Risk Management Assignment

Toronto General Hospital

**l200 Elizabeth St, Toronto, ON M5G 2C4,
Canada**

OCTOMBER 2022

Sri Lanka Institute of Information Technology

Information Assurance & Security (IT3070)

Group Assignment

Y3.S2.WE.IT.1.01

Group Members

Mayadunne J.N.A	IT20020958
Withana W.D.T.S.J	IT20062392

Contents

1.0 Allegro worksheets 1

1.1 Med-Jacking........ 1

1.2 Insider Attack........ 3

1.3 Ransomware........ 5

1.4 SPEAR Phishing Attack 7

1.5 DDoS Attack........ 9

2.0 References........ 12

1.0 Allegro worksheets

1.1 Med-Jacking

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**
Information Asset Risk	Threat	Information Asset	Respirators from General Electric, blood gas analyzers, X-ray machines, PET scanners, CT scanners, MRI machines, and anesthetic devices.
		Area of Concern	*A sort of cyber-attack is a medical device hijack, or "med jack."* *They concentrate on a hospital's medical equipment as a point of weakness.*
		(1) Actor *Who would exploit the area of concern or threat?*	User External party
		(2) Means *How would the actor do it? What would they do?*	Due to hospital medical equipment' malware or an exploit of the med-devices' malware, which opens a backdoor to the hospital's private data and allows the intruder to move laterally through networks,
		(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?*	Only the Authorized Staff members should be able to access the data that generate from the medical devices and also access the confidential data.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	□ **High** ✓ **Medium** □ **Low**

	(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**
	Exposing medical payments made by patients to outsiders.	Reputation & Customer Confidence	7	3.5
		Financial	6	3

	These documents contain information about the patient's calls, their illnesses, their treatments, scan results, etc. These two documents include very sensitive information that is crucial to patients and healthcare employees.	Productivity	8	4
		Safety & Health	8	4
	If something happens to the patients because of the modified data records, the reputation of the hospital will be ruined.	Fines & Legal Penalties	5	2.5
		User Defined Impact Area	0	0
			Relative Risk Score	**17**

(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?*
Ensuring authorized access to records	Authorized hospital employees should have access to record, and staff members should be knowledgeable about the security state of the devices. If staff members see any illegal activity, they should be instructed as quickly as feasible in the next measures to take.
Keep backup Recodes of the devices	Keep records of the device's security state as well as its functionality so that we may learn more about it and utilize it in the future to secure it.
Ensure All the med-devises	All medical equipment must be handled by an authorized individual with adequate paperwork, checked daily or weekly, and kept up to date with recodes and random machine inspections to guarantee security status.

Justification of probability

Attribute	Value	Justification
Probability	Medium (50%)	The Probability medical devices are in medium level Since it contains sensitive data related to internal administration of the hospital. if an attack occurs it can be led to Data disclosure, Health impacts. Reputation damage, Unauthorized data modification

1.2 Insider Attack

Allegro - Worksheet 10			**INFORMATION ASSET RISK WORKSHEET**
Information Asset Risk	Threat	Information Asset	Infrastructure-wide computers, nursing stations with patient records
		Area of Concern	*The malware takes down and disables vital hospital systems by building a botnet and uploading it on hard drives.*
		(1) Actor *Who would exploit the area of concern or threat?*	Interns staff members, visitors, authorized persons or patients
		(2) Means *How would the actor do it? What would they do?*	The hospital system can be used by internal workers to build a botnet. By uploading malware to the network and computers, nursing homes, and HVAC systems. The assailant may set up He even entered the hospital's network and is now able to publish the information.
		(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?*	Only the Authorized Staff members should be able to access the hospital system and computers.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High** □ **Medium** □ **Low**

(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**
In the event that this system is compromised, all employee information will be made public to third parties.	Reputation & Customer Confidence	9	6.75
	Financial	6	4.5
If the HRM System gets attacked, it may affect the productivity level of the hospital and affecting to medicines patient also have to struggle So, it may affect the hospital existence	Productivity	7	5.25
	Safety & Health	8	6
If have rebuild the system or improving cost will high cost will be high	Fines & Legal Penalties	8	6
	User Defined Impact Area	0	0
		Relative Risk Score	28.5

