FACULTY OF SCIENCE
IFN541 Information Security Management - Assessment Task 2: Report
Risk management report

Student

Yi-Chen, CHEN N11564628

Hsiang-Jen, Yu N11453559

Chin-Wei, WU N11414561

Pin-Chieh, CHIU N11532360

Professor

Tony Rhodes

Submission date

05/26/2024

Table of Contents

1 Introduction

This risk management report is for our client, Handseed International Hospital.

Handseed International Hospital is a large private medical center located in the capital city of Taiwan. The hospital employs over 1200 staff members. Additionally, the hospital has more than 850 patient beds, distributed as follows: the Research Department Building has 199 employees and 50 beds, the Medical Department Building has 600 employees and 554 beds, and the Clinical Department Building has 479 employees and 329 beds. All three buildings are located together in one area.

The hospital primarily offers services related to human health. The hospital's clients are people with health issues. It operates three distinct departments, each providing specialized services:

1. **Research Department**:
    - Investigating and developing new medicines and vaccines. Staff activities include researching and analyzing medical data using academic papers for medical records. This enables clients to explore new treatment methods for their illnesses.
2. **Medical Department**:
    - Providing hospitalization services such as conducting surgeries, medical practice, and patient care.This department serves individuals who need surgery and hospitalization.
3. **Clinical Department**:
    - Providing clinical services such as medical consultations, prescriptions, and managing appointment procedures.

The hospital has several critical information assets, which must be safeguarded to maintain the hospital’s integrity, reputation, and efficient functioning.

1. **Electronic Health Records:** These records, typically stored in an electronic medical record system, contain detailed information about patient health conditions and profiles. Without a dedicated information security process, these documents could be leaked to the public or the Internet, infringing on patient privacy and putting them at unpredictable risk. Such breaches could lead to a loss of patient loyalty and damage the hospital's reputation.

2. **Employment Records:** These records include essential information about hospital staff members, securely stored within the human resources department. They contain personal background, career positions, and specialist abilities. This information is crucial for various management tasks such as promotions, recruitment, and commissions. Unauthorized access or alterations could disrupt career management plans and result in significant errors in job distribution.

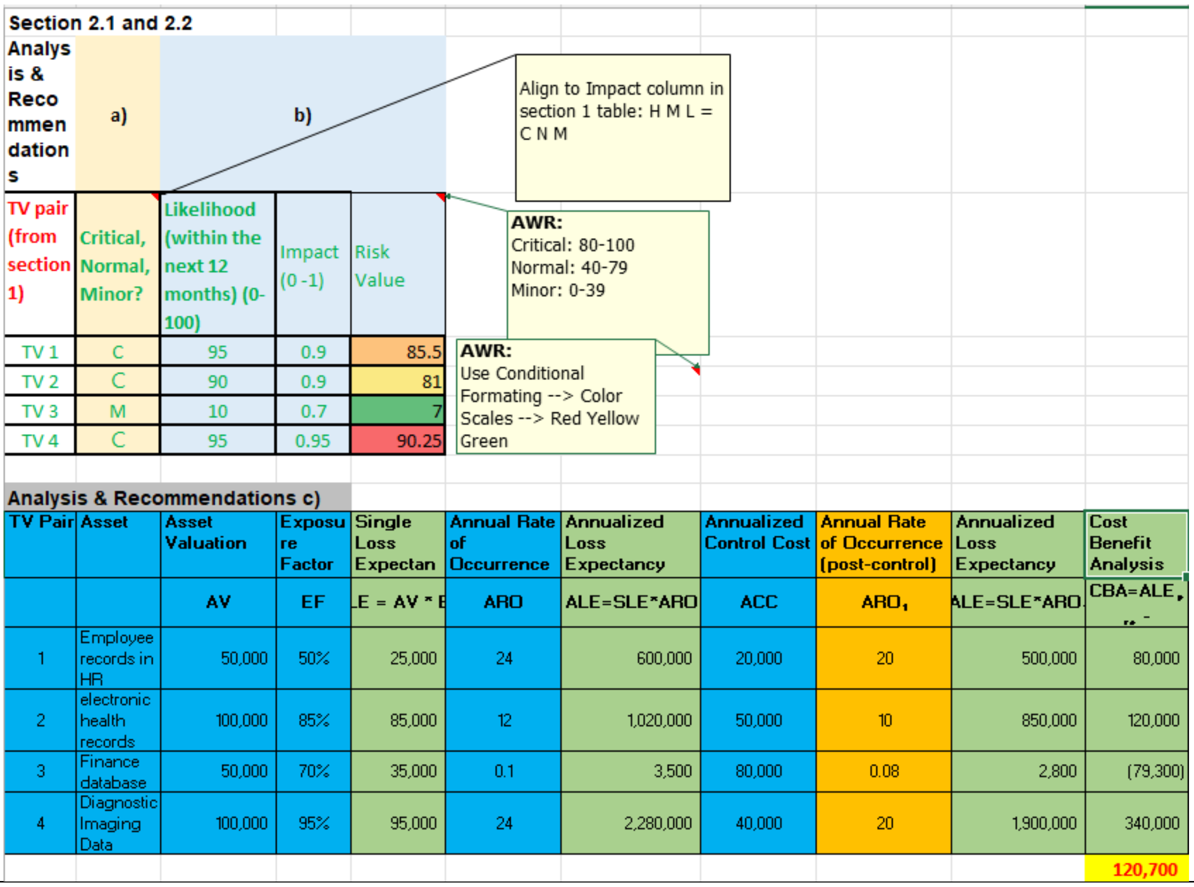
3. **Financial Records:** Stored in the finance or accounting department, these records contain critical information about the hospital's financial status, including health insurance, patient payment bills, hospital revenue, and equipment purchase receipts. These records are essential for budget balance, financial management, and maintaining financial stability. Unauthorized alterations could disrupt hospital operations and cause substantial financial loss, making it crucial to safeguard these records to ensure integrity and accuracy in financial management processes.

