SWINBURNE UNIVERSITY OF TECHNOLOGY

Faculty of Business & Law

Cyber Security For Business
INF20031

Assignment 1

Cybersecurity Report

TUTOR

Anu Bhardwaj

STUDENT

Tran Anh Thu Pham – 10381840

Word count: 2757

HAWTHORN – AUGUST 2024

Table of Content

I. Executive Summary

This report evaluates cybersecurity risks at Bayview Regional Health Centre (BRHC) and proposes mitigation strategies. Data breaches are identified as the highest risk due to their severe impact on patient data and organization data. Phishing attacks and authorization access also pose significant risks, while financial data theft is a medium-level concern. The report recommends enhancing access controls, implementing encryption, providing employee training and updating incident response plans to address these risks effectively. Strengthening these areas will help BRHC protect critical information, ensure regulatory compliance and maintain patient trust.

II. Approach to Information Security risk management and information risk assessment

At Bayview Regional Health Centre (BRHC), securing patient data, financial information and operational processes is critical to ensuring both compliance and trust. This Cybersecurity Status Report will evaluate the current security posture of BRHC's systems and identify vulnerabilities that expose the organisation to potential cyber risks.

My approach to Information Security Risk Management involves identifying information assets, identifying possible threats to these assets, and accessing assets' vulnerabilities. Each part of this report will be implemented following specific standards. Using the Asset-Threat-Vulnerability (ATV) framework, I will categorize the most 7 critical assets and the corresponding risks they face. For Information Risk Assessment, I will evaluate the security controls in place, and identify gaps and assets and how well BRHC is equipped to handle potential incidents. Lastly, the mitigation plan, incorporating mitigation strategy and internal controls will be implemented for all identified risks.

III. Bayview Regional Health Centre's strategic environment and Cybersecurity mission statement

1. Overview of BRHC's environment, value-creating activities and current risk posture

Bayview Regional Health Centre (BRHC) operates in a rural healthcare environment in Victoria focusing on delivering high-quality healthcare service to patients at the clinic and through telehealth services. Their strategic value comes from improving healthcare accessibility for rural patients while managing critical healthcare information integrated with the Medilink system. However, BRHC's current systems and processes are vulnerable to some threats such as unauthorized access and data breaches. Key vulnerabilities include insufficient access controls, and responsibility gaps in IT management, especially the cloud-based solution and incident response.

2. BRHC's Cybersecurity mission statement

At Bayview Regional Health Centre, safeguarding the confidentiality, integrity and availability of patient data and critical organization information is our top priority. We are committed to fostering a culture of cybersecurity awareness and ensuring the adoption of robust security measures across all departments of the organization. Our core values are delivering accessible and high-quality healthcare to rural communities.

Our risk appetite prioritizes patient data safety and privacy, and we accept minimal risks only in areas that do not compromise clinical care and patient trust. BRHC will maintain compliance with healthcare regulations, and continuously improve our cybersecurity defences to adapt to evolving threats.

Our target risk tolerance is low for threats to patient data confidentiality, integrity and availability, operational disruption and unauthorized access to sensitive information. We will adopt proactive risk mitigation strategies, ensure timely audits and ensure our staffs follow security best practices.

Category	Risk Appetite
Policy	balanced
Strategic	high
Financial Markets	balanced
People and Culture	high
Operational	balanced
Compliance	limited

Fig 1. BRHC Risk Appetite

IV. Key roles and responsibilities of individuals and business functions at BRHC

Roles no	Roles	Responsibilities
1	Doctors (GPs and Specialist)	• Ensure patient data are accessed and stored securely • Not sharing patient data with unauthorized personnel • Ensure the communication with the patient is secure • Report any suspicious activity or data breach to the BRHC IT department
2	Nurses (including those conducting home visits)	• Ensure patient records are accessed and stored securely • Report any suspicious activity or data breach to the BRHC IT department
3	Allied Health Professionals	• Maintain the confidentiality of patient data • Ensure the communication with the patient is secure

