IT3070

Information Assurance & Security

3rd Year 1st Semester

Risk management assignment – 2023

Registration Number	Name
IT21291500	Premajayantha W.H.S.I
IT21290992	Manamperi R.S

Table Of Contents

1 Company Overview

This section contains example worksheets from an assessment of the NIBM Campus. NIBM Campus has a vision and mission. The vision is to be the best education institute in Sri Lanka. The mission of the NIBM Campus, “We are in the business of developing competencies in people and organizations through training and consultancy”. Through its emphasis on teaching, learning, and training, the College imparts knowledge and skills to promote human growth and opportunity, promote economic growth and competitiveness, and increase living standards. This example helps the reader understand the assessment process by showing how the Octavia Allegro worksheets seem after they are done.

This assessment does not, for example, include a danger questionnaire that has been filled out, but it does cover three crucial factors in identifying information risk that impacts the availability and continuity of systems and data. It includes an example of a strategy that may be used to lessen the real risks and associated problems. The evaluation as stated takes into account the three critical factors that impact the secrecy and integrity of such systems and data, as well as the availability of information that creates the risk, but another example leaves out the answers to the danger questionnaire. The risks are therefore assessed by taking into account the questionnaire for consideration in the questionnaire and the probability factors connected with the hazards faced while creating mitigation techniques.

2 Risk Scenarios

2.1 Data breach of student and Academic staff

2.1.1 Allegro Worksheet

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Information Asset	Academic Staff Database, Students Database	
	Area of Concern	Unsecured database	
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Cybercriminals
		(2) Means *How would the actor do it? What would they do?*	• Phishing Cybercriminals may send phishing emails with harmful links or attachments to NIBM Campus staff members or students. Malware is downloaded to the recipient's computer when they open a malicious attachment or click on a malicious link. The virus may then be used to steal information from the student database and the NIBM Campus network. • SQL injection SQL injection is a sort of attack that takes advantage of holes in SQL databases. To steal data or alter the database, cybercriminals might insert malicious SQL code into a database query.
		(3) Motive *What is the actor's reason for doing it?*	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?*	Encrypting data while it is in use and in transit, using strict access restrictions, updating software often, and putting in place a firewall and intrusion detection system are a few technological security methods that may be used. A security policy should be created and put into place, staff members should be trained on security best practices, and the security policy and training programs should be reviewed and updated on a regular basis. Data backup procedures, environmental controls, and safe data storage are all examples of physical security measures.		
		(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**
In addition to safeguarding the university's image, it is the university's duty to look into any publication of student information that poses significant harm to that institution's reputation. Alternatively, the kids can be scared to go to college.	Reputation & Customer Confidence	9	6.75
	Financial	9	6.75
It might take several hours of labor to investigate data breaches. If parents sue the university over a data breach affecting a student, the university will have to pay for legal defense and any associated costs.	Productivity	7	5.25
	Fines & Legal Penalties	8	6
	Identify theft and fraud	7	5.25
	Emotional distress for students, academic staff and families	9	6.75
		Relative Risk Score	**36.75**

2.1.2 Risk Mitigation

(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?*		
Security awareness Training	Security awareness training teaches employees how to identify and avoid cyberattacks.		
Strong Access Control	Only those who require access should be able to access information systems and data, according to access restrictions. A secure area with access control should be used to store the student and staff database server.		
Security Patching	Regular software patches should be applied to fix known vulnerabilities.		
Network Security	Firewalls and intrusion detection systems are examples of network security mechanisms that can assist defend against attacks.		
Incident Response Plan	To handle security problems, organizations should have an incident response strategy in place.		

