Individual Assignment: Digital Forensics & Cybersecurity Threats

Title: Investigating a Cybersecurity Breach: A Digital Forensics Approach

Duration: 1 Hour

Instructions:

- Read the given case study carefully.
- Answer all questions concisely with relevant justifications.
- Submit your answers in a structured format.

Case Study: Data Breach at XYZ Corporation

XYZ Corporation, a multinational financial services company, recently experienced a cyber-attack. An unauthorized entity accessed the internal network and exfiltrated sensitive client data, including financial records and personally identifiable information. The company's IT team noticed anomalies in system logs and detected a suspicious file transfer.

As a digital forensic investigator, you have been assigned to analyze the breach and propose necessary countermeasures.

Task 1: Understanding the Cyber Attack *(20 Marks)*

1. Identify and explain the possible type of attack that occurred in XYZ Corporation. (e.g., Phishing, Malware, Advanced Persistent Threats, Zero-Day Exploits, etc.)
2. Discuss how this attack could have been executed based on the given scenario.
3. What are the immediate steps you would take to contain the attack and prevent further data loss?

Task 2: Digital Forensics Investigation Process *(30 Marks)*

1. Explain the key steps involved in digital forensics investigation based on the ACPO (Association of Chief Police Officers) guidelines.
2. Discuss the importance of maintaining the Chain of Custody when handling digital evidence.
3. List at least three digital forensic tools you would use to analyze the compromised system and justify their usage.

Task 3: Malware Analysis & Prevention *(20 Marks)*

1. Based on the available evidence, suggest how malware (such as Trojans, Worms, or Ransomware) could have played a role in this breach.
2. Explain how hashing techniques (MD5, SHA-1, or SHA-3) can be used to verify the integrity of evidence.
3. Describe two anti-forensic techniques that attackers may use to cover their tracks and how forensic investigators can counter them.

Task 4: Cybersecurity Protection Measures *(30 Marks)*

1. Identify and explain at least three countermeasures that XYZ Corporation could implement to prevent such attacks in the future.
2. Discuss the importance of security policies and governance in an organization's cybersecurity framework.
3. Propose a basic incident response plan for handling future cyber threats.

Submission Guidelines:

- Your answers should be well-structured with clear headings.
- Provide real-world examples where applicable.
- Cite any external references used.
- Submit your response in a document format (Word/PDF).