2 Risk Management Plan

Note: Table fields:

Threat	Threat Agent, Intentional / unintentional	Asset	Asset Value	EF, ARO	Vulnerability	Exploit	Organisational Risk Impact (H, M, L)	Mitigation	Justification	Annualized Control Cost
Phishing	Human, intentional	Employee records in HR	50,000	50%, 24	Anti-malware software is not up to date	Attacker sends e-mail with malicious link embedded	H	Install up-to-date internet security software	Detects malware and prevents installation	20,000
Leakage of medical records (Firewall)	Technology, intentional	electronic health records	100,000	85%, 12	Firewall outdated/ unreliable	Hacker sends malicious packets	H	Install and configure a reliable and robust firewall system	Able to defend various types of computer viruses.	50,000
Earthquake to damage physical server	Environment, unintentional	Finance database	50,000	70%, 0.1	In earthquake region	Earthquake occurs	L	Develop Business Continuity and Disaster Recovery Plans	To recover from natural disaster.	80,000
Weak Access Controls	Technology Accessibility, unintentional	Diagnostic Imaging Data in the clinical department	100,000	95%, 24	Unauthorisation of Diagnostic Imaging information	if electronic medical records (EMRs) be hacked, leading to treatment delays or errors.	H	Conduct the comprehensive assessment of role access to EMRs, and reallocated the appropriated authorization distribution	Allow the right staff to the EMRs and avoid the treatment delay	40,000

3 Analysis and Recommendations



Section 2.1 and 2.2

Analysis & Recommendations	a)	b)		
TV pair (from section 1)	Critical, Normal, Minor?	Likelihood (within the next 12 months) (0-100)	Impact (0 -1)	Risk Value
TV 1	C	95	0.9	85.5
TV 2	C	90	0.9	81
TV 3	M	10	0.7	7
TV 4	C	95	0.95	90.25

Align to Impact column in section 1 table: H M L = C N M

AWR:
Critical: 80-100
Normal: 40-79
Minor: 0-39

AWR:
Use Conditional Formating --> Color Scales --> Red Yellow Green

Analysis & Recommendations c)

TV Pair	Asset	Asset Valuation	Exposure Factor	Single Loss Expectan	Annual Rate of Occurrence	Annualized Loss Expectancy	Annualized Control Cost	Annual Rate of Occurrence (post-control)	Annualized Loss Expectancy	Cost Benefit Analysis
		AV	EF	LE = AV * E	ARO	ALE=SLE*ARO	ACC	ARO$_1$	ALE=SLE*ARO	CBA=ALE,
1	Employee records in HR	50,000	50%	25,000	24	600,000	20,000	20	500,000	80,000
2	electronic health records	100,000	85%	85,000	12	1,020,000	50,000	10	850,000	120,000
3	Finance database	50,000	70%	35,000	0.1	3,500	80,000	0.08	2,800	(79,300)
4	Diagnostic Imaging Data	100,000	95%	95,000	24	2,280,000	40,000	20	1,900,000	340,000
										120,700

Based on the above data, the order of the risk management priority is TV4, TV2, TV1, and TV3 from top to bottom. TV1 has a higher risk value than TV2, however, the company pays more attention on the aspect of cost benefit since our risk appetite is not low meaning the risk priority is less important to the organisation, therefore we will prioritize TV2 over TV 1.