4	Centre Manager (Susan Davis)	• Oversees the implementation of cybersecurity policies and procedures • Ensure BRHC staffs are security awareness trained • Make decisions regarding data access and control of sensitive data
5	Front Office Personnel	• Ensure patient data is secure during scheduling tasks • Be aware of phishing attack • Report any suspicious activity or data breach to the BRHC IT department
6	Practice Manager	• Ensure compliance with cybersecurity policies within the practice • Oversee the security of financial and patient data • Review BRHC security status with the IT department and suggest improvements
7	Managing Accountant (Micheal Thompson)	• Protect financial data from unauthorized access and breaches • Ensure secure financial transaction • Support the adoption of secure cloud solutions for financial management
8	Accounts Reconciliation Officer (Anna Lee)	• Ensure the BRHC inventory and financial data are secured • Follow IT guidelines for data protection and report any security incidents
9	HR and Payroll Manager (Sarah Jennings)	• Protect employee records and payroll data from unauthorized access • Ensure the HR data storage is secure
10	IT Specialist (Liam Park)	• Support BRHC staff with cybersecurity issues • Manage the response to IT incidents, such as the recent DDoS attack
11	Software Developer (Justin Hayes)	• Manage the system's database and servers • Collaborate with the IT specialist and organisation manager to address security issues
12	Managing Directors (Dr Emma Clarkson and Dr Jason Morelli)	• Manage all aspects of the operation including the security activities

Table 1. Key roles and responsibilities at BRHC

All the responsibilities related to cyber security have been assigned to specific roles in the organization; however, there are still some responsibility gaps. Specifically, the HR and Payroll Manager explores cloud-based HR solutions without prioritizing data security and compliance, focusing more on functionality. Additionally, the lack of responsibility in the IT department could lead to the potential security incident in the organization. For instance, there is no formal incident response plan. The IT specialist has not developed a structured incident response plan despite previous attacks. The software developer does not update the Medilink system which is outdated and not adequately secured to meet modern security standards.

V. Full inventory of all information assets in BRHC

Asset no	Information assets	Roles
1	Patient records	• Nurses • Centre Manager • IT Specialist • Software Developer • Managing Directors
2	Appointment and Consultation data	• Front Office Personnel • IT Specialist • Software Developer • Managing Directors
3	Prescription and Medical Report	• Doctors (GPs and Specialist) • Allied Health Professionals • IT Specialist • Software Developer • Managing Directors
4	Referrals and Admissions Data	• Doctors (GPs and Specialist) • Nurses • IT Specialist • Software Developer • Managing Directors
5	Clinical and Non-clinical Information communication	• Centre Manager • IT Specialist • IT Specialist • Software Developer • Managing Directors
6	Telehealth records	• Doctors (GPs and Specialist) • IT Specialist • IT Specialist • Software Developer • Managing Directors
7	Administrative data	• Centre Manager • Front Office Personnel • IT Specialist • Software Developer • Managing Directors
8	Financial information	• Accounts Reconciliation Officer (Anna Lee) • IT Specialist • Software Developer

		• Managing Directors
9	Staff records	• HR and Payroll Manager (Sarah Jennings) • IT Specialist • Software Developer • Managing Directors
10	Inventory data	• Accounts Reconciliation Officer (Anna Lee) • IT Specialist • Software Developer • Managing Directors
11	Accounting data	• Managing Accountant (Micheal Thompson) • IT Specialist • Software Developer • Managing Directors
12	HR and Payroll Information	• HR and Payroll Manager (Sarah Jennings) • IT Specialist • Software Developer • Managing Directors

Table 2. Full inventory list for information assets at BRHC

VI. ATV table for the top 7 operationally important information assets ISO/IEC 27005 helps identify threats and vulnerabilities)

Asset No	Information Asset	Threat	Vulnerability
1	Patient records	• Unauthorized access • Data breaches	• Insufficient access controls and monitoring • Handle sensitive data outside of the clinic's secure environment • Outdated security measures in the Medilink system
2	Appointment and Consultation data	• Phishing attack or social engineering attack • Unauthorized access • Data breaches	• Lack of phishing awareness training for front office personnel • Unsecured communication channels • Outdated security measures in the Medilink system

