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.

Drawing on deontological principles, this report provides recommendations for preventing similar failures in the future, including implementing strict access

controls, encrypting sensitive data, conducting regular security audits, and providing regular security training for employees. The report concludes by emphasizing the importance of a shared responsibility model for cloud security, a culture of security within organizations, and collaboration and information sharing within the cybersecurity community.

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.

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.

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.

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

One's WAF was not properly configured in this case, allowing Thompson to send malicious requests to the backend servers and retrieve sensitive data.

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.

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.

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 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 immediately launched an investigation into the breach. 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 during 2016, 2017, and 2018.

Capital One notified affected customers of the breach and offered free credit monitoring and identity protection services to compensate. The company also worked to improve 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. In the context of the Capital One breach, the company had a clear moral duty to protect its customers' sensitive personal and financial information, which it failed to uphold.

At the core of the ethical failure was Capital One's inadequate security measures and lack of proper oversight. The company had a moral obligation to implement robust security controls, regularly audit and test these controls, and ensure that its employees were properly trained in security best practices. However, the misconfigured AWS S3 bucket and the flawed WAF demonstrate that Capital One did not take these obligations seriously enough. The company's failure to secure its systems and protect customer data clearly breached its ethical duties.

Moreover, 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 disclosing 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.

From a deontological perspective, Capital One's leadership and management are primarily responsible for the breach. The company's executives and board of directors had a moral duty to ensure that the organization had adequate security measures and was prepared to respond effectively to security incidents. 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.

However, the responsibility for the breach also extends beyond Capital One's leadership. 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 been properly trained or may not have taken their responsibilities seriously enough. Additionally, AWS, as the cloud service provider, had a shared responsibility to ensure that its services were secure and that its customers were properly educated about security best practices.

Capital One should have prioritized the security and privacy of its customers' data above all else. The company should have invested in robust security measures, such as encryption, access controls, and monitoring systems, to prevent unauthorized access to sensitive information. It should have also conducted regular security audits and penetration testing to identify and remediate vulnerabilities before they could be exploited by attackers.

Furthermore, Capital One should have had a well-developed incident response plan in place to ensure that it could quickly and effectively respond to security breaches. This plan should have included clear protocols for notifying affected customers, providing them with support and resources, and working with law enforcement and other stakeholders to investigate and mitigate the damage caused by the breach.

Recommendations

Drawing on deontological principles, Capital One should take the following actions to prevent similar failures in the future:

1. Implement strict access controls for AWS S3 buckets and other cloud resources. This includes using stronger authentication mechanisms, such as multi-factor authentication (MFA), and applying the principle of "least privilege," ensuring that users and applications only have access to the resources they need to perform their tasks.
2. Encrypt sensitive data at rest and in transit. This helps protect data even if unauthorized access occurs, as the attacker would need the decryption keys to read the data.
3. Regularly audit and test security controls to identify and remediate vulnerabilities proactively. This includes conducting penetration testing, vulnerability scanning, and configuration reviews to ensure that security best practices are being followed.
4. Implement robust monitoring and alerting systems to detect and respond to security incidents promptly. This includes using tools such as Security Information and Event Management (SIEM) systems, which can correlate log data from multiple sources and identify suspicious activity.
5. Develop and test incident response plans to ensure that the organization can effectively respond to and contain security incidents. This includes

establishing clear roles and responsibilities, communication protocols, and procedures for investigating and remediating incidents.

6. Provide regular security training and awareness programs for employees to ensure that they understand their responsibilities for protecting sensitive data and can identify and report potential security threats.
7. Collaborate with industry partners and regulators to share threat intelligence and best practices for preventing and responding to security incidents.

While implementing these recommendations may require significant investments in technology, processes, and personnel, the benefits of preventing data breaches and protecting customer trust far outweigh the costs.

Conclusion

The Capital One data breach serves as 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 taken steps to improve 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

*Still need to format the sources and add in-text citations.

1. https://www.capitalone.com/digital/facts2019/
2. https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html
3. https://www.justice.gov/usao-wdwa/page/file/1194001/dl?inline
4. https://medium.com/nerd-for-tech/capital-one-data-breach-2019-f85a259eaa60
5. https://blog.appsecco.com/an-ssrf-privileged-aws-keys-and-the-capital-one-breach-4c3c2cded3af
6. https://www.researchgate.net/publication/361860348_A_Systematic_Analysis_of_the_Capital_One_Data_Breach_Critical_Lessons_Learned
7. https://www.cnet.com/news/politics/amazon-tells-senators-it-isnt-to-blame-for-capital-one-breach/
8. https://www.cnet.com/personal-finance/capital-one-190-million-data-breach-settlement-today-is-deadline-to-file-claim/
9. https://www.darkreading.com/cyberattacks-data-breaches/capital-one-attacker-exploited-misconfigured-aws-databases