Question 1

Score: **5/5**

Case Study: Pegasus Airlines Data Breach (Part A)

Root Cause

The root cause of the Pegasus Airlines data breach was a configuration error within their AWS S3 bucket permissions. This oversight allowed unauthorized public access to sensitive data, including flight charts and crew personally identifiable information (PII), resulting from an employee's mistake. Contributing factors included insufficient IT security training and a lack of rigorous reviews of access controls.

Actions Taken

Upon confirmation of the breach on March 24, 2022, Pegasus Airlines took immediate steps to secure the exposed AWS S3 bucket by revising access controls. The IT security team, alongside cybersecurity experts, conducted a comprehensive investigation to assess and mitigate vulnerabilities. Additional employee training programs were initiated to strengthen data management practices and prevent future occurrences.

Evaluate Effectiveness and Timeliness

Question 1: What immediate action did Pegasus Airlines take upon confirming the data breach?

○ They notified all affected customers immediately.

○ They migrated all data to a new server.

○ They fired the employee responsible for the error.

● They revised access controls on the AWS S3 bucket. ✓
Revising access controls was their immediate action.

Question 2

Score: **5/5**

What was the outcome of the response actions?

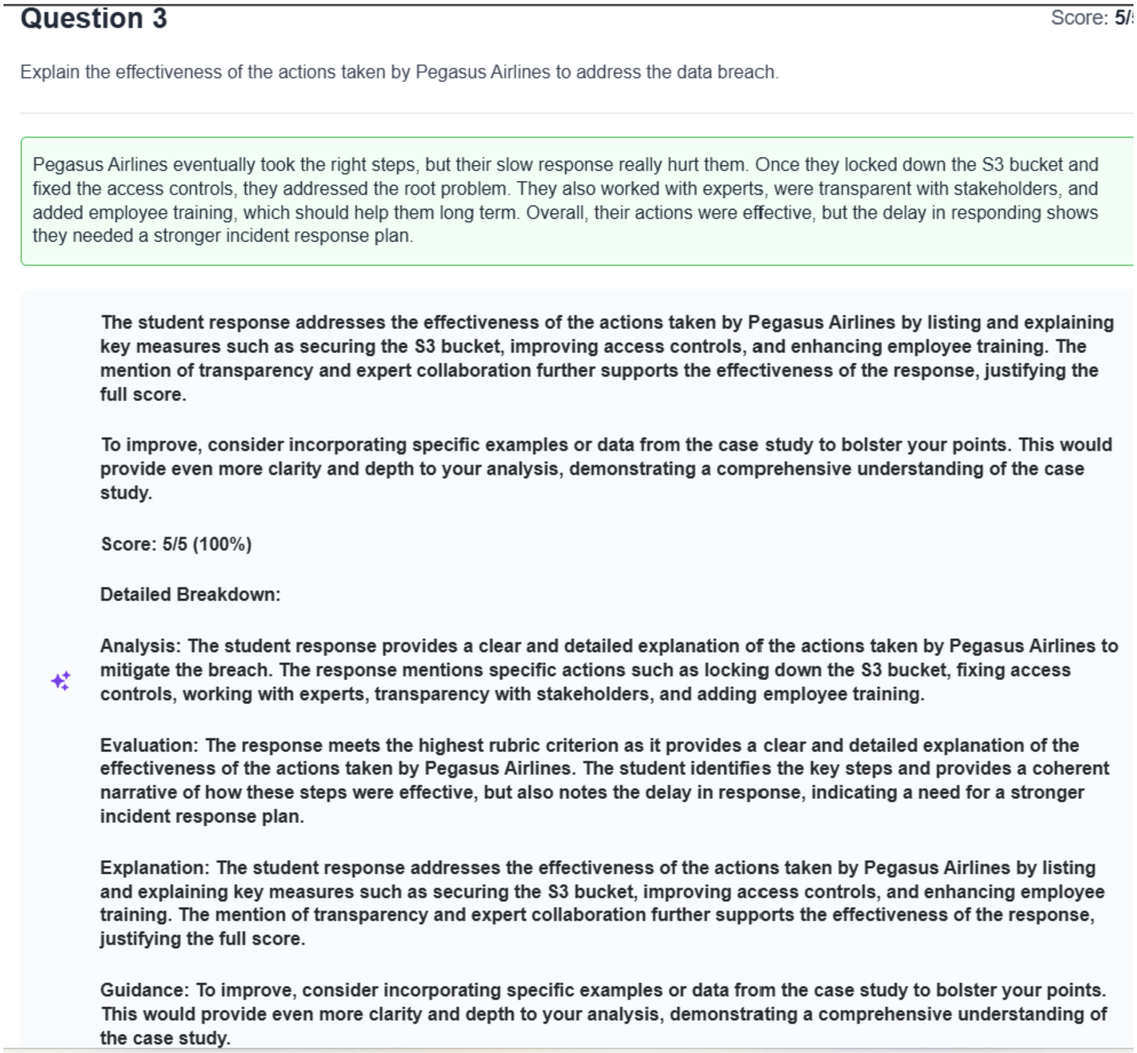
● They were effective in securing the data and fortifying systems. ✓
The response actions were very effective and successful in securing data.

