

# 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: 15 / 15 (100%)



## Question 1

Score: 5/5

### Case Study: Equiniti Cybersecurity Breach

In 2022, Equiniti Trust Company, formerly American Stock Transfer & Trust, fell victim to a phishing attack where cybercriminals impersonated a legitimate employee to steal \$4.78 million through fraudulent transactions. The attackers used an email thread with a U.S.-based client to trick Equiniti into issuing and liquidating shares, though some funds were later recovered. In 2023, a second breach involved the theft of Social Security numbers, which allowed hackers to create fake accounts and transfer \$1.9 million from legitimate clients. Both incidents resulted in regulatory penalties and highlighted gaps in Equiniti's cybersecurity measures.

#### Root Causes

The root cause of the failure in the first Equiniti attack was a lack of robust cybersecurity measures, which left the organization vulnerable to a phishing attack. This vulnerability was further exacerbated by outdated software systems and insufficient employee training in identifying and responding to potential threats. The second breach at Equiniti exposed a fundamental flaw in their control design. The company relied on a single factor, the Social Security number, to grant access to all user accounts, which proved inadequate in the face of modern cyber threats. The two breaches highlighted the urgent need for stronger protocols and proactive measures to safeguard sensitive financial data.

#### Actions Taken

In response to the breaches, Equiniti took the following actions:

- o Immediately launched an incident response team to mitigate the breach and assess the extent of the damage.
- o Updated all outdated software systems to address security vulnerabilities by deploying patches and implementing new tools.
- o Conducted company-wide cybersecurity training to educate employees on identifying phishing attempts and other potential threats.
- o Hired external cybersecurity consultants to conduct a thorough audit of their systems and provide recommendations for improvement.
- o Enhanced internal communication systems to ensure quicker and more transparent suspicious activity reporting.

#### Evaluation of Effectiveness and Timeliness

The actions taken proved moderately effective in addressing the immediate threat and preventing further breaches. For example, the software updates closed key vulnerabilities and employee training significantly reduced phishing susceptibility within six months. However, some measures, such as the audit and implementation of new tools, were delayed due to budget constraints, impacting their overall timeliness. Metrics such as reduced phishing success rates and improved system patching compliance demonstrated the effectiveness of the response.

#### Successes, Gaps, and Failures

Notable successes included the containment of the breach and the marked improvement in employee awareness of cybersecurity risks. However, gaps remained, particularly in the timeliness of implementing long-term solutions, like upgrading legacy systems. A key failure was the organization's initial underestimation of the resource allocation required for a robust cybersecurity framework, which delayed full recovery and future-proofing efforts.

#### Impact on the Organization

Operationally, the breach caused immediate disruptions, including system downtime and lost productivity, while the financial cost of containment and recovery strained the budget. Strategically, the incident damaged stakeholder trust and highlighted weaknesses in risk management, pushing the company to re-evaluate its priorities. In the long term, the changes implemented have the potential to strengthen Equiniti's resilience, but only if the gaps identified are addressed thoroughly.

#### Lessons Learned

Key lessons learned include the importance of proactive measures, such as regular software updates and employee training, to prevent incidents before they occur. Additionally, the case highlighted the need for a clear, well-funded cybersecurity strategy and the value of external expertise in identifying and addressing vulnerabilities. Communication and transparency during an incident were crucial to maintaining trust and mitigating reputational damage.

Recommendations for Future Actions

- The following actions could help to prevent similar incidents in the future:
- o Invest in a dedicated cybersecurity team to oversee system integrity and lead proactive risk assessments.
  - o Establish a continuous employee training program to ensure awareness of evolving threats.
  - o Create a robust incident response plan with clear communication protocols.
  - o Implement additional security measures like multi-factor authentication (MFA) to strengthen access control.
  - o Update and audit all digital systems regularly and integrate threat detection tools powered by artificial intelligence.
  - o Allocate a dedicated budget for cybersecurity, ensuring resources are available for rapid and effective responses.

Conclusion

**Question 1:** What vulnerabilities in Equiniti's security practices were exposed during the two breaches, and how did these weaknesses contribute to the attacks?


Equiniti's breaches revealed several critical weaknesses in its security practices. First, their systems lacked proper patch management, leaving exploitable vulnerabilities unaddressed and allowing attackers to target outdated software. Second, the company had weak monitoring and detection capabilities, which delayed the identification of suspicious activity and gave attackers more time to steal data. Third, sensitive information was not adequately protected through encryption or layered defenses, increasing the impact of exposure once attackers gained access. In addition, many employees lacked sufficient training and awareness regarding phishing attacks, which contributed to the high success rate of credential theft. Finally, Equiniti relied on single-factor authentication, making stolen credentials enough for attackers to access accounts without additional barriers. These weaknesses combined to create a high-risk environment where attackers could not only gain initial access but also escalate privileges, move laterally, and exfiltrate sensitive data undetected.

