# Assessment Task 2: Cyber security threats 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  **Provided:**  MS Teams  Threat Register template  Action Plan  Cybersecurity Policy 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 has task is based on a case study and requires you to review  the latest cyber security threats and trends and to make suggested  improvements for the organisation.  Part A Review latest cyber security threats and trends  For this task you will identify and document 8 cybersecurity threats and trends that may impact the organisation.  Part B Develop an action plan  You will develop an action plan based on the outcomes of the previous tasks to implement 2 cyber security measures.  Part C Develop a set of policies and procedures  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. |

## Assessment Task 2 Instructions

You have been asked to manage the organisation's approach to cybersecurity and to identify possible threats. You will need to develop protective measures to address the identified threats.

You will need to use the MP Tech Solutions as an organisation or your own workplace.

## Part A Review latest cyber security threats and trends

#### Develop a threat register

Using Word software, and the Threat Register template provided, document **8 cybersecurity threats** **and trends** that may impact the organisation.

For each potential threat and trend, you need to:

* Assign a unique cybersecurity threat id number (column 1)
* Provide an appropriate name for the threat (column 2)
* Provide a brief description of the threat (column 3)

#### Register an event

Using Word software, document in the **1 likely threat event for each of the 8 threats** you identified in the previous task.

For each threat event, you need to:

* Assign a unique cybersecurity threat event id number (column 4)
* Provide a brief description of the threat event (column 5)

#### Risk Assessment and mitigation

Using Word software, document a threat assessment of the **8 threat events** you have identified in the previous task.

Add the information to the **Threat Register**.

For each threat event, you need to:

* Determine the consequence of each threat using the Threat Consequence Table provided.
* Determine the likelihood of each threat using the Threat Likelihood Table provided.
* Determine the current threat level rating of each threat based on the threat consequence and threat likelihood using the Threat Matrix provided
* List appropriate cybersecurity protection measures for each threat.
* Determine the expected level of effectiveness of the proposed cybersecurity protection measures for each threat event using the Cybersecurity Effectiveness Rating Scale provided.
* Using the Cybersecurity Effectiveness Rating Scale, determine and document the new threat level rating of each threat based on the effectiveness of the identified cybersecurity protection measures.

Submit your answers electronically via the Learning Management System.

File Naming Convention:

BSBXCS402 AT2 ***Student Name & Student Number***.docx

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Threat Register** | | | | | | | | | | |
| **Cybersecurity threats**  **(Task 2.1)** | | | **THREAT EVENT REGISTER**  **(Task 2.2)** | | **RISK ASSESSMENT AND MITIGATION**  **(Task 2.3)** | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** |
| **Threat ID** | **Threat type** | **Threat description** | **Threat Event ID** | **Threat Event description** | **Likelihood** | **Consequence** | **Current threat level** | **Cyber security protection measures** | **Expected effectiveness**  **(1-5)** | **New threat level** |
| 1 | T1 | Credential stuffing | Attacks take advantage of using that reuse passwords across various platforms by using stolen login credentials from one breach to access other accounts without authorization | N/A | N/A | High | Unauthorized access, data theft | High | Multi-factor authentication, account monitoring, password policies | 4 | Moderate |
| 2 | T2 | Denial of Service (DoS) | Cybercriminals overwhelm a system or network with an overwhelming amount of requests or traffic, rendering it inaccessible to authorized users, upsetting business processes, and resulting in losses. | N/A | N/A | High | Disrupted operations, financial loss | High | DDoS protection services, traffic filtering, server scalability | 4 | Moderate |
| 3 | T3 | Form jacking | Cybercriminals insert harmful code into online payment processing pages or forms in order to get sensitive data, including credit cand numbers, from unwary consumers doing online purchases. | N/A | N/A | Moderate | Stolen payment details High | Secure | payment gateways, website security audits, user education | 4 | Moderate |
| 4 | T4 | Insider threat | Malicious or negligent insiders, including employees, contractors, or business partners, pose a significant risk to organizations by intentionally or unintentionally leaking sensitive information or sabotaging systems. | N/A | N/A | Moderate | Data leaks, system sabotage | Moderate | Access controls, user monitoring, employee training | 4 | Moderate |
| 5 | T5 | Adware | malicious software that displays pop-ups and/or ads as a way to raise revenue by users clicking on these ads. | N/A | N/A | Moderate | User irritation, potential data exposure | Moderate | Anti-adware software, ad-blocking extensions, user education | 3 | Low |
| 6 | T6 | Rootkit | a type of software program which is designed so that they can remain hidden to the user, but which allows cybercriminals to remotely control your computer. | N/A | N/A | High | Unauthorized access, data theft | High | Rootkit detection software, regular system scans, firmware updates | 4 | Moderate |
| 7 | T7 | Spyware | a type of software application that secretly records online activity by collecting personal information such as usernames, passwords and surfing habits. | N/A | N/A | High | Privacy invasion, identity theft | High | Anti-spyware software, firewall protection, user education | 4 | Moderate |
| 8 | T8 | Virus | is a type of malicious program designed to alter the way a device operates and to spread from one device to another. | N/A | N/A | High | System corruption, data loss | High | Antivirus software, regular system scans, user education | 4 | Moderate |

## Part B Develop an action plan

Using Word software, develop an **action plan** based on the outcomes of the previous tasks to implement 2 cyber security measures you have identified in the previous task to address **2 different cyber security matters** (threats/risks). You may cover both cyber security measures in the one action plan or develop 2 separate action plans.