3.1 Analysis and recommendations for employee data in HR (TV4)

According to the above analysis, it's advised that TV4 should be the top priority of threat management. It clearly shows that **TV4 has the highest risk value and the highest cost-benefit.** Moreover, TV4 threatens the important asset "Diagnostic Imaging Data," which is one of the main particular organizations as enhancing patient care quality. The cybersecurity challenges in the healthcare sector are distinctive because of the sensitive nature of the information at stake and the potential impact on patient safety (Argaw, S. T,2020).

The recommended mitigation action is to reallocate the appropriate authorization distribution. To be specific, perform a detailed assessment of role-based access to Electronic Medical Records (EMRs) and adjust the authorization allocations as necessary. Nursing stuff play a crucial role in safeguarding healthcare data due to their significant representation in the healthcare workforce and direct access to such data(Mikuletič, S.2024). The justification for this action is that it allows the correct personnel access to the Electronic Medical Records (EMRs), thereby preventing delays in treatment.

3.2 Analysis and recommendations for Electronic Health Records (TV2)

TV2 has the second highest cost-benefit, which determines that it should rank second in risk priority. For the Electronic Health Records, which is categorized as a critical risk, the asset valuation is $100,000 with an exposure factor of 85%. The Single Loss Expectancy (SLE) is $85,000, and the Annual Rate of Occurrence (ARO) is 12, leading to an Annualized Loss Expectancy (ALE) pre-control of $1,020,000. After implementing control measures with an Annualized Control Cost (ACC) of $50,000, the ARO reduces to 10, and the ALE post-control drops to $850,000. This results in a positive Cost Benefit Analysis (CBA) of $120,000. Given these findings, it is recommended to continue with the current control measures and consider further investments to reduce the ARO below 10, if feasible, to minimize the risk even more (Beresniak et al, 2016).

In contrast, the TV 2 asset, identified as a critical risk, has an asset valuation of $90 with a 90% exposure factor. The SLE is $81, and the ARO is 0.9, resulting in an ALE pre-control of $72.9. The implemented controls cost $81 annually, but the ARO post-control escalates to 81, causing the ALE post-control to rise to $6,561. This leads to a negative CBA of -$6,569.1. Therefore, it is recommended to discontinue these ineffective control measures and instead focus on maintaining basic protective measures along with regular monitoring to ensure the risk remains minimal (Wang et al, 2021).

By following these recommendations, the organization can ensure a balanced approach to managing risks, focusing on cost-effective measures and maintaining the security of critical assets.

3.3 Analysis and recommendations for employee data in HR (TV1)

TV1 has a higher risk value than TV2, however, the cost of benefit of TV1 is lower than TV2 while the risk priority is less important to the organisation. Outdated anti-malware software poses a critical risk to HR, increasing the likelihood of phishing attacks on sensitive employee records. These records contain personal information, job details, and potentially sensitive HR concerns, making them high-value targets. The high risk of phishing attacks, with an Annualized Rate of Occurrence (ARO) of 24 and an Exposure Factor (EF) of 50%, could lead to significant data breaches, identity theft, and operational disruptions. Upgrading to modern internet security software is a crucial mitigation strategy. This software effectively detects and blocks phishing attempts, significantly reducing the frequency and severity of attacks. With a $20,000 annualized cost, the new software can lower the Annualized Loss Expectancy (ALE) from $600,000 to $12,500, offering a substantial cost-benefit advantage.

Plan of Action and Future Considerations

The immediate action is to install the latest internet security software to protect HR systems from phishing attempts. Continuous monitoring is essential, with regular updates and patches to address new threats. Staff should receive ongoing phishing awareness training to recognize and report phishing attempts. Regular security audits will help evaluate the effectiveness of the security software and make necessary adjustments. As cyber threats evolve, reviewing and updating security measures is crucial. To enhance overall protection, the company should consider implementing multilayered security approaches, such as email filtering, two-factor authentication, and advanced threat detection technologies.

3.4 Analysis and recommendations for employee data in Finance Database (TV3)

TV3 has the lowest risk value and the lowest cost-benefit. Despite the fact that the Finance Database (TV3) contains the lowest ARO value in the table, it is highly recommended to re-evaluate the risk every once in a years. In our analysis, section 2.1 shows a minor level of likelihood and risk value, while the ARO values of pre-control and post-control in section 2.2 shows a slight difference, from 0.1 to 0.08.Therefore, the company may renounce the improvement this time in order to have a better use of money, such as to enhance Diagnostic Imaging Data's (TV4) weakness with very high ALE and bring a higher cost benefit to the company.

