BSBXCS402

Promote workplace cyber security awareness and best practices

Assessment 1 of 6

Short Answer Questions

SWIN BUR NE OPEN ED

Version 1

Assessment Instructions

Task overview

This assessment task is divided into six (6) 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

Explain the legislative requirements relating to cyber security provided in the table below.

Assessor instructions: Students must explain the legislative requirements relating to cyber security provided in the table below.

Students' wording may vary, but their responses need to reflect the content in the sample answer provided below.

Legislative Requirements	Explanation *[Approximate word count: 100 – 120 words per requirement]*
Data protection	<<Insert your response here>> In Australia, data protection is primarily governed by the Privacy Act 1988 (Cth). The Privacy Act includes the Australian Privacy Principles (APPs), which outline how private sector organisations should handle, use, and manage personal information. Key aspects include: • **Collection and Use:** Organisations must only collect personal information that is necessary for their functions or activities. They must also obtain consent and inform individuals about the purpose of the collection. • **Data Security:** Organisations are required to take reasonable steps to protect personal information from unauthorised access, disclosure, misuse, or loss. • **Access and Correction:** Individuals have the right to access their personal information held by an organisation and request corrections if necessary.
Implications of Notifiable Data Breach legislation on an organisation and other associated Australian privacy laws	<<Insert your response here>> The Notifiable Data Breaches (NDB) scheme, introduced in February 2018, amends the Privacy Act to require organisations to notify individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm. Key points include: • **Mandatory Notification:** Organizations are obligated to notify affected individuals and the OAIC when they become aware of an eligible data breach. • **Assessment of Harm:** Organizations must assess whether a data breach is likely to result in serious harm, which may include physical, psychological, emotional, economic, or financial harm. • **Timely Notification:** Notifications must be made as soon as practicable after becoming aware of a breach.
Established international legislation	<<Insert your response here>>

	Australia, when trading and communicating with overseas companies, will be required to comply with local cyber security requirements. For example, the General Data Protection Regulation (GDPR) is the data privacy convention adopted in the European Union. Any Australian business sending or receiving personal information regarding EU citizens is required to comply with the GDPR. In the USA, the amended Data Privacy Act encompasses compliance requirements for the handling of personal data belonging to citizens of the USA. Australian businesses should consult with the Department of Foreign Affairs and Trade (DFAT) and the Australian Cyber Security Centre to discover more about international cybersecurity requirements.

Question 2

Explain what the organisational policies and procedures provided in the table below are meant to cover.

Assessor instructions: Students must explain what the organisational policies and procedures provided in the table below are meant to cover.

Students' wording may vary, but their responses need to reflect the content in the sample answer provided below.

Organisational Policies and Procedures relating to:	Explanation *[Approximate word count: 50 – 100 words]*
Securely storing, sharing and managing information	<<Insert your response here>> The policy for securely storing, sharing, and managing information in a cybersecurity context aims to establish guidelines for protecting sensitive data throughout its lifecycle. This includes specifying secure storage practices, access controls, and encryption methods. The policy should cover protocols for sharing information securely, emphasising encrypted communication channels. Additionally, it should address management practices, such as regular audits, to ensure ongoing compliance with security standards and regulations.
Encryption, and protocols for its uses	<<Insert your response here>> The encryption policy is designed to provide a framework for implementing and maintaining robust encryption measures to protect sensitive information. It covers the types of data that require encryption, the encryption algorithms and protocols to be used, and the circumstances under which encryption should be applied. The policy ensures that encryption is implemented consistently across the organisation, both for data at rest and during transmission, using industry-accepted best practices.
Data classification and management	<<Insert your response here>> The data classification and management policy focuses on categorising data based on its sensitivity and importance. It outlines the criteria for classifying data into different levels, such

