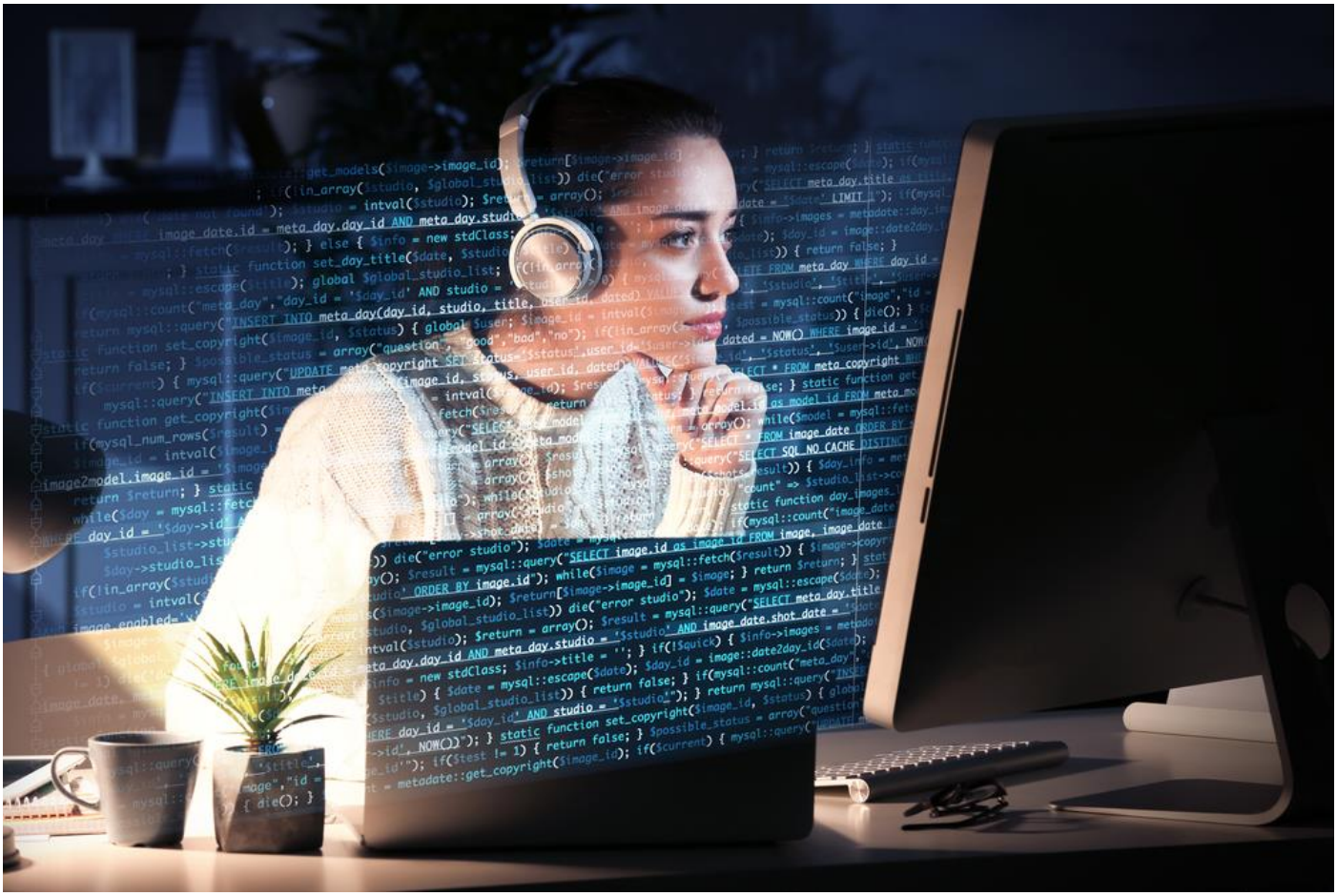


BSBXCS401

Maintain security of digital devices

Assessment 2 of 3

Project

Assessment Instructions

Task overview

This assessment task is divided into five (5) 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 Information Technology Policy & Procedure.
- CBSA Document Management Policy & 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.

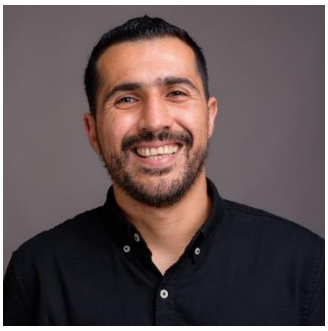
Please consider the environment before printing this assessment.

