John Munguia

CS 499

August 3, 2025

**Cloud Misconfigurations and Compliance Gaps: The 2019 Capital One Data Breach**

In 2019, Capital One experienced a major security breach involving over 100 million individuals in the United States and 6 million in Canada. Although the unauthorized access occurred in March, it was not discovered until July. The breach became widely known because Capital One had a strong reputation for using modern cloud infrastructure and following cybersecurity best practices. The attacker exploited a misconfigured security tool, which raised questions about the company’s ability to enforce secure configurations despite its compliance claims. The public disclosure and official report can be found at <https://www.capitalone.com/about/newsroom/capital-one-announces-data-security-incident/>

The breach happened due to a server-side request forgery (SSRF) attack. The attacker discovered that a web application firewall (WAF) was misconfigured, which allowed commands from outside the system to reach internal AWS metadata services. These services provided temporary credentials that were then used to access over 700 cloud storage buckets. Using Amazon’s command-line interface, the attacker copied about 30 gigabytes of data, including names, addresses, phone numbers, and credit scores. Though some of the data was encrypted, weak access controls and role configurations allowed the attacker to bypass those protections. The individual behind the attack, Paige Thompson, was a former AWS employee, giving her insight into how the systems worked. Capital One only became aware of the incident when someone emailed them after finding leaked data on GitHub.

The immediate threat was the large-scale theft of personal information. If left unresolved, the attacker could have continued stealing more data or selling it to others, leading to identity theft and financial fraud. The breach also exposed Capital One to lawsuits, regulatory investigations, and reputational harm. The company had logs that captured the attack activity, but no alerts were triggered in time, showing that their monitoring tools were either not configured correctly or not actively reviewed.

The breach could have been prevented through stronger technical controls and secure development practices. The WAF should have been configured to block access to metadata services. The system should have also followed the principle of least privilege, limiting what each role and credential could do. Developers and administrators should have used vulnerability scans and configuration audits to catch the issue before it was exploited. Tools like AWS CloudTrail could have helped by sending alerts based on suspicious command activity.

To reduce the chances of this kind of attack, organizations can follow established cybersecurity policies. Capital One claimed to use the NIST Cybersecurity Framework, which includes guidelines for identity and access management, vulnerability management, and real-time monitoring. According to a research study by MIT, over 60 NIST controls could have stopped or reduced the damage if they had been fully implemented. These include managing access credentials, limiting permissions, and actively tracking system behavior.

This case also relates to the Triple A model: Authentication, Authorization, and Accounting. Authentication failed because metadata credentials were too easily accessed. Authorization was too broad, giving the attacker more access than necessary. Accounting was not effective because logs existed but were not being monitored actively enough to catch the attack in time. This breakdown across all three areas shows how important it is to apply the model in both planning and real-time operations.

The concept of Defense in Depth is also important. This strategy focuses on having multiple layers of security so that if one fails, others can still protect the system. In Capital One’s case, the firewall failed, access controls were too loose, and monitoring did not flag anything unusual. If any of these had been properly in place, the attack might have been blocked or detected earlier. A complete Defense in Depth approach includes secure configurations, layered access controls, automated alerts, and active oversight from security teams.

In conclusion, the Capital One breach was not caused by a lack of technology, but by weaknesses in how security tools were configured and monitored. Even though the company followed many best practices on paper, those practices were not enough without proper enforcement. This case shows the importance of applying security frameworks like NIST, using the Triple A model correctly, and implementing strong layered defenses. Companies need to go beyond compliance and make sure their systems are actively secured, monitored, and tested to protect against evolving cyber threats.