BSBXCS401

Maintain security of digital devices

Assessment 3 of 3

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 & Procedure
- Device and Risk Register
- Gap Analysis Template

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

This is a continuation of Assessment 2 – Project.

For the purpose of this assessment, you will act as Sally Fischer, System Analyst in the IT department of Complete Business Solutions Australia CBSA.

You have been tasked by Con Kafatos, head of IT, to develop a Gap Analysis based on the information provided by the staff.
Refer to the email from Con Kafatos for instructions on creating a digital device register for CBSA's IT team.

To: Sally Fischer

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

Date/time: 15/11/2022 9:30 p.m.

Subject: Device Register

Good afternoon Sally,

I've received input from all the staff based on our request to list the information stored on their devices. Some of the data that has come back is incomplete. Can you go through the data and categorise the level of risk associated with using the CBSA Risk Management Policy & Procedure (IM009) related to each device and identify any gaps you've found? There is space in the document for your recommendations based on your findings. We can then roll it out to the team.

- Staff: Con Kafatos

  Device: Laptop 1001

  Mac address: 00-3B-3S-F5-C3-D2

  Malware installed: Yes

  VPN in use: Yes

  Data stored: Passwords for server, Passwords for email, Access to cloud storage (auto login), Device password, Company staff registry.
- Staff: Con Kafatos

  Device: Tablet 2001

  Mac address: 95-34-D3-Q2-G8-5B

  Malware installed: Yes

  VPN in use: No

  Data stored: Passwords for server, Email logins, and Company staff registry.
- Staff: Sally Fischer

  Device: Laptop 1002

  Mac address: 67-O4-P1-C7-4R-G1

  Malware installed: Yes

  VPN in use: Yes

Data stored: Email passwords, Login for central IT system, router configuration login, access to cloud storage.

- Staff: Tan Yamamoto

  Device: Desktop 3001

  Mac address: 9G-67-D3-34-89-M1

  Malware installed: Yes

  VPN in use: No

  Data stored: Software development logins, email logins, cloud storage login, software in development – prototypes.

- Staff: Tina Yates

  Device: Desktop 3002

  Mac address: 4F-56-V3-L9-D3-12

  Malware installed: Yes

  VPN in use: No

  Data stored: Software development logins, email logins, cloud storage login, software in development – prototypes.

- Staff: Sam Tailor

  Device: Laptop 1003

  Mac address: 56-M2-12-B4-A4-C9

  Malware installed: No

  VPN in use: Yes

  Data stored: Email logins, cloud storage login.

- Staff: James Hanson

  Device: Desktop 3003

  Mac address: 89-09-Q1-N4-DF-56

  Malware installed: Yes

  VPN in use: No

  Data stored: Email logins, Cloud storage login, Graphic design templates.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 1

Your first task is to use the information provided by the CBSA staff about the information stored on their devices and input it into the register of digital devices. You will then need to categorise the level of risk associated with each device. To do so, you will need to access and review the following:

- CBSA Risk Management Policy & Procedure.

Then you will need to access and fill out the **Device and Risk Register** and submit it along with this assessment using the following naming convention:

- **<StudentNumber> Device and Risk Register**

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

- assess risk associated with data stored on devices
- conduct gap analysis based on best practices in cyber security
- make recommendations to company staff about how to secure devices appropriately.

Ensure the following document has been completed with all the data as per the email and submitted for assessment:

- Gap Analysis, Device and Risk Register.

More specifically:

- The student should refer to CBSA Risk Management Policies and Procedures and must identify a reasonable level of risk associated with the data stored on each device. Responses may vary.
- Students must identify the gaps as applicable, categorise the risk level for each gap and include a possible solution to the potential risk associated with the gap.
- Student recommendations must be similar to tighten processes, encryption, two-factor authentication or other methods to ensure that each and every device is secure.

See **Device and Risk Register - Assessor Guide** for benchmark response.

To:	Sally Fischer
From:	Con Kafatos (con.kafatos@cbsa.com.au)
Date/time:	15/02/2023 9:30 p.m.
Subject:	Device Register

Good afternoon Sally,

It's been a tough day for us. As you know, we've had James Mollison join the team as a new staff member this week, and he hasn't set up his device correctly. I received a notification this morning that his computer has been infected with several viruses and other malware. Luckily the firewall protocols that we have in place prevented the malware from getting into the server and infecting other computers. It has caused considerable damage to his device. We are also lucky that his access to our cloud data wasn't infiltrated.