Case Study

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

In this assessment, you will be working on a project of internally reviewing and improving CBSA practice protection strategies to maintain the security of two different electronic devices.

You have been tasked by Con Kafatos, head of IT, to develop a plan to protect CBSA from any cyber-attacks and prevent further cyber security breaches. Refer to the email from Con below for details on the scope of the issue at CBSA.



To: Sally Fischer

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

Date/time: 29/9/2022 10:05 a.m.

Subject: Cyber Security Breaches

Good morning Sally,

It's come to my attention that the company is sitting in a vulnerable position in terms of cyber security at CBSA. First, we don't have a functioning cyber security policy or guidelines for staff. I know for a fact that some staff members are not using the best practices available to secure devices, and this is leaving us vulnerable to attack.

This is what I know so far:

Several staff members have been using their personal mobile phones or other mobile devices for business-related activities, like checking emails and accessing apps. Some staff have installed an email client and input their usernames and passwords onto their personal devices. Most are not running any anti-malware software nor using a VPN to access the internet when conducting business activities on their personal devices.

Gavin Stead, the company's Managing Director, has also reported accessing the cloud-based file management system on his laptop while out of the office, sometimes using it in airports, café, at home and in the offices of various industry contacts.

The three tablets that staff use when they have client consultations outside of the office are not adequately encrypted, nor do they run a VPN that connects to the company server.

It seems to me that most of this can be taken care of with some basic protocols and policies.

Can you please complete the cyber security review template and create a physical security plan?

Also, I've been on the phone with several anti-malware companies and decided that we are going to purchase a company plan from Avast One. I'll be getting that finalised soon, and, in the meantime, I want you to create some tutorials that show the staff how to set up their devices with all the best practice protocols that you would recommend in the cyber security plan. Keep it simple and informative. You'll need to make both written and video tutorials so that we can cover everything for the staff to follow along. We will then have you develop an updated version of the CBSA Information Technology Policy and Procedure based on the new protocols.

Keep me up to date with how you are progressing.

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 research and describe the best practice security protocols that can be used as strategies to protect CBSA. You will also need to explain what kind of cyber security each protocol provides. To do so, you will need to access and review the following:

- CBSA Information Technology Policy & Procedure.
- CBSA Document Management Policy & Procedures.

Then complete your responses in the **Cyber Security Systems Review Plan Template** below.

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

- create a review plan using the best practice security protocols and describe the benefit it provides to CBSA
- demonstrate an understanding of the purpose of each protocol or strategy used in cyber security.

Responses must demonstrate that the student has a strong understanding of how each cyber security protocol can be used as a strategy to benefit the organisation. A sample completed template has been provided for the assessor. More specifically:

- The student must complete all parts of the template.
- The student must identify what tool/process will be used to identify threats.

The student has identified how the best practices support the cyber security for CBSA. All points 1–7 are complete

Cyber Security Systems Review Plan Template		
Best practice security protocols	**What tool/process will you use?**	**How will this best practice provide security to CBSA?**
1. **Use of two-factor authentication in place across company devices.**	<<Insert your response here>> *Survey staff* *Check devices*	<<Insert your response here>> *The login method is much more secure with two-factor authentication. Prevents hacking the device and gaining easy access to all the data.*
2. **Password robustness.**	<<Insert your response here>> *Survey staff* *Check devices*	<<Insert your response here>> *Passwords are complex and difficult to guess.*

3. **Cloud-based file management in place/ use.**	<<Insert your response here>> *Survey staff* *Check devices*	<<Insert your response here>> *Data stored in the cloud is more secure because methods of encryption are stronger. They are safer from physical attacks because cloud servers are larger and more complex than personal computers.*
4. **Anti-malware software in use and up to date.**	<<Insert your response here>> *Survey staff* *Check devices*	<<Insert your response here>> *Prevents threats like viruses, malware, trojans or worms from entering the computer. If kept up to date, the software can recognise current threats.*
5. **Devices are encrypted/ password protected.**	<<Insert your response here>> *Survey staff* *Check devices*	<<Insert your response here>> *Encrypted and password protection ensures that data is kept safe and inaccessible to hackers. This is the base level of security to consider when devices are lost or stolen.*
6. **Latest patch installed.**	<<Insert your response here>> *Check devices*	<<Insert your response here>> *Up-to-date operating systems and software to ensure the highest level of protection from hackers.*
7. **Use of external drives/ USB storage.**	<<Insert your response here>> *Survey staff* *Computer logs.*	<<Insert your response here>> *The use of eternal devices poses a threat because a person will physically input a drive that could be carrying malware. In this instance, the malware does not have to pass through firewalls, password protection or other means to block it.*

