Cybersecurity Project

Risk Assessment Report

Hospital Network Design
Incorporating A.I. improved security and IoT handling

ACKNOWLEDGEMENT

This risk assessment utilises the preparation and execution processes, where applicable, as recommended in the National Institute of Standards and Technology (Guide for conducting risk assessments, 2012).

Some parts of this report's layout and elements are modified portions taken from the Risk_Assessment_Report_Template.docx provided for public use by the Defence Counterintelligence and Security Agency (Dcsa.mil, 2021).

TABLE OF CONTENTS

RISK ASSESSMENT PREPARATION

This risk assessment utilises the preparation processes as a potent way to gather information that is required to accurately carry out the actual risk assessment, and to also document the assessed system state.

PURPOSE OF THIS RISK ASSESSMENT

Threats to networks and information systems range from designed attacks, human and machine errors, environmental instability, and structural or hardware failures, that can result in varying degrees of disruptions and harm to the operational or economic interests of the hospital.

This risk assessment report considers where threats or weakness potentially exist in the hospital's network system and identifies where correction efforts are to be applied to remedy or reduce such vulnerabilities. Whilst fully eliminating risks is the most desirable outcome, realistically several risks can only be skilfully managed with preventative measures that reduce the risks likelihood and potency. This will provide a higher level of cybersecurity, data protection, availability, and operational readiness of the hospital's network and information systems.

SCOPE OF THE ASSESSMENT

For this cybersecurity project, the scope of this risk assessment is focused on implementable strategies for managing risks and system vulnerabilities, primarily for the planning stages of the hospital network design, security design, and security policy making.

Typically, such assessment efforts for network security focus strongly on external risk factors, but for this project the assessment scope has intense focus on internal risk factors arising from the cross-section system used by the hospital personnel, service partners, and patients. External risk factors are also realistically assessed and planned for.

This is an initial assessment and is not comprehensive of all risks and vulnerabilities to the hospital network and information systems. A re-evaluation assessment will cover the partial deployment and demonstration portion of this cybersecurity project.

RISK MODEL AND ANALYTICAL APPROACHES OF THIS ASSESSMENT

This risk assessment was conducted using the guidelines, the preparation and execution processes; as outlined in the Guide for Conducting Risk Assessments NIST SP 800-30, by the National Institute of Standards and Technology (Guide for conducting risk assessments, 2012).

The NIST prescribed <*Select Qualitative / Quantitative / Semi-Quantitative*> process was chosen as the measurement approach for this assessment. Risks are defined according to the threat event, the likelihood that threat occurs, predefined and known system vulnerabilities, other extenuating factors, and the potential impact these events have on the operation abilities of the hospital and its staff.

RISK ASSESSMENT FACTORS

The risks are defined and analysed using the following NIST recommended risk assessment factors.

IDENTIFIED THREAT SOURCES

The following table lists potential threat sources, categorised into generalised sources that healthcare IT networks and information systems are prone to.

Table 1: Potential Threat Sources

TYPE OF THREAT SOURCE	DESCRIPTION
ADVERSARIAL - Individual (outsider, insider, trusted, privileged) - Group (ad-hoc or established) - Organization (competitor, supplier, partner, patient) - Criminal elements (hackers, threat actors)	Individuals or groups that seek to exploit the hospital's dependence on cyber resources (e.g., information in electronic form, information and communications, and the communications and information-handling capabilities provided by those technologies.
PERSONNEL (STAFF) - Standard user - Privileged user/Administrator	Erroneous actions taken by hospital personnel while executing their everyday responsibilities.
STRUCTURAL - IT Equipment (networking, storage, processing, comm., display, sensor, controller) - Environmental conditions • Temperature/humidity controls • Power supply - Software • Operating system • Networking system • Information system	Failures of physical networking hardware or computational equipment, logical systems and software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.
ENVIRONMENTAL - Natural or man-made (fire, flood, earthquake, etc.) - Infrastructure failure/outage (electrical, internet, phones.)	Natural disasters and failures of critical infrastructures on which the organization depends, but is outside the control of the organization. Can be characterized in terms of severity and duration.

Modified, from source (Dcsa.mil, 2021).

IDENTIFIED THREAT EVENTS

At this stage of planning for the cybersecurity project, research into common vulnerabilities and risks associated with healthcare network and information systems, has identified the following threat events that should be planned for and mitigated.

