BSBXCS402

# Promote workplace cyber security awareness and best practices

## Assessment 6 of 6

Project

SWIN BUR NE OPEN ED

## Assessment Instructions

### Task overview

Read the instructions carefully before typing your response in the space provided.

### Additional resources and supporting documents

To complete this assessment, you will need:

- Learning Resources
- CBSA Lessons Learned Form
- CBSA Email Template
- Cybersecurity Awareness Policy and Procedures (from the previous assessment)

## 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.

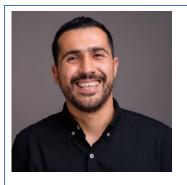Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

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 complete a self-reflection exercise on the training session you delivered to help with continuous improvement for CBSA. Read Con's Email below:

| | | |
|---|---|---|
| | **To:** | Tan Yamamoto (tan.yamamoto@cbsa.com.au) |
| | **From:** | Con Kafatos (con.kafatos@cbsa.com.au) |
| | **Date/time:** | Tuesday 11:19 a.m. |
| | **Subject:** | Document Lessons Learned |

Good morning Tan,

A.        Thanks for conducting the training session the other day; I heard it went well!

B.        I would like you to complete a self-reflection exercise on the training session you delivered to help with continuous improvement for CBSA, your personal development as well as to maintain a record of the update to the cybersecurity program.

I would also like you to update the Cybersecurity Awareness Policy and Procedures based on any feedback received from the participants in the training session and based on your self-reflection. You can then send an email to all staff the updated policy outlining what improvements were made.

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 CBSA Lessons Learned form, undertake a self-reflection exercise, documenting the following:

- what went well during the training session

- what could be improved during the training session

- at least one recommendation on how the Cybersecurity Awareness Policy and Procedures could be improved.

- submit the document along with this assessment, using the following naming convention:

    **<StudentNumber>Lessons Learned**

You can include the project name as Cybersecurity Awareness Program and input your name as the project manager.

B.    Update the Cybersecurity Awareness Policy and Procedures to include at least one improvement as documented in the Lessons Learned document from the previous task.

- submit the document along with this assessment, using the following naming convention:

   **<StudentNumber>Cybersecurity Awareness Policy and Procedures – UPDATED**

C. Develop an email to notify all CBSA employees of the insights learned from the training session using the CBSA Email Template, including:

- Specifying the people to whom the email will be sent. Use 'All CBSA Employees'.

- Specifying that the email is being sent by yourself.

- Specifying the date and time that the email was developed.

- Specifying a relevant subject line.

- Specifying the document that will be attached to the email.

- Specifying a relevant opening, body and closing section of the email notifying the employees of lessons that were learned from your self-reflection review and the update made to the Cybersecurity Awareness Policy and Procedures.

- submit the document along with this assessment, using the following naming convention:

   **<StudentNumber>Email**

   [Approximate word count: 130 – 150 words]

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

- maintain the cybersecurity awareness program, reflecting organisation-wide best practice

- maintain related records of the cyber security awareness program

- present insights from training to required personnel and potential related impacts on the workplace

- document outcomes of the review and suggested improvements for consideration by required personnel

- communicate review outcomes and cyber security improvement requirements according to organisational policies and procedures.

More specifically, the student:

- Completed the Lessons Learned form as per sample.

- Documented at least one update to the Cybersecurity Awareness Policy and Procedures based on the self-reflection they documented in the Lessons Learned Form. The cybersecurity policies and procedures can be included with the following:

  o Updating anti-malware to secure the devices from viruses.

  o All devices will be installed with the latest anti-malware software by the IT Team.

  o All patches and updates from the software will be downloaded as and when released and all staff will be notified.

- Completed the Email Template as per the sample.

Benchmark answers are provided below:

- ***Lessons Learned Form Template***

| What went well | *Trainees responded well to the training session. They showed great interest and asked many clarifying questions.* |
| --- | --- |
| [Approximate word count: 15 – 30 words] | |

SWIN
BUR
NE

OPEN
ED

| | |
|---|---|
| **What needs improvement**<br><br>[Approximate word count: 15 – 30 words] | *Trainee knowledge was limited on cybersecurity threat events, so more in-depth training on the threat events and clarity on procedures to follow would improve their knowledge.* |
| **Recommendations for future improvements**<br><br>[Provide two (2) recommendations. One of them needs to relate to your training based on your training session plan] | *Develop procedures for more identified threat events in the Cybersecurity Awareness Policy and Procedures so further training can improve employee understanding of cybersecurity threats. Also the policy needs to be updated with the process of updating anti-malware at regular intervals.*<br><br>*Allocate more time for Q&A to address staff enquiries.* |

- ▪ *Email Template*

*To: All CBSA Employees*

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

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

*Date/time: XX/XX/20XX 10:17 a.m.*

*Subject: Cybersecurity Insights*

*Attachments: Cybersecurity Awareness Policy and Procedures*

*To all employees*

*After conducting the recent cybersecurity awareness training session, I just wanted to share some insights from this training as follows:*

- ▪ *What went well: the trainees responded well to the training session, agreeing that it was worthwhile and important to be well aware of the cyber threats and cybersecurity procedures.*

- ▪ *What needs improvement: trainee's current knowledge was limited on cybersecurity threat events, so more in-depth training on the threat events would help improve their knowledge.*

- ▪ *Recommendations for future improvements: develop more procedures for more threat events in the Cybersecurity Awareness Policy and Procedures so further training can improve employee understanding of cybersecurity threats. The Cybersecurity policy and procedure have been revised to include the process of updating anti-malware on all CBSA systems.*

*In line with the recommendation, I have attached the updated Cybersecurity Awareness Policy and Procedures for your review.*

*Please let me know if you need clarification on any of the above.*

*Kind regards,*

*Tan Yamamoto*

SWiN BUR NE

OPEN ED

**Assessment checklist:**

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

| | Task 1 | |
|---|---|---|
| 1 | ▪ CBSA Lessons Learned Form<br>▪ CBSA Email Template<br>▪ Cybersecurity Awareness Policy and Procedures (from the previous assessment) | ☐<br>☐<br>☐ |

**Congratulations you have reached the end of Assessment 6!**