Student ID Number: 23199937

INDIVIDUAL ASSESSMENT

Semester 1 2024

PAPER NAME: **Information Security Management**

PAPER CODE: **COMP718**

INSTRUCTIONS:

1. **ACADEMIC INTEGRITY GUIDELINES**
   The following actions may be deemed to constitute a breach of the General Academic Regulations Part 7: Academic Discipline, Section 2 Dishonesty During Assessment or Course of Study
   - 2.1.1 copies from, or inappropriately communicates with another person
   - 2.1.3 plagiarises the work of another person without indicating that the work is not the student's own – using the full work or partial work of another person without giving due credit to the original creator of that work
   - 2.1.4 Unauthorised collaboration in Assessment - collaborates with others in the preparation of material, except where this has been approved as an assessment requirement. This includes contract cheating where a student obtains services to produce or assist with an assessment
   - 2.1.5 resubmits previously submitted work without prior approval of the exam board
   - 2.1.6 Using any other unfair means

Question option 1:

The history of cyber security provides us with a number of famous cases to reflect on; what can we learn from these cases? Write a well-researched report on a cybersecurity villain (an individual or a group):

a) The report should provide a sufficiently detailed and referenced overview of the case you have selected.

b) Next, the report should provide an in-depth discussion of how the lessons learned from your research can be used to improve the organization's response to information security incidents and breaches and in particular, the incident response plan.

a)
Introduction

The field of cybersecurity has undergone major changes in recent decades, as demonstrated by several significant events that have exposed the weaknesses and dangers present in our digital environment. One of the key figures in the history of cybersecurity is Adrian Lamo, whose controversial hacking activities have captured the attention and concern of the cybersecurity community. This report examines the case of Adrian Lamo, offering a comprehensive look at his actions, their consequences, and the insights gained for enhancing how organizations address information security incidents.

Overview of Adrian Lamo

Adrian Lamo, also known as the "homeless hacker," became famous in the early 2000s for his hacking skills. Born on February 20, 1981, Lamo's unique lifestyle and hacking abilities made him a controversial figure in the cybersecurity community. He was recognized for his talent in breaching large company networks and exposing their security weaknesses, frequently reaching out to inform them about their vulnerabilities.

Activities and legal issues

1. **New York Times Hack (2002)**

    - One of Lamo's most famous hacks involved the New York Times. He managed to infiltrate the newspaper's internal network, gaining access to confidential databases, including contact information for contributors and employees. Lamo used the paper's LexisNexis account to conduct unauthorized searches.

    - This incident drew significant media attention and led to Lamo's eventual arrest. He was charged with computer fraud and abuse, resulting in a sentence of six months of home detention and two years of probation.

2. **Microsoft and Yahoo Hacks**

    - Lamo also breached the networks of Microsoft and Yahoo, exploiting vulnerabilities to gain access to sensitive information. In Microsoft's case, he accessed the company's internal project files and emails. These actions were part of his broader strategy to expose security weaknesses in major corporations.

    - In July 2004, Lamo was sentenced to two years' probation, with six months to be served in home detention, and ordered to pay $65,000 in restitution. He was convicted of compromising security at The New York Times, Microsoft, Yahoo!, and WorldCom.

3. **Reporting Chelsea Manning (WikiLeaks)**

    - In 2010, Lamo became infamous for his role in the arrest of Chelsea Manning, a former U.S. Army intelligence analyst. Manning had contacted Lamo and confided in him about leaking classified information to WikiLeaks. Lamo reported Manning to the authorities, leading to her arrest and subsequent conviction. This act drew mixed reactions, with some praising Lamo for his civic duty while others criticized him for betraying a fellow hacker.

b)
Lessons Learned from Adrian Lamo's Case

The case of Adrian Lamo provides valuable insights into the weaknesses that can exist within an organization’s security infrastructure and highlights the importance of a well-structured incident response plan. By examining the lessons learned from Lamo's activities, organizations can significantly enhance their ability to respond to information security incidents and breaches. This section will discuss how these lessons can be applied to improve an organization’s response to such incidents, focusing specifically on the incident response plan.

1. **Enhancing Detection Capabilities**

Lesson Learned: Early Detection is Crucial

One of the key takeaways from Adrian Lamo's activities is the importance of early detection. Many of Lamo’s exploits went undetected for extended periods, giving him ample time to access and manipulate sensitive information.

Implementation Strategies:

1. **Advanced Monitoring Tools**: Invest in advanced security monitoring tools that leverage artificial intelligence (AI) and machine learning (ML) to detect anomalies and potential threats in real-time. These tools can analyse vast amounts of data and identify unusual patterns that may indicate a breach.

