Module 4 Topic 2

Worksheet

1. Using your own research, give at least three examples for each threat on the following table.

Physical Security Threat	Vandalism
Employee (Human) Accidental Threat	Accidental Data Deletion
Sabotage	Cyber Sabotage

2. Fill the following table by giving a brief explanation for each terminology

Risk	The potential for loss, damage, or any other negative outcome resulting from a threat exploiting a vulnerability. Risks can arise from various sources, including physical, cyber, and human factors.
Countermeasures	Actions, devices, procedures, or techniques that reduce or eliminate risks. These can include security policies, technical controls, and physical safeguards designed to protect assets and mitigate threats.
Impact	The effect or consequence of a risk materializing. Impact can vary in severity and can affect an organization's operations, finances, reputation, and legal standing.

3. CIA features were introduced to you. There are different effects of a failure to preserve CIA features. Write 3 **immediate effects** related to loss of **Availability**.

Service Downtime	Users are unable to access critical systems or services, leading to interruptions in business operations and potential financial losses
Productivity Loss	Employees are unable to perform their tasks efficiently due to the unavailability of necessary resources, resulting in decreased productivity
Customer Dissatisfaction	Customers may experience delays or inability to access services, leading to frustration and potential loss of trust in the organisation

4. What could be **further business consequences** of availability failures?

Financial Losses	Prolonged downtime can lead to significant revenue loss due to halted operations and missed sales opportunities. Additionally, businesses may incur extra costs for emergency fixes and overtime pay
Reputational Damage	Consistent availability issues can erode customer trust and damage the company's reputation. This can result in a loss of existing customers and difficulty attracting new ones
Legal and Compliance Issues	Failure to maintain availability can lead to non-compliance with industry regulations and contractual obligations, potentially resulting in legal penalties and fines
Operational Disruptions	Extended unavailability can disrupt supply chains, delay production schedules, and affect overall business continuity
Competitive Disadvantage	Persistent availability problems can give competitors an edge, as customers may switch to more reliable alternatives
Employee Morale	Frequent availability issues can lead to frustration and decreased morale among employees, impacting productivity and job satisfaction

5. Go to the VERIS website with the following link:
https://verisframework.org/incident-desc.html

Go to the Incident Details Section. Answer the following:

Threat actors (definition)	Entities that cause or contribute to an incident
External actor (definition)	External threats originate from sources outside of the organisation and its network of partners
Examples of an external actor	Criminal groups, lone hackers, former employees, and government entities
Internal Actor (definition)	Internal threats originating from within the organisation
Examples of Internal actor	Company full-time employees, independent contractors, interns, and other staff

6. What are the 10 main essential steps to cyber security according to National Cyber Security Centre in the UK?

[10 Steps to Cyber Security - NCSC.GOV.UK]

1. **Risk Management Regime**: Establish a risk management framework to identify, assess, and manage cyber risks.
2. **Engagement and Training**: Ensure all employees are aware of cyber security risks and are trained to follow best practices.
3. **Asset Management**: Maintain an inventory of all IT assets and ensure they are properly managed and protected.
4. **Architecture and Configuration**: Design and configure systems securely to minimise vulnerabilities.
5. **Vulnerability Management**: Regularly identify, assess, and mitigate vulnerabilities in your systems.
6. **Identity and Access Management**: Control who has access to your systems and data and ensure access is granted appropriately.
7. **Data Security**: Protect data at rest and in transit using encryption and other security measures.
8. **Logging and Monitoring**: Continuously monitor systems and networks for unusual activity and maintain logs for analysis.
9. **Incident Management**: Develop and test incident response plans to address and recover from security incidents quickly.
10. **Supply Chain Security**: Ensure that third-party suppliers and partners adhere to your security standards

7. What are the 18 Critical Security Controls, according to CIS Controls Version 8.1 and why do they matter?
[The 18 CIS Critical Security Controls (cisecurity.org)]

1	Inventory and Control of Enterprise Assets	Ensures all hardware devices are known, tracked, and protected, reducing unauthorised access
2	Inventory and Control of Software Assets	Helps prevent unauthorised software from running, reducing the risk of malware and vulnerabilities
3	Data Protection	Safeguards sensitive information from breaches, ensuring privacy and compliance with regulations
4	Secure Configuration of Enterprise Assets and Software	Reduces vulnerabilities by ensuring systems are securely configured and maintained.
5	Account Management	Controls user access to systems, preventing unauthorised access and potential breaches

6	Access Control Management	Ensures only authorised users can access specific resources, enhancing security
7	Continuous Vulnerability Management	Regularly identifies and mitigates vulnerabilities, reducing the risk of exploitation
8	Audit Log Management	Provides a record of system activities, aiding in detecting and responding to security incidents
9	Email and Web Browser Protections	Protects against threats from email and web vectors, reducing the risk of phishing and malware
10	Malware Defenses	Prevents, detects, and removes malicious software, protecting systems from damage and data breaches
11	Data Recovery	Ensures critical data can be restored in case of loss, maintaining business continuity
12	Network Infrastructure Management	Secures network devices and configurations, preventing unauthorised access and attacks
13	Security Awareness and Skills Training	Educates employees on security best practices, reducing the risk of human error
14	Service Provider Management	Manages risks associated with third-party providers, ensuring they adhere to security standards
15	Application Software Security	Ensures software is developed and maintained securely, reducing vulnerabilities
16	Incident Response Management	Prepares for and responds to security incidents, minimising damage and recovery time
17	Penetration Testing	Tests the effectiveness of security controls, identifying weaknesses before attackers do
18	Security Governance	Establishes a framework for managing and overseeing the security program, ensuring accountability and continuous improvement