IRMG PMA

Student ID or IDs for group work	2126529
Words	2608

Date set	Friday 14th October 2022
Submission date (excluding extensions)	Monday 14th November 2022 by 12:00pm (UK time)
Submission guidance	To be submitted electronically via Tabula
Late submission policy	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late. For **Postgraduate** students only, who started their **current course before 1 August 2019**, the daily penalty is **3 marks** rather than 5.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

Module title & code	WM055-15 IRMG
Module owner	Harjinder Lallie
Module tutor	EB
Module marker	EB
Assessment type	Essay
Weighting of mark	100%

Table of Contents

1. Abstract

The implementation of cyber security risk assessments is essential for healthcare organisations, not only to protect patients from risk but also to ensure the organisation's operations. Thus, we will conduct a cyber security risk assessment of IoMT devices in the hospital to enhance the hospital's cyber security capabilities.

2. Introduction

To ensure cyber security in the hospital, we will conduct a comprehensive risk assessment of the hospital from a cyber security perspective to improve and enhance the IoMT device's cyber security and reduce the cyber security risk of the hospital.

The report contains three key points below and will describe them in 4-6 chapters.

- A critical analysis of and consideration of the suitability of various risk management standards, controls and policies applicable to the continued use of IoMT devices in a hospital setting.
- A risk analysis of the IoMT devices identified above and a corresponding risk mitigation strategy for the continued use of these devices.
- Recommendations on how the hospital can move towards reducing risk and in particular considerations that should be given when replacing these devices with newer IoMT devices.

3. Risk Appetite

After getting to know the hospital, we have developed a risk appetite for this hospital below:

"As a hospital, protecting the safety of people is of paramount importance". Therefore, we must control all aspects of risk to ensure the safety of patients and medical staff.

Firstly, we must comply with all regulations and laws within the industry.

Moreover, we must control the use, maintenance and updating of all devices in terms of protection and data protection measures. The hospital must prevent the transmission, sharing and processing of unauthorised data.

Also, we will not tolerate a significant and unidentified loss of funds.

Furthermore, we will not tolerate incidents that harm patients and medical staff.

Finally, we must ensure that the above risks maintain the hospital's reputation.

4. A critical analysis of and consideration of the suitability of various risk management standards, controls and policies applicable to the continued use of IoMT devices in a hospital setting

In this section, we will perform a critical analysis based on security standards in the continued use of IoMT devices in the hospital. Moreover, we will consider which risk management standards are best suited to this case based on the controls and policies that build up the risk management standard.

4.1 Critical analysis of cyber security standards

After an in-depth understanding of many risk standards, we find many risk standards for medical institutions or devices. However, they are not comprehensive enough for cyber security risk management and are unsuitable for risk assessment in this hospital. Thus, we have selected what we believe to be the two most authoritative and internationally renowned standards for this case, namely NIST CSF and ISO27001, and well-detailed analysis below:

- NIST CSF and ISO27001:

- Scope

  CSF and ISO 27001 are both suitable for organisations of all sizes and industries[1][2].

- Goal

  CSF improves enterprise cyber security with three elements: Framework Core, Framework Tiers and Framework Profiles[1]. However, ISO27001 enhances corporate cyber security in four steps: Plan, Do, Check, Action[2].

- Implementation

  The CSF starts with warm regards to identify and improve an organisation's pain points. The process will focus on business operations, risk tolerance and the technical environment to build a network security plan that suits the organisation's environment. Moreover, CSF also ranks the security risks across the organisation, prioritises the more serious security vulnerabilities, and builds a complete management cycle for the different stages of security incidents to improve overall security maturity step by step[1].

  The ISO 27001 starts with a goal-oriented approach to implementing the standard to improve the confidentiality, integrity and availability of cyber security in a phased manner. The process establishes the organisation's cyber security risk objectives, defines policies and controls for the cyber security system, and then implements the policies and controls against the defined objectives[2].