3	Prescription and Medical Report	• Unauthorized access • Data breaches	• Use insecure communication methods such as email, fax, etc. • Outdated security measures in the Medilink system
4	Referrals and Admissions Data	• Unauthorized access • Data breaches	• Use insecure communication methods such as email, fax, etc. • Outdated security measures in the Medilink system
5	Financial information	• Financial data theft • Unauthorized access • Data breaches	• Lack of secure devices and data protection protocols • Reliance on manual processes • Outdated security measures in the Medilink system
6	Inventory data	• Unauthorized access • Data breaches	• Insufficient access controls and monitoring • Lack of instant reporting and monitoring • Outdated security measures in the Medilink system
7	HR and Payroll Information	• Unauthorized access • Data breaches	• Lack of robust security in HR and payroll system • Focus on functionality over security in exploring cloud-based HR solution • Outdated security measures in the Medilink system

Table 3. Threats and vulnerabilities of the top 7 critical information assets

Below is an analysis of the threats and vulnerabilities specific to the top 7 critical assets:

Medilink system is outdated and can lead to all security threats to the assets listed in the table above because modern threats require advanced security measures that Medilink cannot fully address. This system's monitoring and control is the responsibility of the IT Specialist and Software Developer. Referring to the case study, the Medilink system is now running on 20 years of patches and extensions. Since the system rapidly developed with additional functionalities such as the direct file exchange and HR extension, Medilink faces up to satisfy these changes.

Lastly, the managing directors monitor all the activities of the organization related to security issues. Therefore, all the information assets' protection is their responsibility.

1. Patient Records
   All employees have access to the patient data, which indicates insufficient access controls. The centre manager, Susan Davis is slightly concerned about granting all employees access to patient data at any time, but she believes the convenience outweighs the risks. This decision of the centre manager can lead to unauthorised access to sensitive data. Additionally, the access control in BRHC is inadequate because the sensitive data is handled outside of the clinic's environment. The home visit nurses often download patient data onto their tablets to record visit details which can lead to data breaches.

2. Appointment and Consultation data
   Referring to the BRHC case study, there is no mention of training provided to front office personnel to recognise phishing or engineering attacks. Since they regularly handle appointment and consultation data, a lack of awareness could expose the organization to these attacks. Additionally, the case study mentions that patient consultation results are sometimes sent via email or fax when there are issues accessing the system. Front office personnel handle appointment scheduling and communication tasks; however, email and fax are unsecured channels that could expose patient appointment data to unauthorized access and data breaches during the booking process.

3. Prescription and Medical Report
   The case study states that when rural doctors and allied health professionals encounter issues accessing the system, they often resort to sending patient consultation results via email or fax. This insecure communication method can expose sensitive information including prescription and medical reports to unauthorized access and data breaches.

4. Referrals and Admissions Data
   Similar to other patient-related data listed above, referrals and admissions information can be vulnerable to threats such as unauthorized access or data breaches. These interceptions are usually caused by using unsecured communication methods like email and fax. This method is often used by doctors and nurses when they can not access the system.

5. Financial information
   The case study states that Anna Lee, the Accounts Reconciliation, exports and converts daily accounts data to CSV format and uses Excel spreadsheets to manage financial tasks such as placing orders, reconciling accounts and banking. This reliance on manual processes outside of secure, integrated financial systems increases the risk of financial data theft, data breaches and unauthorized access. Additionally, Anna Lee continues using her laptop for work tasks, even though her previous laptop was lost at a nearby café. This

demonstrates a lack of secure devices and data protection protocols for financial management.

6. Inventory data
   Similar to the vulnerability of financial information assets, the accounts reconciliation officer, exports and converts the inventory list to CSV format and uses Excel spreadsheets on her laptop and her previous laptop was lost emphasizing the vulnerability of this data asset due to the lack of secure access controls and monitoring. Additionally, the Medilink system lacks real-time batch reporting capabilities for generating inventory lists. This creates a significant delay in reporting and monitoring, making it difficult to track inventory data in real-time and promptly respond to any issues.

7. HR and Payroll Information
   The case study mentions that Sarah Jennings, the HR and Payroll manager is overwhelmed by the limitations of the outdated system. This suggests that the existing R and payroll system is not adequately equipped with modern security features. Additionally, Sarah Jennings is exploring cloud technologies and Software as a Service (SaaS) to improve HR functionalities. However, it is noted that she is prioritizing functionality over the location of the data storage which creates a significant vulnerability if data protection and compliance measures are not prioritized.