    - Example: Implementing a Security Information and Event Management (SIEM) system that collects and analyses log data from various sources to provide real-time analysis of security alerts.

2. **Regular Security Audits and Penetration Testing**: Conduct regular security audits and penetration testing to identify vulnerabilities. Employ ethical hackers to simulate attacks and uncover weaknesses before malicious actors can exploit them.

    - Example: Quarterly penetration tests by third-party security firms to ensure objectivity and thoroughness.

3. **Threat Intelligence**: Utilize threat intelligence to stay informed about emerging threats and vulnerabilities. Subscribe to threat intelligence feeds and collaborate with industry peers to share information about potential threats.

    - Example: Participating in Information Sharing and Analysis Centres (ISACs) relevant to the organization's industry.

2. Strengthening the Incident Response Team

Lesson Learned: Clear Roles and Responsibilities

Lamo's case underscores the importance of having a dedicated and well-prepared incident response team. Clear roles and responsibilities are crucial for an effective response to security incidents.

Implementation Strategies:

1. **Dedicated Response Team**: Assemble a dedicated incident response team comprising members from various departments, including IT, legal, communications, and HR. Each member should have a clearly defined role and responsibility.

    - Example: A Computer Security Incident Response Team (CSIRT) with designated roles such as Incident Coordinator, Legal Advisor, and Communications Officer.

2. **Training and Drills**: Conduct regular training sessions and simulated incident response drills to ensure that all team members are prepared to act swiftly and effectively during a real incident.

- Example: Bi-annual tabletop exercises that simulate different types of security incidents, such as data breaches or ransomware attacks.

3. **Communication Protocols**: Develop clear communication protocols for internal and external stakeholders. This includes procedures for notifying affected parties, coordinating with law enforcement, and managing media inquiries.

    - Example: A communication matrix that outlines who should be contacted and in what order during various types of incidents.

3. **Developing and Updating the Incident Response Plan**

Lesson Learned: Continuous Improvement

Lamo's activities revealed that even well-secured systems can have vulnerabilities. An effective incident response plan must be continuously updated to address new threats and incorporate lessons learned from past incidents.

Implementation Strategies:

1. Regular Plan Reviews: Conduct regular reviews of the incident response plan to ensure it remains current with evolving threats and regulatory requirements. Update the plan based on feedback from post-incident reviews and changes in the threat landscape.

    - Example: Annual reviews and updates of the incident response plan, with additional reviews following significant security incidents or changes in regulatory requirements.

2. Post-Incident Reviews: After every security incident, conduct a thorough post-incident review to identify what went wrong, what went well, and how the response can be improved. Use these insights to refine the incident response plan.

    - Example: A structured post-incident review process that includes interviews with key responders, timeline analysis, and a detailed report of findings and recommendations.

3. Integration with Business Continuity Plans: Ensure that the incident response plan is integrated with the organization's broader business continuity and disaster recovery plans. This ensures that critical business operations can continue or be quickly restored following a security incident.

    - Example: Cross-referencing the incident response plan with the business continuity plan to align recovery objectives and priorities.

Question option 2:

One-Time Pad (OTP) is an important security control as it can be used to build an unbreakable cryptographic system. Write a well-researched report on OTPs:

a) The report should explain who was behind the initial idea, when OTPs were first used, in what application they were found, and how they are used today? To get a better idea about OTP, visit an online OTP creation site (such as www.braingle.com/brainteasers/codes/onetimepad.php) and practice creating your own ciphertext with OTP. You may even exchange your OTPs with other students to see how you might try to break them.

b) Next, the report should provide an in-depth discussion of how OTPs can be used for improving the organization's response to information security incidents and breaches – e.g., would it be practical to use OTPs? Why or why not? In what contexts should they be used?

a)

1. **Who was behind the initial idea?**
   - **a. History of One-Time Pads**

     The concept of One-Time Pads originated in the early 20th century, with significant contributions from several key figures. In 1917, Gilbert Vernam, an AT&T engineer, developed a cipher system that used a tape of random numbers for encryption. This invention marked a crucial step forward in cryptographic technology. However, it was Major Joseph Mauborgne who expanded on Vernam's work, demonstrating that if the encryption key (pad) was truly random, used only once, and kept secret, the resulting ciphertext would be theoretically unbreakable. This collaborative effort laid the foundation for the One-Time Pad as we know it today.

     The theoretical significance of the One-Time Pad was later recognized and proved by information theorist Claude Shannon in the 1940s. Around the same time, Soviet information theorist Vladimir Kotelnikov independently proved the absolute security of the One-Time Pad. His findings were presented in a report in 1941, which remains classified to this day.

