|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Student Name |  | | Student Number | |  |
| Unit Code/s & Name/s | VU23217 Recognise the need for cyber security in an organisation | | | | |
| Cluster Name  *If applicable* | N/A | | | | |
| Assessment Type | Assignment  Project  Case Study  Portfolio  Third Party Report (Workplace)  Third Party Report (Peer)  Other | | | | |
| Assessment Name | Cyber Security Methodology Recommendation Portfolio | | Assessment Task No. | | 2 of 2 |
| Assessment Due Date | Week 8 | | Date Submitted | | / / |
| **Assessor Feedback:** | | | | | |
| **Attempt 1** | Satisfactory | Unsatisfactory | | Date | / / |
| Assessor Name |  | | Assessor Signature | |  |
| **Student provided with feedback and reassessment arrangements**  *(check box when completed)* | | | Date scheduled for reassessment | | / / |
| **Attempt 2** | Satisfactory | Unsatisfactory | | Date | / / |
| Assessor Name |  | | Assessor Signature | |  |
| Note to Assessor: Please record below any reasonable adjustment that has occurred during this assessment e.g. written assessment given orally. | | | | | |
|  | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Assessment Criteria / Benchmarks  ***The evidence submitted demonstrates that the student has satisfactorily:*** | Attempt 1 | | Attempt 2 | |
| **Date**  \_\_/\_\_/\_\_ | | **Date**  \_\_/\_\_/\_\_ | |
| Y | N | Y | N |
| PART 1 – Cyber-security concepts |  |  |  |  |
| 1.1 Definitions for the following concepts have been provided.  a) A cyber-security threat |  |  |  |  |
| b) Threat actors |  |  |  |  |
| c) Threat vectors |  |  |  |  |
| d) Threat goals |  |  |  |  |
| 1.2 Cyber-security attacks  a) Characteristics of a cyber-security attack outlined |  |  |  |  |
| b) Explanation of how an attack operates - example to illustrate the answer provided |  |  |  |  |
| 1.3 Three (3) common and emerging cyber-security attacks, and techniques used by threat actors to infiltrate an organisation explained. References provided. |  |  |  |  |
| 1.4 At least three (3) current cyber-threat trends identified and their potential effect on the organisation’s data outlined. |  |  |  |  |
| 1.5 Research and explain the following cyber-security terms:  a) Botnets |  |  |  |  |
| b) Malware |  |  |  |  |
| c) Viruses |  |  |  |  |
| d) Worms |  |  |  |  |
| e) Root Kits |  |  |  |  |
| PART 2 – Task 1: Identify organisations’ data risks, vulnerabilities and cyber-security needs. For each scenario: |  |  |  |  |
| 2.1 Describe the organisation’s data types and associated data risks for each type of data identified. |  |  |  |  |
| 2.2 Identify the different ways data is accessed in the organisation. |  |  |  |  |
| 2.3 Consider the risk that a security breach poses for the organisation and describe the reason the organisation has to protect:  a) Organisational data |  |  |  |  |
| b) Online identity of users and their private data |  |  |  |  |
| 2.4 Based on each organisation’s data, identify the potential vulnerabilities of the organisation. Identified and explained at least three (3) vulnerabilities. |  |  |  |  |
| 2.5 For each vulnerability identified, explain the techniques that attackers could use to infiltrate the data. |  |  |  |  |
| 2.6 For each organisation, list and explain the cyber-attack methods that could be utilised to bring their infrastructure defences down. |  |  |  |  |
| PART 2 – Task 2: Identify cyber-security measures for the organisation. For each scenario: |  |  |  |  |
| 2.7 Based on the information obtained in Task 1, outline a strategy to defend the organisation’s data from threat actors. The strategy includes:  a) Cyber-defence methods |  |  |  |  |
| b) Cyber-defence techniques |  |  |  |  |
| c) Organisational policies and procedures |  |  |  |  |
| 2.8 Recommend four (4) essential cyber-security awareness practices for the scenarios presented. |  |  |  |  |
| PART 3 – Task 1: Methods and tools selection. For each scenario: |  |  |  |  |
| 3.1 Methods to protect the organisation’s data for each scenario have been identified and description provided. |  |  |  |  |
| 3.2 Required setup to protect the organisation from cyber-security attacks has been outlined. The setup includes:  a) Common infrastructure |  |  |  |  |
| b) Equipment |  |  |  |  |
| c) Software |  |  |  |  |
| 3.3 Measures to protect the organisation from cyber attacks have been investigated and proposed. The measures must include:  a) Relevant cyber-security policies and procedures |  |  |  |  |
| b) Cyber-security tools and systems |  |  |  |  |
| 3.4 Measures to protect the organisation from cyber attacks have been investigated and proposed. The measures must include:  a) Relevant cyber-security policies and procedures |  |  |  |  |
| b) Cyber-security tools and systems |  |  |  |  |
| 3.5 Behaviour-based security differences from a traditional firewall have been identified. Appropriate method selected for scenario and justified. |  |  |  |  |
| PART 3 – Task 2: Protecting personal data of an internet service user |  |  |  |  |
| 3.6 Online service selected and terms and privacy/security policies located and read. Processes to keep personal information secure and private have been presented. |  |  |  |  |
| PART 3 – Task 3: Demonstration – Cyber Kill Chain process and malware |  |  |  |  |
| 3.6 Cyber Kill Chain – malware demonstration activity completed. Screenshots were provided as evidence. |  |  |  |  |
| 3.7 Questions answered after demonstration completion.  a) Was the malware attack successful or not? |  |  |  |  |
| b) If successful, how do you know that it was successful? |  |  |  |  |
| c) If not, what defence mechanism on your PC prevented the attack? |  |  |  |  |
| PART 4 – Internet of Things (IoT) devices  Concentrate on the scenario that is more likely to use IoT devices. |  |  |  |  |
| 4.1 Identified at least three (3) examples of IoT devices that could be implemented in the scenario selected. |  |  |  |  |
| 4.2 For each IoT device identified in 4.1, manufacturers’ details provided on:  a) The methods that the device uses to protect data privacy |  |  |  |  |
| b) The techniques used to protect devices from cyber threats |  |  |  |  |
| c) User authentication techniques |  |  |  |  |
| d) Devices’ vulnerabilities  References provided. |  |  |  |  |
| 4.3 **IoT demonstration activity** – screenshot submitted. |  |  |  |  |
| PART 5 – Current cyber-security frameworks |  |  |  |  |
| 5.1 National Institute of Standards and Technology Cyber Security Framework (NIST CSF) includes:  Definition  Fundamentals  Purpose  Objectives |  |  |  |  |
| 5.2 Australian Cyber Security Centre (ACSC) includes:  Definition  Essential Eight Strategies  Purpose  Objectives |  |  |  |  |
| 5.3 Centre for Internet Security (CIS) includes:  Definition  CIS controls  Purpose  Objectives |  |  |  |  |
| PART 6 – Contingency task |  |  |  |  |
| 6.1 Scenario where a new director considers the student’s recommendation for cyber-security implementation excessive for the type of data managed. How do they proceed? Appropriate answer provided. |  |  |  |  |