Table 2: Potential Network/Information System Threat Events

TYPE	IDENTIFIED THREAT EVENTS
Adversarial	**Hacking, data theft, data loss risks.** Electronic health records, or EHRs, contain sensitive and private information pertaining to patients' medical data, and are a prime target for threat actors and data thieves. Hospitals and healthcare facilities also process and store large amounts of financial records and payment data, and research data. Breaches in EHRs and other sensitive data is a constant risk, and top priority for network and data security.
Adversarial, Personnel	**Ransomware and phishing risks.** In the last decade, hospitals have become one of the main targets for phishing and ransomware attacks. Ransomware has a high impact risk potential, as blackmailers can often cripple systems and demand huge payouts. For hospitals, critical systems are required to operate and attend to patients and are thus paramount in carrying out their life saving duties. System readiness and availability is crucial. Compliance with patient confidentiality also applies (see loss of compliance section below).
Adversarial, Personnel	**Reliance on medical IoTs, WIFI and remote access risks.** Through wireless networks (WIFI), Bluetooth, and remote connectivity; hospitals and healthcare systems make use of many medical devices that all transmit and store sensitive data, in the cloud or elsewhere. From monitoring equipment to smart devices like insulin pens, inhalers, wearable tech, to mobile devices that are required to fulfil medical staff duties; many vulnerabilities and risks are introduced into the network. Remote access to core information systems also introduces risks.
Structural	**Aging network infrastructure, software, and third-party reliance, risks.** As information technology and medical treatment innovations rapidly evolve, this results in an increasing complexity and interdependency of aging infrastructure and newer patched networks, a myriad of new and old software, and heavy reliance on third-party solution vendors and organizations for the processing and storage of medical records (EUHs), drug databases, and treatment protocols. This introduces several vulnerabilities and risks.
Personnel	**Loss of compliance risks.** Many countries have strict regulatory laws that govern patient privacy and confidentiality, and how their data is collected and stored. For example, the HIPAA was passed in 1996 in the USA, with The Privacy Act 1988 as the Australian counterpart. Inadequate cyber security, or improperly managed security may result in breaches of patient records, and thus a breach of compliance and regulatory requirements (financial penalties and litigation may apply).

TYPE	IDENTIFIED THREAT EVENTS
Personnel	**Lack of cybersecurity awareness risks.** Hospitals and healthcare facilities operate with hundreds or even thousands of personnel, filling a vast range of roles and duties that often require use of restricted systems and access to sensitive information. Studies have repeatedly shown that inadequate cybersecurity awareness training is commonplace and often leads to a large portion of system breaches and compromises. Without proper training, implementation, and enforcement of security policies, even the best cybersecurity deployment is at constant risk.
Environmental	**Natural disasters and failures of critical systems.** As already noted, the operational readiness of critical systems is of the highest performance, as they are required to service patients with, often in a lifesaving capacity. Events such as a sustained loss of electricity, internet connectivity, and telecommunications, could have severe consequences. Redundancies, backups, and other contingencies can help mitigate the threat impact.

LIKELIHOOD OF THREAT EVENTS / SUCCESS OF THREAT EVENTS

The assessment scale tables provide qualitative values by which threat events and risks can be measured, ranging from 'very low' to 'very high' scales. This provides the risk assessor a tangible value to calculate the likelihood the risk event will occur. This helps prioritise what risk events to plan more for.

Table 3: Assessment Scale – Likelihood of Threat Event Initiation (Adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the threat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

Modified, from source (Dcsa.mil, 2021).

Table 4: Assessment Scale – Likelihood of Threat Event Occurrence (Non-adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Personnel error, insecure activity, accident, or act of nature is **almost certain** to occur.
High	80-95	8	Personnel error, insecure activity, accident, or act of nature is **highly likely** to occur.
Moderate	21-79	5	Personnel error, insecure activity, accident, or act of nature is **somewhat likely** to occur.
Low	5-20	2	Personnel error, insecure activity, accident, or act of nature is **unlikely** to occur.
Very Low	0-4	0	Personnel error, insecure activity, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

Modified, from source (Dcsa.mil, 2021).

POTENTIAL ADVERSE IMPACT

The assessment scale tables provide qualitative values by which threat events and risks can be measured, ranging from 'very low' to 'very high' scales. This provides the risk assessor a tangible value to calculate the potential impact the risk event could have. This helps understand what risk events have critical impact to the hospital's operations.

Table 5: Assessment Scale – Impact of Threat Events

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic adverse effects** on the hospital's operations and ability to service patients, organizational assets, personnel and their duties, and other partner organizations.
High	80-95	8	Threat event could be expected to have a **severe or catastrophic adverse effect** (described above).
Moderate	21-79	5	Threat event could be expected to have a **serious adverse effect** (described above).
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect (described above).
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect (described above).

Modified, from source (Dcsa.mil, 2021).

RISKS COMBINATION, LIKELIHOOD AND IMPACT

Combining the risks, their likelihood, and potential impact greatly helps understand what risk events have the most critical impact on the hospital's operations, assisting in mitigation plans.