   - **b. Initial Applications**

     The initial documented application of OTPs occurred in World War II, where the Soviet Union utilized OTPs extensively for important military and diplomatic communications. They utilized physical one-time pads, which were sheets of paper containing random key material, distributed to users and then destroyed after a single use. This approach guaranteed that even if the encrypted message was intercepted, it would be impossible to decrypt without the specific pad used for encryption.

c. Modern Uses

Currently, OTPs are widely regarded as the most secure form of communication, especially in situations where complete confidentiality is essential. Nevertheless, their usage in day-to-day communication is limited due to practical constraints.

- Military and Diplomatic Communications: For the most sensitive transmissions where security cannot be compromised.
- Sensitive Data Transfers: In scenarios where absolute security is necessary, such as transferring top-secret documents or personal information like banking system, healthcare.
- Cryptographic Research: OTPs are often used as a benchmark for developing and testing new cryptographic algorithms.

d. Creating an OTP Ciphertext

After visit an online OTP creation site (www.braingle.com/brainteasers/codes/onetimepad.php) and practice creating my own ciphertext with OTP, I can understand and can show how to demonstrate it process.

1. Message: “COMP718”
2. OTP: “CIJTHUUHMLFRU”
3. Enciphered Message: “EWVI”

Step 1: Convert the Message and Key to Numerical Values

- Message: "COMP": C = 2; O = 14; M = 12; P = 15
- Key: "CIJTHUUHMLFRU"(First 4 letters): C = 2; I = 8; J = 9; T = 19

Step 2: Perform the Encryption

- C (2) + C (2) = 2 + 2 = 4 → E
- (14) + I (8) = 14 + 8 = 22 → W
- M (12) + J (9) = 12 + 9 = 21 → V
- P (15) + T (19) = 15 + 19 = 34 → 34 % 26 = 8 → I

Final Result: The Enciphered Message

- Thus, the message "COMP" encrypted with the One-Time Pad key "CIJT" results in the ciphertext "EWVI."

b)

1. Practicality of OTPs

One-time passwords (OTPs) offer complete confidentiality, but applying them in today's workplaces comes with various obstacles:

- Managing Keys: Ensuring truly random keys that are as long as the message and used only once presents logistical hurdles.
- Distributing Keys: Safely sharing and storing keys without risking their confidentiality is complex, especially across extensive networks.

- Scalability: Handling the generation, distribution, and management of large quantities of key material for routine communication is not feasible.

2. Improving Incident Response with OTPs

Despite these challenges, OTPs can enhance specific aspects of an organization's information security strategy:

- High-Value Communications can be kept secure by using OTPs to communicate critical information, making it impossible for attackers to decipher the message even if they gain access to the network.

- Encrypting backup data with OTPs ensures that sensitive information remains secure in case backup storage is compromised, especially for protecting legacy data that is not frequently accessed.

- OTPs can be utilized for secure coordination among incident response teams during an incident, ensuring that plans and strategies cannot be intercepted or deciphered by attackers.

3. Contexts for Using OTPs

- Keep top-secret documents safe by using OTPs to encrypt and send highly sensitive information securely.

- When dealing with critical infrastructure, use OTPs for communication to prevent catastrophic consequences in case of compromise.

- In the event of a breach, rely on OTPs as a temporary secure communication method when other channels may be compromised.

4. Limitations and Alternatives

While OTPs offer unmatched security, their limitations mean they are not a panacea for all security challenges. Organizations should consider:

- Mixing OTPs with different encryption techniques can help maintain a balance between security and convenience. For instance, using standard encryption for everyday communication and OTPs for sensitive information can enhance overall security measures.

- Utilizing sophisticated key management systems can effectively manage the intricacies of OTPs, ensuring a more secure environment for data protection.

- Providing proper education and training to employees on OTP usage, key management, and security protocols is crucial to enhance overall cybersecurity measures within an organization.

References:

1. **"Adrian Lamo.". Wikipedia (https://en.wikipedia.org/wiki/Adrian_Lamo)**
2. **Who Is Adrian Lamo? (https://bluegoatcyber.com/blog/who-is-adrian-lamo/)**
3. **How to Build and Manage an Efficient Incident Response Team (https://dig8ital.com/post/incident-response-team/)**
4. **"One-Time Pad.". Wikipedia. (https://en.wikipedia.org/wiki/One-time_pad)**
5. **Braingle. "One-Time Pad Cipher." (https://www.braingle.com/brainteasers/codes/onetimepad.php)**
6. **"NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide."(https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)**
7.