VII. Likelihood and impact analysis for the 7 most critical identified information assets

(NIST 800-30 provides detailed methodologies for assessing the likelihood and impacts)

Asset No	Information Assets	Threat	Likelihood (1 – 5)	Impact (1 – 5)	Risk-Rating Factor
1	Patient records	Unauthorized access	2	5	10
		Data breaches	3	5	15
2	Appointment and Consultation data	Phishing attack or social engineering attack	4	3	12
		Unauthorized access	2	5	10
		Data breaches	3	5	15

3	Prescription and Medical Report	Unauthorized access	2	5	10
		Data breaches	3	5	15
4	Referrals and Admissions Data	Unauthorized access	2	5	10
		Data breaches	3	5	15
5	Financial information	Financial data theft	2	4	8
		Unauthorized access	2	5	10
		Data breaches	3	5	15
6	Inventory data	Unauthorized access	2	5	10
		Data breaches	3	5	15
7	HR and Payroll Information	Unauthorized access	2	5	10
		Data breaches	3	5	15

Table 4. Likelihood and impact analysis for the 7 most critical identified information assets

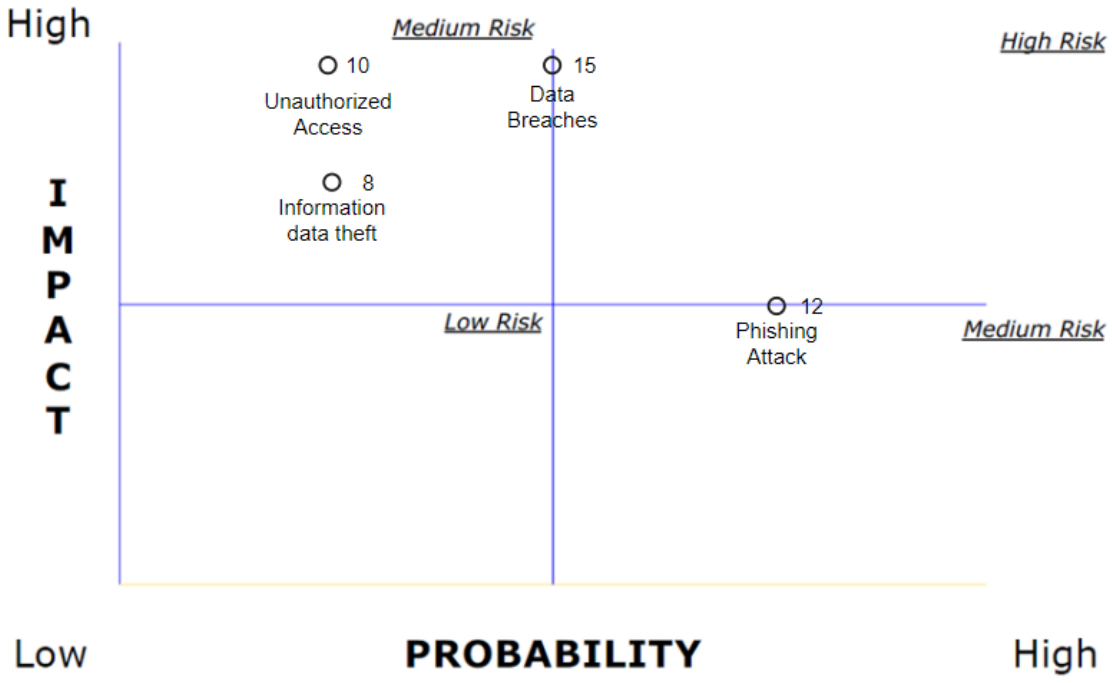

Fig 2. Risk's likelihood and impact analysis using Jacobson's window

VIII. Evaluation and prioritisation of the most significant associated information risks

Refer to the risk rating window and the likelihood and impact analysis table above, the evaluation and prioritization table of the most significant associated information risk is listed below:

Risk Order	Risk	Risk Factor	Risk Level
1	Data Breaches	15	High
2	Phishing Attack or Social Engineering Attack	12	High
3	Unauthorized Access	10	Medium
4	Financial Data Theft	8	Medium

Table 5. Evaluation and prioritisation of the most significant associated information risks

Here are justifications for the accessed order of priority:

1. Data Breaches (Risk Factor: 15, high):

   Data Breaches are ranked highest due to the involvement of susceptible and critical information assets, related to patient data. These assets are central to BRHC's operations, and a breach could result in severe legal consequences, regulatory penalties, reputational damage and loss of patient trust. The widespread impact across multiple assets and the high likelihood of breaches due to healthcare service being the most important target justifies its top position in the risk order.