2.1.3 Justification of probability and Severity values

2. Attribute	Value	Justification
(6) Probability	75 %	The possibility of a data breach is significant because to the rise in the quantity and sophistication of assaults, the volume and value of data, the rising reliance on technology, and the human element. Due to its lack of resources, reputation as an easy target, and the storage of sensitive data in student databases, the education industry is particularly susceptible to data breaches.
Reputation & Customer Confidence	9	A data breach may harm a company's reputation in a variety of different ways. First off, it demonstrates that the company hasn't taken enough precautions to safeguard the data of its clients. Customers may lose faith in the company as a result and be less likely to do business with it in the future. (9/10)
Financial	9	A critical danger that might have catastrophic repercussions for an institution is a student database leak. A data breach can result in large financial losses, and the organization might also be subject to regulatory fines and penalties. Families and students may go through emotional hardship, and their identities could be taken and used fraudulently. Additionally, the reputation of the school can suffer, making it challenging to recruit and keep teachers, staff, and students. (9/10)
Productivity	7	Numerous factors might have an impact on productivity. As they deal with the fallout from a hack, such as resetting passwords and checking credit reports, employees could become distracted and less productive. They could also be less willing to experiment or take chances out of concern that a mistake could result in yet another violation. That could hinder originality and creativity. Additionally, if workers believe their company is not doing enough to secure personal data, they may be less engaged and dedicated at work. Lower morale and increased turnover rates may result from this. (7/10)
Fines & Legal Penalties	8	Organizations who fail to secure the data of their consumers are becoming subject to hefty fines and penalties from regulatory bodies throughout the world. Organizations may be subject to civil claims from people whose data was stolen in a data breach in addition to regulatory sanctions. If the data breach caused considerable monetary or emotional injury to someone, these cases may result in hefty damages judgments. (8/10)
Identify theft and fraud	7	Both people and businesses may be significantly impacted by data breaches. The potential of identity theft and fraud is among the most catastrophic effects of a data breach. Criminals may get sensitive personal data, including names, Social Security numbers, credit card numbers, and bank account details, when there is a data breach. The use of this information can then be made for fraud and identity theft. (7/10)
Emotional distress for	9	The rating of 9 for emotional distress for students, faculty, and families highlights the severe negative effects that a data breach can have on people

students, academic staff and families		affecter's mental and emotional health. (9/10)

2.2 Unauthorized access to financial system

2.2.1 Allegro Worksheet

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Threat	Information Asset	Financial System
		Area of Concern	Unauthorized access to financial system
		(1) Actor *Who would exploit the area of concern or threat?*	Cybercriminals
		(2) Means *How would the actor do it? What would they do?*	• Social Engineering Social engineering is a sort of attack where the attacker takes advantage of psychological vulnerabilities in people to access data or systems. An attacker may, for instance, phone a customer service agent and claim to be a client. The attacker could next attempt to dupe the customer service agent into providing them with access to their account information. • Exploiting Vulnerabilities Vulnerabilities are flaws in software or systems that attackers can use to obtain unauthorized access. To identify and take advantage of weaknesses in financial systems, attackers may employ a range of instruments and methods.
		(3) Motive *What is the actor's reason for doing it?*	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?*	Strong security measures, including firewalls, intrusion detection systems, and access restrictions, should be used to safeguard the financial system. The best practices for cybersecurity should be taught to employees. If there is a data breach, the company should have a strategy in place on how to handle it.		
		(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 Damage	9	4.5
	Financial	9	4.5
	Productivity	7	3.5
	Fines & Legal Penalties	9	4.5
	Identify theft and fraud	9	4.5
	Increase costs of cyber security	8	4
	Relative Risk Score		**25.5**

2.2.2 Risk Mitigation

(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?*		
Implement strong security controls	By preventing hostile traffic and spotting unusual behavior, firewalls and intrusion detection systems can help safeguard the financial system from unwanted access. You may limit who has access to the financial system and what they can do there by using access controls. When sensitive data is stolen, encryption can be used to prevent access to it.		
Educate employees on cybersecurity best practices	The weakest link in the security chain is frequently employees. Attackers frequently use phishing emails to penetrate banking systems. Employees must get training on recognizing and avoiding phishing emails. Additionally, training should cover how to generate secure passwords and update software for employees.		
Implement multi-factor authentication	Multi-factor authentication (MFA), which requires users to provide two or more factors, such as a password and a one-time code, in order to log in, adds an additional layer of protection to the login process.		
Use security information and event management (SIEM) tools	SIEM technologies can aid in keeping an eye out for shady behavior in the financial sector. SIEM technologies can spot trends and abnormalities that can point to an active assault.		
Conduct regular security assessments	Security evaluations can assist in locating financial system flaws that attackers might try to exploit.		