(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?*
Enable firewall, installing antivirus, Anti-Phishing and endpoint security.	Installing antivirus, anti-Phishing software, and safe end point protection on the network and the machines. Enabling the firewall. and make sure all the security tools and techniques are current. anti-Phishing It is advisable to install programs like *BrandShield* Anti-Phishing. These tools provide notifications and can identify bogus emails.
Keep Backup Data and Network	The hospital must have a backup system available because the information and networks are highly important. Situations like these can be sorted using a backup system. then everything may go immediately.
Proper maintains of rules which are followed by users	Establishing and maintain rules for all those working in the hospital. The capacity to provide training on internet security and cyber-attacks will increase productivity. These actions will stop employees from taking unauthorized activity for their own benefit and will result in staff discipline.

Justification of probability

Attribute	Value	Justification
Probability	High (75%	Given that the inside personnel have unrestricted access to the facility, the likelihood of an insider attack might be very high. Given that medical gadgets are essential resources for a hospital, this could pose a threat to them, which would have a significant impact.

1.3 Ransomware

Allegro - Worksheet 10			**Information Asset Risk Worksheet**
Information Asset Risk	Threat	Information Asset	Computers, diagnostic tools, and a personal and medical information file
		Area of Concern	*The hackers were able to infiltrate hospital systems by taking advantage of a Windows vulnerability.*
		(1) Actor *Who would exploit the area of concern or threat?*	Attacker
		(2) Means *How would the actor do it? What would they do?*	Through the use of out-of-date JBoss server software, the attacker uploaded malware to the hospital systems through staff members' regular workstations.
		(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 patient's medical and other information is only accessible to authorized staff members and the relevant patient.
		(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High** □ **Medium** □ **Low**

	(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**
	When it comes to recovering access to files and networks, as well as if diagnostic equipment is damaged and needs to be repaired, significant network and system damage, as well as data loss, can result in enormous expenses.	Reputation & Customer Confidence	6	4.5
		Financial	9	6.75
	The daily staff workstation may be destroyed and rendered inoperable during the attack; as a result, the hospital's network will no longer be able to access daily data, which will reduce the hospital's productivity.	Productivity	8	6
		Safety & Health	4	3
	The hospital will incur significant costs if it needs to file a lawsuit due to security concerns, threats, or attacks.	Fines & Legal Penalties	7	5.25
		User Defined Impact Area	0	0
			Relative Risk Score	25.5

(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?*
Having a backup network	In order to prevent the assault from completely disrupting the work done via a computer network and to allow hospitals to continue providing some level of customer service, the hospital should have a backup network or computer system available.
Activate endpoint security, firewall, and antivirus	On the hospital's network, install a reliable antivirus program and firewall, and make sure they're current. It's crucial to set up a powerful firewall and keep your security software updated.

maintain data backups	Ensure that your most important data is regularly backed up so that you can always recover any impacted files from a known-good backup. Restoring your files from a backup is the fastest way to get back in touch with your data. Due to this, we may restore the backup data, lessen certain really risks, and decrease the likelihood of total data loss.

Justification of probability

Attribute	Value	Justification
probability	High (75%)	As they interfere with computers and gadgets that are meant to target critical medical data and diagnostic instruments, these attacks raise the possibility of a ransomware attack. If we evaluate its effect, it is considerable since extortion software hurts hospitals by 75%.

1.4 SPEAR Phishing Attack

Allegro - Worksheet 10			**Information Asset Risk Worksheet**
Information Asset Risk	**Threat**	Information Asset	Computer networks and medical computers of the Hospital
		Area of Concern	*Through social media and email, an attacker distributes vulnerable links or files to its targets.*
		(1) Actor *Who would exploit the area of concern or threat?*	Through email or social media, an attacker sends victims unsecure attachments or links.
		(2) Means *How would the actor do it? What would they do?*	When a hospital employee opens a virus-filled email sent by the attacker, the entire hospital network or hospital computers can get infected, erasing all confidential data and possibly crashing the network.
		(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?*	Access to hospital computer data, which may be modified or removed, is restricted to unauthorised parties and only permitted hospital staff personnel can access it.		
(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium**	✓ **Low**