○ They exposed more data to threats.

○ They had no impact on the systems.

○ They were ineffective and left the systems vulnerable.

The response actions were very effective and successful in securing data.



Question 3

Score: **5/**

Explain the effectiveness of the actions taken by Pegasus Airlines to address the data breach.

Pegasus Airlines eventually took the right steps, but their slow response really hurt them. Once they locked down the S3 bucket and fixed the access controls, they addressed the root problem. They also worked with experts, were transparent with stakeholders, and added employee training, which should help them long term. Overall, their actions were effective, but the delay in responding shows they needed a stronger incident response plan.

The student response addresses the effectiveness of the actions taken by Pegasus Airlines by listing and explaining key measures such as securing the S3 bucket, improving access controls, and enhancing employee training. The mention of transparency and expert collaboration further supports the effectiveness of the response, justifying the full score.

To improve, consider incorporating specific examples or data from the case study to bolster your points. This would provide even more clarity and depth to your analysis, demonstrating a comprehensive understanding of the case study.

Score: 5/5 (100%)

Detailed Breakdown:

Analysis: The student response provides a clear and detailed explanation of the actions taken by Pegasus Airlines to mitigate the breach. The response mentions specific actions such as locking down the S3 bucket, fixing access controls, working with experts, transparency with stakeholders, and adding employee training.

Evaluation: The response meets the highest rubric criterion as it provides a clear and detailed explanation of the effectiveness of the actions taken by Pegasus Airlines. The student identifies the key steps and provides a coherent narrative of how these steps were effective, but also notes the delay in response, indicating a need for a stronger incident response plan.

Explanation: The student response addresses the effectiveness of the actions taken by Pegasus Airlines by listing and explaining key measures such as securing the S3 bucket, improving access controls, and enhancing employee training. The mention of transparency and expert collaboration further supports the effectiveness of the response, justifying the full score.

Guidance: To improve, consider incorporating specific examples or data from the case study to bolster your points. This would provide even more clarity and depth to your analysis, demonstrating a comprehensive understanding of the case study.

Question 4

Score: **5/5**

Case Study: Pegasus Airlines Data Breach (Part B)

Successes, Gaps, and Failures: The quick implementation of advanced security measures and enhancement of employee training programs were crucial successes. However, delayed communication signifies a failure in the organization's incident response protocol. An identified gap was the need for ongoing, robust security training to avoid misconfigurations in the future.

Impact on the Organization: The breach temporarily diminished public trust, posing short-term operational challenges and long-term strategic implications. While the improved security measures may enhance future resilience, the breach highlighted vulnerabilities that could affect customer confidence. Strategically, the incident emphasized the need for continuous IT infrastructure assessments.