2.2.3 Justification of probability and Severity values

2. Attribute	Value	Justification
(6) Probability	50 %	A critical danger that might have an enormous effect on a company and its clients is unauthorized access to a financial system. Financial losses, identity theft, reputational harm, regulatory fines and penalties, and legal responsibility are just a few of the effects of illegal access. The complexity of financial systems, the value of the data contained in financial systems, and the level of expertise of attackers are a few variables that might increase the danger of unauthorized access to a financial system. By implementing the necessary security precautions, the possibility of illegal access to a financial system can be decreased despite its medium likelihood.
Reputation Damage	9	Unauthorized access to a financial system has a reputational harm value of 9 since it may significantly affect both a business and its clients. A financial institution's reputation and client confidence may suffer if it suffers a data breach. Customers may stop believing that the company would secure their data, which might result in a decline in business and revenue. Additionally, a data leak might harm a company's standing in the financial sector. The likelihood of other financial institutions doing business with a company that has experienced a data breach may be reduced. (9/10)
Financial	9	Unauthorized access to a financial system is classified as having a financial severity of 9 since it can seriously harm a company and its clients. Financial systems keep track of private information including bank account numbers, Social Security numbers, and credit card numbers. Attackers can use this information to perpetrate fraud, identity theft, and other crimes. It is very important to them. A data breach can also stop users from accessing their accounts or conducting transactions, causing a financial system to malfunction. Both the organization's reputation and financial results may suffer because of this. Additionally, firms could spend a lot of money on investigating and fixing data breaches, as well as warning clients and authorities. (9/10)
Productivity	7	Unauthorized access to a financial system has a loss of productivity value of 7 since it can significantly affect an organization's operations. Employees may be distracted from their job as a result of a data breach while they deal with the fallout, such as changing their passwords and checking their credit reports for fraudulent activity. supporting consumers who have been impacted by the data breach, such as supporting them in filing claims with their banks or credit card providers, may require employees to spend time on their end. Additionally, the company might need to put new security measures into place, which could include devoting time and resources away from other activities to train staff on cybersecurity best practices or update security software. (7/10)

Fines & Legal Penalties	9	Unauthorized access to a financial system has a fines and legal penalties value of 9 since it can seriously harm an organization's reputation and bottom line. A number of rules that are intended to safeguard consumer data and stop financial crimes are applicable to financial institutions. Regulators may impose fines and penalties on organizations that break these rules. Additionally, businesses may be obliged to pay settlements or damages judgments when they are sued by clients who have incurred monetary losses or other harm because of a data breach. (9/10)
Identify theft and fraud	9	Unauthorized access to a financial system has a rating of 9 for identity theft and fraud since it can seriously harm people's money. When someone obtains another person's personal data, such as their name, address, Social Security number, or credit card number, and uses it to conduct fraud or other crimes, this is known as identity theft and fraud. A data breach exposes people's personal information to attackers, increasing their risk of fraud and identity theft. Attackers may use this information to start new accounts, apply for loans, or make unlawful purchases in the victims' identities.(9/10)
Increase costs of cyber security	8	Because businesses must spend more security measures to shield their systems from increasingly complex assaults, the cost of cybersecurity for illegal access to a financial system has increased by 8. Because they store sensitive data like credit card numbers, Social Security numbers, and bank account information, financial systems are a top target for hackers. It is possible to perpetrate fraud, identity theft, and other crimes with this information. Organizations must invest in new and sophisticated security measures to protect themselves as attackers create new and sophisticated attack strategies. This can entail putting in place new security software, educating staff members about cybersecurity best practices, and employing security specialists. (8/10)

2.3 Denial-of-service attack

2.3.1 Allegro Worksheet

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Information Asset	Admin staff, Academic Staff, Students	
	Area of Concern	DOSS Attacks using botnets	
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Intruder who uses Botnets
		(2) Means *How would the actor do it? What would they do?*	• Flooding the target system with traffic The attacker might bombard the target system with many requests, overloading it and blocking access to reputable users. An instance of a volumetric DoS assault is this. Exploiting Vulnerabilities • Exploiting vulnerabilities in the target system. The attacker can utilize flaws in the hardware or software of the target system to make it crash or stop responding. An exploit-based DoS attack is what this is.
		(3) Motive *What is the actor's reason for doing it?*	Intentional
		(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?*	We must cooperate with our internet service provider (ISP) to supply clean bandwidth to our network in order to defend it against DDOS assaults. Potential DDOS packets may be identified and filtered away by ISPs before they reach your border, preventing

			such assaults from consuming up all of your bandwidth.		
		(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 &Customer Confidence	5	3.75
	Financial	8	6
	Productivity	3	2.25
	Fines & Legal Penalties	3	2.25
	Relative Risk Score		**14.25**