(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**
If the network was disrupted by the assault and all the data was destroyed, the network and computers would need to be rebuilt, which would cost the hospital a lot of money.	Reputation & Customer Confidence	7	1.75
	Financial	6	1.5
Computers slow down and interfere with routine actions that are carried out across the network when the system, network, and computers are disturbed. This may lead to a lower productivity of the entire hospital staff	Productivity	8	2
	Safety & Health	5	1.25
If the hospital needs to take legal action about security, threat, and assault, that procedure will cost the hospital a significant number of investors. when Attacker tries to trick the user, attacker has to do some investigation about the victim, then he will ended up with victims sensitive information's.	Fines & Legal Penalties	6	1.5
	Employees Privacy	4	1
		Relative Risk Score	9

(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?*

Educate hospital workers about phishing attacks.	It is crucial to educate staff members about the many sorts of phishing attacks and the security precautions they may take if they come under this kind of assault. This will assist to prevent some serious harm that phishing attacks can do.
Data entry personnel	Establish a division of labor such that one group of the data entry staff enters the data while another checks to see if the values correspond to the hospital charts. Collusion would still occur, but doing this would lessen the likelihood of it happening.
equip network PCs with anti-phishing softwares.	Installing anti-phishing software will enable us to prevent phishing assaults on our PCs or network. These tools will alert staff members if they received a fraudulent email before they click on the email or any other phishing sites.

Justification of probability

Attribute	Value	Justification
Probability	Medium (50%)	Since Phishing attacks take down the whole hospital network and computers, their chance is high. Given that hospitals suffer a 50% loss as a result of phishing assaults, the impact will be substantial.

1.5 DDoS Attack

Allegro - Worksheet 10			INFORMATION ASSET RISK WORKSHEET
Information Asset Risk	Threat	Information Asset	HRM, Drug Distributing System, LIS, Emergency Medical Service System
		Area of Concern	*DDoS attacks against the hospital's online services occur regularly via the hospital website.*
		(1) Actor *Who would exploit the area of concern or threat?*	Attacker
		(2) Means *How would the actor do it? What would they do?*	Denial of service (DoS) attacks include distributed denial of service (DDoS) attacks as a subclass. A botnet, or group of interconnected online devices, is used in a DDoS assault to

	flood a target website with fictitious traffic. This traffic may lead to the unavailability of the hospital's system.
(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?*	Patients should be able to access online services of the hospital.
(6) Probability *What is the likelihood that this threat scenario could occur?*	✓ **High** ✓ **Medium** ❑ **Low**

(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**
Customers attempting to use the hospital website to check their appointments, channeling details, doctors' details, and other information related to their condition will be unable to do so because the hospital server This will result in cost loss and a bad reputation for the hospital.	Reputation & Customer Confidence	6	3
	Financial	7	3.5
After the assault, the hospital must rebuild or restore all the data that was destroyed due to the attack; this can have a significant financial impact on the hospital. Additionally, productivity won't resume until servers	Productivity	4	2
	Safety & Health	2	1
If the online services provide by the hospital not accessible to the patient it'll affected to the existence of the hospital.	Fines & Legal Penalties	5	2.5
	Availability of the Services	9	4.5
		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?*
Deploy Firewalls for Sophisticated Application attacks	Additionally, due to the unique nature of these attacks, you should be able to easily create customized mitigations against illegitimate requests which could have characteristics like disguising as good traffic or coming from bad IPs, unexpected geographies, etc.
Backups and Alternatives	Always have a backup server or connection method ready to serve consumers in case the primary server or website is attacked.
Rate Limiting	Limiting the number of patients requests a server will accept over a certain time.

Justification of probability

Attribute	Value	Justification
Probability	Medium (50%)	DDoS assaults will be 50% more harmful to the hospital because they may interrupt internet access there, but since daily operations will still go on, they won't completely stop.

2.0 References

Types of Information Systems Used in Healthcare Facilities

Toronto General Hospital - University Health Network

DDoS Mitigation Techniques

Insider Threat | Malicious Insider

cyber hijacking