[1]. NIST. (2018) Framework for Improving Critical Infrastructure Cybersecurity. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[2]. ISO/IEC. (2013) ISO/IEC 27001:2013. Available from: https://www.qal-iran.ir/WebsiteImages/iso/21.PDF

4.2 Best risk management framework

Based on the controls and policies that build up the risk management standards, we believe CSF is the best risk management framework for the continued use of IoMT devices in the hospital by considering controls and policies for businesses:

- Controls

  In terms of controls, we first briefly list the controls that need to be considered for the continued use of IoMT devices in the hospital, as shown in Table A.:

Table A.

	Administrative controls	**Technical controls**	**Physical controls**
Preventive	Recruitment procedures Staff Confidentiality Policy Security Awareness Training Access Control Procedures Supply Chain Monitoring Procedures	Password Firewall Anti-virus software IPS	Guards Mantraps Identification cards Anti-theft locks
Detective	Access logs	IDS Honeypots Audit logs	CCTV Sensor Cameras
Corrective	Employee Termination Cyber security Incident Response Procedures	Network Interruption and Isolation Digital Forensics	Fire System
Recovery	BCP DRP	Backup tools	Rebuilt devices to perfect condition

  We can find that both CSF and ISO27001 can cover the controls above. However, if we consider the breadth and depth of control measures, CSF is more comprehensive than ISO 27001. For example, in the case of cyber security incident control, ISO 27001 only considers incident management procedures, response, assessment, response and evidence collection[1]. In contrast, CSF covers not only the previous areas but also how incident reports are presented, the sequence of personnel actions during an incident, and the implementation of more accurate incident management and response through external stakeholders[2]. The CSF not only contains a framework similar to ISO 27001 but also complements ISO 27001 in terms of "detection", "response", and "recovery".

- Policies

  Regarding policy, we can reference the hospital's background and risk appetite. The hospital has not conducted an IT audit for 12 years but must control the risk component at all levels to ensure the safety of patients and medical staff. Although ISO27001 can solve the current problems, it is a goal-oriented approach, and the symptoms may not be addressed, which means similar problems may still occur. In contrast, the CSF is very suitable for this situation, as it will assess all phases in the hospital, including operational status, risk tolerance and technical environment, to establish a cyber security plan that is appropriate for the hospital. In addition, the five elements in security management cycles in CSF make it easier for the hospital to focus on problem areas and reduce security risks in hospitals[1].

5. A risk analysis of the IoMT devices identified above, and a corresponding risk mitigation strategy for the continued use of these devices

In this section, we will conduct a risk analysis of all IoMT devices in the hospital and risk mitigation strategies for the continued use of these devices. We provide solutions in three parts: Threat Narrative and Mitigations, Table of Vulnerabilities, and Threat Register.

5.1 Threat Narrative and Mitigations

In this part, we present the threat narrative and mitigations section in Table B.[3], which contains the corresponding weaknesses for the vulnerabilities, business asset impact and mitigation strategy for continued use of IoMT devices.

- All Threats can be weaknesses IoMT advice.
- All Threat Actors can be terrorist groups or hacktivists.
- All Exploit can be publicly available Metasploit modules.

Table B.[3]