2.3.2 Risk Mitigation

(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?*		
Implement strong security controls	To do this, hostile traffic can be blocked using firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).		
Firewalls	A firewall is a piece of network security equipment that keeps an eye on and manages incoming and outgoing network traffic in accordance with pre-established security rules. Firewalls can aid in preventing harmful traffic from entering your network, such as traffic from well-known botnets.		
Intrusion detection systems (IDS)	A network security tool called IDS scans network traffic for irregular activities. DoS assaults are one type of attack that IDS systems can identify. An IDS can issue an alert after seeing an attack and then take action to stop it, such as blocking the attacker's IP address or dumping the malicious traffic.		
Intrusion prevention systems (IPS)	Like an IDS, an IPS may also take action to stop attacks from happening. An IPS, for instance, might delete malicious packets from an active connection or stop malicious data before it enters your network.		
Monitor your network for suspicious activity	This will help you to identify and respond to DoS attacks quickly.		
Network monitoring tools	You may use network monitoring software to find unusual activities on your network. Network monitoring tools, for instance, may examine traffic patterns and spot odd traffic spikes that can be a sign of a DoS assault.		
Security information and event management (SIEM) systems	Firewalls, IDS systems, and IPS systems are just a few examples of the security equipment that SIEM systems may gather and analyze data from. SIEM systems can assist you in recognizing and responding to sophisticated assaults, such as denial-of-service (DoS) attacks that may include several security devices.		
Have a plan in place to respond to a DoS attack	This strategy should include actions to lessen the effects of the assault and swiftly resume service to authorized users.		

2.3.3 Justification of probability and Severity values

2. Attribute	Value	Justification
(6) Probability	75 %	The likelihood is very high. Since one individual may seize control of the botnets and utterly wreck a system if the DDOS assault is successful. Sometimes it would be quite detrimental to the academic activity if it occurred during the online exam. A botnet may be managed by one person, momentarily taking down a whole system.
Reputation Damage	5	The reputation will suffer from this. If the website is disabled, students could start to question the accuracy of the information there. The website can enrage students as well. Therefore, the high effect value is given a rating of (5/10).
Financial	8	Specialists will need to be enlisted as soon as possible to deal with such an onslaught. Security measures must also be put in place to prevent similar problems from happening again. Consequently, an 8/10 high impact grade is given.
Productivity	3	As a result, the system will totally disintegrate. No one will be able to log in until the server is rebooted. such that neither academic employees nor administrative workers may access the webpage. As a result, the value is 3. (3/10)
Fines & Legal Penalties	3	The school must investigate the incident and take legal action against those involved if a course website has been attacked. Therefore, that school is required to pay for that expenditure. The result is a 3 out of 10 rating.

2.4 Ransomware attack on Critical Systems

2.4.1 Allegro Worksheet

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Information Asset	Critical Systems	
	Area of Concern	Ransomware attack	
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Criminal Organizations / Hacktivists
		(2) Means *How would the actor do it? What would they do?*	• Phishing emails Emails that are intended to deceive the receiver into clicking on a harmful link or opening a harmful attachment are known as phishing emails. Ransomware can be installed on the recipient's machine if they click the link or open the attachment. • Exploiting software vulnerabilities Attackers can access machines and set up ransomware by taking advantage of software flaws. Attackers may focus on well-known software flaws or they may create brand-new exploits. • Using brute-force attacks Attacks known as brute-force attempts include the attacker making guesses at a user's password. The attacker may be able to access the user's account and set up ransomware if they are successful. • Using social engineering Using deception, an attacker can fool a user into granting them access to a computer or network by using social

	engineering. For instance, to access a user's computer, an attacker may phone the user and claim to be from IT support.
(3) Motive *What is the actor's reason for doing it?*	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?*	The most popular means of ransomware defense are comprehensive antivirus and anti-malware programs. They are able to search, find, and react to online threats.
(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
Loss of access to critical data and systems	9	6.75
Financial losses due to downtime and ransom payments	8	6
Damage to reputation and customer confidence	8	6
Legal and regulatory compliance issues	7	5.25
Disruption to public safety and essential services	6	4.5
Environmental damage	5	3.75
Loss of life or injury	4	4
Relative Risk Score		**36.25**

