IT3070
Information Assurance and Security 3rd Year, 1st Semester

Risk Management Assignment

Student Name	IT Number
Gunasekara.W.M.W.A.G.T.N.A.(Leader)	IT21303548
Kokuhannadige.C.K.	IT21349188

Submitted to

Sri Lanka Institute of Information Technology

Table of Contents

01) Introduction

We imagine TC hospitals is our organization. It is a leading healthcare organization dedicated to providing exceptional patient care and advancing medical research. With a steadfast commitment to the well-being of our patients, we have become a trusted name in the healthcare industry. Our core mission revolves around the efficient management of critical information assets, ensuring the highest standards of security and confidentiality. In the modern healthcare landscape, information technology plays a crucial role in the delivery of patient care, administrative processes, and the overall functioning of hospitals. Hospital IT assets encompass a range of technological resources and strategies that are essential for safeguarding sensitive patient data, ensuring the integrity of healthcare systems, and protecting against cyber threats.

02) Risk Scenarios

2.1) Data breach exposures

2.2) Changing false data & destroy the data in CMS (Company Management System)

2.3) Phishing Attack for Financial Information and Financial records

2.4) Attacked by hacker or malware

2.5) An insider revealing critical information about the hospital for personal and financial gain

03) Allegro worksheet

3.1) Data breach exposures

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Medicines details		
	Area of Concern	Data breach exposures include medicines information		
	(1) Actor *Who would exploit the area of concern or threat?*	Internal staff member		
	(2) Means *How would the actor do it? What would they do?*	Internal staff members who might or might not be aware of the company rules and compliances might expose sensitive medicine data, which is also referred to as "insider data," to a third party.		
	(3) Motive *What is the actor's reason for doing it?*	deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure**	❑ **Destruction**	
		❑ **Modification**	❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Financial issues may arise if sensitive product data is available to outsiders and important product data is only accessible by authorized individuals.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value 1-10**	**Score**
If there is any accidental decrease in the monthly output of the firm, it will be a financial loss. In this regard, problems may arise between the parties concerned.	Reputation & Customer	8	6.0
	Financial	10	7.5

	when there has been a change in the product data in any way. Auditing and re-entering it involves significant labor	Productivity	8	6.0
		Safety & Health	4	3.0
	Government parties affiliated with the institution will take immediate legal action when Treasury Bill and bond data is accessed by outsiders.	Fines & Legal Penalties	8	6.0
		User Defined Impact Area	0	0
			Relative Risk Score	**28.5**

3.2) Changing false data & destroy the data in CMS

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk		Information Asset	Company Management system (CMS)		
		Area of Concern	Replace the false data with new data by changing the data and destroying the data.		
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Outside attacker		
		(2) Means *How would the actor do it? What would they do?*	Intruders can acquire account information, employee information, and other information by misleading the system if they manage to breach the firewalls and get access to the system. Afterward, alter the data.		
		(3) Motive *What is the actor's reason for doing it?*	deliberate		
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	The system will crash if the system administrator is not keeping an eye on it and is not aware of external risks from unauthorized users.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		

		Impact Area	Value 1-10	Score
	When employees' and company-related data is stolen through the company management system in the company, the employees lose trust in the company. Employees may be motivated to leave the firm and find another job	Reputation & Customer	6	4.5
		Financial	8	6
	Violating the agency's regulations on the exposure of sensitive client data and corporate data may subject the	Productivity	8	6
		Safety & Health	7	4.25
	The value of stolen products has a huge negative impact on the organization's finances and productivity.	Fines & Legal Penalties	7	4.25
		User Defined Impact Area	4	3.0
			Relative Risk Score	**28.0**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ Accept	❑ Defer	❑ Mitigate	❑ Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Data backup and recovery	Your data may occasionally be maliciously deleted in data breaches. Your data should be regularly backed up so that it can be quickly restored in the event of data loss, server failure, or even a natural disaster. To prevent you from losing crucial data, your IT staff should have automatic offsite backup solutions installed on a regular basis.
Protect portable devices	Flash drives, cell phones, tablets, and other portable electronics are simple targets for theft or loss. Ensure that portable devices have secure passwords, anti-theft software installed, and other security measures in place to ensure that only authorized users may access them.
Remote monitoring	Your network is continuously monitored through remote monitoring. You may collaborate with a managed IT services company to avoid having to hire IT personnel full-time to watch after your systems.

