# Assessment Task 3: Supporting cyber security practices in the workplace

|  |  |
| --- | --- |
| Course code and title | Promote workplace cyber security awareness and best practices |
| Unit code and  title | ICT50220||BSBXCS402 |
| Due date | Session 7 |
| Resources  required | **Learner to provide:**   * Computer Access with Microphone & Video (optional) & Internet * Organisation’s cybersecurity policies and procedures or the Australian Cyber Security Centre’s guides   **Provided:**   * MS Teams * MP Tech Solutions Company Profile * Cybersecurity Awareness Survey Template * Cybersecurity Finding Review Report * Cybersecurity awareness program Template |
| Decision making rules | To achieve an overall satisfactory result for this assessment task:   * Learners must achieve a satisfactory result for each item in the **Assessment Checklist/s.** |
| Learner  instructions | This assessment will occur in the workplace or simulated environment.  Part A identify and review cyber security practices in the work area  This task requires you to   * Identify current knowledge and awareness of cybersecurity by developing questions which you will the use to undertake consultation with the staff from the organisation. * You will need to record these consultation meetings as evidence of having discussed this with the staff. If you are filming the recording your assessor will provide you with the instructions to assist in producing a quality video, that meets compliance and confidentiality requirements where applicable. * You will then review the findings against cybersecurity legislative and organisational requirements and write a report for management.   Part B Create a cyber security awareness program  For this task you are required to developacybersecurity awareness program for colleagues that support and promote cybersecurity practice and awareness in relation to **2 different cyber security matters.**  Part C Arrange delivery of the cybersecurity awareness program  This task requires you to arrange the training and information updates in the workplace of the cybersecurity awareness you developed in part B of this assessment task.  Refer to the task outline for further information.   * Check Moodle Unit for Assessment due date * You will be able to ask clarification questions of your instructor during your weekly MS Teams meeting or your Face to Face session * Reasonable adjustment may include an extension of time, oral questions and answers etc. * All assessments are to be submitted electronically   If you have any questions about the task or concerns about your ability to complete the task, please discuss this with your Assessor. |

## Part A Identify and review cyber security practices in the work area

1. Using your organisation’s cybersecurity policies and procedures and/or the Australian Cyber Security Centre’s guides, you need to develop **8 questions to ascertain the work area’s level of cybersecurity awareness** in the areas of:

* securely storing, sharing and managing information
* encryption, and protocols for its uses
* data classification and management
* media/document labelling
* data governance
* bring your own device
* acceptable use

Document your questions in the Workplace Cybersecurity Awareness Survey Template.

|  |  |  |  |
| --- | --- | --- | --- |
| **Cybersecurity Awareness Survey Template** | | | |
| **Name of the person assessed:** | | **Wang YiZhuo** | |
| **Email address:** | | **w769763549@outlook.com** | |
| **Department:** | | **Information Technology - 1 (3+2)** | |
| **Questions**  *List 8 questions you will ask to ascertain the work areas level of cybersecurity awareness.* | | | |
|  | Question | | Person’s response |
|  | What constitutes a cyber-attack? | | A cyberattack is an attempt by a hacker to disrupt or destroy a computer network or system. Cyberattacks can be malicious, such as stopping a computer, stealing data, or using a compromised computer as a springboard for other attacks. |
|  | What are the four classifications of data? | | Typically, data can be categorized into four groups: public, exclusively internal, confidential, and restricted. |
|  | What are the four principles of cybersecurity? | | These principles of cybersecurity are organized into four primary actions: govern, safeguard, detect, and react. |
|  | Are you aware of the location of your existing code of ethics? | | In fact, a physical copy is available to everyone in the office, and whenever it is updated, a digital version is distributed to all employees. There are also awareness-raising signs and posters. |
|  | How crucial do you perceive cybersecurity awareness to be in the workplace? | | Cybersecurity awareness holds immense significance in every workplace, and it's imperative that every employee receives training on prevailing cybersecurity trends and threats pertinent to the organization, such as phishing scams. |
|  | How does cybersecurity apply to your role in the workplace, and why is it vital to educate employees about it? | | It is crucial for employees to stay on top of current threats to prevent any data loss or cyberattacks, as the human element is often the weakest link in any company. Without awareness of risks and procedures, mistakes can easily occur. |
|  | Do you feel you've received sufficient training in terms of cybersecurity awareness and procedures? | | No, I feel like I haven't gotten enough training, and I'm unsure about what I should watch out for and how to spot scams to safeguard our clients' data. |
|  | How do you ensure the secure storage, sharing, and management of sensitive information in your workspace? | | Ensuring that information is stored, shared and managed securely is critical to protecting sensitive data from unauthorized access or disclosure.  What protocols or measures are implemented to ensure data is stored securely, shared only with authorized individuals, and managed effectively to avoid data loss or leakage. |
| Any other feedback or suggestions:  I highly suggest conducting regular training sessions to tackle emerging risks and vulnerabilities, ensuring all employees grasp their significance.  It's imperative to provide additional training on the code of ethics, elucidating employee responsibilities and underscoring adherence.  Consistent training sessions are indispensable for keeping employees abreast of evolving risks and vulnerabilities. | | | |