2.4.2 Risk Mitigation

(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?*		
Regular software updates	Maintain the most recent versions of the operating system, programs, and firmware.		
Employee security awareness training	Inform staff members on best practices for cybersecurity, including how to spot and prevent phishing emails and social engineering con games.		
Regular data backups	Back up data regularly and store backups offsite.		
Network segmentation	If ransomware does penetrate the network, divide it into smaller areas to stop its growth.		
Incident response plan	Establish a plan for incident response that outlines the actions your company will take in the event of a ransomware attack.		
Cyber insurance	If you want to protect yourself from the financial damages brought on by a ransomware attack, think about getting cyber insurance.		

2.4.3 Justification of probability and Severity values

2. Attribute	Value	Justification
(6) Probability	75 %	Critical systems are a target of the increasingly widespread and sophisticated ransomware assaults. This is because vital systems are frequently crucial to an organization's ability to function, and a successful assault can result in serious disruption and monetary losses. Ransomware assaults are also quite lucrative, which makes them a very alluring offer for thieves.
Loss of access to critical data and systems	9	The loss of access to vital information and systems has a value of 9 because it might seriously harm a business. An organization's ability to operate is frequently dependent on critical systems, and without access to these systems, an organization may not be able to do so. Aside from the operational interruption brought on by the loss of access to vital data and systems, businesses may also suffer large financial losses. An organization could suffer financial losses, for instance, if it is unable to run its operations. Additionally, a company could need to pay a ransom to recover access to its data and systems.
Financial losses due to downtime and ransom payments	8	Downtime and ransom payments' financial losses have a rating of 8 because they can significantly affect an organization's bottom line. Downtime is the time that a company cannot conduct business as usual as a result of a ransomware assault.
Damage to reputation and customer confidence	8	An organization's capacity to draw in and keep consumers may be significantly impacted by reputational and customer confidence loss, which has a value of 8. Customers may lose faith in a company's capacity to secure their data if they find out it has been the target of a ransomware assault. Customers may decide to use rivals instead or stop doing business with the company as a result. An company may find it challenging to draw in new clients if its reputation has been tarnished. Businesses and people are becoming more hesitant to work with organizations that have been hacked, and they may be hesitant to provide these organizations access to their personal information.
Legal and regulatory compliance issues	7	Issues with legal and regulatory compliance have a rating of 7 because they can significantly affect an organization's finances and operational performance. Various rules and regulations that control the gathering, use, and storage of personal data are applicable to organizations in a wide range of industries. The attackers may access sensitive personal information including names, addresses, Social Security numbers, and credit card details if an enterprise falls victim to a ransomware assault. The organization can then be subject to fines, penalties, and other legal repercussions for breaking these rules and laws.

Disruption to public safety and essential services	6	The interruption of critical services and public safety gets a score of 6 because it may have a big impact on the community. Attacks by ransomware on vital infrastructure, such as water, power, and transportation networks, can interrupt vital services and jeopardize public safety. For instance, a power grid assault by ransomware might result in massive power outages, which would affect hospitals, emergency services, and other vital infrastructure. Water supply contamination from a ransomware assault on a water system might endanger the public's health. Additionally, a ransomware assault on a transportation system might obstruct public transit, making it impossible for individuals to go to their places of employment, attendance at school, and other crucial destinations.
Environmental damage	5	Due to its potential to significantly affect both the environment and human health, environmental harm has a rating of 5. Environmental harm can result from ransomware attacks on vital infrastructure including electricity grids, water systems, and transportation networks. For instance, a ransomware assault on a power infrastructure can cause pollution to be released into the air and water. Water contamination from a ransomware assault on a water infrastructure might cause algal blooms and other environmental issues. Additionally, if a transportation system is the target of a ransomware assault, it may be impossible for people to use public transit, which would increase traffic and air pollution.
Loss of life or injury	4	Because it is the most serious result of a ransomware assault, the loss of life or injury receives a value of 4. Attacks by ransomware on vital infrastructure, such hospitals, electricity grids, and water systems, may result in fatalities or serious injuries. For instance, a ransomware assault on a hospital might impede patient treatment, causing severe harm or even death. Hospitals and other vital services might lose power as a result of a ransomware assault on a power system, which could potentially result in fatalities or serious injuries. Additionally, a ransomware assault on a water system might contaminate the water supply, causing diseases spread through the water and other health issues that could result in death or injury.

