BSBXCS402

Promote workplace cyber security awareness and best practices

Assessment 2 of 6

Project

Assessment Instructions

Task overview

This assessment task is divided into three (3) tasks. 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
- CBSA Risk Management Policy & Procedures
- Organisational chart

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.

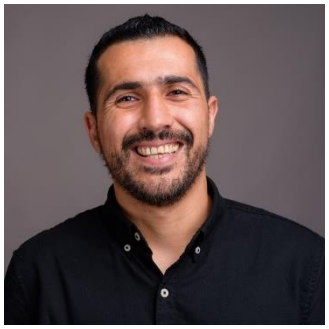
Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Case Study

For the purpose of this assessment, you will play the role of Tan Yamamoto (Software Developer in the IT team at Complete Business Solutions Australia CBSA.

You have been tasked by Con Kafatos, head of IT, to take up a new project of researching possible cybersecurity risks and threats. Read Con's Email below:



To:	Tan Yamamoto (tan.yamamoto@cbsa.com.au)
From:	Con Kafatos (con.kafatos@cbsa.com.au)
Date/time:	Monday 10:32 a.m.
Subject:	Documenting and Assessing Cybersecurity Threats and Risks
Attachments:	Cybersecurity Threat Register Template.docx, Cybersecurity Threat Event Register Template.docx

Good morning Tan,

A. I want you to take up a new project of researching possible cybersecurity risks, trends and threats that CBSA might face in its day-to-day operations.

B. I have attached three templates for you to use.

C. Please document all the threats you find using the attached Cybersecurity Threat Register Template. Once you have done this, please determine the risks of these threats, documenting these in the attached Cybersecurity Threat Event Register Template.

Please contact me if you have any questions.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 1

A. Document at least five cybersecurity threats that may impact CBSA's day-to-day operations using the Cybersecurity Threat Register Template provided. For each threat, you must:
   - assign a unique cybersecurity threat ID number
   - provide a descriptive name for the cybersecurity threat
   - provide a brief description of the cybersecurity threat.

B. Document at least one threat event for each of the five threats you identified in the Cybersecurity Threat Register Template using the Threat Event Register template provided. For each threat event, you must:
   - assign a unique cybersecurity threat event ID number
   - provide a descriptive name for the cybersecurity threat event

- provide a brief description of the cybersecurity threat event
- specify the cybersecurity threat ID number from the Cybersecurity Threat Register Template that is relevant to the cybersecurity threat event.

C. Research the following website www.cyber.gov.au, and briefly explain the five (5) cybersecurity trends identified in 2022 – 2023, in the Cybersecurity Trends Template below.

Assessor instructions: The purpose of this task is to assess the student's ability to review and document the latest cyber security threats and trends impacting an organisation.

1] Students should complete the cybersecurity threat register as per the sample provided. It should include numbers only or a combination of numbers and letters to uniquely identify each threat. It should also contain a relevant name and a brief description of each of the threats identified.

Students provided at least five threats in total. They must be relevant to CBSA operations. In addition to those provided in the table, some examples are:

- Insider threat: an employee or contractor within the organisation who undertakes sabotage or malicious attacks on the organisation's systems, networks, or data.
- Internet of Things (IoT): where security gaps in using IoT software and devices are exploited.
- Ransomware: malware that encrypts a victim's access to files or their device until a sum of money is paid to remove this encryption.
- Wi-Fi security vulnerabilities: where security gaps in the use of Wi-Fi within the organisation are exploited.

Note that other cybersecurity threats names exist that are not listed above, or which might have variations of their names. For example, virus or trojan horses instead of malware. Accept name variations of the list above or other cybersecurity threats not listed.

2] Students should complete the cybersecurity threat event register as per the sample provided. It should include numbers only or a combination of numbers and letters to uniquely identify each threat. It should also contain a relevant name and a brief description of each of the threats identified.

3] The cybersecurity threat ID must be correctly associated with its Threat Event ID between the cybersecurity threat register template and the cybersecurity threat event register template.

4] Students must briefly explain all the five cybersecurity trends provided in the ASD Cyber Threat Report 2022-2023 | Cyber.gov.au.

Benchmark answers are provided below.

