Legendary Performance!

Congratulations on successfully completing this assignment! Your grade has been recorded. Feel free to close this tab and return to the main course page.

Required passing grade: 40%

Status: **Passed**

Final Score: 20 / 20 (100%)

Question 1

Score: 5/5

Case Study: Deepfake Case Study (Part A)

Root cause: The root cause of the breach was the use of deepfake technology to manipulate a video conference call. The initial point of failure was a phishing message that tricked a finance department employee into believing they were communicating with the CFO. The factors contributing to this vulnerability included human error, inadequate phishing training, and insufficient verification processes for high-stakes financial transactions.

Actions taken: Once the breach was discovered, the company implemented several immediate actions to mitigate further losses:

o They reported the incident to the Hong Kong police. The police conducted an international investigation to identify and apprehend the perpetrators behind the scam.

o The organization improved its verification protocols for financial transactions with mandatory multi-level approvals and real-time verification.

o In collaboration with regulators, financial institutions revised fraud alert systems to detect similar threats more effectively.

o Cybersecurity companies began to train employees and create materials to help reiterate the importance of cybersecurity awareness and strict security policies and procedures across the organization.

Evaluate effectiveness and timeliness: While the scam was not immediately identified, immediate measures were taken to prevent future occurrences once the breach was discovered. Their reporting and collaboration with Hong Kong police and international agencies provided an excellent attempt at identifying the scope of the attack and the possibility of recovering lost funds.

Despite this extensive investigation, there is no indication that the perpetrators or the $200 million were ever found, suggesting that while the company responded urgently, their measures may not have been sufficient or executed early enough to preserve financial assets and apprehend the criminals.

The success of the initial phishing attack raises questions about the effectiveness of security awareness initiatives among employees. After the breach, it does seem that the company and others within the industry made a concerted effort to improve their internal authorization and access policies. Further detail and analysis could provide insight into whether these initiatives should be intensified or focused differently.

Successes, Gaps, and Failures

Question 1: What was one of the successes achieved during the response to the phishing breach?

- ○ The company halted all financial transactions permanently.
- ○ They fired the employee who fell for the phishing message.
- ◉ The organization reported the incident to the Hong Kong police for investigation. ✓
  Correct! Reporting to the police was a significant step in addressing the breach
- ○ The company immediately recovered the $200 million lost.

Correct! Reporting to the police was a significant step in addressing the breach

Question 2

Score: **5/5**

Which of the following gaps were identified and addressed after the breach? Select all that apply.

- [ ] Lack of data encryption for sensitive transactions

- [x] Inadequate phishing training for employees
  Correct! Insufficient phishing awareness left employees vulnerable, prompting the company to enhance training and reinforce cybersecurity protocols

- [ ] Weak password policies across the organization

- [x] Human error leading to vulnerability
  Correct! Human error, including falling for the phishing message, played a significant role and was addressed through better processes and training

Correct! Insufficient phishing awareness left employees vulnerable, prompting the company to enhance training and reinforce cybersecurity protocols.
Correct! Human error, including falling for the phishing message, played a significant role and was addressed through better processes and training.
You selected all correct options!

Question 3

Score: **5/5**

Describe the failures that occurred during the breach. (50 words)

During the Deepfake breach, failures included inadequate phishing awareness training, lack of strong verification protocols for large transactions, and overreliance on video conferencing without secondary confirmation. Human error played a central role, as the employee trusted the fraudulent deepfake meeting and processed transfers without independent validation, leading to significant financial loss.

The student earns the full 5 points because they correctly identify several failures: inadequate phishing awareness, insufficient verification protocols, and reliance on video conferencing without confirmation. These are key aspects of the breach, showing a thorough understanding.

To further enhance your response, consider providing more specific examples or consequences of each failure mentioned, which could offer deeper insight into the impact of these failures.

Score: 5/5 (100%)

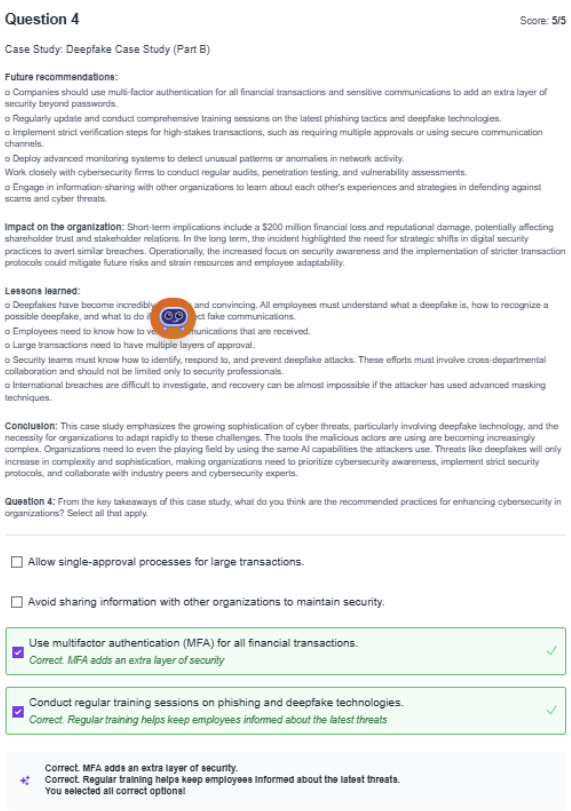
Detailed Breakdown:

