ITC 3093: Computer Security

Assessment No. 1

Written Assignment (Case Study)

Assignment Instructions:

Read the following instructions carefully:

1. This is an individual assignment.
2. Perform all the tasks that are required on this assessment.
3. Please use the following formatting guidelines for submitting the completed assignment:
    i. Font Size : 12 or 14
    ii. Font Type : Times New Roman or Arial
    iii. Line space : 1.5
4. You must write your **name** and **student ID** on the cover page of your assignment.
5. You must complete each task on your own and you are encouraged to conduct your own research based on class or work exercises, hand-outs, notes, and external sources as a support tool.
6. Anything that is not your own work must be acknowledged through **referencing**. **Plagiarism** would be dealt with zero tolerance, and you would fail the assessment.
7. You must complete all tasks in clear and comprehensible English language.
8. Any student caught **cheating** will receive **zero** marks. If copying is identified, **all parties** will receive **zero** marks.

This assessment covers:

LO No.	Learning Outcomes	Possible Marks
1	Analyse the impact of security threats and different types of security risk on an organization's computing assets and information system operations	40%
2	Evaluate and explain the ethical, privacy and legal impacts on organisational information systems security decisions	10%

Instructions for the candidates

1. The assignment will contribute 20**%** towards the entire “Computer Security” paper.

2. This submission must meet the following requirements:

- Your assignment must be submitted using PDF format or any other format.
- All written components (including tables and figures with text) must be readable by Turnitin similarity software.
- Appendices, listed and attached at the end of the assignment.
- Times New Roman or Arial font with heading font size as 14 and body font size as 12
- Typing should be one space-and-a-half. Tables, bibliographies, and quotes should be single spaced.
- Correct spelling and appropriate use of grammar
- Detailed Bibliography
- Entire submission must be on Turnitin(online)
- Have margins and line indentation as 1.5.
- Pages numbered.
- Questions correctly labelled and numbered.

Assessment overview:

In this assignment, you will analyse the impact of security threats and different security risks on an organisation’s computing assets and information system operations.

Assessment Task:

Choose a common Organization of special interest to you. And create a report following the breakdown provide bellow.

Introduction (5 marks)

Assignment Title: Analysing the Impact of Security Threats and Different Types of Security Risks on an Organization's Computing Assets and Information System Operations.

(Modify the title to align with the selected organization.)

Overview: Security threats and risks are critical for any organisation that relies on computing assets and information systems operations. The growing sophistication of cyber-attacks and the increased dependence on technology has increased the risk of cyber threats for businesses of all sizes.

(Provide an overview aligned with the report. Highlighting the impacts of the security threats you have identified for the selected organization)

Task 1: Types of Security Threats and Risks (10 marks)

In this section, you will analyse the various security threats and risks the organisation faces. You should include the following points:

- Define security threats and risks.
- Differentiate between internal and external security threats.
- Identify common security threats, such as malware, phishing, ransomware, denial-of-service attacks, and social engineering.
- Analyse the impact of security threats on the organisation's computing assets and information system operations.

Task 2: Impact of Security Threats on the Organization (10 marks)

In this section, you will analyse the impact of security threats on the organisation's computing assets and information system operations. You should include the following points:

- Explain the consequences of a successful security breach, such as data loss, financial loss, reputational damage, and legal liability.
- Analyse the impact of security threats on the organisation's productivity, efficiency, and competitive advantage.
- Discuss the importance of contingency planning and incident response to minimise the impact of security threats.

Task 3: Mitigating Security Threats and Risks (10 marks)

In this section, you will analyse the strategies that organisation can implement to mitigate security threats and risks. You should include the following points:

- Identify the critical components of an effective security strategy, such as risk assessment, access control, encryption, and security awareness training.
- Discuss the importance of implementing security policies and procedures to mitigate security risks.
- Analyse the role of security technologies, such as firewalls, intrusion detection systems, and antivirus software, in mitigating security threats.
- Discuss the importance of continuously monitoring and updating security measures to ensure ongoing protection against evolving security threats.

Summarization :(5 marks)

Conclusion: In conclusion, the report should contain security and risks that significantly threaten the organisation's computing assets and information system operations. By understanding the different types of security threats and risks, analysing their impact on an organisation, and implementing effective mitigation strategies, organisations can reduce their exposure to security threats and minimise their effects. Restate what proactive security approach the organisation must take to protect their assets, operations, and reputation.

Formatting (5 marks)

APA (5 marks)

Marking Guideline

Criteria		Mark Allocated	Mark Obtained	Remarks
Introduction (5 marks)				
	Rationalise why security threats and risks are critical for any organisation.	2		
	Clarify the computing assets and information systems operations.	1		
	Justify the risk of cyber threats for businesses of all sizes.	2		
Task 1: Types of Security Threats and Risks (10 marks)				
	Analyse the various security threats and risks organisations face.	2		
	Define security threats and risks.	2		
	Differentiate between internal and external security threats.	2		
	Identify common security threats, such as malware, phishing, ransomware, denial-of-service attacks, and social engineering.	2		
	Analyse the impact of security threats on an organisation’s computing assets and information system operations.	2		
Task 2: Impact of Security Threats on an Organization (10 marks)				
	Analyse the impact of security threats on an organisation’s computing assets and information system operations.	2.5		
	Explain the consequences of a successful security breach, such as data loss, financial	2.5		

	loss, reputational damage, and legal liability.			
	Analyse the impact of security threats on an organisation's productivity, efficiency, and competitive advantage.	2.5		
	Discuss the importance of contingency planning and incident response to minimise the impact of security threats.	2.5		
Task 3: Mitigating Security Threats and Risks (10 marks)				
	Analyse the strategies that organisations can implement to mitigate security threats and risks.	2		
	Identify the critical components of an effective security strategy, such as risk assessment, access control, encryption, and security awareness training.	2		
	Discuss the importance of implementing security policies and procedures to mitigate security risks.	2		
	Analyse the role of security technologies, such as firewalls, intrusion detection systems, and antivirus software, in mitigating security threats.	2		
	Discuss the importance of continuously monitoring and updating security measures to ensure ongoing protection against evolving security threats.	2		
Conclusion (5 marks)				
	Summarise how security and risks significantly threaten an organisation’s computing assets and information system operations.	2		

	Why organisations must take a proactive security approach to protect their assets, operations, and reputation.	1		
	By understanding the different types of security threats and risks, analysing their impact on an organisation, and implementing effective mitigation strategies, how organisations can reduce their exposure to security threats and minimise their effects.	2		
Formatting (5 marks)				
	Title Page	1		
	Table of Contents	1		
	Introduction and Body	1		
	Body with main headings	1		
	Body with sub-headings	1		
APA (5 marks)				
	APA 7th Edition	1		
	Reference in the paragraph body	2		
	Reference list	2		