BSBXCS402

Promote workplace cyber security awareness and best practices

Assessment 5 of 6

Role Play

Assessment Instructions

Task overview

Read the instructions carefully before participating in the Role Play.

Additional resources and supporting documents

To complete this assessment, you will need:

- Learning Resources
- Cybersecurity Awareness Policy and Procedure (developed in the previous assessment).
- Training Session Plan (developed in 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.

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 your manager, Con Kafatos, to deliver a training session on the Cybersecurity Awareness Policy and Procedures you developed in the previous assessment task.

Task 1

- You are to train CBSA staff members from different departments in the Cybersecurity Awareness Policy and Procedures that you have developed, including:
  - the Cybersecurity Awareness Policy and Procedure you developed in the previous assessment task, including the two procedures you developed.
- At the end of the session, you must ask questions to gather feedback from the participants on possible improvements to the policy and procedure or the training delivery itself.
- You must follow the Training Session Plan you developed in the previous assessment
- You must comply with CBSA's Communication Policy and Procedures during the training session.

Your training session should run for approximately 15 - 20 minutes.

During the role play, your assessor will be looking to see that you can:

- communicate cyber security policies and procedures to CBSA staff members from different departments
- asked relevant questions to gather feedback from the participants
- answer queries from the participants clarifying doubts about the procedures
- obtain feedback for improvements to the cybersecurity policies and procedures
- provide sufficient training and information updates that support practice or awareness concerning two different cyber security matters.

Assessor instructions: The purpose of this task is to observe the student's skills in a simulated environment. The student must demonstrate the following skills:

- communicating cyber security policies and procedures to CBSA staff members from different departments
- provide sufficient training and information updates that support practice or awareness concerning two different cyber security matters.

Role play instructions

In this task, you will participate in a role/play meeting with **two (2) others**. These may be sourced using one of the following options:

- peers to who you are already working within the industry your qualification relates to.
- fellow students who will play the role of the stakeholders. Please contact your fellow students via the Discussion Forum and coordinate your role play with them directly.

The role play/meeting must not exceed **20 minutes** in duration and must address all elements of the Observation Checklist below.

If you are unable to find participants to play the role of the other team members, contact your assessor via the Discussion Forum, who will discuss options for pairing up with other students to complete this task.

Option 1: Peer participants

Should you complete this task with your peers, you must fully brief all participants, providing them with the context of the role play/meeting, a role outline to play and a copy of the observation checklist so that they can prepare for the recording.

Peers will need to state their name and job title at the start of the recording to inform consent.

Option 2: Fellow student participants

Fellow students participating in the recording must be provided with context to their role and responsibilities in the session and have reviewed the assessment activity and observation checklist so that they can prepare for the recording.

Students will need to state their name and that they are a student (as their job title) at the start of the recording to inform consent.

Participants' briefing instructions:

Each participant must be assigned a position according to the CBSA Organisation Chart. The roles selected must be from different CBSA departments as we need interdisciplinary teams.

Roles: Training Participants

You have been tasked to attend a cybersecurity training session delivered by the student.

- During the role play, you must be accommodating to the students' presented information by paying attention to what is being presented and displaying good non-verbal communication cues (nodding head, leaning forward, not crossing arms or slouching, etc.)
- You should ask clarifying questions if you don't understand the presented information, such as:
  - Why is cybersecurity so important?
  - Can you explain spam emails and how to identify if the email address is fake
  - Can you explain how external devices can be a threat?
- When asked by the student for any feedback on any improvements, you can highlight how anti-malware updates would be handled in future.

Recording instructions

Your role play must be recorded with all participants captured in a virtual room using a system such as Zoom, Skype or Teams.

Consent to participate in the recording must be captured for all participants at the start of the meeting. This is achieved by the student reading the following statement at the start of the recording, with all participants replying with their name and job title to inform consent.

"This session/presentation is being recorded for assessment purposes for my course with Swinburne Open Education. This session will be recorded and submitted through my course online learning platform to my Assessor for grading. All participant/s in this session indicate their consent to be included in this recording by stating their name and job title."

The time taken to capture consent at the start of the recording does not count towards the recording time limit.

Include this recording as part of your assessment submission.

ASSESSOR OBSERVATION CHECKLIST

Students are required to upload a video of themselves and **two (2) others** engaged in a short meeting.

The participants must be fully briefed as outlined in the role play instructions.

The meeting should be a maximum of **20 minutes.**

Students must demonstrate each of the performance criteria outlined in the observation checklist below.

ACTIVITY	SATISFACTORY YES / NO			ASSESSOR COMMENTS
Task checklist				
• The student communicated cyber security policies and procedures to CBSA staff members from different departments.				The student explained what cybersecurity is, and explained the different sections of the cybersecurity awareness policy and procedures they developed, including: • purpose • policy • procedures.
• The student asked questions to gather feedback from the participants.				The student should ask questions to the participants to obtain feedback on the possible improvements to the policy and procedure or the training delivery itself, such as: • Are you comfortable with these procedures that I have trained?

				• Should I provide any examples? • Is there any point that you would like to add to the procedures I've developed?
• The student sufficiently answered queries from the participants clarifying doubts about the procedures.				Students answered any questions from the participants. For example, cyber-attacks are very common and can expose all the confidential information or corrupt the entire server. Cybersecurity safeguards all types of intellectual property and personal information against theft and loss. For spam emails, look out for the sender, the subject line and the email address as it is not in a standard format, or the grammar will be incorrect, etc.
• Student asked for feedback on improvements to the cybersecurity policies and procedures.				In the course of the discussion, the student should ask for feedback on improvements from the participants and confirm that the policy will be updated with it.
• Provided sufficient training and information updates that support practice or awareness concerning two different cyber security matters.				The student must train on the two procedures and updates they developed, ensuring that the training participants clearly understand these procedures. For example, procedures around setting passwords, spam emails and use of external storage devices.

Assessment checklist:

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

1	Task 1 – Role Play	☐

Congratulations you have reached the end of Assessment 5!