BSBXCS403

Contribute to cyber security threat assessments

Assessment 1 of 4

Short Answer Questions

Assessment Instructions

Task overview

This assessment task is divided into fourteen (14) questions. Read each question carefully before typing your response in the space provided.

Additional resources and supporting documents

To complete this assessment, you will need:

- Learning Resources

Assessment Information

Submission

You are entitled to three (3) attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the LMS. Hand-written assessments will not be accepted unless previously arranged with your assessor.

Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:

- the processes for conducting the assessment (e.g. allowing additional time)
- the evidence gathering techniques (e.g. oral rather than written questioning, use of a scribe, modifications to equipment)

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Question 1

Briefly outline the aim of the following Australian legislative acts relevant to cybersecurity and data protection:

- Privacy Act 1988 (Cth)
- Security of Critical Infrastructure Act 2018 (Cth)
- Telecommunications (Interception and Access) Act 1979 (Cth).

[Approximate word count: 50 – 100 words]

Assessor instructions: Students must briefly outline the aim of the Australian legislative acts relevant to cybersecurity and data protection in the table below.

The response must include the following:

<<Insert your response here>>

- Privacy Act 1988 (Cth) aims to protect people's personal information by regulating what data can be collected, how it can be used and who can access it.
- Security of Critical Infrastructure Act 2018 (Cth) aims to manage Australia-wide security risks from sabotage, coercion and espionage by foreign entities, including those posed by cyber connectivity.
- Telecommunications (Interception and Access) Act 1979 (Cth) aims to provide a legal framework for the privacy of private communication between two parties except in investigating serious crimes.

Question 2

Summarise the Australian Privacy Principles of the Privacy Act 1988 (Cth).

[Approximate word count: 50 – 100 words]

Assessor instructions: Students must summarise the Australian Privacy Principles of the Privacy Act 1988 (Cth) in the table below.

The response must include the following:

<<Insert your response here>>

The Australian Privacy Principles (APPs) provide guidelines to organisations on how to meet the requirements of the Privacy Act 1988. The thirteen APPs provide guidelines on the rights, obligations, and standards for:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information.

Question 3

Outline what an organisation that must comply with the Privacy Act 1988 must do in the event of a notifiable data breach under the Notifiable Data Breaches scheme.

[Approximate word count: 50 – 100 words]

Assessor instructions: Students must outline what an organisation that must comply with the Privacy Act 1988 must do in the event of a notifiable data breach under the Notifiable Data Breaches scheme in the table below.

The response must include the following:

<<Insert your response here>> The organisation must notify the following: • Individuals affected if the data breach is likely to cause them serious harm. • The Office of the Australian Information Commissioner (OAIC). • Put the data breach notification on their website if they are unable to contact all affected individuals. • Promote the data breach via other channels such as social media, advertisements, or newspapers.

Question 4

Outline what a notifiable data breach notification must include under the Notifiable Data Breaches scheme.

[Approximate word count: 40 – 80 words]

Assessor instructions: Students must outline what a notifiable data breach notification must include under the Notifiable Data Breaches scheme.

The response must include the following:

<<Insert your response here>> The organisation must include the following information in the notifications: • the organisation or agency's name and contact details • the kinds of personal information involved in the breach • a description of the data breach • recommendations for the steps you can take in response.

Question 5

Briefly outline the following international legislation relevant to cybersecurity and data protection:

- European Union General Data Protection Regulation (GDPR)
- The United Kingdom Data Protection Act 2018.

[Approximate word count: 50 – 100 words]

Assessor instructions: Students must briefly outline the international legislation relevant to cybersecurity and data protection.

The response must include the following:

<<Insert your response here>> ▪ The European Union General Data Protection Regulation (GDPR): imposes obligations on any organisation that collects data related to people in the European Union for the protection and use of this data.

- The United Kingdom Data Protection Act 2018: is the United Kingdom's implementation of the GDPR and imposes controls on how personal information is used by organisations, businesses or the government entities that collect this information in the UK.

Question 6

List three [3] potential organisational impacts of cybersecurity attacks.

Assessor instructions: Students must list three [3] potential organisational impacts of cybersecurity attacks.

The response must include three [3] of the following:

<<Insert your response here>>

- loss of business data/intellectual property
- financial loss through theft
- disruption in trading
- loss of business reputation through bad press
- loss of customer confidence
- loss of business/contracts
- course action/fines.