Maintain up-to-date security software	To prevent a security breach, it's crucial to take the appropriate steps. It is possible to buy security software and automate it to work continuously. To protect your company from data breaches, use firewalls, anti-virus software, and anti-spyware programs. Set things up appropriately by collaborating closely with a team or provider of internet security.

3.3) Network Failure

Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk / Threat	Information Asset	System Network		
	Area of Concern	Network failure		
	(1) Actor *Who would exploit the area of concern or threat?*	Network Administrator		
	(2) Means *How would the actor do it? What would they do?*	It can be a accident such as an employee pull a plug accidentally or network administrator misconfigured system intentionally.		
	(3) Motive *What is the actor's reason for doing it?*	Intentional or accidental		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	When a network failure happen attacker can pass through the protocols.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Reputation of the company will get lower after a network failure occurs because customers might have questionable image about the responsibilities of the company.	Reputation & Customer	7	1.75
	Financial	6	1.5
	Productivity	7	1.75

	Productivity will reduce since the employees of the company can not access to the computer system and	Safety & Health	0	0
	Company will have to face legal penalties if dissatisfied customer took legal action against the company.	Fines & Legal Penalties	4	1
		User Defined Impact Area	0	0
			Relative Risk Score	**6**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Monitoring	Network administrator should constantly pay attention for the network and so he can fix the performance issues before they happen. Network administrator can use network monitoring software and identify potential issues.
Remove incompatible devices	Most old equipment are not compatible with modern devices. Using incompatible devices can cause network failure because they are incompatible with other devices in the network. Getting rid of these incompatible devices gives the smooth flow to the rest of the network.
Backup power supply	Having a backup power supply will prevent network failures through the power cuts. Also plugging redundant devices into different power circuits can prevent an entire network failure.
Training employees and staff	Training employees can reduce the probability of accidental network failures. Company management can organize a workshop or seminar and inform the employees. As a example they can tell about areas that they should avoid when cleaning process and give basic knowledge about how hardware.

3.4) Attacked by hacker or malware

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk / Threat	Information Asset	Hospital Network		
	Area of Concern	Attacked by hacker or malware		
	(1) Actor *Who would exploit the area of concern or threat?*	Hackers who want the patient's record		
	(2) Means *How would the actor do it? What would they do?*	Using a DDOS attack tool or virus.		
	(3) Motive *What is the actor's reason for doing it?*	They can sell the patient's record and information to get money.		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	They can attack the hospital's network by DDOS or virus .And the hackers can make the backdoor when they break the hospital's network defense.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
The DDOS attack is made targeting the financial side. With this attack the system services might be blocked disrupting the hospital services. The related parties like insurance companies, patients might be agitated with the hospital which causes a decrease in reputation and patient confidence. Therefore, the risk caused is high.	Reputation & Customer Confidence	8	4
Since the attack is made to the online transaction data, money will be lost. And also, all related sides of the finance management system will also be affected. Therefore, the risk caused to this aspect is very high.	Financial	9	4.5

	Due to the attack, the financial services may not be available. And it might take a while to recover the system which will disrupt the daily routine of the hospital. Hence reducing productivity. Reduction of the productivity means the risk level is high.	Productivity	7	3.5
	Due to the attack, the finance aspect is affected, and the security is breached, this will lead to the downgrading of the overall safety and health of the hospital. Since one aspect is affected the risk value is average.	Safety & Health	5	2.5
	Without knowing the situation, the patient might take legal actions since their personal and confidential information has been revealed. The hospital will have to face fines & legal penalties up to a certain level because the hospital has somehow broken the data protection policy. Since these fines and penalties are unavoidable the risk level is 4.	Fines & Legal Penalties	4	2
		User Defined Impact Area	-	-
			Relative Risk Score	**16.5**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
hospital network server's room	We can update the physical firewalls in network gate way and router and choose a high-level security firewalls for a system.		

