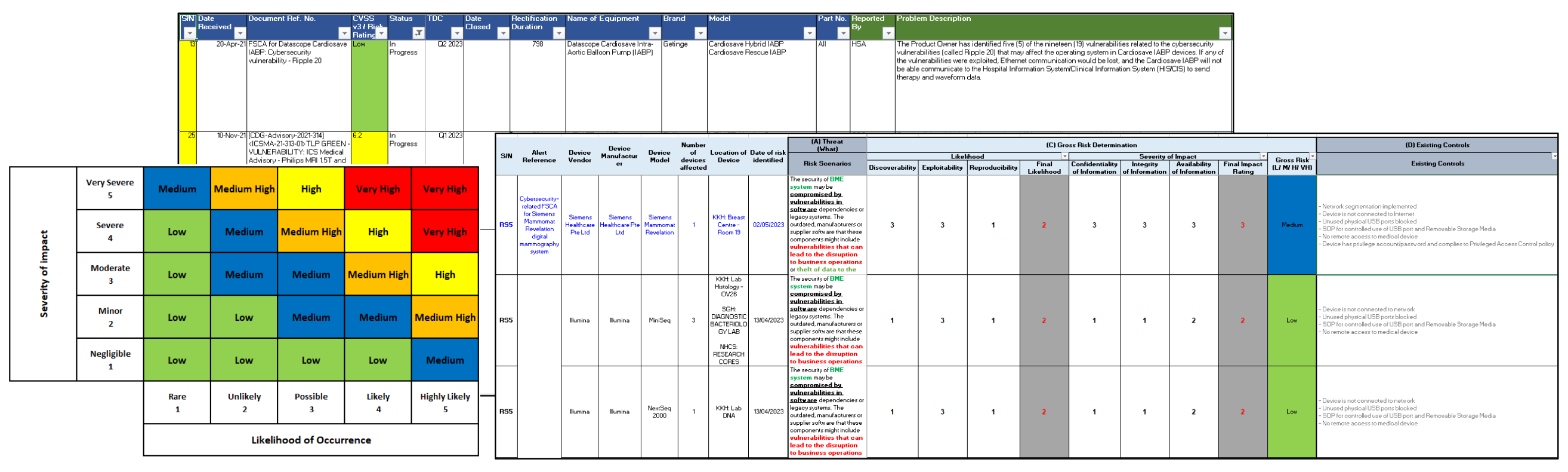
MOU partnership with NUS

PROCESS refers to governance of policies, procedures, and controls in place to manage and mitigate cybersecurity risks on MDS. New processes, vulnerabilities and weaknesses were identified and enhanced.

- ✓ Inception of Cybersecurity Incident Response Plan (CIRP) for MDS.
- ✓ Inception of cybersecurity vulnerability alerts management framework for MDS.
- ✓ Enhancing policies on the controlled use of portable storage media.
- ✓ Tightening of physical ports lockdown from USB ports to all interface ports (including SD card, CF card, LAN, RS232, etc.).


SingHealth
Cybersecurity Incident Response Plan for Medical Devices and Systems (MDS)