I want you to update the device register and indicate that he hasn't installed the malware correctly. You'll find his device on the network with the MAC address 34-T5-Y6-23-Q1-98, and I've named his device Desktop 3004.

Would also be a good time to ensure that the recommendations you implemented three months ago have stayed intact. I haven't received any reports from other staff, so I think it's all working well, but it is good practice to review this every quarter. If everything looks good, there's no need to update it.

Just a quick note also, I recently had my company credit card used in unauthorised transactions online, and I am now wondering if it is because I used it on my work device. Is this something that I need to set up with the credit card company, or is it related to the device security?

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 2

Now you will need to update the Gap Analysis, Device and Risk Register based on the new information received from Con Kafatos.

You must identify recommendations for the two staff members who have had their computers hacked.

Refer to Con Kafatos' email about the cases of cyber security breaches.

You will need to save and submit it along with this assessment using the following naming convention:

- **<StudentNumber> Device and Risk Register UPDATED**

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

- assess risk associated with data stored on devices

- conduct gap analysis for the new employee's device based on best practices in cyber security
- conduct a review and make recommendations to staff whose device has been attacked.

Ensure the following document has been submitted for assessment:

- *Gap Analysis, Device and Risk Register to include details about Con's breach and three-monthly review:*

  Recommendations for Con's credit card authority should be directed to the credit card company to set up two-factor authentication rather than looking at the devices in use.

- *Input James Mollison's details as follows:*
  - *Name: James Mollison*
  - *MAC address: 34-T5-Y6-23-Q1-98*
  - *Device name: Desktop 3004*
  - *Antimalware software is not set up on James Mollison's device.*
  - *Low-level risk is identified as the staff is new to the company, and no data is stored as of yet.*
  - *At a minimum, recommendations should indicate setting up antimalware software correctly and keeping it up to date.*

See **Device and Risk Register - Assessor Guide** for benchmark response.

To:	Sally Fischer
From:	Con Kafatos (con.kafatos@cbsa.com.au)
Date/time:	15/02/2023 9:30 p.m.
Subject:	Gaps

Good afternoon Sally,

Dear Sally,

I trust this email finds you well. Recently, several staff members reached out to me with concerns regarding our current cybersecurity practices. After careful consideration, it has become apparent that there are areas where our best practices may be falling short. I wanted to bring these matters to your attention as we work towards enhancing our overall cybersecurity posture.

Our Cyber Security Systems Review Plan, while in place, seems to lack comprehensive coverage. It has been brought to my attention that the current system review does not adequately integrate emerging threat intelligence sources, leaving us potentially exposed to new and sophisticated threats.

I also noticed that there are inconsistencies in the enforcement of cybersecurity protocols. Some staff members report challenges in ensuring that best practices are consistently followed throughout the organisation.

The inconsistency in enforcing cybersecurity protocols poses a risk, as it may lead to potential gaps in implementation. It's crucial to address these discrepancies to ensure uniform adherence to security practices.

Other than that, all staff members who were asked to provide feedback about the cyber security practices followed by CBSA, stated that they were very pleased and that they found the video tutorials particularly helpful as they made the process easy and quick even for the staff members that were not familiar with the applications.

Therefore, I would like you to conduct a gap analysis to evaluate the effectiveness of all applied best practice strategies and organise a meeting to discuss it.

Thank you for your attention to this matter, and I look forward to your guidance.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 3

Now you will need to conduct a Gap Analysis based on the email received from Con Kafatos.

You will need to access and fill out the **Gap Analysis Template.**

You will need to save and submit it along with this assessment using the following naming convention:

- <StudentNumber> Gap Analysis

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

- Conduct a gap analysis to evaluate the effectiveness of all applied best practice strategies.

Ensure the following document has been submitted for assessment:

- *For each section, specific details were provided about the current state, strengths, and gaps related to the corresponding best practice..*
- *Gaps are identified for the following two practices:*
  - *Cyber Security Systems Review Plan*
  - *Open Communication Among Staff*
- *Strength identified for the video tutorials..*
- *The information under the Action column is clear and actionable, providing a foundation for improvement in cybersecurity practices.*

See **Gap Analysis - Assessor Guide** for benchmark responses and instructions.

Assessment checklist:

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

1	Task 1 –**Device and Risk Register**	□
2	Task 2 –**Device and Risk Register UPDATED**	□
3	Task 3 – **Gap Analysis**	

Congratulations you have reached the end of Assessment 3!