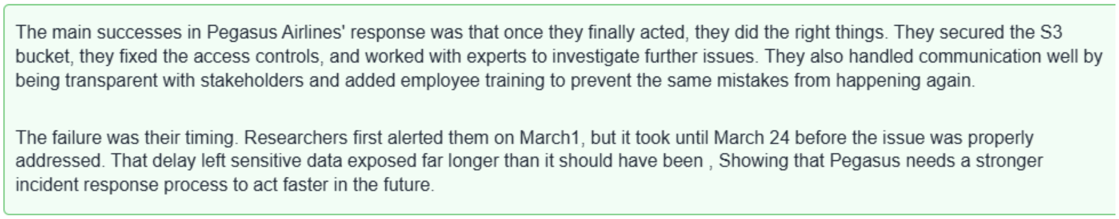
The implications could have been far more severe if the Pegasus Airlines data breach had not been identified and addressed. First, unauthorized access to sensitive information such as flight charts and personal identifiable information (PII) of crew members could have led to identity theft and fraudulent activities. The reputational damage might have escalated, resulting in a significant loss of customer trust and loyalty. Financially, Pegasus Airlines could have faced hefty fines and legal actions for non-compliance with data protection regulations, further straining its resources. Additionally, prolonged exposure would have enhanced the risk of the data being exploited or sold on the black market, compromising the safety and security of air travel operations. The breach could have destabilized the company's operations and financial stability, highlighting the critical importance of timely and effective cybersecurity measures.

Lessons Learned: Key lessons included the importance of regular and comprehensive security training, the necessity for rigorous data access reviews, and the vital role of swift communication in breach response. The incident highlighted positive outcomes, such as the capacity to mobilize resources effectively once breaches are identified.

Recommendations for Future Actions: Pegasus Airlines should establish a more responsive incident communication protocol and ensure regular audits of security measures. Ongoing and more intensive cybersecurity training should be provided for all staff. Implementing automated monitoring systems to detect misconfigurations promptly could also prevent similar future breaches.

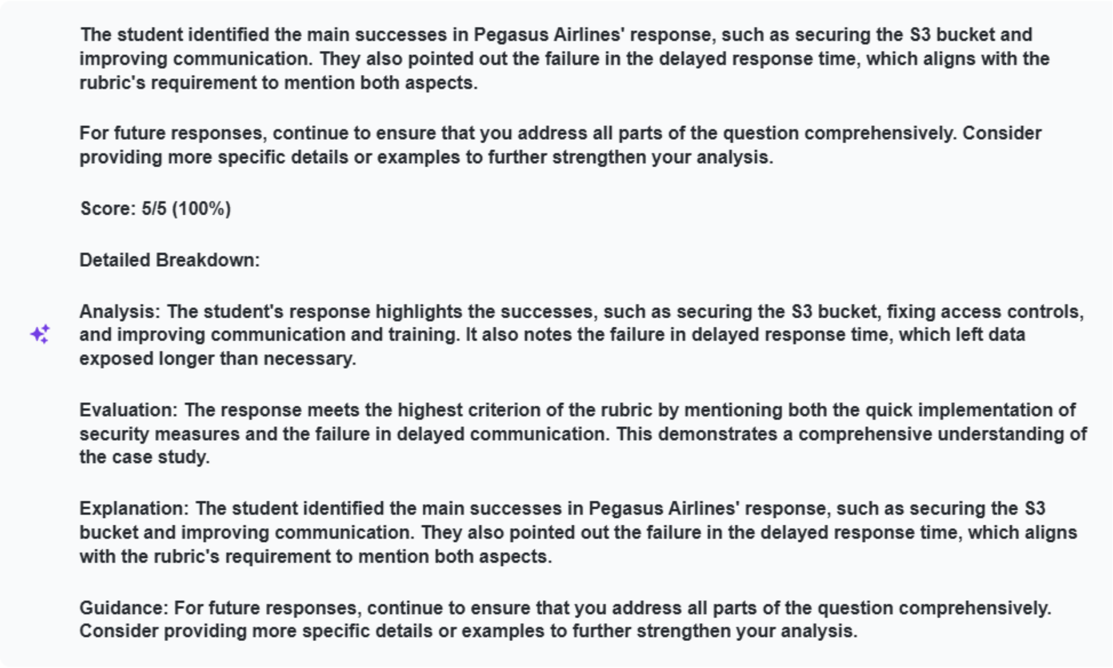
Conclusion: This case study underscores the growing importance of cybersecurity within the aviation industry. The Pegasus Airlines breach highlights common vulnerabilities and the need for strategic and vigilant data security measures. In the long term, strengthened data protection protocols could be beneficial to balancing technological advancement and data security.