	as public, internal use only, confidential, or highly confidential. The policy includes measures for implementing access controls based on data classification, ensuring that appropriate security measures are applied to safeguard data according to its significance. It also addresses data handling procedures and regular reviews to adjust classifications as needed.
Media/document labelling	<<Insert your response here>> The media/document labelling policy sets out the standards and procedures for marking both physical and digital media or documents with appropriate classifications. This ensures that individuals handling the information understand its sensitivity and adhere to the corresponding security measures. The policy aims to prevent accidental disclosure and supports a consistent approach to handling and protecting information assets throughout their lifecycle.
Data governance	<<Insert your response here>> The data governance policy establishes the framework for managing and overseeing the organisation's data assets. It includes roles and responsibilities for data stewardship, guidelines for data quality, integrity, and security, and processes for regular audits. The policy ensures that data is treated as a valuable organisational asset, promoting responsible use, protection, and leveraging of data for strategic purposes. It aligns data practices with business objectives and regulatory requirements.
Acceptable use	<<Insert your response here>> The acceptable use policy outlines the acceptable behaviours and practices concerning the use of organisational technology resources. It covers the responsible use of computers, networks, and internet access to prevent security incidents, unauthorised access, or misuse. The policy sets boundaries for acceptable behaviour, specifies consequences for policy violations, and contributes to creating a cybersecurity-aware culture within the organisation.
Bring your own device	<<Insert your response here>> The BYOD policy addresses the security implications associated with employees using their personal devices for work purposes. It defines security requirements for personal devices, including antivirus software, encryption, and software updates. The policy aims to strike a balance between employee flexibility and maintaining a secure computing environment, highlighting the shared responsibility between the organisation and employees to ensure the security of sensitive information accessed or stored on personal devices. It helps mitigate risks associated with BYOD practices while promoting compliance with cybersecurity standards.

Question 3

List and explain three (3) Australian government sources of information on current threats.

[Approximate word count: 150 – 170 words]

Assessor instructions: Students must list and explain three (3) Australian government sources of information on current threats.

Students can choose any three of the six sources provided in the benchmark answer below.

Australian government sources of information on current threats

1. <<Insert your response here>>
2. <<Insert your response here>>
3. <<Insert your response here>>

1. **Australian Cyber Security Centre (ACSC):**
    - **Explanation:** The ACSC is the central cybersecurity agency in Australia, providing information, guidance, and assistance to enhance the cybersecurity resilience of the nation. It offers a wide range of resources, including threat intelligence, advisories, and alerts to keep organizations and individuals informed about the latest cyber threats.
    - **Website:** Australian Cyber Security Centre (ACSC)
2. **Stay Smart Online:**
    - **Explanation:** Stay Smart Online is an Australian government initiative that provides a variety of resources and advice to help individuals and businesses protect themselves from cyber threats. It includes alerts, tips, and educational materials to promote cybersecurity awareness.
    - **Website:** Stay Smart Online
3. **Cyber Security Incident Management Arrangements (CIMA):**
    - **Explanation:** CIMA is a framework established by the ACSC to guide the response to and management of cybersecurity incidents. It provides information on incident response planning, coordination, and communication during cyber incidents.
    - **Resource:** CIMA Overview
4. **Essential Eight Maturity Model:**
    - **Explanation:** The Essential Eight Maturity Model is a cybersecurity framework developed by the ACSC. It outlines strategies to mitigate the most common cyber threats. The model helps organizations assess their cybersecurity maturity and provides guidance on improving their security posture.
    - **Resource:** Essential Eight Maturity Model
5. **Australian Signals Directorate (ASD) Signals Directorate (ASD):**
    - **Explanation:** The ASD is an intelligence agency responsible for signals intelligence and information security. It collaborates with the ACSC to provide cybersecurity guidance and resources. The ASD publishes the Australian Government Information Security Manual (ISM), which offers guidance on securing information and systems.
    - **Resource:** Australian Signals Directorate
6. **Cyber Security Awareness Week:**
    - **Explanation:** The Australian government organizes Cyber Security Awareness Week annually to promote awareness of cybersecurity issues and best practices. It includes events, resources, and campaigns aimed at educating individuals and organizations about staying secure online.

- **Resource:** Stay Smart Online - Cyber Security Awareness Week

Question 4

List and describe the five (5) most common risks associated with workplace cyber security.

[Approximate word count: 250 - 300 words]

Assessor instructions: Students must list and describe the five (5) most common risks associated with workplace cyber security.

Students' wording may vary, but their responses need to reflect the content in the sample answer provided below.