Document at least **5 actions** for the implementation of each cyber security measure.

You will need to list each action, a responsibility as per the organisational chart given in the scenario, a timeline to complete each action, plus the resources required to complete each action.

Submit your answers electronically via the Learning Management System.

* e.g. AB\_BSBXCS402\_Task 2 Action Plan \_v1.0

|  |  |  |  |
| --- | --- | --- | --- |
| **Action Plan** | | | |
| **Action** | **Responsibility** | **Timeline** | **Resources** |
| Implement Multi-Factor Authentication (MFA) | IT Security Team | Within one month | MFA software, IT personnel |
| Configure MFA Settings | IT Security Team | Within one month | IT personnel, MFA software |
| Monitor MFA Usage and Effectiveness | IT Security Team | Ongoing | Monitoring tools, IT personnel |
| Develop Phishing Simulation Exercises | Training and Development Team | Within one month | Simulation software, cyber security experts |
| Monitor Phishing Awareness Levels | Training and Development Team | Ongoing | Monitoring tools, cyber security experts |

## Part C Develop cyber security policies & procedures

Using Word software, develop Cybersecurity Policies and relevant procedures for MP Tech Solutions that provide guidelines that employees should adhere to. Use the Policies and Procedures template provided.

The policies and procedures must address at least **2 different cyber security matters (threats)**.

You can either cover both different cyber security matters in one template or develop 2 separate sets each covering one cyber security matter.

Within the one or two sets of policy and procedure templates you must document:

* Under the “**Purpose**” heading,
  + state the purpose of the policies and procedures relevant to 2 different cyber security matters
  + relevant cybersecurity legislation.
* Under the “**Objectives**” heading, cover the objectives relevant to at least 2 different cyber security matters.
* Under the “**Scope**” heading, who the policy applies to.
* Under the “**Policy**” heading, include a policy statement including several different cybersecurity awareness requirements/responsibilities and what staff can and can’t do for each of the 2 different cyber security matters.
* Under the “**Procedures**” heading, document at least 2 work procedures relevant to the 2 different cyber security matters. This should be a series of sequential steps on what is to occur.
* Under the “**Version Number**” heading, a version number of the policy.

Upload your solution to the BSBXCS Moodle shell Assessment Task 2

File Naming Convention:

BSBXCS402 AT2 ***Student Name & Student Number***.docx

|  |
| --- |
| **Cybersecurity Policy & Procedures** |
| **Purpose** |
| *The main objective of this policy is to establish comprehensive standard procedures designed to protect our company’s digital assets and data and ensure strict compliance with relevant cybersecurity legislation.* |
| **Objectives** |
| *1. Guarantee the confidentiality, accessibility, and authenticity of corporate data and information systems.*  *2. Recognize and address security vulnerabilities and threats to bolster the overall cybersecurity stance.*  *3. Uphold adherence to all legal and regulatory mandates concerning cybersecurity.*  *4. Cultivate a sense of responsibility and consciousness among staff members regarding optimal cybersecurity protocols.*  *5. Implement incident response protocols to efficiently mitigate and recover from security breaches.* |
| **Scope** |
| *This policy applies to everyone, including employees, independent contractors, third-party vendors, and anyone else who has access to our company's information systems and data.* |
| **Policy** |
| *Every employee and organization must adhere to the established policies and procedures impartially. Each entity is tasked with the responsibility of continually providing training to ensure that all staff members stay abreast of the latest policies.* |
| **Procedures** |
| *Staff members need to generate secure, distinctive passwords for their accounts and revise them periodically, ideally every 90 days. Whenever possible, it's recommended to activate multi-factor authentication (MFA) to enhance the security of account access.* |
| **Last updated** |
| *2023* |

## Assessment Checklist: Task 2 - Cyber security threats in the workplace

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Learner name** | | YiZhuo Wang | **Learner ID** | | S1554654 | |
| **Assessor name** | |  | **Date** | |  | |
| Assessment checklist  assessor to complete the following | | | | | | |
| documentS | | | | | | |
| **The LEARNER:** | | | | **SATISFACTORY** | | **NOT SATISFACTORY** |
|  | Completed correctly all sections of the Threat Register | | |  | |  |
|  | Completed correctly all sections of the Action Plan | | |  | |  |
|  | Completed correctly all sections of the Cybersecurity Policy and procedure | | |  | |  |
| **Feedback:** | | | | | | |

## Assessment Task Summary: Task 2 - Cyber security threats 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, \_\_YiZhuo wang\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ have been advised of the outcome of this assessment task.  PRINT NAME | | | | | | | |
| LEARNER Signature | | YiZhuo Wang+S1554654 | | Date |  | | |