2.5 Insider Threat

2.5.1 Allegro Worksheet

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET	
Information Asset Risk	Information Asset	Sensitive data (e.g., customer information, intellectual property, financial data)	
	Area of Concern	Insider access	
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	An employee / A Contractor / A third-party vendor
		(2) Means *How would the actor do it? What would they do?*	• Steal data. An insider attacker could take financial information, client information, or other sensitive data. The information might subsequently be sold to criminals, used as a form of extortion against the company, or made public. Exploiting software vulnerabilities • Espionage An insider attacker could spy on company operations and take trade secrets or other sensitive data. Then, a rival may receive this knowledge or utilize it to their advantage in the marketplace. • Sabotage systems An insider attacker may compromise an organization's systems by deleting or distorting data, putting malware on a system, or altering system settings. Operations may be disrupted, and financial losses may result.
		(3) Motive *What is the actor's reason for doing it?*	Financial gain, Revenge, Ideological beliefs

		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	To safeguard businesses from unauthorized access, information asset destruction, alteration, or interruption, security standards for insider assaults are crucial. Current or former workers, contractors, or even customers with authorized access to a company's systems and data are all potential perpetrators of insider assaults. Strong access restrictions must be implemented as one of the key security needs. This entails limiting employee access to the information and tools they require to carry out their tasks. Monitoring all access to critical systems and data for irregular behavior is also crucial.		
		(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 &Customer Confidence	9	4.5
	Financial losses	8	4
	Productivity	6	3
	Fines & Legal Penalties	7	3.5
	Employee Morale	6	3
	Relative Risk Score		**18**

2.5.2 Risk Mitigation

(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?*		
Implementing strong access controls	Employees should only be given access to the systems and data they require to do their jobs. Reduce employee privileges by using a zero-trust security strategy and keep an eye on who has access to what systems and data.		
Conducting background checks on all employees and contractors	To find any possible red flags, run background checks on all employees and contractors.		
Providing security awareness training to all employees:	All personnel should get security awareness training so they can see and report questionable activities. Insider threats, phishing scams, and social engineering attempts should all be included in this training.		
Having a plan in place to respond to insider attacks	Create an incident response strategy to deal with insider threats quickly and successfully. This strategy should involve actions to locate the perpetrator, minimize damage, and close the breach.		
Segregation of duties	Separate responsibilities so that no one worker has excessive authority over important systems or data.		
Auditing and logging	All user behavior should be audited and logged so that any questionable behavior may be found and looked into.		