Table 6: Assessment Scale – Level of Risk (Combination of Likelihood and Impact)

Likelihood (That Occurrence Results in Adverse Impact)	**Level of Impact**				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Modified, from source (Dcsa.mil, 2021).

RISK ASSESSMENT RESULTS

The risk assessment approach in this table (Table 7) is to determine the relevant threats to the hospital's network and information systems listing them in the table below and detailing their relevant mitigating factors and controls (using the identified general threats table—Table 2—and other perceived risks that are specific to the scope of this cybersecurity project).

Table 7: Risk Assessment Results

Threat Event	Vulnerabilities / Predisposing Characteristics	Mitigating Factors	Likelihood (Tbls 4, 5)	Impact (Tbl 6)	Risk (Tbl 7)
Ransomware *(Adversarial)*	Malware encrypts data, potential data loss or corruption, loss of system services availability, or financial costs due to loss of productivity and blackmail.	Security preventative measures, layered zones, access controls, data backups.	Moderate	Very High	High
Phishing *(Adversarial, Personnel)*	Social engineering attack, facilitates ransomware, system intrusion, data theft or loss, viruses, malware.	Firewalls, attachment scanners, quarantining, personnel awareness training, email policy.	Moderate	Very High	High
System Penetration Attacks, Hacking. *(Adversarial)*	Hospital network, WIFI, information systems, databases, patient records, online services, staff workstations, and sensitive medical equipment at risk of compromise or theft of data.	Security preventative measures, firewalls, layered zones, access controls, monitoring, encryption, DDOS preventions, etc.	Moderate	Very High	High
Virus introduced into a system. *(Adversarial)*	Any computer used to access information outside the secured domain, infected by a virus. Could introduce malware, cripple systems, facilitate data theft.	Software firewalls and antivirus installed. Monitoring and quarantine policies. Subnetting zoning, gateway and router controls.	Moderate	Very High	High

Threat Event	Vulnerabilities / Predisposing Characteristics	Mitigating Factors	Likelihood (Tbls 4, 5)	Impact (Tbl 6)	Risk (Tbl 7)
Hospital staff introducing risk events. (*Personnel*)	Data suggests that humans introduce most risks from within a secure system. Poor behaviour, insecure activities and operational mistakes that introduce adversarial events such as malware, viruses, and system intrusion. Or activities that increase structural risks.	Enforcement of access rules, resource use, and password policies. Strong cybersecurity awareness training with regular updates and audits. Personnel behaviour and resource-use monitoring.	Moderate	Very High	High
Use of third party services (*Personnel*)	Shared patient records (EHR), treatment data, drug data, financial services, partner healthcare professionals, all introduce risk into the hospital network and information systems.	Strong personnel access rules, password policies, software updates and patches, monitoring and auditing policies.	Moderate	Moderate	Moderate
Loss of data compliance (*Personnel*)	The Privacy Act 1998 dictates laws governing the handling of confidential information and data. Large breaches in confidentiality laws resulting in litigation and fines.	Electronic patient records, confidential information, and personal financial records to be securely handled, and stored. Appropriate secure communication protocols, encryption, and security measures. Policies for data handling, and regular system audits. Staff training.	Moderate	Low	Moderate
Software failures, and vulnerabilities (*Structural*)	Software failure leading to loss of services, anything from viewing patient records, running critical enterprise frameworks, to filling out reports.	Regular updating and maintenance of software, stable versions only, using licensed software with tech support. Redundancy setups of critical software for backup use.	Low	Moderate	Low

Threat Event	Vulnerabilities / Predisposing Characteristics	Mitigating Factors	Likelihood (Tbls 4, 5)	Impact (Tbl 6)	Risk (Tbl 7)
Data loss, or database fail (*Structural*)	Server or software component failure leading to partial loss of databases serving or storing critical information. Information systems and services dependent on the data may fail to operate correctly.	Redundant server infrastructure, or backup databases configured to take on requests in an active database failure. Server and database maintenance, and upgrade program. Policies and monitoring strategies.	Moderate	Moderate	High
Network hardware failure, WIFI failure (*Structural*)	Hardware component failure leading to partial loss of network infrastructure or information systems. Also resulting in medical IoT device loss of connectivity, and operability.	Redundant network infrastructure installed for failover. Network maintenance, and upgrade program. Policies and monitoring strategies.	Moderate	Moderate	High
Downgrade or loss of physical security IT components (*Structural*)	Security cameras, alarms, and other sensors being compromised due to aging equipment or penetration attacks.	Live monitoring of security components operability, with automatic red flags and alarms. Maintenance and upgrade policies, and reaction plans.	Low	High	Low
Loss of internet, or outside connectivity (*Structural*)	Partial operational loss of information systems, such as access to EHRs, third party services, financial services, etc.	Redundant internet connections for critical systems, consider sourcing both fiber and wireless connectivity.	Low	Moderate	Moderate
Loss of power, Loss of network and critical information systems (*Environmental*)	Natural disasters or breakdown of the power grid resulting in loss of all IT systems availability.	Redundant power supply for critical systems, large format battery storage, generators.	Very Low	Very High	Moderate