Risks associated with workplace cyber security

1. <<Insert your response here>>
2. <<Insert your response here>>
3. <<Insert your response here>>
4. <<Insert your response here>>
5. <<Insert your response here>>

1. **Phishing Attacks:**
   - **Description:** Phishing, a prevalent cyber threat, involves deceptive emails, messages, or websites designed to trick employees into divulging sensitive information. By posing as trustworthy entities, attackers can gain unauthorised access to confidential data, making phishing a significant risk to workplace cybersecurity. Employee awareness training and robust email filtering systems are essential defences against this threat.
2. **Weak Passwords and Authentication:**
   - **Description:** Inadequate password practices, such as using weak passwords or reusing them across accounts, present a substantial risk to workplace cybersecurity. Weak authentication mechanisms make it easier for unauthorised access. Establishing strong password policies, encouraging multi-factor authentication, and regularly updating passwords help fortify defences against this vulnerability.
3. **Insider Threats:**
   - **Description:** Insider threats arise when individuals with insider knowledge, such as employees or contractors, misuse their access privileges. These threats can be intentional (malicious) or unintentional (negligent), leading to data leaks, the introduction of malware, or other activities compromising the organisation's security. Managing insider threats requires a combination of employee training, strict access controls, and continuous monitoring.
4. **Ransomware Attacks:**
   - **Description:** Ransomware is malicious software that encrypts files or systems, demanding a ransom for their release. Ransomware attacks can result in severe consequences, including data loss, operational disruptions, and financial harm. To mitigate this risk, organisations

should implement robust cybersecurity measures, including regular data backups, employee education, and advanced threat detection tools.

5. **Unpatched Software and System Vulnerabilities:**
   - **Description:** Failure to promptly apply software updates and patches leaves workplace systems vulnerable to exploitation by cybercriminals. Unpatched software often contains known vulnerabilities that attackers can target to gain unauthorised access, install malware, or execute other malicious activities. Establishing a comprehensive patch management strategy is crucial to addressing this risk and maintaining a secure digital environment. Regular software updates, vulnerability assessments, and timely patching are essential components of an effective defence against this threat.

Question 5

List and describe five [5] strategies and techniques for promoting workplace cybersecurity in the table provided below.

[Approximate word count: 120 – 200 words]

Assessor instructions: Students must list and describe five [5] strategies and techniques for promoting workplace cybersecurity in the table provided below.

Students can choose any five of the eleven strategies and techniques provided in the benchmark answer below.

Strategies and techniques for promoting workplace cybersecurity

1. <<Insert your response here>>
2. <<Insert your response here>>
3. <<Insert your response here>>
4. <<Insert your response here>>
5. <<Insert your response here>>

1. **Employee Training and Awareness:**
   - Conduct regular cybersecurity awareness training programs to educate employees about common threats, phishing attacks, and best practices for maintaining cybersecurity.
   - Ensure employees are aware of the importance of strong passwords, the risks associated with sharing credentials, and the significance of reporting suspicious activities promptly.
2. **Create and Enforce Strong Password Policies:**
   - Implement and enforce policies that require employees to use strong, unique passwords.
   - Encourage the use of multi-factor authentication to add an extra layer of security.
3. **Regular Software Updates and Patch Management:**
   - Establish a robust patch management system to ensure that all software, including operating systems and applications, is regularly updated.
   - Automate software updates whenever possible to minimise the risk of vulnerabilities.
4. **Access Control and Least Privilege Principle:**
   - Implement the principle of least privilege, granting employees the minimum level of access needed to perform their job functions.

- Regularly review and update user access privileges to align with their roles and responsibilities.

5. **Network Security Measures:**
   - Use firewalls, intrusion detection/prevention systems, and secure Wi-Fi networks to protect the organisation's network.
   - Employ virtual private networks (VPNs) for secure remote access, especially for employees working outside the office.
6. **Incident Response Planning:**
   - Develop and regularly update an incident response plan to guide the organisation's response to cybersecurity incidents.
   - Conduct regular drills and simulations to ensure that employees are familiar with the procedures to follow in case of a security incident.
7. **Data Encryption:**
   - Encrypt sensitive data both in transit and at rest to protect it from unauthorised access.
   - Implement encryption for communication channels and devices to safeguard information from potential breaches.
8. **Mobile Device Management (MDM):**
   - Establish policies and use MDM solutions to manage and secure mobile devices used for work purposes.
   - Implement remote wipe capabilities for lost or stolen devices to protect sensitive data.
9. **Regular Security Audits and Assessments:**
   - Conduct periodic security audits and assessments to identify vulnerabilities and weaknesses in the organisation's cybersecurity posture.
   - Use penetration testing to simulate real-world attacks and assess the effectiveness of existing security measures.
10. **Collaborate with Cybersecurity Authorities:**
    - Stay informed about the latest cybersecurity threats by collaborating with cybersecurity authorities, such as the Australian Cyber Security Centre (ACSC).
    - Participate in information sharing and threat intelligence programs to enhance the organisation's situational awareness.
11. **Secure Remote Work Practices:**
    - Establish secure protocols for remote work, including the use of virtual private networks (VPNs) and secure communication tools.
    - Provide guidelines for secure home network configurations and the use of personal devices for work purposes.