2.5.3 Justification of probability and Severity values

2. Attribute	Value	Justification
(6) Probability	50 %	Insider assaults are rated as having a "medium" chance in many companies, which is indicative of how complicated and varied this danger is. Insider threats can originate from several sources and reasons, even though some firms have implemented security measures and staff training programs to reduce insider risks. While businesses have made measures to minimize insider dangers, a "medium" likelihood means that there may still be openings or weaknesses that might be potentially abused by nefarious insiders. Based on elements including the organization's industry, size, security culture, and prior experiences with insider events, the particular chance might vary greatly. Therefore, a "medium" evaluation is a sober admission that continued efforts and awareness are needed to successfully manage and lower the risk of insider assaults. To keep up with changing insider threat vectors, organizations should continuously assess and improve their security procedures.
Reputation &Customer Confidence	9	In the case of an insider assault, a score of 9 for Reputation & Customer Confidence indicates that these repercussions may be quite serious. The reason is that an insider assault jeopardizes sensitive information and systems while also undermining stakeholders' and partners' confidence. Customers' perceptions that their data or sensitive information has been misused or compromised can seriously harm a company's reputation. This harm frequently has long-lasting implications, which may include customer loss, legal repercussions, and challenges in regaining confidence. Such occurrences frequently attract media attention, which increases their impact and makes it difficult to quickly ameliorate them. A score of 9 demonstrates how crucial it is to protect an organization's image and consumer confidence in the face of insider threats.
Financial losses	8	An insider attack's grade of 8 for financial losses emphasizes the serious financial impact such attacks may have on businesses. The rationale is the high expenses involved in containing the attack, retrieving lost data, putting in place improved security measures, and maybe incurring legal repercussions and fines. Insider assaults can also impair corporate operations, causing downtime, lost productivity, and sometimes even a loss of income. Beyond immediate costs, there are long-term financial effects that have an impact on an organization's bottom line. The significant financial cost and possible economic strain that insider assaults may have on enterprises is shown by the rating of 8, which is 8.
Productivity	6	Insider attacks are given a productivity grade of 6, which means they might have a somewhat negative impact on an organization's overall productivity. This ranking is justified by the fact that, although while insider assaults can result in disruptions, downtime, and the need for additional resources for recovery and investigation, businesses frequently have safeguards in place to lessen some of these consequences. The impact might differ significantly

		depending on the type and scope of the assault, the organization's readiness, and its capacity for quick action. While temporary productivity loss is possible, efficient event response tactics may frequently make it bearable. Insider assaults, on the other hand, might cause lengthy and large productivity losses in more extreme situations, necessitating a moderate grade of 6 to emphasize their potential impact.
Fines & Legal Penalties	7	The potential for financial penalties and legal repercussions for organizations because of security breaches is represented by a grade of 7 for Fines & Legal Penalties in the context of an insider attack. The argument is that insider assaults frequently entail breaches of contract requirements to preserve sensitive information, industry standards, and data protection legislation. Regulatory bodies may apply fines and penalties when these violations occur, particularly in industries with rigorous compliance standards like healthcare or banking. Affected persons may also file legal actions against organizations seeking damages recompense. A grade of 7 indicates that, although the fines and punishments might vary, insider attack victims' organizations may face considerable and expensive legal repercussions.
Employee Morale	6	The possibility that insider attacks will have a moderate effect on an organization's overall morale is indicated by a rating of 6 for employee morale. The rationale for this is that insider assaults, especially when carried out by someone from within the firm, can foster a climate of mistrust and insecurity among personnel. Employee morale, job satisfaction, and productivity may suffer as a result. However, firms that have clear incident management procedures and good communication channels might lessen some of these adverse consequences. The morale may be affected, but it is controllable, and proactive actions may help resolve these issues and gradually create a happy work atmosphere again, according to the rating of 6.

3 References

[1] "Openlearn," The open university of England, [Online]. Available: https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems- computer/network-security/content-section-3.4 .

[2] "How Does data security?", netwrix.com, 2019. [Online]. Available: https://www.netwrix.com/data_security_best_practices.html [Accessed: 09- Sep2019]

[3] " Student Data Privacy Protection ", Netwrix blog, 2020. [Online]. Available: https://blog.netwrix.com/2019/09/24/student-data-privacy-protection-explained/ [Accessed: 09- Sep- 2019].

[4] "How to protect database from hackers?", vpnMentor.com, 2021. [Online]. Available: https://www.vpnmentor.com/blog/how-to-secure-website-database/ [Accessed: 08- Sep- 2019].

[5] "Database Security", IBM, 2019. [Online]. Available: https://www.ibm.com/cloud/learn/database-security#toc-why-is-it--VjZYsvf2 [Accessed:08- Sep- 2019].

[6] "How to prevent DDoS attacks?", Adminhacks.com, 2019. [Online]. Available:https://adminhacks.com/ddos-attacks.html. [Accessed: 08- Sep- 2019].

[7] " Ways to Protect Data from Natural Disasters", Stellerinfo, 2019 [Online]. Available: https://www.stellarinfo.com/blog/ways-to-protect-data-from-naturaldisasters/[Accessed: 09- Sep- 2019].

- Further reading

[1] 800 G Street, N.W., Suite 8-130 Washington D.C. 20006, Resources.hsdl.org, 2000.[Online]. Available:

https://www.hsdl.org/?view&did=997 [Accessed: 07- Sep2019].