	Vulnerability	Business Asset Impact	Mitigation Strategy
Hamilton Medical AG,T1-Ventillator v2.2.3	CVE-2020-27278 CVE-2020-27282 CVE-2020-27290	Sensitive information leak Financial loss Loss of life Damage to reputation	Update to v2.23 or later Create a patch management strategy
Baxter PrismaFlex v2	CVE-2020-12036 CVE-2020-12035 CVE-2020-12037	Sensitive information leak Financial loss Loss of life Damage to reputation	Only authorised users can access to the device Create the configuration of medical devices Establish a Certificate Policy.
Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump, Version 1.1, 1.5, and 1.6	CVE-2017-12725 CVE-2017-12718 CVE-2017-12720 CVE-2017-12724 CVE-2017-12721 CVE-2017-12726 CVE-2017-12723 CVE-2017-12722	Sensitive information leak Financial loss Loss of life Damage to reputation	Close the FTP server. Assign a static IP address and monitor for any suspicious activity. Install the device on an isolated network. Security awareness training
Medtronic Paradigm wireless insulin pump 512, 522, 712, and 722	CVE-2019-10964	Sensitive information leak Financial loss Loss of life Damage to reputation	Rigorous scrutiny of externally connected device Security awareness training
Welch Allyn Service Tool (v1)	CVE-2021-27408 CVE-2021-27410	Sensitive information leak Financial loss Loss of life Damage to reputation	Update to v1.10 or later. Create a patch management strategy.
Welch Allyn Connex Central Station (CS) v1.1	CVE-2021-27408 CVE-2021-27410	Sensitive information leak Financial loss Loss of life Damage to reputation	Update to v1.84 or later Create a patch management strategy.
Synaptive Medical ClearCanvas ImageServer 3.0	CVE-2020-8788	Sensitive information leak Financial loss Damage to reputation	Front-end input filter HTML translation Disable unauthorised script execution

	Vulnerability	Business Asset Impact	Mitigation Strategy
Philips Healthcare Tasy Electronic Medical Record (EMR) 3.06	CVE-2021-39375 CVE-2021-39376	Sensitive information leak Financial loss Damage to reputation	Update to v3.06.1804 or later Create a patch management strategy.
Clinic's Patient Management System v1.0	CVE-2022-36242	Sensitive information leak Financial loss Damage to reputation	Input translation Filter characters Filter on the WAF Rewrite device code
Sourcecodester Medical Hub Directory Site 1.0	CVE-2022-28533	Sensitive information leak Financial loss Damage to reputation	Input translation Filter characters Filter on the WAF Rewrite device code
SourceCodester Electronic Medical Records System	CVE-2022-2676	Sensitive information leak Financial loss Damage to reputation	Input translation Filter characters Filter on the WAF Rewrite device code
Medical Store Management System v1.0	CVE-2022-25394	Sensitive information leak Financial loss Damage to reputation	Input translation Filter characters Filter on the WAF Rewrite device code

5.2 Statistics of Vulnerabilities

In this part, we present the statistics of vulnerabilities for the continued use of IoMT devices in Table C., which gives us an idea of the number of weaknesses.

Table C.

	SQL	Use of Hardcode	Buffer overflow	device configuration	Authentication	XML	XSS	Transmission of sensitive data
Sum	5	3	3	3	2	1	1	1

[3]. MITRE. (2022) Common Vulnerabilities and Exposures. Available from: https://cve.mitre.org/

5.3 Threat Register

In this part, we present the threat register for continued use of IoMT devices, which contains the threat corresponding matrix in Table D.[4] and impact, likelihood and severity for continued use of IoMT devices in Table E.

Table D.[4]

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

- Impact:

- Severe: Device vulnerability is directly related to patient treatment and will have an immediate impact on the patient's life.
- Significant: Device vulnerability is directly related to patient treatment and has a long-term impact on the patient's life.
- Moderate: Device vulnerability is indirectly related to patient treatment and can have an immediate hospital flow impact.
- Minor: Device vulnerability is indirectly related to patient treatment and can cause a hospital process impact over time.
- Negligible: Device vulnerability is related to indirect patient treatment and does not cause a hospital process impact over time.

- Likelihood:

- Since every device can be attacked over the network, and anyone can use network attacks, we have adjusted them to Very Likely.

[4]. IOWA. (2022) Determining Risk Levels. Available from: https://itsecurity.uiowa.edu/resources/everyone/determining-risk-levels

Table E.