Question 6

List and explain four (4) techniques for implementing and promoting workplace cyber security awareness and four (4) techniques for facilitating training that promotes cyber security awareness, including the use of simulated activities in the table provided below.

[Approximate word count: 120 – 150 words per section]

Assessor instructions: Students must list and explain four (4) techniques for implementing and promoting workplace cyber security awareness and four (4) techniques for facilitating training that promotes cyber security awareness, including the use of simulated activities in the table provided below.

Students can choose any four of the techniques provided in each section in the benchmark answer below.

Techniques for implementing and promoting workplace cyber security awareness

1. <<Insert your response here>>
2. <<Insert your response here>>
3. <<Insert your response here>>
4. <<Insert your response here>>

1. **Communication and Regular Updates:**
    - Establish regular communication channels to disseminate cybersecurity information.
    - Share updates on emerging threats, best practices, and policy changes through newsletters, intranet, or internal emails.
2. **Interactive Workshops and Webinars:**
    - Conduct interactive workshops or webinars to engage employees in discussions about cybersecurity.
    - Provide practical tips, case studies, and real-world examples to illustrate potential risks and solutions.
3. **Awareness Campaigns:**
    - Launch awareness campaigns with catchy slogans, posters, and digital displays to capture employees' attention.
    - Use different mediums such as posters, screensavers, and internal messaging systems to reinforce key cybersecurity messages.
4. **Gamification:**
    - Introduce gamified elements into cybersecurity training to make it more engaging.
    - Develop cybersecurity quizzes, challenges, or competitions with rewards to encourage participation and knowledge retention.
5. **Employee Incentives:**
    - Offer incentives or recognition for employees who demonstrate good cybersecurity practices.
    - Encourage reporting of security incidents and near-misses by creating a positive reporting culture.
6. **Phishing Simulations:**
    - Conduct regular phishing simulations to test employees' ability to recognise and respond to phishing emails.
    - Provide immediate feedback and educational content to employees who fall for simulated phishing attacks.

Techniques for facilitating training that promotes cyber security awareness

1. <<Insert your response here>>
2. <<Insert your response here>>
3. <<Insert your response here>>
4. <<Insert your response here>>

1. **Interactive Training Modules:**
    - Develop interactive training modules that cover key cybersecurity topics, including password security, safe browsing habits, and recognising social engineering tactics.

    - Include multimedia elements such as videos, animations, and quizzes to enhance engagement.

2. **Simulated Cybersecurity Scenarios:**
    - Create realistic simulated cybersecurity scenarios that mimic potential threats and attacks.
    - Conduct tabletop exercises where employees can collaboratively respond to simulated incidents, fostering a proactive and prepared mindset.
3. **Role-Specific Training:**
    - Tailor training content to specific roles within the organisation, addressing the unique cybersecurity challenges each role may face.
    - Provide examples and case studies relevant to different departments or job functions.
4. **Continuous Learning Platforms:**
    - Implement continuous learning platforms that offer ongoing cybersecurity education.
    - Use online courses, webinars, or mobile learning apps to provide bite-sized, accessible content that employees can engage with regularly.
5. **Collaborative Learning Sessions:**
    - Facilitate collaborative learning sessions where employees can share insights, experiences, and best practices related to cybersecurity.
    - Encourage teamwork in solving cybersecurity challenges and exchanging knowledge.
6. **Incident Response Drills:**
    - Conduct simulated incident response drills to familiarise employees with the procedures to follow in the event of a cybersecurity incident.
    - Evaluate and refine response plans based on the outcomes of these drills.
7. **Metrics and Assessments:**
    - Implement metrics and assessments to measure the effectiveness of cybersecurity training programs.
    - Use metrics such as click-through rates on simulated phishing exercises and improvement in employees' knowledge over time.

Assessment checklist:

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

1	Six (6) short answer questions to be completed in the spaces provided.	□

✓

Congratulations you have reached the end of Assessment 1!