The student receives full points because they have addressed all the key vulnerabilities outlined in the rubric: outdated software, insufficient employee training, lack of robust cybersecurity measures, and reliance on single-factor authentication. Each point is explained with clarity and supported by evidence from the case study.

To further enhance your response, consider incorporating specific examples or data points from the case study to strengthen your analysis. This would provide even more depth and context to your explanations.

Score: 5/5 (100%)

Detailed Breakdown:

 **Analysis:** The student's response identifies several critical vulnerabilities in Equiniti's security practices, including lack of proper patch management, weak monitoring and detection capabilities, insufficient protection of sensitive information, lack of employee training, and reliance on single-factor authentication. These points are well-integrated into the explanation and supported by details from the case study.

**Evaluation:** The response meets the highest rubric criterion by thoroughly identifying and explaining all key vulnerabilities in Equiniti's security practices. The explanation is clear, detailed, and well-supported by the case study, addressing all critical points.

**Explanation:** The student receives full points because they have addressed all the key vulnerabilities outlined in the rubric: outdated software, insufficient employee training, lack of robust cybersecurity measures, and reliance on single-factor authentication. Each point is explained with clarity and supported by evidence from the case study.

**Guidance:** To further enhance your response, consider incorporating specific examples or data points from the case study to strengthen your analysis. This would provide even more depth and context to your explanations.

## Question 2

Score: 5/5

Why is relying on a single factor, like a Social Security number, insufficient for access control in modern cybersecurity?

Relying on a single factor such as a Social Security number (SSN) is insufficient because SSNs are widely exposed through data breaches, easily stolen, and cannot be changed once compromised. Using them as the sole means of authentication creates a single point of failure, if the attacker has the SSN, they effectively bypass security. Modern cybersecurity requires multi-factor authentication (MFA), which combines at least two factors (something you know, something you have, something you are) to add layered protection. MFA ensures that even if one factor is compromised, attackers cannot gain access without the additional verification. This layered approach significantly reduces the risk of unauthorized access and identity theft.

The response earns full points because it thoroughly explains the insufficiency of single-factor authentication using SSNs, supports this with relevant risks, and proposes a viable alternative in multi-factor authentication.

To further enhance your response, consider incorporating specific examples or case studies that illustrate the consequences of relying solely on SSNs for authentication. This could provide even stronger support for your argument.

Score: 5/5 (100%)

Detailed Breakdown:



**Analysis:** The student response clearly explains the insufficiency of using a Social Security number as the sole factor for access control. It addresses the risks of data breaches and the immutability of SSNs, providing a strong rationale for the need for multi-factor authentication.

**Evaluation:** The response meets the highest criterion of the rubric by providing a comprehensive explanation with relevant examples and supporting information. It is clear and well-structured, addressing potential risks and suggesting alternative solutions.

**Explanation:** The response earns full points because it thoroughly explains the insufficiency of single-factor authentication using SSNs, supports this with relevant risks, and proposes a viable alternative in multi-factor authentication.

**Guidance:** To further enhance your response, consider incorporating specific examples or case studies that illustrate the consequences of relying solely on SSNs for authentication. This could provide even stronger support for your argument.

## Question 3

Score: 5/5

What measures can organizations take to improve their defense against cyber threats? Select all that apply.

Implement multi-factor authentication for all access points.



*Correct! MFA adds an extra layer of security by requiring more than one form of authentication to access critical systems. This makes it much harder for attackers to gain access even if they obtain one authentication factor like a password.*



☐ Rely on employee awareness training to prevent all types of attacks.

Conduct regular risk assessments and security audits to identify vulnerabilities.



*Correct! Risk assessments and audits are essential to identifying vulnerabilities and understanding potential threats. Regular evaluations help organizations stay ahead of evolving risks, ensuring that their security measures remain effective.*



☐ Ignore outdated software systems, as they are rarely targeted by attackers.

Deploy advanced threat detection tools powered by artificial intelligence.



*Correct. AI-driven tools can identify anomalies and potential threats in real-time, providing faster responses to emerging cyber risks. These tools use machine learning to detect patterns and help prevent attacks before they cause harm.*



**Correct! MFA adds an extra layer of security by requiring more than one form of authentication to access critical systems. This makes it much harder for attackers to gain access even if they obtain one authentication factor like a password..**  
**Correct! Risk assessments and audits are essential to identifying vulnerabilities and understanding potential threats. Regular evaluations help organizations stay ahead of evolving risks, ensuring that their security measures remain effective..**  
**Correct. AI-driven tools can identify anomalies and potential threats in real-time, providing faster responses to emerging cyber risks. These tools use machine learning to detect patterns and help prevent attacks before they cause harm..**  
**You selected all correct options!**

