BSBXCS403

Contribute to cyber security threat assessments

Assessment 2 of 4

Project

Assessment Instructions

Task overview

This assessment task is divided into four (4) 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 and Procedures

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 undertake research using various Australian Government sources of current cybersecurity risks and threats. Read Con's Email below:

To:	Tan Yamamoto
From:	Con Kafatos (con.kafatos@cbsa.com.au)
Date/time:	Monday 10:18 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,

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

I have attached two templates for you to use.

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 them 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. Using the Cybersecurity Threat Register Template provided document at least five cybersecurity threats that may impact CBSA's day-to-day operations. 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 Cybersecurity 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.

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.

The student must complete the Cybersecurity Threat Register as per the sample provided. It should include numbers only or a combination of numbers and letters to identify each threat uniquely. It should also contain a relevant name and a brief description of each identified threat.

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

- 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 threat names exist that are not listed above or might have variations of their names, for example, a virus or trojan horse instead of malware. Accept name variations of the list above or other cybersecurity threats not listed.

The student must complete the Cybersecurity Threat Event Register as per the sample provided. It should include numbers only or a combination of numbers and letters to identify each threat uniquely. It should also contain a relevant name and a brief description of each identified threat.

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, as shown in the sample.

Sample answers are provided below.

CYBERSECURITY THREAT REGISTER TEMPLATE		
ID	**Threat**	**Description**
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.*

CYBERSECURITY THREAT REGISTER TEMPLATE		
ID	**Threat**	**Description**
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**	**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*

Case Study

You have been tasked by Con Kafatos, head of IT, to undertake research to identify recommended industry protection measures (mitigation strategies) against cybersecurity threats using a web browser. Read Con's Email below:

To: Tan Yamamoto

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

Date/time: Tuesday 9:18 a.m.

Subject: Cybersecurity Threats Risk Assessment

Attachment: Cybersecurity Threat Risk Assessment Template.docx

Good morning Tan,

Thank you for identifying and documenting cybersecurity threats that CBSA might encounter.

Please undertake a risk assessment of these identified cybersecurity threats using the attached template. Review the current cyber security practices that CBSA implements (by reviewing our policies and procedures) and recommend at least one cybersecurity control measure 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

Task 2

Undertake research to identify recommended industry protection measures (mitigation strategies) against cybersecurity threats using a web browser. Then undertake a risk assessment of each cybersecurity threat and document your assessment using the supplied Cybersecurity Threat Risk Assessment Template, ensuring the following:

- Document the threat event ID number for each threat you identified in Part A.
- Document the threat event name for each threat you identified in Part A.
- Document the risk likelihood for each threat event by selecting a likelihood level defined in **CBSA's Risk Management Policy and Procedures** provided in your resources.
- Document the risk consequence for each threat event by selecting a consequence level defined in **CBSA's Risk Management Policy and Procedures**.
- 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 event.
- Document at least one risk control measure for each cybersecurity threat event.

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 the 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 likelihood level defined in the Risk Management Policy and Procedure ranging from rare, unlikely, possible, likely, and almost certain.
- Must assign a risk consequence level defined in the Risk Management policy and procedure ranging from insignificant, minor, moderate, major, and catastrophic.
- 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.

A sample answer is provided below.

CYBERSECURITY THREAT RISK ASSESSMENT TEMPLATE					
Threat Event ID	**Threat Event**	**Threat Likelihood**	**Threat Consequence**	**Threat Risk Rating**	**Recommended Control Measure(s)**
TE1	*Protocol attack*	*Likely*	*Moderate*	*Moderate*	*Develop a DDoS Response Plan*
TE2	*Inadequate operating system security*	*Rare*	*Moderate*	*Low*	*IT policy and procedure update*
TE3	*Virus*	*Likely*	*Major*	*High*	*Anti-malware software*
TE4	*IP Spoofing*	*Unlikely*	*Minor*	*Low*	*Network monitoring software*
TE5	*Email phishing*	*Likely*	*Moderate*	*Moderate*	*Staff training on email phishing*

Case Study

You have been tasked by Con Kafatos, head of IT, to develop an Action Plan using the Action Plan Template. Read Con's Email below:

To: Tan Yamamoto

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

Date/time: Thursday 11:58 a.m.

