CRT01

UNIVERSITY OF BOLTON

SCHOOL OF CREATIVE TECHNOLOGIES

BSC (HONS) COMPUTING (CYBER SECURITY)

SEMESTER 1 EXAMINATION 2024/25

INFORMATION SECURITY MANAGEMENT

MODULE NO: SEC6203

Date: Friday 10th January 2025 **Time 2:00pm – 4:00pm**

INSTRUCTIONS TO CANDIDATES:

There are FIVE questions on this exam brief.

Answer ANY FOUR of the five questions

All questions carry equal marks.

1. Cybersecurity breaches often exploit human vulnerabilities rather than purely technical flaws.
    a. Analyse the role of human factor exploitation in cyber-attacks, and provide examples of how attackers leverage these weaknesses. (5)
    b. Evaluate at least two common types of human factor exploitation techniques used by cyber attackers and present your anlaysis based on what make these techniques effective. (10)
    c. Propose and critically evaluate strategies that organizations can implement to mitigate the risks associated with human factor exploitation. How do these strategies address the identified weaknesses, and what challenges might organizations face in implementing them? (10)

(25 Marks)

2. Organizations often adopt policies, standards, guidelines, and procedures as a strategy to implement and manage information security effectively.
    a. Critically analyse policies, standards, guidelines, and procedures framework in the context of information security. Assess how adopting these elements as a cohesive strategy can enhance an organization's ability to manage information security risks. Include in your answer the challenges organizations might face when implementing these elements and how they can be addressed. (15)
    b. Evaluate the role of international standards (such as ISO/IEC 27001) in shaping the development and adoption of information security policies, standards, guidelines, and procedures. How do these frameworks help in aligning organizational practices with industry best practices. (10)

(25 Marks)

3. Organizations face a wide range of security risks that can impact their operations, data, and reputation. Effective security risk management is critical to identifying, assessing, and mitigating these risks.
    a. Analyse security risk management and the importance of each component in the context of an organization's overall security strategy. **(10 marks)**

    b. Enumerate the steps involved in a typical security risk management process by referring to a specific ISO or NIST framework. Critically analyse how an organization might apply these steps to manage a specific security risk, such as data breaches, insider threats, or social engineering attacks.
    (15 marks)

(Total 25 Marks)

4. Security policy document and data classification.
    a. Critically assess the key components required to write an effective security policy for an organization. Analyze how each component contributes to the overall security strategy and evaluate the challenges an organization might face when developing, implementing, and enforcing the policy. **(15 marks)**

    b. Evaluate the role of data classification in ensuring compliance with security standards and regulations (e.g., GDPR, PCI DSS). Support your evaluation by discussing how proper data classification influences access control, data handling, and incident response protocols within the organization.

(10 marks)

(Total 25 Marks)

PLEASE TURN THE PAGE

5. Cryptography is the science of securing information through encoding techniques that ensure confidentiality, integrity, and authenticity in communication and data storage. It plays a fundamental role in modern security systems, protecting sensitive information from unauthorized access and ensuring secure transactions across digital platforms.
   a. Assess the role of cryptography in securing modern communication systems.
   (5 marks)
   b. Critically analyze different cryptographic techniques such as symmetric and asymmetric encryption, hash functions, and digital signatures.
   (10 marks)
   c. Evaluate the strengths and limitations of these techniques in protecting sensitive data, considering their practical implementation challenges and vulnerabilities. **(10 marks)**

(Total 25 Marks)

END OF QUESTIONS