## Consult with stakeholders

1. You are now required to interview a **minimum of 6** **people in the work area. Record your interview with each of the 6 people. This may be done as a group consultation however each person will need to complete the survey form.**

It is important to obtain information from people working in a range of different disciplines within the organisation (e.g.; finance, administration, legal etc).

1. You will now collate and review the information you have obtained and provide a report for management about the findings. Your report will need to use clear, specific and industry-related terminology relating to cyber security

|  |  |  |
| --- | --- | --- |
| **Cyber Security Finding Review Report** | | |
| Overview of findings from information gathered from work area - including current trends identified in the work areas cybersecurity awareness and workplace practice of the staff. | | |
| As we all know, cybersecurity is a process designed to protect networks and devices from external compromise. Companies often hire cybersecurity professionals to protect their sensitive information, maintain employee productivity, and increase customer confidence  in their products and services.  The following is the overview of findings from information gathered including current  trends identified in the work areas cybersecurity awareness and workplace practice of the  staff  1.Denial of Service, or DOS  Where a hacker consumes all of a server’s resources, so there’s nothing for legitimate  users to access  2.Man in the Middle Attack  Hackers are placed between the victim's machine and the router to sniff out packets  3.Phishing  Where a hacker sends a seemingly legitimate-looking email asking users to disclose  personal information  4.Malware  Where victims are hit with a worm or virus that renders their devices useless | | |
| Examples where current practice is complying with organisational policies and procedures:   * Employing robust passwords and utilizing a password management utility. * Implementing two-factor or multi-factor authentication methods. * Educating oneself on phishing schemes and adopting a skeptical stance towards emails, phone calls, and flyers. | | |
| 3 Cybersecurity work practices or awareness that do not align with the organisation’s policies and procedures or best practice (Potential threats) | | Potential impact on the company |
|  | Implementing multifactor authentication | Cybercriminals face greater difficulty accessing employee accounts without multi-factor authentication (MFA). |
|  | Reinforcing secure password practices | Strengthening passwords enhances computer protection against hackers and malware. Employees should maintain robust passwords for all computer accounts. |
|  | Conducting cybersecurity training for employees | Inadequate safety training for employees results in decreased vigilance, making it more likely to miss potential threats and fail to report incoming events. |
| Suggested ways to improve cybersecurity awareness for each of the 3 potential threats identified | | |
|  | Employing anti-virus protection and firewall | |
|  | Familiarizing oneself with phishing scams and being highly cautious of emails, phone calls, and flyers | |
|  | Utilizing anti-virus protection and firewall | |