Cybersecurity Threat Register Template		
ID	Threat	Description [Approximate word count: 15 – 40 words]
T1	*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.*

T2	*Inadequate patch management*	*Information technology staff aren't implementing a scheduled patch update of software when improvements to this software have been made, leading to potential security gaps.*
T3	*Malware*	*Malicious software designed to harm or infect devices, services, or networks.*
T4	*Man-in-the-middle (MitM)*	*An attack designed to intercept communications between two parties by positioning themselves somewhere between the two parties' communication methods.*
T5	*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.*

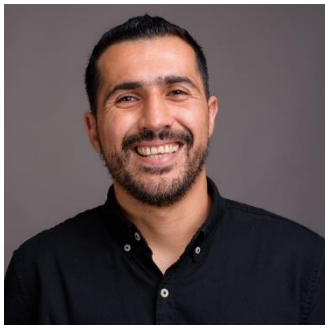
Cybersecurity Threat Event Register Template			
Threat Event ID	**Threat Event**	**Description** [Approximate word count: up tp 30 words]	**Threat ID**
TE1	*Protocol attack*	*Floods the network traffic with SYN packets.*	*T1*
TE2	*Inadequate operating system security*	*Operating system doesn't have the latest security patches installed.*	*T2*
TE3	*Virus*	*Modifies a file by inserting code into the file.*	*T3*
TE4	*IP Spoofing*	*Intercept of communication by changing the IP headers of a TCP packet.*	*T4*
TE5	*Email phishing*	*An email that prompts a call to action to negate some issue that the user will face unless they click on a link in the email.*	*T5*

Cybersecurity Trends Template	
Trend	**Brief Explanation** [Approximate word count: 18 – 150 words]
1. ***State actors focused on critical infrastructure – data theft and disruption of business***	*Globally, government and critical infrastructure networks were targeted by state cyber actors as part of ongoing information-gathering campaigns or disruption activities. The AUKUS partnership, with its focus on nuclear submarines and other advanced military capabilities, is likely a target for state actors looking to steal intellectual property for their own military programs. Cyber operations are increasingly the preferred vector for state actors to conduct espionage and foreign interference.*

	In 2022–23, ASD joined international partners to call out Russia's Federal Security Service's use of 'Snake' malware for cyber espionage, and also highlighted activity associated with a People's Republic of China state-sponsored cyber actor that used 'living-off-the-land' techniques to compromise critical infrastructure organisations.
2. ***Australian critical infrastructure was targeted via increasingly interconnected systems.***	*Operational technology connected to the internet and into corporate networks has provided opportunities for malicious cyber actors to attack these systems. In 2022–23, ASD responded to 143 cybersecurity incidents related to critical infrastructure.*
3. ***Cybercriminals continued to adapt tactics to extract maximum payment from victims.***	*Cybercriminals constantly evolved their operations against Australian organisations, fuelled by a global industry of access brokers and extortionists. ASD responded to 127 extortion-related incidents: 118 of these incidents involved ransomware or other forms of restriction to systems, files or accounts. Business email compromise remained a key vector to conduct cybercrime. Ransomware also remained a highly destructive cybercrime type, as did hacktivists' denial-of-service attacks, impacting organisations' business operations.*
4. ***Data breaches impacted many Australians***	*Significant data breaches resulted in millions of Australians having their information stolen and leaked on the dark web.*
5. ***One in 5 critical vulnerabilities was exploited within 48 hours.***	*This was despite patching or mitigation advice being available. Malicious cyber actors used these critical flaws to cause significant incidents and compromise networks, aided by inadequate patching.* *Cyber security is increasingly challenged by complex ICT supply chains and advances in fields such as artificial intelligence. To boost cyber security, Australia must consider not only technical controls such as ASD's Essential Eight, but also growing a positive cyber-secure culture across business and the community. This includes prioritising secure-by-design and secure-by-default products during both development (vendors) and procurement (customers).* *ASD's first year of REDSPICE increased cyber threat intelligence sharing, the uplift of critical infrastructure, and an enhanced 24/7 national incident response capability.* *Genuine partnerships across both the public and private sectors have remained essential to Australia's cyber resilience; and ASD's Cyber Security Partnership Program has grown to include over 110,000 organisations and individuals.*

Task 2

Read the email from Con and then complete the tasks below.



To:	Tan Yamamoto (tan.yamamoto@cbsa.com.au)
From:	Con Kafatos (con.kafatos@cbsa.com.au)
Date/time:	Wednesday 3:02 p.m.
Subject:	Cybersecurity Threats Risk Assessment
Attachment:	Cybersecurity Threat Risk Assessment Template.docx

Good afternoon Tan,

D. Thanks for identifying and documenting cybersecurity threats that CBSA might encounter.

Please undertake a risk assessment of these identified cybersecurity threats using the attached template, including reviewing current cyber security practices that CBSA implements (by reviewing our policies and procedures) and recommending at least one cybersecurity control measures that we can use to control each cybersecurity threat.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

A. Undertake research to:
   - Determine recommended protection measures against all the identified cybersecurity threats in Part A.
   - Review CBSA's current policies and procedures relating to IT to determine current cyber security practices using a web browser.

