The Captial One Cybersecurity Breach

Celeste Meraz-Luna

Old Dominion University

CYSE 300

Professor Diwakar Yalpi

May 25, 2025

In July 2019, Capital One experienced a significant cybersecurity breach that compromised the personal data of over 100 million individuals in the United States and Canada. This incident stands as a prime example of the complexities and challenges associated with cloud security, particularly concerning misconfigurations and insider threats. This paper examines the vulnerabilities exploited during the breach, the nature of the threats involved, the repercussions faced by Capital One, and the cybersecurity measures that could have mitigated or prevented the incident.

The breach primarily resulted from a misconfigured Web Application Firewall within Capital One's Amazon Web Services cloud infrastructure. This misconfiguration allowed unauthorized access through a Server-Side Request Forgery vulnerability, enabling the attacker to obtain security credentials for privileged accounts. These credentials provided access to sensitive data stored in AWS S3 buckets (Novaes Neto et al., 2020).

The attackers, Paige Thompson, a former AWS employee, exploited her knowledge of AWS infrastructure to carry out the breach. By leveraging the SSRF vulnerability and misconfigured IAM roles, she accessed and downloaded sensitive data, including names, addresses, credit scores, and social security numbers. Thompson's insider knowledge and technical expertise were critical factors in the success of the attack (Khan et al., 2022). As noted by Chen, Chowdhury, and Latif (2021), data breaches in corporate settings often involve a combination of external exploitation and internal mismanagement, which was clearly evident in Capital One's case.

The breach had significant financial, legal, and reputational consequences for Capital One. The company faced an $80 million fine from the Office of the Comptroller of the Currency for failing to establish effective risk assessment processes before migrating to the cloud. Additionally, Capital One agreed to a $190 million settlement to compensate affected customers.

Cybersecurity measures that could have mitigated or prevented the breach, include proper configuration management, principle of least privilege and enhanced monitoring and logging. Regular audits and automated tools could have detected and corrected the WAF misconfiguration, closing the SSRF vulnerability. Also, implementing strict IAM policies ensures that services and users have only the necessary permissions and would help limit the attacker's ability to access sensitive data. Lastly, complete monitoring of network activity and access logs could have detected unusual behavior sooner and would have allowed a quicker response to the breach.

The Capital One data breach underscores the critical importance of strong cybersecurity practices, especially in cloud environments. Misconfigurations, excessive permissions, and insider threats can have devasting consequences if not properly managed. Organizations must prioritize proper configuration management, the principle of least privilege and enhanced monitoring and logging to protect the sensitive data and maintain customer trust.

References

Chen, D., Chowdhury, M. M., & Latif, S. (2021, October). Data breaches in corporate setting. In 2021 international conference on electrical, computer, communications and mechatronics engineering (ICECCME) (pp. 01-06). IEEE.

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the capital one data breach: Critical lessons learned. ACM Transactions on Privacy and Security, 26(1), 1-29.

Novaes Neto, N., Madnick, S., Moraes G de Paula, A., & Malara Borges, N. (2020). A case study of the capital one data breach. Stuart E. and Moraes G. de Paula, Anchises and Malara Borges, Natasha, A Case Study of the Capital One Data Breach (January 1, 2020).