Considering millions of financial transactions take place in the global financial community every day, risk management analysts and financial practitioners must constantly learn new things to improve their knowledge and concentrate on effectively analysing risk (Ahmed et al., 2022). Therefore, the importance of financial data should not be ignoed, and secondly, periodic re-evaluating of the risk could effectively prevent peer-virulent price competition due to financial assets leaking unexpectedly, as well as ensure that the organisation remains aware of its overall security strength.

4 Teamwork Reflection

4.1.1 What your group thought worked well?

- **Effective Communication and Task Distribution:**
  Several essential variables contributed to our group's high level of collaboration. First, open and constant communication via group chats and video conversations kept everyone informed and enabled speedy problem resolution, resulting in a collaborative atmosphere. Second, job distribution was based on each member's capabilities, with analytical duties allocated to those with strong analytical skills and writing assignments assigned to those with outstanding writing talents, resulting in high-quality work and rapid task completion.

- **Structured Meetings and Effective Teamwork:**

  we had organized meetings twice a week with specific topics to keep our conversations focused and effective. Meeting minutes were distributed to ensure that everyone was informed of choices and duties. The group displayed good teamwork and mutual support, with members eager to assist one another, ensuring no one felt overwhelmed and improving our team relationships and efficiency.

4.1.2 What your group thought did not work well or was the least effective aspect of your group's teamwork?

- **Challenges in Coordinating Meeting Times:**

One of the major challenges we faced in our group's teamwork was coordinating meeting times. Given that we all had different schedules and were quite busy with our respective courses, finding a common time for discussions and collaboration was extremely difficult. Additionally, there was the problem of distance. To address this issue, we could implement early planning by scheduling regular meetings well in advance to ensure that everyone can accommodate these into their schedules.

- **Solutions for Effective Collaboration:**

  Utilizing online collaboration tools such as Zoom, Microsoft Teams, or Google Meet would allow for virtual meetings when in-person meetings are not feasible. We could also make use of asynchronous collaboration through shared documents and communication platforms like my.sharepoint, allowing for continuous and flexible collaboration, even if we can't meet at the same time. Finally, setting clear deadlines and responsibilities for each team member would ensure that progress is made consistently, even outside of meetings. By incorporating these strategies, we can improve our coordination and enhance the effectiveness of our teamwork.

4.1.3 What did your group learn that could be used to improve group effectiveness/group dynamics in the future?

- **At least one member participates in each week's tutorial :**

  As we mentioned before, travelling to the university and going to classes regularly are difficulties for group members who are staying in a faraway place from the campus. As a result, in order to guarantee our study performance and efficiency are maintained, it is important that we have a group member attend the tutorial every week, note key critical points to share with the whole group after the class, and clarify each question from last week. Finally, by doing so, we could ensure our team does not miss any crucial information due to travel difficulties or unexpected events like a cat bite leading to a serious infection.

- **Real-time study & chill together:**

  Face-to-face study with team members can improve our study efficiency, and relaxing together can further bring dynamics to the group. During this semester, we study together after classes and exchange our knowledge separately to help each team member have a better understanding of class details. Additionally, we found that not only studying but also chilling out together could encourage our motivation to get better study performance when we know each other well. Therefore, we often dine together after a long day of study with some of our members, which effectively helps us relieve stress.

5 References

Academic report writing: Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1), 146–146. https://doi.org/10.1186/s12911-020-01161-7

Ahmed, A. a. A., Rajesh, S., Lohana, S., Ray, S., Maroor, J. P., & Naved, M. (2022). Using machine learning and data mining to evaluate modern financial management techniques. In *Smart innovation, systems and technologies* (pp. 249–257). https://doi.org/10.1007/978-981-19-0108-9_26

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*, 102490–102490. https://doi.org/10.1016/j.cose.2021.102490

Beresniak, A., Schmidt, A., Proeve, J., Bolanos, E., Patel, N., Ammour, N., Sundgren, M., Ericson, M., Karakoyun, T., Coorevits, P., Kalra, D., De Moor, G., & Dupont, D. (2016). Cost-benefit assessment of using electronic health records data for clinical research versus current practices: Contribution of the Electronic Health Records for Clinical Research (EHR4CR) European Project. *Contemporary Clinical Trials*, *46*, 85–91. https://doi.org/10.1016/j.cct.2015.11.011

Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. *Computers & Security*, *132*, 103364-. https://doi.org/10.1016/j.cose.2023.103364

Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. *Computers & Security*, *136*, 103489-. https://doi.org/10.1016/j.cose.2023.103489

Wang, Q., Xu, R., & Volkow, N. D. (2021). Increased risk of COVID-19 infection and mortality in people with mental disorders: analysis from electronic health records in the United States. *World Psychiatry*, *20*(1), 124–130. https://doi.org/10.1002/wps.20806