Task 2

Based on the instructions you received from Con Kafatos, you will create a brief and informative instructional guide for all staff using the **Cyber Security Instructional Guide.**

- Create an instructional guide with step-by-step instructions, including screenshots to illustrate how to install anti-malware software, and monitor and evaluate security threats. Download and install the following apps:
  - Avast One: https://www.avast.com/
  - Authy [two-factor authenticator]: https://authy.com/
- Your guide must include clear instructions on how to do the following so that they are updated and configured correctly as part of the start-up procedure.
  - Monitor the latest developments in digital security.
  - Encrypt two different types of devices.
  - Install and use a two-factor authentication app [Authy].
  - Install, use and update anti-malware software [Avast One].
  - Install and use a VPN [Avast One browser] to access company data when not in the office.
  - Instructions on how to set up strong passwords.

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

- **<Student Number> Cyber Security Instructional Guide**

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

- create instructional information to assist company staff to use best practices in cyber security for at least two devices.

The student must complete the instructional guide with a sufficient description of each category and attach screenshots that guide through the instructions clearly. More specifically:

- The student must illustrate how to encrypt two digital devices, such as one smartphone and one laptop (or tablet, or desktop PC). See **Cyber Security Instructional Guide - Assessor Guide** for benchmark response.
- The student must describe where to look and what to look for when the company seeks to monitor the latest developments in cyber security. Responses can include websites with relevant information, such as:
    - https://cybermap.kaspersky.com/
    - https://www.akamai.com/internet-station
- Encryption of a device refers to the use of passwords or other authentication methods to restrict access to the device. Encryption also refers to operating systems that have built-in encryption processes that allow for the encryption of all the data on the device. A complete guide, including screenshots, must be included to demonstrate the requirements for encryption as provided in the **Cyber Security Instructional Guide - Assessor Guide**.
- The student should illustrate how to download, install and set up the anti-malware software Avast One. The guide must include screenshots of the process. Examples are given in the **Cyber Security Instructional Guide - Assessor Guide**.
- The student must describe the purpose of using a VPN and when to use it, for example, in this case, to allow the company server to believe that the person accessing the server is in the correct location to gain access. The student can describe when to use the VPN, for example, when accessing company data outside the secure company servers. Instructions on how to set up a VPN must include screenshots of the VPN client using the Avast Browser.
- The student can describe the qualities of a strong password. Including the use of upper and lowercase letters, numbers and special characters. Instructions on not using easy-to-guess words or phrases.

Task 3

For this part of the task, you will create two video tutorials showing CBSA staff how to set up their two devices using best practices in cyber security.

- Use two different devices that you have access to and create a video tutorial for each. The two video tutorials must present clear instructions and demonstrate how to do the following:
    - download and install the free version of Avast One
    - set up two-factor authentication using the Authy authentication app
    - use of VPN when not on the company network (can be done using Avast One browser or a third-party app of your choice)
    - encrypt the devices using native operating system processes or any selected software
    - update software and applications.
- You can create the videos using a free version of Zoom that will allow you to create 40-minute videos. The steps to use Zoom are:
    - download and install Zoom
    - open the program and begin a call

– share your screen and record yourself giving instructions and showing what to do on your screen.

The end result will be a recording of your screen where you can show how to do the above-mentioned tasks. Your speech will be recorded, and that can serve as a video tutorial.

Save and submit your videos along with this assessment using the following naming conventions:

- **<Student Number>** Video Tutorial 1
- **<Student Number>** Video Tutorial 2

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

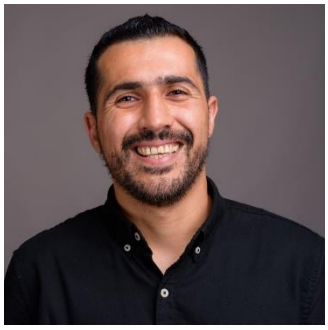
- set up and maintain security of two digital devices using best practices in cyber security.