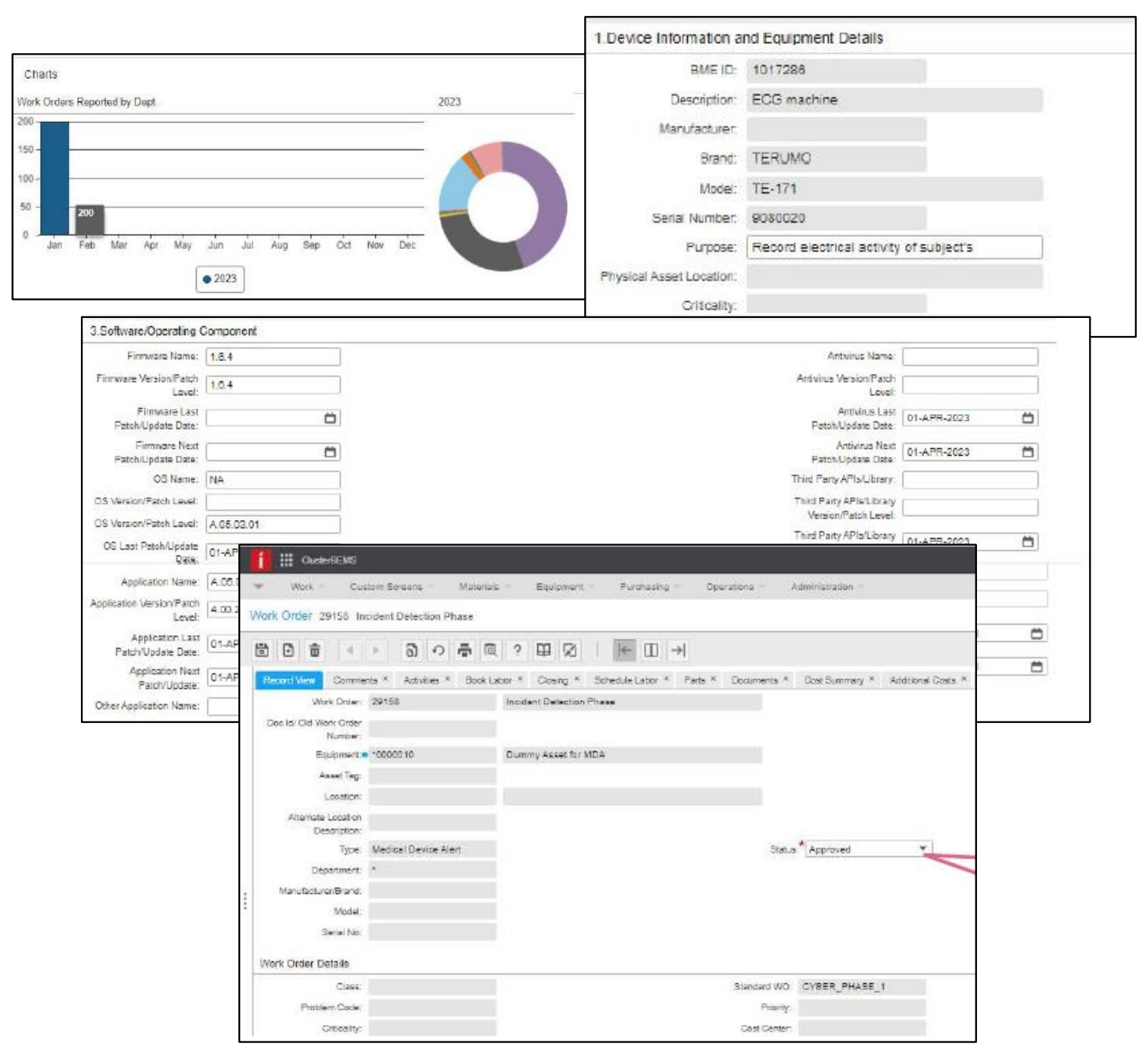
CIRP for MDS


Low
Medium
Medium High
High
Very High
Likelihood of Occurrence
Severity of Impact

Cybersecurity vulnerability alerts management for MDS

TECHNOLOGY refers to tools, systems, and software used, providing capabilities to protect, detect, and respond to potential threats in real-time, as well as aiding in investigation efforts. It provides a range of security controls to reduce cybersecurity risks.

- ✓ Implementation of Cluster Biomedical Equipment Management System (BEMS) for oversight and tracking of MDS in the event of a cybersecurity incident.
- ✓ Work-in-progress for an IoT/IoMT Monitoring Tool to discover vulnerabilities and risks of connected MDS.



Cluster BEMS for oversight and tracking of MDS

RESULTS

- ❖ Our staffs/stakeholders were better equipped to respond to cybersecurity incidents/threats related to MDS.
- ❖ Increased oversight of MDS discovered, adoption of cybersecurity controls in research, education, and clinical trial units.
- ❖ Since December 2020, 83 MDS vulnerability alerts were resolved, preventing 3013 devices from potential exploitation.
- ❖ Eliminated inefficiencies and human errors in manual maintenance of MDS via Cluster BEMS.

CONCLUSION

MDS cybersecurity is an essential aspect of patient safety in this era of digitisation. Mitigating cybersecurity risks helps MDS remain safe, effective and secured throughout its lifecycle.

As technology advances, new vulnerabilities would emerge. We must remain vigilant and adapt to emerging threats to continue to improve our MDS security landscape.

Through these efforts, the results of improved security for MDS would be evident, **Enabling Healthcare Professionals to Provide Safe & Precise Care to Patients!**