The Capital One Breach: A modern technological failure

Tejas Kamtam

Abstract

In July 2019, Capital One, one of the largest banks in the United States, suffered a monumental data breach that exposed sensitive information of nearly 106 million individuals in the US and Canada. The breach resulted from a complex series of events involving a combination of technical vulnerabilities, misconfigured security controls, and human error. The attacker, a former Amazon Web Services (AWS) employee, exploited a misconfigured AWS S3 bucket and used a Server Side Request Forgery (SSRF) attack to gain unauthorized access to Capital One's sensitive customer data.

This post-mortem report, addressed to the FBI and FTC, provides an in-depth analysis of the Capital One breach from a deontological ethical perspective. The report examines the technical and socio-technical factors that contributed to the breach, including the misconfigured S3 bucket, the flawed Web Application Firewall (WAF), and the lack of proper oversight and security training within Capital One. The report argues that the breach represents a significant ethical failure on the part of Capital One, as the company had a clear moral duty to protect its customers' sensitive information, which it failed to uphold (Capital One 2022).

Background

In recent years, many companies, including Capital One, have migrated their IT infrastructure and data to cloud computing platforms like Amazon Web Services (AWS). Cloud computing allows organizations to rent computing resources, such as servers, storage, and databases, from a cloud provider instead of maintaining their own physical infrastructure. This shift has been driven by the scalability, flexibility, and cost-efficiency that cloud computing offers.

AWS, in particular, has become a popular choice for companies due to its extensive range of services and robust security features. AWS provides various cloud storage options, including S3 (Simple Storage Service) buckets, which are used to store and retrieve data. S3 buckets are highly scalable and can be accessed over the internet, making them an attractive option for companies for storing and managing large amounts of data.

However, the move to cloud computing also introduces new security challenges. While AWS provides a secure infrastructure, it is the customer's responsibility to properly configure and manage their resources to ensure data protection. This includes setting up access controls, encrypting data, and monitoring for potential security threats (Ng 2019).

In the case of Capital One, the company had migrated its data to AWS and was using S3 buckets to store sensitive customer information. However, a misconfiguration in the S3 bucket permissions allowed an unauthorized individual, Paige Thompson, to gain access to the data. Thompson, a former AWS employee, exploited a vulnerability in Capital One's web application firewall (WAF) to send requests to the misconfigured S3 bucket and retrieve the sensitive data (Ng 2019).

The Capital One breach highlighted the importance of properly configuring and managing cloud resources. While cloud computing has its benefits to on premises servers, it requires a shared responsibility model for security. While AWS may be responsible for securing the underlying infrastructure and servers, the customers are ultimately responsible for ensuring their data and applications. This includes appropriately configuring access controls, encrypting data, and regularly monitoring for potential security threats.

The Engineering Failure

The Capital One data breach resulted from a complex series of events involving a combination of technical vulnerabilities, misconfigured security controls, and human error. Thompson exploited a misconfigured AWS S3 bucket and used a Server Side Request Forgery (SSRF) attack to gain unauthorized access to Capital One's sensitive customer data (Walikar 2019).

The attack began when Thompson discovered a misconfigured AWS S3 bucket that belonged to Capital One. S3 buckets are cloud storage containers that can be used to store and retrieve data, but they require proper configuration to ensure data security. In this case, the S3 bucket was not properly secured, allowing Thompson to access it without authorization.

Once inside the S3 bucket, Thompson used an SSRF attack to trick a Capital One server into running commands that it should not have been permitted to run. SSRF attacks occur when an attacker sends a request to a server that causes it to perform an unintended action, such as executing a command or returning sensitive data. In this case, Thompson used the SSRF attack to send requests to Capital One's backend servers, executing the commands and returning the sensitive customer data. The SSRF attack was possible because of a misconfiguration in Capital One's Web Application Firewall (WAF). A WAF is a security tool that is designed to monitor, filter, and block HTTP traffic to and from a web application. It acts as a barrier between the application and the internet, protecting against common web-based attacks such as cross-site scripting (XSS), SQL injection, and SSRF. However, Capital In this case, one's WAF was not properly configured, allowing Thompson to send malicious requests to the backend servers and retrieve sensitive data (Jones 2022, Khan 2022, McLean 2019, Walikar 2019).

Once Thompson accessed the sensitive data, she used the "curl" tool to download it from the compromised S3 bucket. Curl is a command-line tool for transceiving data between servers using HTTP. Thompson used curl to send requests to the S3 bucket and retrieve the sensitive data, which she then stored on her own server (Khan 2022, Seals 2022).

After exfiltrating the data, Thompson took steps to cover her tracks. She used a virtual private network (VPN) and a proxy server to mask her IP address and location. A VPN encrypts a user's internet traffic by routing it through a remote server, making it appear like the traffic is coming from the VPN server rather than the user's actual location. Similarly, a proxy server acts as an intermediary between a user's device and the internet, forwarding requests and responses between the two. By using a VPN and a proxy server, Thompson was able to hide her identity and make it more difficult for investigators to trace the attack back to her (Seals 2022).