3.5) An insider revealing critical information about the hospital for personal and financial gain

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	All working systems		
	Area of Concern	All systems containing critical information of the hospital		
Threat	(1) Actor *Who would exploit the area of concern or threat?*	Internal employee		
	(2) Means *How would the actor do it? What would they do?*	Accessing the system with authorized credentials		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate. For personal and financial gain.		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Confidentiality is violated here. The internal employee is disclosing critical information and selling the information to interested parties.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** **75%**	❑ **Medium** **50%**	❑ **Low** **25%**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Once the words spread that information is sold to outsiders the patients and other related parties will be disappointed which will tarnish the reputation and the patient confidence. A financial loss is inevitable because every information sold is critical to the hospital.	Reputation & Customer	8	6
	Financial	8	6
Selling of information might lead to the upgrading of the system which will interrupt the normal activities of the hospital and cause the decrease in productivity.	Productivity	7	5
	Safety & Health	6	4.5
	Fines & Legal Penalties	2	1.5

	After mistaking the situation, related parties could file a lawsuit.	User Defined Impact Area	-	-
			Relative Risk Score	**23**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Software	They are applying access controls to authenticate personnel and grant them access to and use information authorized for their use.
Hardware	Implement policies to prevent employees from using removable devices, which will make it hard for them to copy information.

04) Justifications and probability values

04.1) Data breach exposures

Attribute	Value	Justification
Probability	75%	Probability is in high level, because the company is not aware and not monitoring the emails, or any unauthorized accesses coming from the inside attackers or intruders. Emails received from outside cannot be controlled because the outside emails directly coming without permission. Monitoring tools or methods to check e-mail and external attack content and sizes are not activated in this scenario. At that time, company employees would use portable or flash devices to get data backups from computers. Furthermore, at that moment staff members have permission to utilize cloud storage. The risk of data loss is very high considering data is uncontrollable in the event of a breach.

04.2) Changing false data & destroy the data in CMS

Attribute	Value	Justification
Probability	75%	If company is not monitoring or not checking the company management system daily and regularly, unauthorized access can be able to do anything (replacing, changing, adding new details and many more) in the system, if this data gets into a wrong person, and specially an unauthorized access, that will be a huge problem for the company management system and as well as the company employees. That unauthorized access can do privacy compromised, identities stolen, or fraud committed in their names in the system. And when trade secrets, intellectual property, and other sensitive company data get into the wrong hands, the company or business must suffer from a huge loss of a competitive edge. An absence of controls and employee errors or mistakes are potential causes that will go to a company management system to collapse. Because of these reasons the probability is high and risky.

04.3) **Phishing Attack for Financial Information and Financial records**

Attribute	Value	Justification
Probability	25%	Since this was not a deliberate attack and most likely accidental incident there is low probability of occurring a network failure.

04.4) Attacked by hacker or malware

Attribute	Value	Justification
Probability	50%	The risk level for an attack like this is high and the necessary security measures must have been taken by the management. As the attack was successful the security system is not strong enough to protect the system. Although, the systems are upgraded after the situation, there is a possibility of this

		happening again. So, the probability is moderate.

04.5) An insider revealing critical information about the hospital for personal and financial gain

Attribute	Value	Justification
Probability	75%	Since the insiders have authorized access to inside information the probability of an internal employee revealing critical information is very high.

05) References

- https://lecturecapture.sliit.lk/eplayer.php?id=ZkN0bURkUFpISl81OTgzMA==
- https://courseweb.sliit.lk/mod/resource/view.php?id=243135
- https://courseweb.sliit.lk/mod/resource/view.php?id=249686
- https://satoricyber.com/glossary/data-exposure/#:~:text=Data%20Breach,external%20entity%20accessing%20the%20data.
- https://dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/
- https://www.malwarebytes.com/malware