Threat Event	Vulnerabilities / Predisposing Characteristics	Mitigating Factors	Likelihood (Tbls 4, 5)	Impact (Tbl 6)	Risk (Tbl 7)
Compromise of Hospital IoT devices (*Structural, Adversarial*)	Successful attacks against known vulnerabilities of IoT devices, loss of IoT function, system penetration, compromise of hospital systems, exposing confidential patient data.	Segregated wireless IoT networks, gateway firewall, WPA3 802.1X authentication, IP and MAC filtering, X.509 cryptographic keys, strict communication policies. AI-assisted IDS and IPS, with Cylance AI.	Low	High	High
Cloud Service Risks (*Adversarial*)	Security is managed by the third-party, reduced oversight and control, increased surface area of vulnerability, data traffic exposed over the internet, data interception, service compromise.	Use of trustworthy cloud service providers, cloud access restrictions, encryption of data transmissions, certificate-based authentication. AI assisted IDS and IPS, through AWS Darktrace AI.	Low	High	Moderate
Third-party Application Risks (*Adversarial, Personnel*)	Vulnerabilities in application security, stability of system, integrity of data, potential backdoor or zero-day exploits. Lack of support and security patches.	Policy of evaluating application products, using Enterprise Mobility Evaluation Program, and ASD High Assurance Evaluation Program. Use of Protection Profile (PP) to define the security functionality of programs. Cyber department lab tests applications for vulnerabilities and performance issues.	Very low	Moderate	Moderate

Modified Table Template, from source (Dcsa.mil, 2021).

COMMUNICATING AND MANAGING THE RISKS

Initially, the results of this risk assessment are to be communicated with the network and security specialists who are involved in the planning, implementing, and managing of this cybersecurity project. This will aid in the network design, security design, and security policy formulation, for the hospital network and information systems.

Towards completion of this project, this risk assessment report can be re-evaluated, fine tuning it in preparation for deployment and maintenance of the network and systems.

In a real-world scenario, risk assessment re-evaluation would be run on a cyclic basis, assisting in security auditing and management. Reports would be disseminated to relevant management and security personnel.

Here is a table list of the highest risks, which have the highest potential for negative impact, that have a critical need to be mitigated and monitored during the planning, design, implementation, and management phases.

Table 8: Risks that require the highest level of attention

Risk Threat	Impact Factors	Impact
Ransomware (*Adversarial*)	Malware encrypts data, potential data loss or corruption, loss of system services availability, or financial costs due to loss of productivity and blackmail.	High
System Penetration Attacks, Hacking. (*Adversarial*)	Hospital network, WIFI, information systems, databases, patient records, online services, staff workstations, and sensitive medical equipment at risk of compromise or theft of data.	High
Hospital staff introducing risk events. (*Personnel*)	Data suggests that humans introduce most risks from within a secure system. Poor behaviour, insecure activities and operational mistakes that introduce adversarial events such as malware, viruses, and system intrusion. Or activities that increase structural risks.	High
Data loss, or database fail (*Structural*)	Server or software component failure leading to partial loss of databases serving or storing critical information. Information systems and services dependent on the data may fail to operate correctly.	High
Network hardware failure, WIFI failure (*Structural*)	Hardware component failure leading to partial loss of network infrastructure or information systems. Also resulting in medical IoT device loss of connectivity, and operability.	High
Loss of data compliance (*Personnel*)	The Privacy Act 1998 dictates laws governing the handling of confidential information and data. Large breaches in confidentiality laws resulting in litigation and fines.	High

Revision History

All changes, updates and revisions to this document are to be recorded in the table below, preserving a record for administrative and legal purposes.

Date of Change	Responsible	Summary of Change
July 24, 2022	George Price	Risk Assessment Completed
October 8, 2022	George Price	Risk Assessment review executed, and additional risks were identified: 1. IoT Vulnerability Risks 2. Cloud Service Risks 3. Third-party Healthcare Application Risks

REFERENCES

Dcsa.mil. (2021). [online] Available at: https://www.dcsa.mil/Portals/69/documents/io/rmf/Risk_Assessment_Report_Template_Nov17.docx.

Guide for conducting risk assessments. (2012). [online] doi:10.6028/nist.sp.800-30r1.