Capital One first became aware of the breach on July 17, 2019, when it received an email from an ethical hacker who had discovered the vulnerability. The ethical hacker had found a post on GitHub, a popular code-sharing and version control platform, that contained a list of AWS S3 buckets and their corresponding access keys. The post had been made by Thompson, who had apparently intended to share the information with others.

Upon receiving the email, Capital One launched an investigation into the breach, but by then, the breach had gone unnoticed for nearly a month. The company worked with law enforcement agencies, including the FBI, to identify the scope of the breach and the individuals responsible. Capital One also hired a third-party cybersecurity firm to conduct a forensic analysis of the company's systems to determine the extent of the damage.

The investigation revealed that Thompson had accessed the sensitive data of approximately 106 million Capital One customers, including names, addresses, phone numbers, email addresses, dates of birth, and self-reported income. The breach exposed credit scores, balances, payment history, and transactions for 23 days across 2016, 2017, and 2018.

Capital One notified affected customers of the breach and offered free credit monitoring and identity protection services to compensate (Avery 2022). The company also improved its cybersecurity posture by implementing new security controls and processes, such as enhanced monitoring and alerting systems, more frequent security audits, and additional employee training.

A Deontological Ethical Analysis

The Capital One data breach represents a significant ethical failure that violated the fundamental principles of deontological ethics. Deontology, as developed by philosophers such as Immanuel Kant, holds that the morality of an action should be judged based on its adherence to moral rules and duties rather than its consequences. Two key maxims in deontological ethics are the Universality Principle and the Freedom Principle.

The Universality Principle states that the ethics behind a rule are justified if the same ethics could be applied to every similar situation. In the context of the Capital One breach, the company's use of lax database permissions and inadequate security measures fails to meet this principle. If every company were to adopt similarly weak security practices, it would lead to widespread data breaches and a breakdown of trust in the financial system. Therefore, Capital One's security failures cannot be considered ethically justified under the Universality Principle.

The Freedom Principle, on the other hand, emphasizes that people have free will and the right to make decisions and thus have an ethical duty to their actions. In the case of Capital One, the company's employees, particularly those in IT and security roles, had a moral obligation to ensure that the company's systems and data were properly secured. The fact that the misconfigured S3 bucket and WAF went unnoticed for an extended period suggests that these employees may not have taken their responsibilities seriously enough, violating the Freedom Principle.

Moreover, Capital One's leadership and management had a duty to ensure that the organization had adequate security measures and was prepared to respond effectively to security incidents. The company's executives and board of directors had a moral obligation to oversee and verify that proper security practices were being followed. The fact that the breach went undetected for months and that the company struggled to respond effectively when it was discovered indicates a failure of leadership and a breach of the duty of care that these individuals owed to their customers and shareholders.

Capital One's slow response to the breach and its initial lack of transparency about the scope and severity of the incident also represent ethical lapses. The company had a duty to promptly notify affected customers and provide them with the necessary support and resources to mitigate the potential harm caused by the breach. However, Capital One's delay in discovering the breach and its incomplete initial statements about the extent of the damage suggest that the company prioritized its own reputation and interests over the well-being of its customers, violating the duty of care.

From a deontological perspective, Capital One should have prioritized the security and privacy of its customers' data above all else. The company had a moral duty to invest in robust security measures, conduct regular audits, and ensure that its employees were properly trained in security best practices. By failing to do so, Capital One violated the Universality Principle, as its lax security practices would be unacceptable if universally applied, and the Freedom Principle, as its employees and leadership failed to uphold their ethical duties to protect customer data.

In conclusion, the Capital One data breach represents a clear violation of foundational ethical principles expected of a company handling privacy at this magnitude. The company's inadequate security measures, lack of proper oversight, and slow response to the breach all constitute breaches of its moral duties to its customers and shareholders. Through the lens of deontological ethics, it becomes evident that Capital One's actions and failures cannot be considered ethically justified, and the company must take significant steps to rectify these issues and prevent similar breaches in the future.

Recommendations

Drawing on deontological principles, particularly the Universality Principle and the Freedom Principle, Capital One should implement the following recommendations to prevent similar ethical failures in the future:

1. Implement strict access controls for AWS S3 buckets and other cloud resources.

The Universality Principle demands that the same high standards of access control be applied to all similar situations. If every company were to adopt lax access controls, it would lead to widespread data breaches and erosion of trust. Therefore, implementing strict access controls is an ethical imperative. Capital One should enforce the use of strong authentication mechanisms, such as multi-factor authentication (MFA), for all users accessing sensitive data. Additionally, the company should apply the principle of "least privilege," ensuring that users and applications only have access to the resources they need to perform their tasks. This can be achieved through regular access reviews and by implementing role-based access control (RBAC) policies.

