Business Resilience and Incident Management (MSCCYB1_A, PGDCYB_SEP23)

Mr. Liam McCabe, Mr. Joel Aleburu

Continuous Assessment 2 (60%)

Semester 3, 2024

Contents

Introduction

This assessment requires you to write a structured report that demonstrates your critical understanding and conceptual learning based on the provided themes. Each part of the report should be comprehensive, well-researched, and include critical evaluations. Ensure that your report adheres to level 9 academic standards, including proper citations and references.

Assessing the Impact of Cyber Attacks & Understanding the Threat Landscape

Answer all sections in part a.

Question 1

Comprehensively explain the impact of cyber-attacks on businesses and the importance of understanding the threat landscape. Your answer should include:

- The different types of impacts (e.g., operational, financial, reputational) a cyber-attack can have on a business. ***(10 marks)***
- An overview of the threat landscape, including common threat actors, their motivations, and typical tactics, techniques, and procedures (TTPs). ***(5 marks)***
- The significance of assessing these impacts and understanding the threat landscape for effective cyber security management. ***(5 marks)***

Question 2

Describe the roles and responsibilities of the Blue Team and Red Team in incident response and their importance in maintaining business continuity. Your answer should include:

- Specific actions and responsibilities of the Blue Team during different phases of incident response (preparation, detection, containment, eradication, recovery, and lessons learned). ***(10 marks)***
- Specific actions and responsibilities of the Red Team in simulating attacks and testing defences. ***(5 marks)***
- How both teams collaborate to ensure business continuity and improve overall security posture. ***(5 marks)***

Question 3

Discuss how organizations can scale their incident response (IR) capabilities to maintain business resilience. Include in your answer:

- The key components of a robust IR posture and why they are important. ***(10 marks)***
- Strategies for scaling IR activities in both large and small organizations. ***(5 marks)***
- The role of continuous improvement in IR and how organizations can implement an effective IR improvement process. ***(5 marks)***

Part B: Roles, Responsibilities, and System Forensics

Answer all sections in part B.

Question 4

Explain the mapping of key incident response roles to their activities and the significance of system forensics tools in the incident response process. Your answer should address:

- A detailed mapping of IR roles (e.g., Incident Commander, Forensic Analyst, Communication Lead) to their specific activities during an incident. ***(10 marks)***
- The function and importance of system forensics tools in investigating and responding to cyber incidents. ***(5 marks)***
- How these roles and tools contribute to enhancing business resilience and incident management. (5 marks)

Part C: Regulatory and Operational Resilience & Threat Intelligence

Answer all sections in part c.

Question 5

Explain the role of regulation and operational resilience in incident management from a cyber security perspective, and discuss the importance of threat intelligence. Include in your answer:

- How threat intelligence contributes to robust security implementation and enhances operational resilience. ***(10 marks)***
- The impact of regulatory requirements on business operations and incident management practices. ***(5 marks)***
- The importance of using threat intelligence to improve incident response outcomes. ***(5 marks)***