B. Then undertake a risk assessment of each cybersecurity threat and document your assessment using the supplied Cybersecurity Threat Risk Assessment Template, ensuring that you:
   - document the threat event ID number and the event name for each threat you have identified in Part A
   - use the Risk Rating Matrix in **CBSA's Risk Management Policy and Procedures** to determine and document the risk rating for each threat based on the likelihood and consequence of each threat
   - document at least one risk control measure for each cybersecurity threat.

Assessor instructions: The purpose of this task is to assess the student's ability to:

- review cyber security practices according to organisational policies and procedures
- document outcomes of review and suggested improvements for consideration by required personnel.

The student:

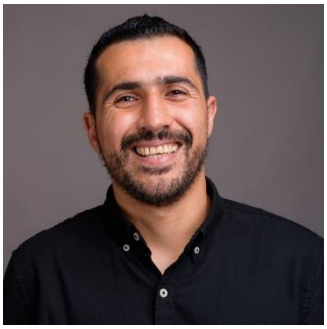
- Must match the threat event ID numbers they documented in the previous part.
- Must match the threat event names they documented in the previous part.
- Must assign a risk rating that is specified in the Risk Management policy and procedure ranging from very low, low, moderate, high, and critical
- Control measures will vary and will be dependent on the threats documented in the previous part.

Benchmark answers are provided below.

Cybersecurity Threat Risk Assessment Template			
Threat Event ID	**Threat Event**	**Threat Risk Rating**	**Recommended Control Measure(s)**
TE1	*Protocol attack*	*Moderate*	*Develop a DDoS Response Plan*
TE2	*Inadequate operating system security*	*Low*	*IT policy and procedure update*
TE3	*Virus*	*High*	*Anti-malware software*
TE4	*IP Spoofing*	*Low*	*Network monitoring software*
TE5	*Email phishing*	*Moderate*	*Staff training on email phishing*

Task 3

Read the email from Con and then complete the tasks below.



To: Tan Yamamoto (tan.yamamoto@cbsa.com.au)

From: Con Kafatos (con.kafatos@cbsa.com.au)

Date/time: Friday 11:16 a.m.

Subject: Develop an action plan

Attachment: Action Plan Template.docx

Good morning Tan,

E. Thanks for completing the risk assessment of possible cybersecurity risks.

F. Please develop an action plan to implement the recommended control measures in a coordinated manner. Use the template that I have attached with this email, and I will review it.

G. Please ensure that you include the following tasks in the action plan, in addition to the actions for your recommended control measures:

- develop a Cybersecurity Awareness Program
- deliver training in the Cybersecurity Awareness Program.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

A. Using a word processor, develop an Action Plan using the Action Plan Template supplied, ensuring that you:
   - document actions that need to be implemented to control each cybersecurity threat
   - document who will be responsible for each task (you can assign yourself or any staff member in the **CBSA Organisation Chart** as appropriate), a timeline for each task's completion and the resources needed for each (specific people, CBSA departments, specific software, etc.)

As per the email from Con, you must make sure you add two further actions, one for developing a Cybersecurity Awareness Program and another for delivering training in this program. You will undertake these two actions in later assessment tasks.

Assessor instructions: The purpose of this task is to assess the student's ability to document outcomes of review and suggested improvements for consideration by required personnel.

The student must:

- Cover all the control measures identified in the previous part and include action tasks for developing a Cybersecurity Awareness Program and training for this program.
- Document the responsibility for each action task in the Responsibility column student or an appropriate staff member from the CBSA organisation chart.
- Provide a date in the future for each action as per the sample.
- Provided a specific resource, if applicable, for each action as per the sample. For example, specific people, CBSA departments, specific software, etc.

Action Plan Template			
Action	**Responsibility**	**Timeline**	**Resources**
Develop a DDoS Response Plan	*Tina Yates*	*XX/XX/20XX*	
Update IT policy and procedures	*Tan Yamamoto*	*XX/XX/20XX*	*IT policy and procedures*
Install anti-malware software	*Tina Yates*	*XX/XX/20XX*	*Anti-malware software*
Install network monitoring software	*Tina Yates*	*XX/XX/20XX*	*Network monitoring software*
Staff training on email phishing and password update	*Tan Yamamoto*	*XX/XX/20XX*	*Training room, existing policies*
Develop cybersecurity awareness program	*Tan Yamamoto*	*XX/XX/20XX*	*Existing Information Technology Policy and Procedure*
Deliver training in cybersecurity awareness program	*Tan Yamamoto*	*XX/XX/20XX*	*Training room*

Assessment checklist:

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

1	Task 1 - Cybersecurity Threat Register - Cybersecurity Threat Event Register - Cybersecurity Trends Template	☐ ☐ ☐
2	Task 2 - Cybersecurity Threat Risk Assessment	☐
3	Task 3 – Action Plan	☐

Congratulations you have reached the end of Assessment 2!