Question 4: What were the main successes and failures identified in Pegasus Airlines' response to the data breach?



The main successes in Pegasus Airlines' response was that once they finally acted, they did the right things. They secured the S3 bucket, they fixed the access controls, and worked with experts to investigate further issues. They also handled communication well by being transparent with stakeholders and added employee training to prevent the same mistakes from happening again.

The failure was their timing. Researchers first alerted them on March1, but it took until March 24 before the issue was properly addressed. That delay left sensitive data exposed far longer than it should have been , Showing that Pegasus needs a stronger incident response process to act faster in the future.



The student identified the main successes in Pegasus Airlines' response, such as securing the S3 bucket and improving communication. They also pointed out the failure in the delayed response time, which aligns with the rubric's requirement to mention both aspects.

For future responses, continue to ensure that you address all parts of the question comprehensively. Consider providing more specific details or examples to further strengthen your analysis.

Score: 5/5 (100%)

Detailed Breakdown:

Analysis: The student's response highlights the successes, such as securing the S3 bucket, fixing access controls, and improving communication and training. It also notes the failure in delayed response time, which left data exposed longer than necessary.

Evaluation: The response meets the highest criterion of the rubric by mentioning both the quick implementation of security measures and the failure in delayed communication. This demonstrates a comprehensive understanding of the case study.

Explanation: The student identified the main successes in Pegasus Airlines' response, such as securing the S3 bucket and improving communication. They also pointed out the failure in the delayed response time, which aligns with the rubric's requirement to mention both aspects.

Guidance: For future responses, continue to ensure that you address all parts of the question comprehensively. Consider providing more specific details or examples to further strengthen your analysis.

Summary

In February 2022, Pegasus Airlines suffered a significant data exposure caused by AWS S3 bucket. Due to a misconfiguration traced back to an employee oversight, the bucket was left publicly accessible, exposing 6.5 terabytes of sensitive data. The exposed files included flight charts, navigation updates, crew assignments, safety protocols, insurance documents, source code, and even plain-text passwords. The breach was discovered by Safety Detectives researchers, who notified Pegasus on March 1. However, the company did not respond until March 24, leaving the data exposed for several weeks.

The root cause of the incident was the misconfigured AWS S3 bucket permissions, which lacked proper access controls and monitoring. Pegasus also failed to detect the issue internally, highlighting weaknesses in their security oversight and incident response processes. Once the company became aware of the problem, they acted to secure the S3 bucket by revising access controls. Their IT team, in collaboration with external cybersecurity experts, conducted a thorough investigation and implemented stronger security measures across their systems. To reassure stakeholders, Pegasus issued public notifications explaining the breach and emphasized transparency in their response. They also invested in enhanced cybersecurity training and awareness programs for employees to reduce the risk of similar errors in the future.

Overall, Pegasus Airlines' response was partially effective. On the positive side, they successfully secured the exposed data, implemented stronger protections, improved staff training, and communicated openly with stakeholders. These actions helped restore trust and strengthen their security posture going forward. However, the delayed response to researcher notifications was a critical failure, as it left sensitive data accessible for far longer than necessary. The case demonstrates how insider oversight and cloud misconfigurations can escalate into major breaches, and it underscores the need for timely incident response, strong monitoring capabilities, and robust compliance practices in the aviation industry.