Ensure the following videos have been submitted for assessment:

- Video tutorial for device 1
- Video tutorial for device 2.

Each video must cover the following criteria:

- In the video, the student must demonstrate having downloaded and installed Avast One on the device.
- They must show the step-by-step process to set it up and running. The student should clearly explain each of the steps in the video.
- In the video, the student must demonstrate downloading and installing Authy on both devices. They must give an example of how to use Authy to sign into any software/app of their choice.
- Student must show the user inputting the code from Authy into the app to gain access.
- In the video, the student must demonstrate having opened the browser and clearly showing the green VPN icon in the search bar and indicating that the connection to the internet is secure and anonymous.
- The student must provide an example for each device on how to set up strong access. They must give an example of how to encrypt the entire device or single folders on the device and add a layer of protection if the device is hacked.
- The student must demonstrate where to check for updates and instruct users how to install updates or patches whenever requested as a practice of cyber security. The student must also verbally explain the steps.



To:	Sally Fischer
From:	Con Kafatos (con.kafatos@cbsa.com.au)
Date/time:	01/11/2022 1:30 p.m.
Subject:	Draft Memo to All Staff

Good afternoon Sally,

Nice work on the tutorials. I've reviewed your work, and I can see you put a lot of time into creating these. Well done!

I think it's time we communicate this to all the staff and get everyone on board with a new physical security plan.

Please create a Physical Security Plan which explains the best practices in physical security. Here's what you'll need to include in your email and the plan:

- Reference to the instructional tutorials that you have created (written and video).

Provide guidance on which software we've selected and instruct them to follow the tutorials for set-up.

- Requirements for using personal devices for work-related activities.
- Guidance on the physical security measures for using external storage devices, lost/stolen devices and being wary of unknown people following them into the building.
- Reference to creating strong passwords, not accessing unknown emails, not installing third-party apps without authorisation, etc.
- Information about storing files only in our cloud-based file storage system, which is encrypted and the most secure storage method.
- Use of VPN to access their files.

I think the most important thing is to ensure staff are aware of creating strong passwords and using the encryption processes.

The last thing is to request from all staff, an updated list of the documents stored on their devices. We will use this information to create a register of all devices in use and categorise the risk level to put the appropriate measures into practice.

We'll need all staff to action this within five working days, so please indicate that in your email.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 4

Refer to the instructions given by Con Kafatos in his email above. You need to create a physical security plan and email it to all staff with instructions and guidance on the best practices of cyber security.

Create **a physical security plan** using the template below to circulate to all CBSA staff. Introduce the concept of physical security and explain why this is important for all staff to follow. Your plan must address the following points:

- people following and entering the building
- sharing passwords
- use of external storage devices
- what to do if a USB is found in or around the building
- the use of company devices outside of the office
- the use of public USB charging stations.

You will need to use the Physical Security Plan Template provided below.

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

- *to create a physical security plan and communicate to all staff*

The student's physical security plan must meet the following criteria:

- *The student must create a physical security plan using the template provided and include the best practices of cyber security and address the following points:*
    - *people following and entering the building*
    - *sharing passwords*
    - *use of external storage devices*
    - *what to do if a USB is found in or around the building*
    - *the use of company devices outside of the office*
    - *the use of public USB charging stations.*

A sample answer is provided below:

Physical Security Plan Template
Introduction: *Introduce and explain what physical security is and what it covers.* *[Approximate word count: 50 – 70 words]* <<Insert your response here>> The student must introduce the physical security plan by covering the following points: ▪ Physical security of digital devices covers the use of the device in certain circumstances, in particular, use outside of the office. ▪ Physical security of digital devices ensures that devices remain secure even when used on potentially insecure networks. ▪ Physical security ensures that all staff members are aware of who enters the premises, thereby limiting access to potentially sensitive information.
Importance: *Discuss the importance of physical security* *[Approximate word count: 30- 50 words]* <<Insert your response here>> The student must identify why this is important by stating that: ▪ Physical security is the responsibility of all staff. ▪ Physical security is vulnerable in ways that digital security is not and requires added vigilance and careful use of digital devices.
Plan: *Address all six [6] points mentioned in the task instructions.* <<Insert your response here>> The student will create a physical security plan by covering the following points at a minimum:

- Be aware of unknown people who may follow you into the building. If you see any unknown users in the office, report them to security immediately.
- Do not give out your passwords to anyone. Keep passwords secret at all times.
- Do not use external storage devices in company devices.
- If you find an external storage device, do not plug it into your computer. Report it and hand it over to IT staff immediately.
- If you are using your company device outside of the office, check your surroundings to ensure nobody is watching as you enter your password or other sensitive details.
- Do not plug in your device to charge in a public USB charging port. Use a power outlet to charge your devices.