Subject: Develop an action plan

Attachment: Action Plan Template.docx

Good morning Tan,

Thank you for completing the risk assessment of possible cybersecurity risks.

Please develop an action plan to implement the recommended control measures in a coordinated manner.

Please ensure that you develop a Cybersecurity Security Audit Checklist in the action plan in addition to the actions for your recommended control measures.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 3

Using a word processor, develop an Action Plan using the Action Plan Template supplied, ensuring the following:

- 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 org chart as appropriate.] Provide 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 one further action for developing a Cybersecurity Security Audit Checklist. You will undertake this action in a later assessment.

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 document action tasks in the Action column to implement control measures It must cover all the control measures identified in the previous part and include an action task for developing a cybersecurity security audit checklist.
- The student must document the responsibility for each action task in the Responsibility column. It must be either the student or an appropriate staff member from the CBSA org chart.

- The student must provide a date in the future for each action as per the sample.
- If applicable, the student must provide a specific resource for each action as per the sample solution, for example, specific people, CBSA departments, software, etc.

ACTION PLAN			
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 a cybersecurity security audit checklist	*Tan Yamamoto*	*XX/XX/20XX*	*Existing Information Technology Policy and Procedure*

Case Study

You have been tasked by Con Kafatos, head of IT, with evaluating the strength of passwords used by CBSA employees. Read Con's Email below:

To: Tan Yamamoto

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

Date/time: Thursday 11:58 a.m.

Subject: Passwords

Attachment: Passwords.docx

Good morning Tan,

CBSA is implementing a new password policy to enhance security. You will need to assess the strength of a set of passwords based on their complexities by creating and applying a formula to calculate password complexity.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 4

Con gave you the following passwords to calculate their complexity:

- Cyber@123
- P@ssw0rd!
- ABCdef123
- *SecurePwd*

You need to create a formula to calculate password complexity. The formula should consider the following factors:

- Length of the password
- Number of special characters
- Number of uppercase letters

You will need to access your learning resources to assist you with this task.

After you complete your calculations, you will need to explain which password is the strongest and why.

You will need to use the template below to write your formula and the results of your calculations.

Assessor instructions: The purpose of this task is to assess the student's ability to interpret mathematical data, complete complex calculations, and record mathematical data.

The students will need to use this formula as presented in the case study in their learning resources:

(Length×2)+(Number of Special Characters×3)+(Number of Uppercase Letters×2)

Their formula needs to cover all three criteria:

- Length of the password
- Number of special characters
- Number of uppercase letters

Their responses need to reflect the content in the sample answer provided below:

Formula	(Length×2)+(Number of Special Characters×3)+(Number of Uppercase Letters×2)			
Password	**Length**	**Number of Special Characters**	**Number of Uppercase Letters**	**Complexity**
Cyber@123	9 characters	1 (@)	1 (C)	(9×2)+(1×3)+(1×2)=18+3+2=23
P@ssw0rd!	9 characters	2 (@ and !)	1 (P)	(9×2)+(2×3)+(1×2)=18+6+2=26
ABCdef123	9 characters	0	3 (A, B, C)	(9×2)+(0×3)+(3×2)=18+0+6=24
SecurePwd	11 characters	2 (*)	1 (S)	(11×2)+(2×3)+(1×2)=22+6+2=30
Explanation				
Password 4 ("*SecurePwd*") is the strongest among the given passwords. It has the highest complexity and rating, making it more robust against common password attacks as it has more length, special characters upper case letters.				

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	☐ ☐
2	Task 2 ▪ Cybersecurity Threat Risk Assessment	☐
3	Taks 3 ▪ Action Plan	☐
4	Taks 4 ▪ Password Strength	☐

Congratulations you have reached the end of Assessment 2!