Question 7

Briefly summarise the following cybersecurity risks that organisations must be aware of:

- Distributed Denial of Service [DDoS]
- Malware
- Man-in-the-middle [MitM]
- Phishing
- Ransomware.

[Approximate word count: 100 – 150 words]

Assessor instructions: Students must briefly summarise the cybersecurity risks that organisations must be aware of.

The response must include the following:

<<Insert your response here>>

- Distributed Denial of Service [DDoS]: A malicious attack designed to disrupt the normal traffic of an organisation's network or website by trying to overwhelm it with significant Internet traffic.
- Malware: Malicious software designed to harm or infect devices, services, or networks.
- Man-in-the-middle [MitM]: An attack designed to intercept communications between two parties by positioning themselves somewhere between the two parties' communication methods.
- Phishing: A malicious attack where targets are contacted by email, text or phone by the attacker pretending to be a legitimate organisation so that they can gain personal information or gain access to organisational networks and systems.

- Ransomware: Malware that encrypts a victim's access to files or their device until a sum of money is paid to remove this encryption.

Question 8

List the five (5) stages of the threat modelling process.

Assessor instructions: Students must list the five (5) stages of the threat modelling process..

The response must include the following in the correct sequence:

<<Insert your response here>>

1. Apply threat intelligence.
2. Asset identification.
3. Identify mitigation capabilities.
4. Assess risks.
5. Perform threat mapping.

Question 9

Briefly summarise the following stages of the risk management process:

- Hazard identification
- Risk assessment
- Control risks
- Monitor risks.

[Approximate word count: 80 – 120 words]

Assessor instructions: Students must briefly summarise the stages of the risk management process.

The response must include the following:

<<Insert your response here>>

- Hazard identification: The process of identifying and documenting potential hazards which are inherent to the workplace.
- Risk assessment: The process of identifying the risks associated with each hazard and assessing the likelihood of them occurring and their impact if they do to determine an overall risk rating for each.
- Control risks: The process of identifying methods to control each risk to reduce its impact or minimise the likelihood of them occurring.
- Monitor risks: The process of monitoring the control measures for each risk to determine their effectiveness or whether better control measures need to be implemented.

Question 10

List three (3) tools that can improve an organisation's cybersecurity and audit processes.

Assessor instructions: Students must list three (3) tools that can improve an organisation's cybersecurity and audit processes.

The response must include three (3) of the following appropriate tools listed below:

<<Insert your response here>>

- Intruder cloud-based vulnerability scanner
- Kaseya VSA
- ManageEngine Log360
- ManageEngine EventLog Analyzer
- Metasploit
- N-able N-sight
- Netwrix Auditor Monitoring
- Nmap Classic security auditing tool
- OpenVAS Free
- SolarWinds Network Configuration Manager.

Question 11

List three (3) strategies/techniques that can improve an organisation's cybersecurity and audit processes.

Assessor instructions: Students must list three (3) strategies/techniques that can improve an organisation's cybersecurity and audit processes.

The response must include three (3) of the following:

<<Insert your response here>>

- Develop a cybersecurity audit policy.
- Define security objectives to be met by the audit.
- Create an audit checklist of what must be checked.
- Hire an audit consultant.
- Conduct regular internal audits.
- Outsource an external audit.
- Use specialised cybersecurity auditing tools.

Question 12

Outline the aim of an Information Security Policy and its associated procedures.

[Approximate word count: 20 – 30 words]

Assessor instructions: Students must outline the aim of an Information Security Policy and its associated procedures.

The response must include the following:

<<Insert your response here>> Outlines security practices and rules to protect data confidentiality, integrity, and availability that must be implemented and adhered to by organisational employees.

Question 13

Outline the aim of an Internal Communication Policy and its associated procedures.

[Approximate word count: 20 – 30 words]

Assessor instructions: Students must outline the aim of an Internal Communication Policy and its associated procedures.

The response must include the following:

<<Insert your response here>> Outlines the organisation's approach to internal communication with its employees, including what information is to be communicated and the communication channels used to share this information.

Question 14

If your company is dealing with a company in the United States, what is the primary federal cybersecurity regulation you need to comply with?

Assessor instructions: Students must explain what the primary federal cybersecurity regulation in the USA is.

The response needs to reference the Act below:

<<Insert your response here>> The primary law governing cybersecurity in the United States is the Federal Trade Commission Act (FTCA).

Assessment checklist:

Students must have completed all questions within this assessment before submitting. This includes:

1	Fourteen (14) short answer questions to be completed in the spaces provided.	☐

Congratulations you have reached the end of Assessment 1!