2. Encrypt sensitive data at rest and in transit.

The Freedom Principle emphasizes the duty of individuals and organizations to take responsibility for their actions. By encrypting sensitive data, Capital One would be fulfilling its moral obligation to protect customer information, even in the event of unauthorized access. Encrypting data demonstrates a commitment to upholding the company's ethical duties. Capital One should implement industry-standard encryption algorithms like AES-256 to protect sensitive data stored in AWS S3 buckets and other cloud resources. The company should also ensure that data is encrypted in transit using secure protocols like HTTPS and TLS. Encryption keys should be securely managed using a key management service (KMS) and rotated regularly.

3. Regularly audit and test security controls to identify and remediate vulnerabilities proactively.

The Universality Principle requires that the same high-security monitoring and testing standards be applied consistently across all systems and processes. Regular audits and tests ensure that best practices are being followed, reducing the risk of ethical failures. Moreover, the Freedom Principle emphasizes the duty of the company and its employees to take proactive steps to identify and address vulnerabilities before they can be exploited. Capital One should conduct regular penetration testing, vulnerability scanning, and configuration reviews to identify potential weaknesses in its security posture. These tests should be performed by both internal security teams and independent third-party auditors to ensure objectivity. Identified vulnerabilities should be prioritized based on their severity and potential impact, and remediation efforts should be tracked and verified. The company should also implement continuous monitoring solutions to detect and respond to real-time security anomalies.

Conclusion

The Capital One data breach is a stark reminder of the importance of robust cybersecurity practices in the financial industry. The breach exposed the sensitive information of millions of customers, undermining trust in the company and highlighting the need for stronger security controls and incident response capabilities.

Since the breach, Capital One has improved its security posture, including increasing its cybersecurity budget, hiring additional security personnel, and implementing new security technologies and processes. However, much work remains to be done across the industry to prevent similar incidents from occurring in the future.

One key lesson from the Capital One breach is the importance of a shared responsibility model for cloud security. While cloud service providers like AWS offer a range of security features and tools, it is ultimately the customer's responsibility to configure and manage these tools to protect their data properly. Organizations must invest the necessary expertise and resources to ensure their cloud environments are secure and compliant with industry standards and regulations.

Another important lesson is the need for a culture of security within organizations. Cybersecurity cannot be viewed as solely the responsibility of the IT department but rather as a shared responsibility that requires the engagement and commitment of all employees. Regular security training and awareness programs can help foster this culture and ensure that employees are equipped to identify and respond to potential threats.

Finally, the Capital One breach highlights the importance of collaboration and information sharing within the cybersecurity community. By working together to share threat intelligence, best practices, and lessons learned, organizations can better protect themselves and their customers from evolving cyber threats.

References

Avery, D., September 2022, Capital One $190 Million Data Breach Settlement: Today Is the Last Day to Claim Money; CNET, [https://www.cnet.com/personal-finance/capital-one-190-million-data-breach-settlement-today-is-deadline-to-file-claim/]

Capital One, April 2022, Information on the Capital One cyber incident; Capital One Announcements, [https://www.capitalone.com/digital/facts2019/]

Jones, T., December 2022, Capital One Data Breach — 2019; Medium: Nerd for Tech, [https://medium.com/nerd-for-tech/capital-one-data-breach-2019-f85a259eaa60]

Khan, S., et al., July 2022, A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned; ACM Transactions on Privacy and Security, vol. 26, ed. 1, [https://www.researchgate.net/publication/361860348_A_Systematic_Analysis_of_the_Capital_One_Data_Breach_Critical_Lessons_Learned, DOI:10.1145/3546068]

McLean, R., July 2019, A hacker gained access to 100 million Capital One credit card applications and accounts; CNN Business, [https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html]

Ng., A, November 2019, Amazon tells senators it isn't to blame for Capital One breach; CNET,

[https://www.cnet.com/news/politics/amazon-tells-senators-it-isnt-to-blame-for-capital-one-breach/]

Seals, T., June 2022, Capital One Attacker Exploited Misconfigured AWS Databases; Dark Reading, [https://www.darkreading.com/cyberattacks-data-breaches/capital-one-attacker-exploited-misconfigured-aws-databases]

Theiler, M. A., July 2019, United States of America v. Paige A. Thompson, United States District Court for the Western District of Washington at Seattle, [https://www.justice.gov/usao-wdwa/page/file/1194001/dl?inline]

Walikar, R., August 2019, An SSRF, privileged AWS keys and the Capital One breach; Medium: Appsecco, [https://blog.appsecco.com/an-ssrf-privileged-aws-keys-and-the-capital-one-breach-4c3c2cded3af]