2. Phishing or Social Engineering Attacks (Risk Factor: 12, high):

   Phishing attacks often trick employees of sensitive data or credentials. This type of risk is common in healthcare, and the appointment and consultation data are critical assets at risk. Phishing attacks can lead to unauthorized access or data breaches if credentials are stolen, and it is placed second due to its slightly lower but still significant impact.

3. Unauthorized Access (Risk Factor: 10, medium):

   Unauthorized access to critical systems or information assets poses a significant risk since it can lead to data breaches and other security threats. Given that the same sensitive assets as data breaches such as patient records

and medical reports are involved, this risk is high. The impact is severe as unauthorized individuals could exploit these data. However, the likelihood is slightly lower than that of external breaches, especially with strong internal controls, hence placing this third.

4. Financial Data Theft (Risk Factor: 8, medium):

   Financial information theft is damaging but affects fewer assets than previous risks. The impact is medium as it can result in monetary losses, but it doesn't immediately disrupt patient care or the organization's operation like data breaches and unauthorized access. The risk of financial data theft can be controlled through access controls and auditing. Therefore, it is less critical than phishing attacks.

IX. Mitigation Plan

(ISO/IEC 27001 guild the development of policies and controls)

Asset No	Information Assets	Risks	Risk Management Strategy	PDC controls
1	Patient records	Unauthorized access	Avoid	Preventive
		Data breaches	Avoid	Preventive
2	Appointment and Consultation data	Phishing attack or social engineering attack	Reduce	Preventive
		Unauthorized access	Avoid	Preventive
		Data breaches	Avoid	Preventive
3	Prescription and Medical Report	Unauthorized access	Avoid	Preventive
		Data breaches	Avoid	Preventive
4	Referrals and Admissions Data	Unauthorized access	Avoid	Preventive
		Data breaches	Avoid	Preventive
5	Financial information	Financial data theft	Reduce	Preventive
		Unauthorized access	Avoid	Preventive
		Data breaches	Avoid	Preventive
6	Inventory data	Unauthorized access	Avoid	Preventive
		Data breaches	Avoid	Preventive

7	HR and Payroll Information	Unauthorized access	Avoid	Preventive
		Data breaches	Avoid	Preventive

Table 6. Mitigation Plan for the Prioritized Risks

Unauthorized access and data breaches should be avoided because these risks are high-impact, but they can be eliminated by applying internal controls. Financial Data Theft and Phishing Attacks should be reduced since these risks can be mitigated through controls. Additionally, to reduce the risks, preventive controls such as firewalls, encryption, etc can be applied. Lastly, to avoid the risks, preventive controls should be implemented to ensure risks do not materialize.

X. Reference

1. Camp, K. (2020, October 27). *Intro to Jacobson's Window Risk Analysis*. Medium. https://medium.com/@kencamp/intro-to-jacobsons-window-risk-analysis-9163fbeada33

2. Australia, scheme=AGLSTERMS A. corporateName=Reserve B. of, & Australia, scheme=AGLSTERMS A. corporateName=Reserve B. of. (2023, August). Risk Management Policy. Reserve Bank of Australia. https://www.rba.gov.au/about-rba/our-policies/risk-management-policy.html

3. Redirecting. (2024). Instructure.com. https://swinburne.instructure.com/courses/61653/assignments/633030

4. Shane, R. (2009). Risk evaluation and mitigation strategies: Impact on patients, health care providers, and health systems. American Journal of Health-System Pharmacy, 66(24_Supplement_7), S6–S12. https://doi.org/10.2146/ajhp090461

5. Hudson, P. (2003). Applying the lessons of high risk industries to health care. Quality and Safety in Health Care, 12(90001), 7i12. https://doi.org/10.1136/qhc.12.suppl_1.i7