Analysis: The student response highlights multiple failures: inadequate phishing awareness training, lack of strong verification protocols for large transactions, and overreliance on video conferencing without secondary confirmation. These points are clearly articulated and align with the case study details.

Evaluation: The response meets the highest rubric criteria by accurately describing multiple failures associated with the breach, including human error and a lack of verification processes. This indicates a comprehensive grasp of the case study.

Explanation: The student earns the full 5 points because they correctly identify several failures: inadequate phishing awareness, insufficient verification protocols, and reliance on video conferencing without confirmation. These are key aspects of the breach, showing a thorough understanding.

Guidance: To further enhance your response, consider providing more specific examples or consequences of each failure mentioned, which could offer deeper insight into the impact of these failures.



Question 4 Score: 5/5

Case Study: Deepfake Case Study (Part B)

Future recommendations:

- Companies should use multi-factor authentication for all financial transactions and sensitive communications to add an extra layer of security beyond passwords.
- Regularly update and conduct comprehensive training sessions on the latest phishing tactics and deepfake technologies.
- Implement strict verification steps for high-stakes transactions, such as requiring multiple approvals or using secure communication channels.
- Deploy advanced monitoring systems to detect unusual patterns or anomalies in network activity.

Work closely with cybersecurity firms to conduct regular audits, penetration testing, and vulnerability assessments.

- Engage in information-sharing with other organizations to learn about each other's experiences and strategies in defending against scams and cyber threats.

Impact on the organization: Short-term implications include a $200 million financial loss and reputational damage, potentially affecting shareholder trust and stakeholder relations. In the long term, the incident highlighted the need for strategic shifts in digital security practices to avert similar breaches. Operationally, the increased focus on security awareness and the implementation of stricter transaction protocols could mitigate future risks and strain resources and employee adaptability.

Lessons learned:

- Deepfakes have become incredibly [illegible] and convincing. All employees must understand what a deepfake is, how to recognize a possible deepfake, and what to do [illegible] fake communications.
- Employees need to know how to v[illegible]unications that are received.
- Large transactions need to have multiple layers of approval.
- Security teams must know how to identify, respond to, and prevent deepfake attacks. These efforts must involve cross-departmental collaboration and should not be limited only to security professionals.
- International breaches are difficult to investigate, and recovery can be almost impossible if the attacker has used advanced masking techniques.

Conclusion: This case study emphasizes the growing sophistication of cyber threats, particularly involving deepfake technology, and the necessity for organizations to adapt rapidly to these challenges. The tools the malicious actors are using are becoming increasingly complex. Organizations need to even the playing field by using the same AI capabilities the attackers use. Threats like deepfakes will only increase in complexity and sophistication, making organizations need to prioritize cybersecurity awareness, implement strict security protocols, and collaborate with industry peers and cybersecurity experts.

Question 4: From the key takeaways of this case study, what do you think are the recommended practices for enhancing cybersecurity in organizations? Select all that apply.

- [ ] Allow single-approval processes for large transactions.
- [ ] Avoid sharing information with other organizations to maintain security.
- [x] Use multifactor authentication (MFA) for all financial transactions. ✓
  Correct. MFA adds an extra layer of security
- [x] Conduct regular training sessions on phishing and deepfake technologies. ✓
  Correct. Regular training helps keep employees informed about the latest threats

Correct. MFA adds an extra layer of security.
Correct. Regular training helps keep employees informed about the latest threats.
You selected all correct options!

Summary

In 2022, a multinational firm in Hong Kong lost $200 million after scammers used AI-powered deepfake technology to impersonate the company's CFO during a video conference call. The attackers combined phishing messages with a highly convincing fake video meeting, tricking an employee into authorizing multiple financial transfers. The breach exposed critical gaps in verification processes, including reliance on single-approval work flows and insufficient employee training on emerging AI threats. In response the company implemented multi-level protocols and real time verification checks, while law enforcement agencies launched international investigations. The case highlights the growing risk of AI driven social engineering and the importance of multi factor authentication, employee awareness training and robust verification protocols to prevent similar attacks.