Task 5

Refer to the instructions given by Con Kafatos in his email above. Write an email to all staff with instructions and guidance on the best practices of cyber security.

In your email to all staff members, attach and make reference to the following:

- Physical Security Plan
- Cyber Security Instructional Guide
- Video Tutorial 1
- Video Tutorial 2

Ensure you cover all the points mentioned in Con's email, including:

- An overview and the steps to ensure your devices are kept secure and up to date
- An overview of your physical security plan

You will need to use the email template provided below.

[Approximate word count: 400 – 500 words]

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

- *communicate to all staff*
- *to request information that will be used to create a digital register.*
- *Physical Security Plan Template*

The student's physical email must meet the following criteria:

- *The student's email must be written using the CBSA Email Template and must use a professional tone to address the staff. It should include details as requested by Con and the reference documents and Physical Security Plan attached.*
- *The student must make reference to the two sources of further information and instructions on setting up the devices that they created in Part B and Part C of this task.*
- *The student has made a clear request for each staff member to provide a list of data that is held on each of their company devices.*

A sample answer is provided below:

Email Template	
To:	*All staff*
From:	*Sally Fischer (sally.fisher@cbsa.com.au)*
Date/time:	*05/11/2022 4:42 p.m.*
Subject:	*Cyber Security Policy Update*
Attachments:	*Physical Security Plan, Instructional tutorial document, Instructional video 1, Instructional video 2*

<<Write your email here>>

To all staff,

.Most of you will already be aware of these practices, but we need to ensure all staff know and practice cyber security in the best way possible. For everything that we are asking you to do, I've created tutorials on how to install and maintain your devices. Please go through the instructional guide, follow along with the videos and complete the steps as soon as possible to ensure that all our work devices are protected for our next project. This needs to be actioned and all systems up and running within five business days from today.

*Here's an **overview** and the steps to ensure your devices are kept secure and up to date:*

- *We've selected anti-malware software (Avast One) that everyone will be required to download, install and keep up to date.*
- *The use of personal devices for work-related activities is no longer allowed. Please ensure you only use devices issued to you for work purposes and keep your personal devices free of company information.*
- *You must not use any external storage devices (USB or external hard drives) to store or access information. All company files must be stored using our cloud-based storage system.*
- *Refer to the guide on how to set up strong passwords and ensure that you change passwords periodically.*
- *If you use a company device (tablet or laptop) outside of the office network, ensure you use the Avast One browser and switch on the VPN function. Refer to the tutorials for guidance on how to do this.*
- *If you receive suspicious emails or notifications, please report them to the manager of the IT department immediately and DO NOT open any attachments or links that come from unknown sources.*

*Please refer to the **physical security plan** attached. It includes the following:*

- *Be aware of unknown people who may follow you into the building. If you see any unknown users in the office, report them to security immediately.*
- *Do not give out your passwords to anyone.*
- *Do not use external storage devices in company devices.*
- *If you find an external storage device, do not plug it into your computer. Report it and hand it over to IT staff immediately.*
- *If you use your company device outside of the office, check your surroundings to ensure nobody is watching as you enter your password or other sensitive details.*
- *Do not plug your device to charge in a public USB charging port. Use a power outlet to charge your devices.*

If you have any questions, please reach out to me or contact Con for urgent or sensitive matters.

*Also, please send Con and me, an updated **list of the documents** stored on your devices. We will use this information to create a register of all devices used by CBSA Staff.*

Kind regards,

Sally Fisher

Systems Analyst

Assessment checklist:

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

1	Task 1 – **Cyber Security Systems Review Plan Template**	☐
2	Task 2 – **Cyber Security Instructional Guide**	☐
3	Task 3 – **Two (2) video tutorials**	☐
4	Task 4 – **Physical Security Plan**	☐
5	Task 5 – **Email**	☐

Congratulations you have reached the end of Assessment 2!