**BTEC Assignment Brief**

|  |  |
| --- | --- |
| **Qualification** | Pearson BTEC Higher Nationals in Digital Technologies |
| **Unit number and title** | Unit 3: Cyber Security |
| **Learning aim(s)** | By the end of this unit, students will be able to:  **LO1** Explore the nature of cybercrime and cyber threat actors  **LO2** Investigate cyber security threats and hazards  **LO3** Examine the effectiveness of information assurance concepts applied to ICT infrastructure  **LO4** Investigate incident response methods to cyber security threats |
| **Assignment title** | Cyber Security |
| **Assessor** | Khoshimov A |
| **Issue date** | May 01, 2025 |
| **Hand in deadline** |  |

|  |  |
| --- | --- |
| **Scenario or Context** | You are a Cyber Security Analyst at a leading cyber security consultancy firm. Recently, your firm was hired by a major international corporation active in finance, healthcare, and technology. Given the corporation's significant digital presence and the sensitive nature of its data, it faces a multitude of cyber threats. Task: Create a cybersecurity strategy for the chosen organization and present it in a detailed report that addresses the following aspects:   1. **Analysis of Cybercrimes and Threat Actors:**    * Describe the types of cybercrimes (e.g., phishing, ransomware, DDoS) that could threaten the organization and outline their characteristics.    * Identify which organizational resources (e.g., customer data, financial systems, infrastructure) are potential targets and explain why they are vulnerable.    * Analyze the role of digital systems as both “targets” and “tools” in cybersecurity, providing real-world examples (e.g., IoT devices or cloud servers).    * Evaluate the types of malicious cyber activities and propose measures to neutralize threat actors (e.g., legal, technological, or employee training initiatives). 2. **Cybersecurity Threats and Defense Mechanisms:**    * Identify threats and hazards to the organization’s systems, services, or processes (e.g., weak authentication, network security issues).    * Investigate common attack techniques (e.g., SQL injection, social engineering) that could be used against the organization and recommend defense mechanisms (e.g., encryption, multi-factor authentication).    * Assess the role of threat intelligence in defending against these attack techniques, supported by examples (e.g., SIEM systems or real-time monitoring). 3. **Application of Information Assurance Concepts:**    * Explain how information assurance concepts (e.g., risk management, data encryption) can mitigate threats and vulnerabilities in the organization’s ICT infrastructure, providing examples.    * Assess how information assurance concepts can enhance the organization’s cybersecurity resilience (e.g., through ISO 27001 standards or the NIST framework).    * Evaluate the responses implemented by various organizations to address cybersecurity threats (e.g., incident preparedness, data recovery) and compare their effectiveness. 4. **Incident Response Methods:**    * Describe the security standards and regulations relevant to the organization’s sector (e.g., finance, healthcare) and analyze their implications.    * Examine the types of responses implemented to address cybersecurity threats (e.g., incident management, data recovery).    * Analyze the role of criminal and other laws in deterring cybercrime. |

**Learning Outcomes and Assessment Criteria**

|  |  |  |
| --- | --- | --- |
| **Pass** | **Merit** | **Distinction** |
| **LO1** Explore the nature of cybercrime and cyber threat actors | |  |
| **P1** Review types of malicious and/or criminal cyber activity.  **P2** Investigate the potential targets of cybercrime. | **M1** Analyse the concept of digital systems as ‘targets’ and ‘tools’ as related to cyber security, giving real- world examples. | **LO1 and LO2**  **D1** Evaluate types of malicious cyber activity and the action that can be taken to neutralise cyber threat actors. |
| **LO2** Investigate cyber security threats and hazards | |  |
| **P3** Describe security threats and hazards to a system or service or process.  **P4** Investigate common attack techniques and recommend how to defend against them. | **M2** Assess the role of threat intelligence when defending against common attack techniques. |  |
| **LO3** Examine the effectiveness of information assurance concepts applied to ICT infrastructure | |  |
| **P5** Explain how information assurance concepts can mitigate threats and vulnerabilities in ICT infrastructure, giving examples. | **M3** Assess how information assurance could enhance the cyber resilience of ICT infrastructure. | **LO3 and LO4**  **D2** Evaluate the responses that have been implemented by different organisations in response  to cyber security threats. |
|  | |
| **LO4** Investigate incident response methods to cyber security threats. | |  |
| **P6** Describe security standards, regulations and their consequences across at least two sectors. | **M4** Analyse the role of criminal and other law in deterring cybercrime. |  |
| **P7** Examine the types of response that have been implemented in response to cyber security threats. |  |  |

|  |  |
| --- | --- |
| **Sources of information to support you with this Assignment** | Amoroso, E. and Amoroso, M. (2017) From CIA to APT: An Introduction to Cyber Security.  New York: Independently published.  Gillespie, A. A. (2015) Cybercrime. Oxon: Routledge.  Grabosky, G. (2015) Cybercrime (Keynotes Criminology Criminal Justice series).  New York: Oxford University Press.  Stevens, T. (2015) Cyber Security and the Politics of Time. Cambridge:  Cambridge University Press.  Sutton, D. (2017) Cyber Security: A practitioner’s guide. Swindon: BCS. |
| **Other assessment materials attached to this Assignment Brief** |  |