Short Research Paper on Capital one Breach

Emmanuel Dade

Old Dominion University

Cybersecurity 300

Dr. Kovacic

September 5, 2025

Short Research Paper on Capital one Breach

One of the largest breaches in cybersecurity that occurred in 2019 was the Capital One data breach which compromised the sensitive personal information of over 100 million Capital One customers in the United States and Canada. It highlights how small vulnerabilities can be a target for large-scale threats that will impact both organizations and individuals. Understanding what vulnerabilities were involved, what threats exploited those weaknesses, and what repercussions followed suggest that with the proper cybersecurity measures, this incident could have been avoided or at least lessened.

The breach of Capital One resulted from multiple unaddressed vulnerabilities in the years prior; two major ones were misconfiguration and over-dependence on cloud solutions. A web application firewall (WAF) intended to protect Capital One's cloud-based architecture was misconfigured to allow unauthorized access to sensitive data in the storage buckets of Amazon Web Services (AWS) (Khan, Kabanov, Hua, & Madnick, 2022). The misconfiguration is an example of a vulnerability that seems very minor but caused almost fatal damage to the Company. The WAF was supposed to filter malicious requests; however, a failed setting allowed an attacker to send commands, including HTTP headers or any other input, rendering foolproof trickery into granting access. In addition, the vulnerability exists in an organization that has overly relied on cloud solutions; without ensuring security like physical store locations, access becomes easier. Another compounding vulnerability is the lack of internal monitoring software to identify malicious behavior; for over three months, unusual access patterns went unreported from administrative oversight.

Ultimately, the vulnerability was exploited by a server-side request forgery (SSRF) exploit. Server-side request forgery is a vulnerability where an adversary can induce the server-

side application to make HTTP requests (Khan et al., 2022). The perpetrator of the hack, an ex-employee at AWS where the vulnerable WAF existed, exploited it, inducing it into retrieving credentials from an AWS metadata service. She used these retrieved credentials to access a wealth of company resources accessible only with special permissions, including her social security numbers, bank account numbers, credit card applications, and all Capital One addresses (Novaes Neto et al., 2020). The single SSRF exploit highlights greater vulnerabilities within cloud computing; if one area is compromised, everything else can be compromised too.

The repercussions associated with this breach varied for Capital One and individuals. Investigating and remediating the breach cost millions; in 2020, Capital One agreed to pay an $80 million fine due to the incident. In addition, a class action lawsuit settlement cost another $190 million (Khan et al., 2022). For individuals whose information was breached, they faced potential identity theft and fraud after their personal data was exposed via unscrupulous plans; society has limited recourse when this information is obtained and used for nefarious purposes, negatively impacting their financial future. For many who were affected, trust in capital systems was diminished. Beyond person-impacting considerations were larger secondary threats to industries relying upon cloud solutions for Capital One exposed flaws in security protocols that became reexamined across many industries following the exploit.

Learning from this incident, there are specific cybersecurity measures that could have decreased the likelihood of a Capital One data breach. First, more secure configuration settings might have prevented the WWW from being misconfigured in the first place; automatic penetration testing regularly would identify vulnerabilities before criminals exploit them. Other approaches should include obtaining more limited access as even if the exploit occurred to retrieve access credentials from the AWS service metadata service, more limitations could have

been placed on what data could be viewed if standard employee credentials were known (Novaes Neto et al., 2020). Finally, improved active monitoring could have identified suspicious activity within the three-month observation period before anyone accessed information incorrectly or inappropriately. Regular checks on data streams could have reduced risk exposure during the act.

Ultimately, due to this incident, we learn that cybersecurity must be an active process; simply because a company adopts cloud solutions to ease burden does not mean greater risk should be taken without mindful implementation. When these solutions are improperly set up and challenges go unaddressed afterward—more problems occur down the road. Capital One should have known that minuscule red flags could lead to giant hurdles; if one thing is compromised once, it can easily become compromised again. Now that information equity security has become pivotal for personal financial institutions through digital applications, those challenges must be accounted for at every step both organizationally and personally.

Refernce

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)*.