## Part B Create Cybersecurity awareness program about 2 cyber security matters.

Based on your report you are required to developa cybersecurity awareness program for colleagues that support and promote cybersecurity practice and awareness in relation to **2 different cyber security matters.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **cybersecurity awareness program** | | | | |
| **Trainer Name:** | | DAN | | |
| Planned training date: | | 5/18/24 | | |
| Planned training time from/to: | | 11am-12am | | |
| Cyber Security Matter 1:  *Denial of Service (DOS) Attack* | | | | |
| Cyber Security Matter 2:  *Phishing attack* | | | | |
| Objectives of the training to meet organisation-wide practice:  *The primary objective of the training is to formally instruct employees on the different cyber threats in existence, how to recognize them, and the measures required to guarantee their own security as well as the security of the company.*   1. *Educate on the utilization of an anti-virus application.* 2. *Recognize phishing emails.* | | | | |
| Skills to be developed:   1. *Staying abreast of cybersecurity compliance regulations.* 2. *Mitigating the risk of employees falling victim to phishing scams.* | | | Knowledge to be developed:   1. *Embed cybersecurity principles into the company's culture.* 2. *Minimize the probability of a successful breach.* | |
| Training method/s:  Demonstration  Explanation  Showing videos  Providing examples  Research and discussion | | | | |
| Simulated training method (list the technology platforms to assist with promoting cyber security) :  The listed security platforms offer clearly delineated and adaptable response and mitigation strategies against threats, encompassing both automatic and manual options.  Illustrative examples of penetration testing tools and frameworks encompass malware protection, Metasploit, Kali Linux, Zoom meetings, Windows security firewalls, etc. | | | | |
| Training location:  Trainings Hall | | | | |
| Training activities | | | | Resources required |
| 1. | CYBER SECURITY AWARENESS TRAINING | | | Training sessions aimed at increasing awareness of cyber security among employees, focusing on identifying cyber threats, practicing secure password usage, safeguarding personal information, etc. |
| 2. | Simulated network attack drills | | | Conducting drills that simulate network attacks to help employees develop skills in responding to real-world network security threats. |
| 3. | Data security training | | | Providing education to employees on securely managing, storing, and transmitting sensitive data to prevent data breaches. |
| 4. | Network security technical training | | | Technical training sessions designed for IT staff or professionals, covering topics such as network security tools, vulnerability assessment, malware analysis, etc. |
| 5. | Emergency response drills | | | Organizing drills to simulate network security incidents, aiming to enhance employees' ability to respond effectively during emergencies. |
| 6. | Social engineering drills | | | Simulating social engineering attacks to educate employees about recognizing and thwarting phishing emails, deceptive phone calls, and other social engineering tactics, thereby enhancing their awareness and response capabilities. |

## Part C Arrange delivery of the cybersecurity awareness program

You are now required to arrange the training and information updates in the workplace of the cybersecurity awareness you developed in part B of this assessment task.

You will need to provide evidence of delivering this training to the workplace. This may include PowerPoint/slides, video evidence, phishing emails etc.

Your evidence will reflect the training program that you designed in Part B

**Submit your evidence electronically via the Learning Management System.**

* **e.g. AB\_BSBXCS402\_Task 3 Delivery of the cybersecurity program \_v1.0**

## Assessment Checklist: Task 3 - Supporting cyber security practices in the workplace

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Learner name** | | WangYiZhuo | **Learner ID** | | S1554654 | |
| **Assessor name** | |  | **Date** | |  | |
| Assessment checklist  assessor to complete the following | | | | | | |
| documentS | | | | | | |
| **The LEARNER submitted:** | | | | **SATISFACTORY** | | **NOT SATISFACTORY** |
|  | The completed Cybersecurity Awareness Survey from 6 people a range of different disciplines within the organisation (e.g. finance, administration, legal etc). | | |  | |  |
|  | The 6 recordings of the consultation with the 6 colleagues | | |  | |  |
|  | Correctly answered all sections of the Cybersecurity Finding Review Report | | |  | |  |
|  | Developed a Cybersecurity awareness Program relating to 2 different cyber security matters and answered all sections of the Cybersecurity awareness Program template | | |  | |  |
|  | Evidence of having successfully implemented the Cybersecurity awareness Program | | |  | |  |
| **Feedback:** | | | | | | |

## Assessment Task Summary: Task 3 - Supporting cyber security practices in the workplace

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Trainer/Assessor to complete the following:  **THE LEARNER:** | | | | | | Yes | No |
| 1. | Satisfactorily completed all items in Assessment Checklist | | | | |  |  |
| feedback **-** Assessor must include feedback | | | | | | | |
|  | | | | | | | |
| OVERALL TASK result | | | | | | | |
| Satisfactory  Not Satisfactory (resubmission required) – Due date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | |
| Date Assessment Returned | | |  | | | | |
| Trainer/assessor Name | | |  | | | | |
| Trainer/Assessor signature | | | X | | | | |
| **LEARNER DECLARATION**: Please read and sign below | | | | | | | |
| I, \_WangYiZhuo+S1554654\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ have been advised of the outcome of this assessment task.  PRINT NAME | | | | | | | |
| LEARNER Signature | | WangYiZhuo+S1554654 | | Date |  | | |