	Impact	Likelihood	Severity
Hamilton Medical AG,T1-Ventillator v2.2.3	Severe	Very Likely	High
Baxter PrismaFlex v2	Severe	Very Likely	High
Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump, Version 1.1, 1.5, and 1.6	Severe	Very Likely	High
Medtronic Paradigm wireless insulin pump 512, 522, 712, and 722	Severe	Very Likely	High
Welch Allyn Service Tool (v1)	Significant	Very Likely	High
Welch Allyn Connex Central Station (CS) v1.1	Significant	Very Likely	High
Philips Healthcare Tasy Electronic Medical Record (EMR) 3.06	Moderate	Very Likely	High
Synaptive Medical ClearCanvas ImageServer 3.0	Moderate	Very Likely	High
Clinic's Patient Management System v1.0	Moderate	Very Likely	High
Sourcecodester Medical Hub Directory Site 1.0	Moderate	Very Likely	High
SourceCodester Electronic Medical Records System	Moderate	Very Likely	High
Medical Store Management System v1.0	Moderate	Very Likely	High

6. Recommendations on how the hospital can move towards reducing risk and in particular considerations that should be given when replacing these devices with newer IoMT devices

In this section, we will consider the cyber security risks in each phase of the medical device's lifecycle, including procurement, installation and acceptance, management, routine maintenance and disposal, to assess the risks that should be considered when replacing IoMT devices.

6.1 Procurement Risks and Recommendations

- Develop a procurement assessment process: Clearly understand the devices to be procured.
- Develop a supplier selection strategy: Establish precise selection methods, qualification requirements and careful evaluation of suppliers.
- Sign confidentiality agreements and cooperation contracts with suppliers: Confidentiality agreements and strict scrutiny of contract terms are required to avoid information leakage and mismatch after procurement.

6.2 Installation Acceptance Risks and Recommendations

- Inspection and installation of devices: Check that the devices can be installed safely and smoothly and that there are no security gaps.
- Check network connectivity: Verify that the devices can be securely and smoothly connected.
- Data transfer: Verify confidentiality, integrity and availability if data from other machines is to be transferred to the new machine.

6.3 Management Risks and Recommendations

- Establish code of ethics requirements or confidentiality agreements: Prevent leakage of sensitive information and information to external parties.
- List of personnel duties and requirements: Clear descriptions of the skills, competencies or qualifications required for each position within the team.
- Education and training: Training for staff who need to use new devices.
- Build threat information management tools: Gather intelligence on cyber attacks to prevent external network intrusion into the devices.
- Build defensive tools: Defensive tools such as anti-virus tools, WAF, SOC, and SIEM reduce the risk of external network intrusion into the devices.
- Build detection tools: Detection tools such as WAF, SOC, and SIEM reduce the risk of external network intrusion.
- Build system or network architecture recovery tools: Mitigation for external attacked devices.
- Build backup tools and procedures: ensure the confidentiality, integrity and availability of healthcare-related data.
- Build digital evidence preservation tools and procedures: In case of a network intrusion, preservation of evidence is required, including identification, collection, extraction and preservation.
- Establish access control procedures: Delegate appropriate authority to additional staff to ensure organisational security.
- Establish BCP: Ensure the continuity of the organisation's operations in the event of a natural or artificial system failure or disaster.

- Establish DRP: Ensure that disaster prevention measures are in place and that actions and measures are taken during and after a disaster.
- Establish procedures for incident response: When a cyber security incident occurs, there are procedures to respond and report.

6.4 Routine Maintenance Risks and Recommendations

- Regular devices review: Review devices allows early identification of vulnerabilities and prevents exploitation.
- Regular device maintenance: Regular device maintenance ensures up-to-date status and device security.
- Fault analysis reports: Realise why and when devices fail and how to ensure they do not fail in the subsequent use to reduce device risk.
- Devices parts consumption analysis reports: Record the status of each device's parts usage to reduce the risk of device failure.
- Establish a supplier monitoring and auditing strategy: Ensure suppliers can provide items on time to reduce device risk.

6.5 Disposal Risks and Recommendations

- Establish disposal reports: Record the disposal of each piece of device to prevent the leakage of sensitive information.